UNIVERSIDAD DE CHILE
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

EFFICIENT NON-INTERACTIVE ZERO-KNOWLEDGE PROOFS

TESIS PARA OPTAR AL GRADO DE
DOCTOR EN CIENCIAS, MENCIÓN COMPUTACIÓN

ALONSO EMILIO GONZÁLEZ ULLOA

PROFESOR GUÍA:
ALEJANDRO HEVIA ANGULO
PROFESOR CO-GUÍA:
CARLA RÁFOLS SALVADOR

MIEMBROS DE LA COMISIÓN:
JEREMY BARBAY
BENOÎT LIBERT
JORGE PÉREZ ROJAS

Este trabajo ha sido parcialmente financiado por CONICYT,
CONICYT-PCHA/Doctorado Nacional/2013-21130937.

SANTIAGO DE CHILE
2017

RESUMEN DE LA MEMORIA PARA OPTAR
AL TÍTULO DE DOCTOR EN CIENCIAS, MENCIÓN COMPUTACIÓN
POR: ALONSO EMILIO GONZÁLEZ ULLOA
FECHA: 2017
PROF. GUÍA: ALEJANDRO HEVIA ANGULO

EFFICIENT NON-INTERACTIVE ZERO-KNOWLEDGE PROOFS

Non-Interactive Zero-Knowledge (NIZK) proofs, are proofs that yield nothing beyond their validity. As opposed to the interactive variant, NIZK proofs consist of only one message and are more suited for high-latency scenarios and for building inherently non-interactive schemes, like signatures or encryption.

With the advent of pairing-based cryptography many cryptosystems have been built using bilinear groups, that is, three abelian groups $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_T$ of order q together with a bilinear function $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. Statements related to pairing-based cryptographic schemes are naturally expressed as the satisfiability of equations over these groups and integers modulo q.

The Groth-Sahai proof system, introduced by Groth and Sahai at Eurocrypt 2008, provides NIZK proofs for the satisfiability of equations over bilinear groups and over the integers modulo q. Although Groth-Sahai proofs are quite efficient, they easily get expensive unless the statement is very simple. Specifically, proving satisfiability of m equations in n variables requires sending $\Theta(n)$ elements of a bilinear group as commitments to the solutions, and a proof that the solutions satisfy the equations – which we simply call the proof – requiring additional $\Theta(m)$ group elements.

In this thesis we study how to construct aggregated proofs – i.e. proofs of size independent of the number of equations – for different types of equations and how to use them to build more efficient cryptographic schemes.

We show that linear equations admit aggregated proofs of size $\Theta(1)$. We then study the case of quadratic integer equations, more concretely the equation $b(b-1) = 0$ which is the most useful type of quadratic integer equation, and construct an aggregated proof of size $\Theta(1)$. We use these results to build more efficient threshold Groth-Sahai proofs and more efficient ring signatures.

We also study a natural generalization of quadratic equations which we call set-membership proofs – i.e. show that a variable belongs to some set. We first construct an aggregated proof of size $\Theta(t)$, where t is the set size, and of size $\Theta(\log t)$ if the set is of the form $[0, t-1] \subset \mathbb{Z}_q$. Then, we further improve the size of our set-membership proofs and construct aggregated proofs of size $\Theta(\log t)$. We note that some cryptographic schemes can be naturally constructed as set-membership proofs, specifically we study the case of proofs of correctness of a shuffle and range proofs. Starting from set-membership proofs as a common building block, we build the shortest proofs for both proof systems, with respect to the state of the art.

RESUMEN DE LA MEMORIA PARA OPTAR
AL TÍTULO DE DOCTOR EN CIENCIAS, MENCIÓN COMPUTACIÓN
POR: ALONSO EMILIO GONZÁLEZ ULLOA
FECHA: 2017
PROF. GUÍA: ALEJANDRO HEVIA ANGULO

EFFICIENT NON-INTERACTIVE ZERO-KNOWLEDGE PROOFS

Las pruebas no interactivas de conocimiento cero (NIZK, por su acrónimo en inglés) son pruebas que no revelan más información que su propia validez. A diferencia de la variante interactiva, las pruebas NIZK consisten en un sólo mensaje y son más adecuadas para escenarios de alta latencia y para la construcción de esquemas inherentemente no interactivos, como firmas o encriptación.

Con el advenimiento de la criptografía de emparejamiento muchos criptosistemas han sido construidos utilizando grupos bilineales, es decir, tres grupos abelianos $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_T$ de orden q junto con una función bilineal $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$. Las aserciones relativas a esquemas criptográficos basados en emparejamientos se expresan naturalmente como la satisfaciabilidad de ecuaciones sobre estos grupos y los enteros módulo q.

El sistema de desmotración de Groth-Sahai, introducido por Groth y Sahai en Eurocrypt 2008, permite construir pruebas NIZK para la satisfiabilidad de ecuaciones sobre grupos bilineales y sobre los enteros modulo q. Aunque las pruebas de Groth-Sahai son bastante eficientes, se vuelven costosas cuando la aserción es lo suficientemente compleja. Específicamente, demostrar la satisfacibilidad de m ecuaciones en n variables requiere enviar $\Theta(n)$ elementos de un grupo bilineal, que contienen las soluciones de la ecuacion, y una prueba de que las soluciones satisfacen las ecuaciones – que simplemente llamamos la prueba – requiriendo $\Theta(m)$ elementos del grupo.

En esta tesis estudiamos cómo construir pruebas agregadas – es decir, pruebas de tamaño independiente del número de ecuaciones – para diferentes tipos de ecuaciones, y cómo usar estas pruebas para construir esquemas criptográficos más eficientes. Mostramos que las ecuaciones lineales admiten pruebas agregadas de tamaño $\Theta(1)$. A continuación, estudiamos el caso de ecuaciones cuadráticas enteras, más concretamente la ecuación $b(b-1)=0$, que es la ecuación cuadrática más útil, y construimos una prueba agregada de tamaño $\Theta(1)$. Con estos resultados construimos pruebas de Groth-Sahai de umbral más eficientes y firmas de anillo más eficientes.

También estudiamos una generalización natural de las ecuaciones cuadráticas a las que llamamos *set-membership proofs*, donde se muestra que una variable pertenece a algún conjunto. Inicialmente construimos una prueba agregada de tamaño $\Theta(t)$, donde t es el tamaño de conjunto, y de tamaño $\Theta(\log t)$ si el conjunto es de la forma $[0, t-1] \subset \mathbb{Z}_q$. Posteriormente mejoramos el tamaño de nuestras *set-membership proofs* y construimos pruebas agregadas de tamaño $\Theta(\log t)$. Adicionalemente, observamos que algunos esquemas criptográficos pueden ser construidos naturalmente con *set-membership proofs*, específicamente estudiamos el caso de las pruebas de correctitud de un *shuffle* y las pruebas de pertenencia a un rango. Usando *set-membership proofs* construimos las pruebas más eficientes para ambos sistemas de prueba, en comparación con el estado del arte.

A Agata.

Agradecimientos

I would like to thank to the committee, Jorge, Jeremy, and Benoît, for the careful revision of this work. Thanks to Jeremy for the careful reading and the feedback, even though it was outside of his area of research. Special thanks to Benoît for reading in detail all this thesis and providing so valuable feedback.

I also thanks to Alejandro for introducing me to computer science, cryptography, and research. Thank you so much.

My most sincere thanks to Carla. She appeared during the most difficult part of my PhD. and gave a lot of energy for finishing this work. Thank you very much, y te debo una birra.

Thanks also to Eike and the people from the Crypto team at Bochum for receiving me for 4 months. Thanks to Bogdan and the Crypto team at Bristol for receiving me during my stay.

Ahora ya he hablado mucho inglés y empiezo a chacharear en chileno. Gracias a mi papi y mi mami por darme la vida y no quitarmela. Gracias a mi hermanito Jero por ser tan buen hermano en las buenas y en las malas. Gracias a la Paty, Dani e Isa por ser asi tan tela. Gracias a San Expedito por el favor concedido. Gracias a l@s cabr@s wen@s pal huatax y a l@s de la vieja escuela. Gracias a mis gatos que he dejado abandonados: Huiña, Chungunga y Palik (a.k.a. Gato). Ellos son los verdaderos autores de varios de los teoremas que hay en esta tesis.

Gracias especiales y espaciales a la la mia ragazza che mi vuole tanto bene. Un bacio gigante alla mia Leti, la mamma della mia figlia. Grazie mille, per sopportarmi e aiutarmi e per essere una mamma tanto buona. Ti amo guachita.

Por último, gracias a la guagua mas despeinada del mundo. A la niñita que se le ocurrió venir a este mundo justo cuando estaba por terminar el borrador de esta tesis y retrasó todo como en 3 semanas. Lo que obviamente me importa bien poco, porque me ha llenado de amor, ternura, felicidad, y un monton de sensaciones que no tengo idea qué son. Gracias guagualona Agata. Eres un paquete de alegria con patitas gordas y pelo punk.

Milán, 14 de Marzo de 2017.

Contents

Chapter 1

Introduction

With the growth and ubiquity of Internet more and more of our life has been moving from the “physical world” to the “digital world”. Along with these changes new problems have raised: we moved from a world where communication was mostly without any intermediary to a world where communication goes through an uncontrollable set of servers from which no privacy or secrecy guarantee can be obtained. Modern Cryptography has raised as an answer to these and many other related problems, providing *provable* methods for securing information.

Among the vast variety of cryptographic constructions, this thesis is concerned with the study of *non-interactive zero-knowledge proofs*. A zero-knowledge proof, introduced by Goldwasser, Micali, and Rackoff [GMR89], is a protocol between two parties, the *prover* and the *verifier*, where the prover wants to convince the verifier that some statement is true. At the onset of the protocol the verifier is completely convinced that the statement is true without learning any extra information. *non-interactive zero-knowledge proofs*, introduced by Blum, Feldman, and Micali [BFM88], restrict the proof to consist of a single message (in opposition of an interactive protocol) making the protocol more suited for constructing inherenlty non-interactive primitives, such as encryption and signatures, or and high-latency scenarios. The importance of non-interactive zero-knowledge proofs in cryptography was recognized early [NY90, DDN91, BR93], but for many years the existing constructions were either completely impractical or could only be realized under very strong assumptions like the random oracle model, via the Fiat-Shamir heuristic [FS87].

Ideally, a NIZK proof system should be both expressive and efficient, meaning that it should allow to prove statements which are general enough to be useful in practice using a small amount of resources. Furthermore, it should be constructed under mild security assumptions. As it is usually the case for most cryptographic primitives, there is a trade off between these three design goals. For instance, to prove very general statements, one can use the NIZK proof system for circuit satisfiability of Groth, Ostrovsky, and Sahai [GOS06b], which is based on standard assumptions but whose proof size depends on the number of gates. Alternatively, there exist constant-size proofs for any language in NP (e.g. [GGPR13]) but based on very strong and controversial assumptions, namely knowledge-of-exponent type of assumptions (which are non-falsifiable, according to Naor’s classification [Nao03]) or the random oracle model. [1]

Despite the use of non-falsifiable assumptions, the generality of NIZK proofs for NP-

[1] There is evidence that the use of knowledge-of-exponent type of assumptions may be unavoidable for constant-size NIZK proofs for NP-complete languages [GW11].

complete languages hides a subtlety. In order to prove the validity of a statement, it is necessary to express it as the satisfiability of a circuit. Apart from the cost of expressing the statement as a circuit (a Cook reduction), many cryptographic statements are more naturally expressed by other means. In fact, with the advent of *pairing-based cryptography* many cryptosystems have been built using *bilinear groups*, that is, three abelian groups $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ of order q together with a bilinear function $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. As consequence, statements related to pairing-based cryptographic schemes are more naturally expressed as the satisfiability of equations over these groups and $\mathbb{Z}_q$.

The Groth-Sahai proof system (GS proofs) [GS12] provides a proof system for satisfiability of this type of equations: *pairing product equations*. This language suffices to capture almost all of the statements which appear in practice when designing cryptographic schemes over bilinear groups. Although GS proofs are quite efficient, proving satisfiability of m equations in n variables requires sending the solutions, using an appropriated encryption or commitment scheme, requiring $\Theta(n)$ group elements, and a proof that the encrypted values are indeed solutions, requiring $\Theta(m)$ group elements. Although linear in both m and n, the constants are on the order of ~ 10. Consequently, a rough approximation of the average proof size would be $(m+n)10$*64 bytes $= (m+n)640$ bytes, which limits $m+n$ to be less than 1600 whenever we want the proof to be less that 1 Megabyte.[2] For this reason, several recent works have focused on further improving the proof efficiency (e.g. [EG14, EHK$^+$13, Råf15])

A recent line of work [JR13, JR14, KW15, LPJY14] has succeeded in constructing constant-size arguments for very specific statements, namely, for membership in subspaces of $\mathbb{G}_1^m$, where $\mathbb{G}_1$ is some group equipped with a bilinear map where the discrete logarithm is hard. The soundness of the schemes is based on standard, falsifiable assumptions and the proof size is independent of both m and the witness size. These improvements are in a *quasi-adaptive* model (QA-NIZK, [JR13]). This means that the common reference string of these proof systems is specialized to the linear space where one wants to prove membership.

Interestingly, Jutla and Roy [JR14] also showed that their techniques to construct constant-size NIZK in linear spaces can be used to aggregate the GS proofs of m equations in n variables, that is, the proof –without considering the n commitments to variables– is of size $\Theta(1)$. However, aggregation is only possible if the equations are linear and the equation type is more limited when working with more efficient *asymmetric* bilinear groups.

The main objective of this thesis is to explore more efficient proofs for linear and other equations with special focus on asymmetric groups. We put emphasis on constructing *aggregated proofs*, that is, a single proof for many statements whose size is independent from the number of statements. Specifically we consider:

- Linear and quadratic equations over $\mathbb{Z}_q$, where the variables are restricted to be integers modulo q.
- Linear equations over $\mathbb{G}_1$ and/or $\mathbb{G}_2$ with the additional restriction that the constants are fixed – one proof system for each set of equations – and that they can be sampled together with their discrete logarithms.
- Set membership proofs, where one shows that a variable is an element from some set S. This is a natural generalization of *high-degree equations* of the form $p(x) = 0$, where p is a polynomial, that also allows the "roots" to be group elements.

[2] Using Barreto-Nahering curves with security parameter $\lambda = 128$ the base group elements are of size 32 and 64 bytes.

The second objective is to use these more efficient proofs to develop new and more efficient cryptographic protocols.

1.1 Our Results

In this thesis we show that **all linear equations** and **all quadratic equations over $\mathbb{Z}_q$** admit an aggregated proof of size $\Theta(1)$. We also show that **all set-membership proofs** over $\mathbb{Z}_q$, with set size t, admit aggregated proofs of size $\Theta(\log t)$. We show that these results can be extended to linear equations over $\mathbb{G}_1$ and/or $\mathbb{G}_2$ and to set-membership proofs over $\mathbb{G}_1$ or $\mathbb{G}_2$ meeting some restrictions. We use these results to improve the efficiency of several protocols.

In Chapter 3 we develop new techniques to aggregate linear equations, and we obtain aggregated proofs for all linear equations (in particular, two-sided linear equations) in asymmetric bilinear groups. The latter (Type III bilinear groups, according to the classification of Galbraith et al. [GPS08]), are the most attractive from the perspective of a performance and security trade off, specially since the recent attacks on discrete logarithms in finite fields by Joux [Jou14] and subsequent improvements. As applications we construct constant size proofs that many commitments – even in different groups – can be opened to the same values; and one-time linear homomorphic structure preserving signatures for messages splitted in two groups.

Chapter 4 is devoted to obtain efficient proofs for quadratic equations over the integers. We construct constant size proofs for the satisfiability of many equations of the form $b(b-1)=0$. While this is just a particular type of quadratic equation, is the most representative type of quadratic equation and efficient proofs for other equations can be build using the same techniques. We distinguish two cases depending on the commitment scheme used to commit to the solutions: *perfectly binding* or *length-reducing*.

In the perfectly binding case we consider *Groth-Sahai commitments* to $b_1,\ldots,b_n \in \mathbb{Z}_q$ and show that $b_1(b_1-1)=0,\ldots,b_n(b_n-1)=0$ with a constant size proof (we also consider another perfectly binding commitment scheme and obtain similar results). We show how to apply these results to build more efficient signature schemes, more efficient proofs that 1 out of many equations are satisfied, and more efficient set-membership proofs.

Although in the case of length-reducing commitments a proof that $b(b-1)=0$ is in general useless – since in the extreme case of perfectly hiding commitments there is always an opening that satisfies the equation – we introduce a new length-reducing commitment scheme that overcomes this problem. We call this commitment scheme *extended multi-Pedersen commitments* which is a hybrid between Groth-Sahai and multi-Pedersen commitments. We construct a constant size proof that the opening $(b_1,\ldots,b_n)^\top \in \mathbb{Z}_q^n$ of an extended multi-Pedersen commitment satisfies equations $b_1(b_1-1)=0,\ldots,b_n(b_n-1)=0$. Our proof for the length-reducing case is a key ingredient for the results of the last part of this thesis.

Chapter 5 focuses on set-membership proofs, that is, show that a variable x is in some set S of size t. We show that many set-membership proofs – i.e. $x_1,\ldots,x_n \in S$ – can be proven with a single proof of size $\Theta(t)$, when S is a set of group elements, and $\Theta(\log t)$, when S is a range of integers. We call this primitive *aggregated zero-knowledge set-membership proof*, because the proof size is independent of the number of variables. We show that aggregated zero-knowledge set-membership proofs allow efficiency improvements for two non-interactive arguments, namely, range proofs and proofs of correctness of a shuffle. Apart from efficiency improvements, we obtain a unified modular construction for the two aforementioned problems, while state of the art solutions are build from diverse techniques and assumptions.

In Chapter 6 we construct the first $\Theta(\sqrt[3]{n})$ ring signature without random oracles, and is unpublished work. This is the first asymptotic improvement in the standard model since the $\Theta(\sqrt{n})$ ring signature of Chandran et al. [CGS07]. Our construction mixes Chandran et al.'s techniques, set-membership proofs, and some techniques that Groth and Lu used to construct NIZK proofs of a correct shuffle [GL07], in a novel way.

In Chapter 7 we further improve aggregated set-membership proofs, and is also work that has not been published so far. We reduce the size of the proof that $x_1, \ldots, x_n \in S$ from $\Theta(t)$ – using the results from Chapter 5 – to $\Theta(\log t)$, where S is a set of integers of size t. Further, our improved proof works for non-fixed sets – i.e. while each instance of the proof system from Chapter 5 works for a fixed set, a single instance of the new proof system works for any set. Then, we show how to obtain proofs of size $\Theta(\log t)$ when $S \subset \mathbb{G}_s$, $s \in \{1, 2\}$, for fixed sets. Our techniques use a natural "binary tree" representation of S together with a clever usage of QA-NIZK proofs of membership in linear subspaces, Groth-Sahai proofs, and the proof systems from Chapters 3 and 4.

Our results for set-membership proofs are summarized in Table 1.1.

Section	Set Type	Fixed set	Aggregated Proof	Proof Size
4.1.6 (i)	$\subset \mathbb{G}_s$	no	no	$\Theta(\sqrt{t})$
4.1.6 (ii)	$\subset \mathbb{G}_s$	yes	no	$\Theta(\sqrt[3]{t})$
5.3.3 (a)	$[0, t-1]$	no	yes	$\Theta(\log t)$
5.3.3 (b)	$\subset \mathbb{G}_s$	yes	yes	$\Theta(t)$
7.2	$\subset \mathbb{Z}_q$	no	yes	$\Theta(\log t)$
7.2.1	$\subset \mathbb{G}_s$	yes	yes	$\Theta(\log t)$

Table 1.1: Our results for set-membership proofs. We say that the proof system works for a fixed set when each instantiation of the proof system works for a single fixed set. The proof is aggregated if one can prove that $x_1, \ldots, x_n \in S$ with a proof of size independent of n. We denote by t the size of the set.

Chapter 2

Preliminaries

2.1 Notation

Let A a polynomial time probabilistic turing machine (PPT). We denote by $x := \mathsf{A}(y)$ the assignment of x to the output of A when run on input y. Given a distribution $\mathcal{D}$ we write $x \leftarrow \mathcal{D}$ when x is sampled following distribution $\mathcal{D}$, and given a set S we denote $x \leftarrow S$ when x is sampled uniformly from the set S. We denote by $x \leftarrow \mathsf{A}(y)$ the assignment of x to the output of A when run on input y and random coins $r \leftarrow \{0,1\}^\ell$, for ℓ long enough, which can be equivalently written as $x := \mathsf{A}(y; r)$.

We say that a function $f : \mathbb{N} \to \mathbb{R}$ is negligible if for any $c \in \mathbb{N}$ there exists an integer $n_c \in \mathbb{N}$ such that for any $n > n_c$, $f(n) < 1/n^c$. We write $f(n) \in \mathsf{negl}(n)$ as shorthand for "f is negligible" and we write $f(n) \approx g(n)$ when $|f(n) - g(n)| \in \mathsf{negl}(n)$. We say that a function $f : \mathbb{N} \to \mathbb{R}$ is polynomial if there exists $c \in \mathbb{N}, n_c \in \mathbb{N}$ such that for any $n \geq n_c$, $f(n) \leq n^c$. We write $f(n) \in \mathsf{poly}(n)$ as a shorthand for "f is polynomial". We say that two distributions $\mathcal{D}_1, \mathcal{D}_2$ are computationally indistinguishable if for any PPT adversary A, $|\Pr[x \leftarrow \mathcal{D}_1 : \mathsf{A}(x) = 1] - \Pr[x \leftarrow \mathcal{D}_2 : \mathsf{A}(x) = 1]| \approx 0$. We say that a probability $p(n)$ is *overwhelming* if $1 - p(n) \in \mathsf{negl}(n)$

Vectors are denoted in boldface and lower case, usually elements of $\mathbb{Z}_q^n$, and matrices in boldface and upper case, usually elements of $\mathbb{Z}_q^{m \times n}$. We denote by $\mathbf{e}_i^n$ the i th canonical vector of $\mathbb{Z}_q^n$ and by $\mathbf{I}_n$ the identity matrix of size $n \times n$. We n can be understood from the context, we simply write $\mathbf{e}_i$ and $\mathbf{I}$. Given some matrices $\mathbf{A} \in \mathbb{Z}_q^{m \times t}, \mathbf{B} \in \mathbb{Z}_q^{m' \times t'}$, we define the operations

$$\mathbf{A}|\mathbf{B} := \begin{pmatrix} \mathbf{A} & \mathbf{B} \end{pmatrix}, \qquad \mathbf{A}/\mathbf{B} := \begin{pmatrix} \mathbf{A} \\ \mathbf{B} \end{pmatrix}, \qquad \mathrm{diag}(\mathbf{A}, n) := \begin{pmatrix} \mathbf{A} & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & \mathbf{A} \end{pmatrix} \in \mathbb{Z}_q^{mn \times tn}.$$

In Chapter 4 we make extensive use of the set $[n+k] \times [n+k] \setminus \{(i,i) : i \in [n]\}$ and for brevity we denote it by $\mathcal{I}_{n,k}$.

Cryptographic schemes are constituted by many algorithms and among them there is usually a key generation algorithm, which receives the security parameter and returns a set of keys. In all the schemes used in this work the security parameter is used to choose a (bilinear) group of size polynomially related to the security parameter, and then the security parameter is never used again. For this reason the key generation algorithms used in this work receive the group description instead of the security parameter.

2.2 Public-Key Cryptography

Perhaps the most groundbreaking achievement in modern cryptography was the work of Diffie and Hellman [DH76] where they introduce public-key cryptography. Diffie and Hellman conceived systems where each entity publishes a *public key* $\mathcal{X}$ while keeping her *secret key* x. The archetypal usage of these ideas is a *public-key encryption scheme*, where anybody could encrypt messages using the public key and only the beholder of the secret key would be able to decrypt.

Diffie and Hellman instantiated these ideas over cyclic abelian groups where the *discrete logarithm problem* was conjectured to be computationally infeasible. On the other hand, Rivest, Shamir, and Adleman used groups of unknown order and the hardness of factoring large integers in the so called RSA cryptosystems [RSA78]. In this thesis we will always work in Diffie and Hellman's setting, also called the *discrete logarithm setting.*

Next, we introduce the basic definitions used within the discrete logarithm setting. Then we quickly describe the two most classical primitives used in public-key cryptography: encryption and signatures, and we also introduce commitment schemes.

2.2.1 The Discrete Logarithm and the Diffie-Hellman Assumptions

In public-key cryptosystems it should be computationally infeasible to compute the secret key from the public key. This is conjectured to be true when x is the discrete logarithm of $\mathcal{X}$ and $\mathcal{X}$ is a random element in some cyclic group (e.g the set of quadratic residues of $\mathbb{Z}_p$ when p and $(p-1)/2$ are prime numbers).

Definition 2.1 (Abelian Group) [1] *An abelian group is a set $\mathbb{G}$ together with a map $+ : \mathbb{G} \times \mathbb{G} \to \mathbb{G}$ (written in infix notation) and the following properties hold*

Associativity *For all $\mathcal{X}, \mathcal{Y}$, and $\mathcal{Z}$ in $\mathbb{G}$, $(\mathcal{X}+\mathcal{Y})+\mathcal{Z} = \mathcal{X}+(\mathcal{Y}+\mathcal{Z})$ holds.*

Identity element *There exists an element 0 in $\mathbb{G}$, such that for all $\mathcal{X}$ in $\mathbb{G}$, $0+\mathcal{X} = \mathcal{X}+0 = \mathcal{X}$ holds.*

Inverse element *For each $\mathcal{X}$ in $\mathbb{G}$, there exists an element $-\mathcal{X}$ in $\mathbb{G}$ such that $\mathcal{X} + (-\mathcal{X}) = (-\mathcal{X}) + \mathcal{X} = 0$.*

Commutativity *For all $\mathcal{X}, \mathcal{Y}$ in $\mathbb{G}$, $\mathcal{X}+\mathcal{Y} = \mathcal{Y}+\mathcal{X}$.*

We say that $\mathbb{G}$ is cyclic if there exists an element $\mathcal{P} \in \mathbb{G}$, a generator of $\mathbb{G}$, such that $\mathbb{G} = \{\mathcal{P}, 2\mathcal{P}, 3\mathcal{P}, \ldots\}$. We say that $|\mathbb{G}|$ is the order of $\mathbb{G}$.

We denote by $\mathsf{Gen}(1^\lambda)$ a randomized algorithm which on input the security parameter λ outputs $gk := (\mathbb{G}, \mathcal{P}, q)$, $q = |\mathbb{G}|$, the description of a cyclic group of order q.

Definition 2.2 (Discrete Logarithm Assumption (DL)) *We say that the discrete logarithm assumption holds relative to Gen if for any adversary A*

$$\Pr[gk \leftarrow \mathsf{Gen}(1^\lambda); x \leftarrow \mathbb{Z}_q; \mathcal{X} := x\mathcal{P} : \mathsf{A}(gk, \mathcal{X}) = x] \approx 0.$$

Diffie and Hellman also introduced a novel key-exchange protocol, which was later known as the *Diffie-Hellman key-exchange*, based on the following assumption

[1] In this work we will be using additive notation (mostly to avoid tangled expressions in the exponent), while historically the discrete logarithm problem was defined over multiplicative groups (thus using multiplicative notation). Using multiplicative notation the "logarithm" comes from the fact that we want a solution to the equation $g^x = \mathcal{X}$, where g is a generator of $\mathbb{G}$.

Definition 2.3 (Computational Diffie-Hellman Assumption (CDH)) *We say that the computational Diffie-Hellman assumption holds relative to* Gen *if for any adversary* A

$$\Pr[gk \leftarrow \mathsf{Gen}(1^\lambda); x, y \leftarrow \mathbb{Z}_q; \mathcal{X} := x\mathcal{P}; \mathcal{Y} := y\mathcal{P} : \mathsf{A}(gk, \mathcal{X}, \mathcal{Y}) = xy\mathcal{P}] \approx 0.$$

The Diffie-Hellman key-exchange allows two parties A, in possession of random secret $x \in \mathbb{Z}_q$ and $\mathcal{Y} = y\mathcal{P}$, and B, in possession of random secret $y \in \mathbb{Z}_q$ and $\mathcal{X} = x\mathcal{P}$, to compute the shared secret key $\mathcal{Z} = x\mathcal{Y} = y\mathcal{X} = xy\mathcal{P}$. The computational Diffie-Hellman assumption says that the only way to compute the shared secret key is to know one of the secrets. The *decisional Diffie-Hellman* assumptions goes a step beyond and says that the shared key "looks random" to anyone other than A and B

Definition 2.4 (Decisional Diffie-Hellman Assumption (DDH)) *We say that the decisional Diffie-Hellman assumption holds relative to* Gen *if for any adversary* A

$$\Pr\left[\begin{array}{l} gk \leftarrow \mathsf{Gen}(1^\lambda); x, y, z \leftarrow \mathbb{Z}_q, b \leftarrow \{0,1\}; \mathcal{X} := x\mathcal{P}; \mathcal{Y} := y\mathcal{P}; \\ \mathcal{Z} := (bxy + (1-b)z)\mathcal{P} : \mathsf{A}(gk, \mathcal{X}, \mathcal{Y}, \mathcal{Z}) = b \end{array}\right] \approx 1/2$$

2.2.2 Public-Key Encryption

A public-key encryption scheme is a tuple of 3 algorithms $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$. KeyGen is a randomized algorithm which on input a group key gk generates a public/secret key pair. Enc is a randomized algorithm which on input the public key and a *plaintext*, which is an element from the set $\mathcal{M}_{gk}$, returns a *ciphertext*, which is an element from the set $\mathcal{C}_{gk}$. Dec is a deterministic algorithm which on input a ciphertext and the secret key returns a plaintext. It is required that for every pair (pk, sk) output by Gen and any $m \in \mathcal{M}_{gk}$, $\mathsf{Dec}_{sk}(\mathsf{Enc}_{pk}(m)) = m$.

ElGamal introduced the first *semantically secure encryption scheme* based on the DDH assumption [ElG85]. The idea was simple and clean: encrypt a message $\mathcal{M}$ under public key $pk := \mathcal{X}$ picking $r \leftarrow \mathbb{Z}_q$ and computing the ciphertext $\mathsf{Enc}_{pk}(\mathcal{M}; r) := (\mathcal{C}_1, \mathcal{C}_2) = (r\mathcal{P}, \mathcal{M} + r\mathcal{X})$; and decrypt a ciphertext using the secret key x and computing $\mathsf{Dec}_{sk}(\mathcal{C}_1, \mathcal{C}_2) = \mathcal{C}_2 - x\mathcal{C}_1$. It follows that $(\mathcal{C}_1, \mathcal{C}_2)$ hides $\mathcal{M}$ since $r\mathcal{X}$, by the DDH assumption, looks like fresh random value, independent of $\mathcal{C}_1$, making $\mathcal{M} + r\mathcal{X}$ independent of $\mathcal{M}$. Formally, it can be shown that ElGamal cryptosystem is *indistinguishable under chosen plaintext attacks* (also called semantically secure and IND-CPA for short).

Definition 2.5 (IND-CPA [GM84]) *We say that* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *is IND-CPA secure if for any* $\mathsf{A}_1, \mathsf{A}_2$

$$\Pr\left[\begin{array}{l} gk \leftarrow \mathsf{Gen}; (pk, sk) \leftarrow \mathsf{KeyGen}(gk); b \leftarrow \{0,1\}; \\ (m_0, m_1) \leftarrow \mathsf{A}_1(gk, pk); c_b \leftarrow \mathsf{Enc}_{pk}(m_b) : \mathsf{A}_2(gk, pk, c_b) = b \end{array}\right] \approx 1/2.$$

2.2.3 Commitment Schemes

Intuitively, a commitment scheme is a "relaxed encryption scheme" where the function $\mathsf{Enc}_{pk}(\cdot)$ is not necessarily invertible. Although some ciphertexts – now called commitments – may be obtained from different plaintexts – openings – it is (computationally) infeasible to compute two openings for the same commitment. In this way, when an adversary computes some commitment it is committing to the unique opening that she is able to compute.

Syntactically, a commitment scheme is a tuple of three algorithms $(\mathsf{K}, \mathsf{Com}, \mathsf{Vrfy})$. K is a randomized algorithm, which on input a group key gk outputs a commitment key ck.

Com is a randomized algorithm which, on input the commitment key ck and a message m in the message space $\mathcal{M}_{ck}$ outputs a commitment c in the commitment space $\mathcal{C}_{ck}$ and an opening Op. Vrfy is a deterministic algorithm which, on input the commitment key ck, a message m in the message space $\mathcal{M}_{ck}$ and an opening Op, outputs 1 if Op is a valid opening of c to the message m and 0 otherwise. Correctness requires that for any $m \in \mathcal{M}_{ck}$

$$\Pr\left[ck \leftarrow \mathsf{K}(gk); (c, Op) \leftarrow \mathsf{Com}_{ck}(m) : \mathsf{Vrfy}(ck, c, m, Op) = 1\right] = 1.$$

Definition 2.6 *A commitment scheme is computationally binding (resp. perfectly binding) if, for any polynomial-time (resp. unbounded) adversary* A*,*

$$\Pr\left[\begin{array}{l} ck \leftarrow \mathsf{K}(gk); (c, m, Op, m', Op') \leftarrow \mathsf{A}(gk, ck) : \\ \mathsf{Vrfy}(ck, c, m, Op) = 1 \wedge \mathsf{Vrfy}(ck, c, m', Op') = 1 \wedge m \neq m' \end{array}\right]$$

is negligible (resp. zero). It is computationally hiding (resp. perfectly hiding) if, for any polynomial-time (resp. unbounded) adversary A*,*

$$\left|\Pr\left[\begin{array}{l} ck \leftarrow \mathsf{K}(gk); (m_0, m_1, st) \leftarrow \mathsf{A}(gk, ck); b \leftarrow \{0,1\}; \\ (c, Op) \leftarrow \mathsf{Com}_{ck}(m_b); b' \leftarrow \mathsf{A}(st, c) \end{array} : b' = b\right] - \frac{1}{2}\right|$$

is negligible (resp. zero).

In Section 2.6.2 we introduce Groth-Sahai commitments and in Section 4.2.1 we introduce a new commitment scheme which we call extended multi-Pedersen commitments.

2.2.4 Digital Signatures

A digital signature scheme is a tuple of 3 algorithms $(\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Ver})$. KeyGen is a randomized algorithm which on input a group key gk generates a public/secret key pair. Sign is a randomized algorithm which on input the secret key and a *message*, which is an element from the set $\mathcal{M}_{gk}$, returns a *signature*, which is an element from the set $\mathcal{S}_{gk}$. Ver is a deterministic algorithm which on input the public key, a message, and a signature returns 0 or 1. It is required that for every pair (pk, sk) output by KeyGen and any $m \in \mathcal{M}_{gk}$, $\mathsf{Ver}_{pk}(m, \mathsf{Sign}_{sk}(m)) = 1$.

Definition 2.7 (Existencial Unforgeability (UF-CMA)) *We say that* $(\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Ver})$ *is UF-CMA secure if for any* A

$$\Pr\left[\begin{array}{l} gk \leftarrow \mathsf{Gen}; (pk, sk) \leftarrow \mathsf{KeyGen}(gk); \\ (m, \sigma) \leftarrow \mathsf{A}^{\mathsf{Q}}(gk, pk) : \mathsf{Ver}_{pk}(m, \sigma) = 1 \textit{ and } m \notin \mathcal{Q} \end{array}\right] \approx 0,$$

where Q *is an oracle which on input* m *responds with* $\sigma \leftarrow \mathsf{Sign}_{sk}(m)$ *and sets* $\mathcal{Q} \leftarrow \mathcal{Q} \cup \{m\}$*. If* ℓ *is the number of oracle queries made by* A*, we say that* $(\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Ver})$ *is a one-time signature scheme if it is UF-CMA whenever* $\ell \leq 1$*.*

In Section 6.2.4 we introduce a signature scheme known as Boneh-Boyen signatures.

2.3 Bilinear Groups

Groups where the DDH assumption (as well as the discrete logarithm assumption) is believed to be hard were usually constructed as multiplicative subgroups of a finite field of order n, $\mathbb{F}_n$ – for example the set of quadratic residues of $\mathbb{Z}_p$ when p is a safe prime (i.e. $(p-1)/2$ is also a prime number). Koblitz and (independently) Miller proposed as an alternative the usage of *elliptic curves* over $\mathbb{F}_n$ [Kob87, Mil86], that is the set of points (x, y) over $\mathbb{F}_n^2$ which are solutions to the equation $E : y^2 = x^3 + ax + b$, where $a, b \in \mathbb{F}_n$, together with an especial point $\mathcal{O}$. The solutions to E together with $\mathcal{O}$ form an abelian group, denoted by $E(\mathbb{F}_n)$, where $\mathcal{O}$ is the identity element and the group operation is defined as a geometrical operation between the group elements (called the cord-and-tangent method). For the appropriate choice of a and b the discrete logarithm is believed to require exponential time to be computed, while for subgroups of $\mathbb{F}_n$ there are known sub-exponential attacks. As consequence, the size of the elements of $E(\mathbb{F}_n)$ is much smaller than the size of elements of traditional finite fields at an equivalent security level.

However not all elliptic curves offer the same security. For example in some elliptic curves, which we will call bilinear groups for short, one can compute the *Weil pairing* or the *Tate pairing*. These pairings are functions of the form $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ where $\mathbb{G}_1$ and $\mathbb{G}_2$ are cyclic subgroups of $E(\mathbb{F}_n)$ and $\mathbb{G}_T$ is another cyclic group known as the *target group*. The function e is bilinear, because $e(a\mathcal{X}, b\mathcal{Y}) = ab \cdot e(\mathcal{X}, \mathcal{Y})$ for any $\mathcal{X} \in \mathbb{G}_1$ and any $\mathcal{Y} \in \mathbb{G}_2$, and non-degenerate, because $e(\mathcal{P}_1, \mathcal{P}_2)$ is a generator of $\mathbb{G}_T$ when $\mathcal{P}_s$ is a generator of $\mathbb{G}_s$, $s \in \{1, 2\}$. For simplicity assume that $\mathbb{G}_1 = \mathbb{G}_2 = \mathbb{G}$ (this is the case of the Weil pairing) and let $\mathcal{P}$ the generator of $\mathbb{G}$. Intuitively, the function e is "solving CDH in $\mathbb{G}$ but giving the answer in $\mathbb{G}_T$", that is, given $\mathcal{X} = a\mathcal{P}$ and $\mathcal{Y} := b\mathcal{P}$ one can compute $t = e(\mathcal{X}, \mathcal{Y}) = ab \cdot e(\mathcal{P}, \mathcal{P})$. Although this does not gives a solution to the CDH problem in $\mathbb{G}$, it does solve the DDH problem in $\mathbb{G}$. Indeed, $e(\mathcal{X}, \mathcal{Y}) = e(\mathcal{Z}, \mathcal{P})$ is satisfied by $\mathcal{Z} = ab\mathcal{P}$ but only with negligible probability by a random element of $\mathbb{G}$. Moreover, the MOV and the FR reductions compile the DL problem in $E(\mathbb{F}_n)$ into the finite field $\mathbb{F}_{n^\alpha}$, for some α known as the embedding degree, where known sub-exponential algorithms for solving the DL exist [MVO91, FR94]. For these reasons elliptic curves where a pairing function can be efficiently computed were initially considered unsafe for cryptographic purposes.

But this changed with the work of Joux [Jou00], where he showed that pairings can be also used to construct cryptographic schemes rather than to destroy them. Joux noted that pairings can be used to construct a non-interactive three party Diffie-Hellman key exchange [Jou00]. Given public keys $\mathcal{X} = x\mathcal{P}$, $\mathcal{Y} = y\mathcal{P}$, and $\mathcal{Z} = z\mathcal{P}$ and one secret key from x, y, or z, each party can compute the shared key $x \cdot e(\mathcal{Y}, \mathcal{Z}) = y \cdot e(\mathcal{X}, \mathcal{Z}) = z \cdot e(\mathcal{X}, \mathcal{Y}) = xyz \cdot e(\mathcal{P}, \mathcal{P})$. The critical observation was that, although the DDH might be easy in bilinear groups, the DL might be made hard if the size of the group is appropriately increased in order to rule out the sub-exponential attacks implied by the MOV and FR reductions. Moreover, Joux protocol can be proven secure under the *bilinear decisional Diffie-Hellman* assumption, which is believed to be a hard problem in some bilinear groups [BF01], and also CDH and many other assumptions are believed to hold on some bilinear groups [Ver13]. Furthermore, from Joux seminal work many open problems have been solved using bilinear groups, being *identity based encryption* [BF01] the more outstanding example, and many new applications have been found (a number of this applications can be found the survey of Dutta et al. [DBS04]).

2.3.1 Definition

Definition 2.8 (Bilinear Groups) [2] *Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be cyclic groups of prime order q and $\mathcal{P}_s$ the generator of $\mathbb{G}_s$, $s \in \{1,2\}$, and $\mathbb{G}_T$ be another cyclic group of order q. We say that $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ form a bilinear group if there exists a map $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ such that:*

Bilinearity: *For all $a, b \in \mathbb{Z}_q$, for all $\mathcal{X} \in \mathbb{G}_1$, and all $\mathcal{Y} \in \mathbb{G}_2$*

$$e(a\mathcal{X}, b\mathcal{Y}) = ab \cdot e(\mathcal{X}, \mathcal{Y}),$$

Non-degeneracy: *If $\mathcal{X}, \mathcal{Y} \neq 0$, then $e(\mathcal{X}, \mathcal{Y}) \neq 0$,*

Computability: *$e(\mathcal{X}, \mathcal{Y})$ is efficiently computable.*

The first property says that e allows to "homomorphically" compute degree 2 expressions in the field $(\mathbb{Z}_q, +, \cdot)$. Since any $\mathcal{X}$ can be written as $x\mathcal{P}_1$, where x is some element of $\mathbb{Z}_q$ (and the same can be done in $\mathbb{G}_2$), $e(\mathcal{X}, \mathcal{Y}) = xy \cdot e(\mathcal{P}_1, \mathcal{P}_2)$. Non-degeneracy says that e is does not map everything to 0. While the third property says that computing e is practical, the reality is that it is still an expensive operation and is one of the critical performance measures of cryptographic constructions.

Galbraith et al. classify bilinear groups in three types [GPS08]:

Type I: $\mathbb{G}_1 = \mathbb{G}_2$ and also known as *symmetric* groups.

Type II: $\mathbb{G}_1 \neq \mathbb{G}_2$ but there is an efficiently computable homomorphism $\phi : \mathbb{G}_1 \rightarrow \mathbb{G}_2$.

Type III: $\mathbb{G}_1 \neq \mathbb{G}_2$ and no efficiently computable homomorphism is known. Also known as *asymmetric* groups.

Type III bilinear groups are the most attractive from the perspective of a performance and security trade-off, specially since the recent attacks on discrete logarithms in finite fields by Joux [Jou14] and subsequent improvements.

We denote by Gen_a the probabilistic polynomial time algorithm which on input 1^λ, where λ is the security parameter, returns the *group key* which is the description of an asymmetric bilinear group $gk := (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, \mathcal{P}_1, \mathcal{P}_2)$, where $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$ are groups of prime order q, the elements $\mathcal{P}_1, \mathcal{P}_2$ are generators of $\mathbb{G}_1, \mathbb{G}_2$ respectively, and $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ is an efficiently computable, non-degenerate bilinear map.

Implicit Representation of Group Elements

Elements in $\mathbb{G}_s$, are denoted implicitly as $[a]_s := a\mathcal{P}_s$, where $s \in \{1, 2, T\}$ and $\mathcal{P}_T := e(\mathcal{P}_1, \mathcal{P}_2)$. The pairing operation will be written as a product $\cdot$, that is $[a]_1 \cdot [b]_2 = [a]_1[b]_2 = e([a]_1, [b]_2) = [ab]_T$. We sometimes abuse of notation and write $[b]_2[a]_1$ to denote $e([a]_1, [b]_2)$ (note that there is no ambiguity since $e([b]_2, [a]_1)$ is undefined). Given a matrix $\mathbf{T} = (t_{i,j})$, $[\mathbf{T}]_s$ is the natural embedding of $\mathbf{T}$ in $\mathbb{G}_s$, that is, the matrix whose (i, j)th entry is $t_{i,j}\mathcal{P}_s$. We denote by $|\mathbb{G}_s|$ the bit-size of the elements of $\mathbb{G}_s$.

2.3.2 The Decisional k-Linear Diffie-Hellman Family of Assumptions

In type I groups the DDH assumption is easy because, as noted before, using the pairing operation one can check if $[x][y] = [z][1]$ (implicit representation in type I groups can omit

[2] While the usual notation for the target group has been multiplicative, we write it in additive notation. The reason is just to elude cumbersome expressions in the exponent.

the group sub-index). Boneh, Boyen, and Sacham introduced a "DDH like" assumption called the *decisional linear Diffie-Hellman* assumption (DLin) [BBS04], proved that is secure in the generic group model in type I groups, and that it is implied by DDH in type III groups.

Definition 2.9 (DLin assumption) *We say that the DLin assumption in $\mathbb{G}_s$, $s \in \{1,2\}$, holds relative to Gen_a if for any adversary A*

$$\Pr\left[\begin{array}{l} gk \leftarrow \mathsf{Gen}_a(1^\lambda); a_1, a_2, r_1, r_2, z \leftarrow \mathbb{Z}_q, b \leftarrow \{0,1\} : \\ \mathsf{A}(gk, [a_1]_s, [a_2]_s, [r_1 a_1]_s, [r_2 a_2], (1-b)[r_1 + r_2]_s + b[z]_s) = b \end{array}\right] \approx 1/2.$$

The DLin assumption is a natural counterpart of the DDH assumption, and one can easily replace DDH by DLin assumption (e.g. ElGamal encryption can be easily turned into the *linear encryption* scheme). Moreover, Sacham noted that the DDH and DLin assumptions are members of an infinite family of progressively weaker assumptions called the k-Linear family of assumptions (k-Lin) [Sha07].

Definition 2.10 (k-Lin assumption) *We say that the k-Lin assumption in $\mathbb{G}_s$, $s \in \{1,2\}$, holds relative to Gen_a if for any adversary A*

$$\Pr\left[\begin{array}{l} gk \leftarrow \mathsf{Gen}_a(1^\lambda); a_1, \ldots, a_k, r_1, \ldots, r_k, z \leftarrow \mathbb{Z}_q, b \leftarrow \{0,1\} : \\ \mathsf{A}(gk, [a_1]_s, \ldots, [a_k]_s, [r_1 a_1]_s, \ldots, [r_k a_k]_s, (1-b)[\sum_{i=1}^k r_i]_s + b[z]_s) = b \end{array}\right]$$
$$\approx 1/2.$$

Thereby, the DDH assumption is the 1-Lin assumption, DLin is 2-Lin, and it can be proved that $(k+1)$-Lin is weaker than k-Lin.

2.4 Matrix Diffie-Hellman Assumptions

In this section we review *Matrix Diffie-Hellman assumptions* (MDDH) of Escala et al. [EHK+13] which are abstractions and generalizations of the k-Lin family of assumptions. Then, we review *Kernel Matrix Diffie-Hellman assumptions* (KMDH) of Morillo et al. [MRV15], which are the natural computational counterpart of Matrix Diffie-Hellman assumptions.

We also put forward a new Kernel assumption which is specific to asymmetric groups, and we prove its security in the *generic group model.*

2.4.1 decisional Matrix Diffie-Hellman Assumptions

Definition 2.11 *Let $\ell, k \in \mathbb{N}$. We call $\mathcal{D}_{\ell,k}$ a matrix distribution if it outputs (in poly time, with overwhelming probability) matrices in $\mathbb{Z}_q^{\ell \times k}$. We define $\mathcal{D}_k := \mathcal{D}_{k+1,k}$ and $\overline{\mathcal{D}}_k$ the distribution of the first k rows of $\mathbf{A}$ when $\mathbf{A} \leftarrow \mathcal{D}_k$.*

For the following decisional assumption to hold, it is a necessary condition that $\ell > k$. However, in other contexts, we might need $\mathcal{D}_{\ell,k}$ distributions where $\ell \geq k$.

Definition 2.12 (MDDH Assumption in $\mathbb{G}_\gamma$, $\gamma \in \{1,2\}$ [EHK+13]) *Let $\mathcal{D}_{\ell,k}$ be a matrix distribution and $gk \leftarrow \mathsf{Gen}_a(1^\lambda)$. We say that the $\mathcal{D}_{\ell,k}$-Matrix Diffie-Hellman ($\mathcal{D}_{\ell,k}$-$\mathsf{MDDH}_{\mathbb{G}_\gamma}$) assumption holds relative to Gen_a if for all PPT adversaries D,*

$$\mathbf{Adv}_{\mathcal{D}_{\ell,k},\mathsf{Gen}_a}(\mathsf{D}) \quad := \quad |\Pr[\mathsf{D}(gk, [\mathbf{A}]_\gamma, [\mathbf{Aw}]_\gamma) = 1] - \Pr[\mathsf{D}(gk, [\mathbf{A}]_\gamma, [\mathbf{z}]_\gamma) = 1]|$$

is negligible in k, where the probability is taken over $gk \leftarrow \mathsf{Gen}_a(1^\lambda)$, $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}, \mathbf{w} \leftarrow \mathbb{Z}_q^k, [\mathbf{z}]_\gamma \leftarrow \mathbb{G}_\gamma^\ell$ and the coin tosses of adversary D.

In this work we will refer to the following matrix distributions:

$$\mathcal{L}_k : \mathbf{A} = \begin{pmatrix} a_1 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_k \\ 1 & 1 & \dots & 1 \end{pmatrix}, \ \mathcal{L}_{\ell,k} : \mathbf{A} = \begin{pmatrix} \mathbf{B} \\ \mathbf{C} \end{pmatrix}, \ \mathcal{U}_{\ell,k} : \mathbf{A} = \begin{pmatrix} a_{1,1} & \dots & a_{1,k} \\ \vdots & \ddots & \vdots \\ a_{\ell,1} & \dots & a_{\ell,k} \end{pmatrix},$$

where $\mathbf{B} \leftarrow \overline{\mathcal{L}}_k$, $\mathbf{C} \leftarrow \mathbb{Z}_q^{\ell-k,k}$, and $a_i, a_{i,j} \leftarrow \mathbb{Z}_q$. The $\mathcal{L}_k$-MDDH assumption is the k-linear family of decisional assumptions and corresponds to the decisional Diffie-Hellman (DDH) assumption in $\mathbb{G}_\gamma$ when $k = 1$. The SXDH assumption states that DDH holds in $\mathbb{G}_\gamma$ for all $\gamma \in \{1, 2\}$. The $\mathcal{U}_{\ell,k}$ assumption is the *uniform* assumption and is the weakest of all assumptions of size $\ell \times k$.

Further, given any matrix distribution $\mathcal{D}_k$, $m \in \mathbb{N}$ and any $i \in [m]$, we introduce the distribution $\mathcal{D}_k^{m,i}$, which is defined as follows:

$$\mathcal{D}_k^{m,0} : \mathbf{A} = \left(\mathbf{Bw}_1 \dots \mathbf{Bw}_m \ \mathbf{B} \right) \qquad \mathcal{D}_k^{m,i} : \mathbf{A} = \left(\mathbf{Bw}_1 \dots \mathbf{Bw}_{i-1} \ \mathbf{z} \ \mathbf{Bw}_{i+1} \dots \mathbf{Bw}_m \ \mathbf{B} \right)$$

where $\mathbf{B} \leftarrow \mathcal{D}_k$, $\mathbf{w}_i \leftarrow \mathbb{Z}_q^k$ and $\mathbf{z} \leftarrow \mathbb{Z}_q^{k+1}$. The following are two trivial properties of the $\mathcal{D}_k^{m,i}$ distribution.

Lemma 2.13 *Under the $\mathcal{D}_k$-MDDH assumption in $\mathbb{G}_\gamma$, for any $0 < i \leq n$, the distribution of $[\mathbf{A}]_\gamma$ when $\mathbf{A} \leftarrow \mathcal{D}_k^{m,0}$ and when $\mathbf{A} \leftarrow \mathcal{D}_k^{m,i}$ are computationally indistinguishable. Further, if $\ell > k$, for any $i > 0$, if $\mathbf{A} \leftarrow \mathcal{D}_k^{m,i}$, then with overwhelming probability its ith column is linearly independent of the rest.*

2.4.2 Computational Matrix Diffie-Hellman Assumptions

Additionally, we will be using the following family computational assumptions:

Definition 2.14 (Kernel Diffie-Hellman Assumption in $\mathbb{G}_\gamma$ [MRV15]) *Let $gk \leftarrow \mathsf{Gen}_a(1^\lambda)$. The Kernel Diffie-Hellman assumption in $\mathbb{G}_\gamma$ ($\mathcal{D}_{\ell,k}$-$\mathsf{KerMDH}_{\mathbb{G}_\gamma}$) says that every PPT Algorithm has negligible advantage in the following game: given $[\mathbf{A}]_\gamma$, where $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$, find $[\mathbf{x}]_{3-\gamma} \in \mathbb{G}_{3-\gamma}^\ell$, $\mathbf{x} \neq \mathbf{0}$, such that $[\mathbf{x}]_{3-\gamma}^\top [\mathbf{A}]_\gamma = [\mathbf{0}]_T$.*

The Simultaneous Pairing assumption in $\mathbb{G}_\gamma$ ($\mathsf{SP}_{\mathbb{G}_\gamma}$) is the $\mathcal{U}_1$-$\mathsf{KerMDH}_{\mathbb{G}_\gamma}$ assumption. The Kernel Diffie-Hellman assumption is a generalization and abstraction of this assumption to other matrix distributions. The $\mathcal{D}_{\ell,k}$-$\mathsf{KerMDH}_{\mathbb{G}_\gamma}$ assumption is weaker than the $\mathcal{D}_{\ell,k}$-$\mathsf{MDDH}_{\mathbb{G}_\gamma}$ assumption, since a solution to the former allows to decide membership in $\mathbf{Im}([\mathbf{A}]_\gamma)$.

2.4.3 A new Computational Matrix Diffie-Hellman Assumption in Type III Groups

In asymmetric bilinear groups, we introduce a natural variant of the $\mathcal{D}_{\ell,k}$-KerMDH assumption [GHR15a].

Definition 2.15 (Split Kernel Diffie-Hellman Assumption) *Let $gk \leftarrow \mathsf{Gen}_a(1^\lambda)$. The Split Kernel Diffie-Hellman assumption in $\mathbb{G}_1, \mathbb{G}_2$ ($\mathcal{D}_{\ell,k}$-$\mathsf{SKerMDH}$) says that every PPT Algorithm has negligible advantage in the following game: given $([\mathbf{A}]_1, [\mathbf{A}]_2)$, $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$, find a pair of vectors $([\mathbf{r}]_1, [\mathbf{s}]_2) \in \mathbb{G}_1^\ell \times \mathbb{G}_2^\ell$, $\mathbf{r} \neq \mathbf{s}$, such that $[\mathbf{r}]_1^\top [\mathbf{A}]_2 = [\mathbf{s}]_2^\top [\mathbf{A}]_1$.*

While the Kernel Diffie-Hellman assumption says one cannot find a non-zero vector in one of the groups which is in the co-kernel of $\mathbf{A}$, the split assumption says one cannot find a pair of vectors in $\mathbb{G}_1^\ell \times \mathbb{G}_2^\ell$ such that the difference of the vector of their discrete logarithms is in the co-kernel of $\mathbf{A}$. As a particular case we consider the *Split Simultaneous Double Pairing assumption in* $\mathbb{G}_1, \mathbb{G}_2$ (SSDP) which is the $\mathcal{RL}_2$-SKerMDH assumption, where $\mathcal{RL}_2$ is the distribution which results of sampling a matrix from $\mathcal{L}_2$ and replacing the last row by random elements.

To gain confidence in this assumption, we first note that it implies the Kernel MDH assumption and then we prove that the reciprocal is true in the generic bilinear model.

Lemma 2.16 $\mathcal{D}_{\ell,k}$-SKerMDH $\Rightarrow \mathcal{D}_{\ell,k}$-KerMDH$_{\mathbb{G}_2}$.

Proof Suppose there exists an adversary B against the $\mathcal{D}_{\ell,k}$-KerMDH$_{\mathbb{G}_2}$ assumption. We show how to construct an adversary A against the $\mathcal{D}_{\ell,k}$-SKerMDH assumption. Adversary A receives as a challenge $([\mathbf{A}]_1, [\mathbf{A}]_2)$ and forwards $[\mathbf{A}]_2$ to B, who outputs with non-negligible probability a vector $[\mathbf{r}]_1$ such that $[\mathbf{r}]_1^\top [\mathbf{A}]_2 = [\mathbf{0}]_T$. Then A simply outputs $([\mathbf{r}]_1, [\mathbf{0}]_2)$ as a solution to the $\mathcal{D}_{\ell,k}$-SKerMDH challenge. □

Security of the $\mathcal{D}_{\ell,k}$-SKerMDH in the Generic Group Model

The generic group model is an idealized model for analysing the security of cryptographic assumptions or cryptographic schemes. A proof of security in the generic group model guarantees that no attacker, that only uses the algebraic structure of the (bilinear) group, is successful in breaking the assumption/scheme. Conversely, for a generically secure assumption/scheme, a successful attack must exploit the structure of the (bilinear) group that is actually used in the protocol (e.g. a Barreto-Naehring curve in the case of bilinear groups).

We use the natural generalization of Shoup's generic group model [Sho97] to the (a)symmetric bilinear setting, as it was used for instance by Boneh et al. [BBG05]. In such a model an adversary can only access elements of $\mathbb{G}_1, \mathbb{G}_2$ or $\mathbb{G}_T$ via a query to a group oracle, which gives him a randomized encoding of the queried element. The group oracle must be consistent with the group operations (allowing to query for the encoding of constants in either group, for the encoding of the sum of previously queried elements in the same group and for the encoding of the product of pairs in $\mathbb{G}_1 \times \mathbb{G}_2$).

Lemma 2.17 *If* $\mathcal{D}_{\ell,k}$-KerMDH *holds in generic symmetric bilinear groups, then* $\mathcal{D}_{\ell,k}$-SKerMDH *holds in generic asymmetric bilinear groups.*

Proof Suppose there is an adversary A in the asymmetric generic bilinear group model against the $\mathcal{D}_{\ell,k}$-SKerMDH assumption. We show how to construct an adversary B against the $\mathcal{D}_{\ell,k}$-KerMDH$_{\mathbb{G}_2}$ assumption in the symmetric generic group model.

Adversary B has oracle access to the randomized encodings $\sigma : \mathbb{Z}_q \to \{0,1\}^n$, and $\sigma_T : \mathbb{Z}_q \to \{0,1\}^n$. It receives as a challenge $\{\sigma(a_{ij})\}_{1 \le i \le \ell, 1 \le j \le k}$.

Adversary B simulates the generic hardness game for A as follows. It defines encodings $\xi_1 : \mathbb{Z}_q \to \{0,1\}^n$, $\xi_2 : \mathbb{Z}_q \to \{0,1\}^n$ and $\xi_T : \mathbb{Z}_q \to \{0,1\}^n$ as $\xi_1 = \sigma$, $\xi_T = \sigma_T$ and ξ_2 a random encoding function. B keeps a list L_{A} with the values that have been queried by A to the group oracle. The list is initialized as $L_{\mathsf{A}} = \{\{(A_{i,j}, \xi_1(a_{ij}), 1), (A_{i,j}, \xi_2(a_{ij}), 2)\}_{1 \le i \le \ell, 1 \le j \le k}\}$, where $\xi_2(a_{ij}) \in \{0,1\}^n$ are chosen uniformly at random conditioned on being pairwise distinct. Adversary B also keeps a list L_{B} with the queries it makes to its own group oracle. The list L_{B} is initialized as $L_{\mathsf{B}} = \{\{(A_{i,j}, \sigma(a_{ij}), 1)\}_{1 \le i \le \ell, 1 \le j \le k}\}$

Each element in the list L_{A} is a tuple (P_i, s_i, x_i), where $P_i \in \mathbb{Z}_q[A_{11}, \ldots, A_{\ell k}]$, $x_i \in \{1, 2, T\}$ and $s_i = \xi_{x_i}(P_i(a_{11}, \ldots, a_{\ell k}))$. The polynomial P_i is one of the following: a) $P_i = A_{ij}$, i.e. it is one of the initial values in the query list L_{A} or b) a constant polynomial or c) $P_i = P_c + P_d$

for some $(P_c, s_c, x), (P_d, s_d, x) \in L_{\mathsf{A}}$ or d) $P_i = P_c P_d$ for some $(P_c, s_c, 1), (P_d, s_d, 2) \in L_{\mathsf{A}}$, $x_i = T$. For L_{B} the same holds except that $x_i \in \{1, T\}$ and except that d) is changed to: d) $P_i = P_c P_d$ for some $(P_c, s_c, 1), (P_d, s_d, 1) \in L_{\mathsf{B}}$ and $x_i = T$.

Without loss of generality we can identify the queries of A with pairs (P_i, x_i) meeting the restrictions described above. If (P_i, x_i) was queried before, it replies with the same answer s_i.

Else, when B receives a (valid) query (P_i, x_i), if $x_i \in \{1, T\}$ it simply forwards the query to its own group oracle, who replies with s_i. Then (P_i, s_i, x_i) is appended to L_{B} and to L_{A}. If $x_i = 2$, then it forwards the query to its own group oracle as $(P_i, 1)$. When it receives the answer s_i, B appends $(P_i, s_i, 1)$ to L_{B} and it looks for the set S of all tuples $(P_j, s_j, 1) \in L_{\mathsf{B}}$, $P_j \neq P_i$, such that $s_j = s_i$. For every tuple in S, B checks if there is some $\tilde{s}$ such that $(P_j, \tilde{s}, 2)$ is in L_{A} (note that, because of the way L_{A} is constructed, if such $\tilde{s}$ exists it is the same for all P_j).

If such $\tilde{s}$ exists, it appends $(P_i, \tilde{s}, 2)$ in L_{A} and it replies with $\tilde{s}$. Else it chooses some $\tilde{s}$ uniformly at random conditioned on being distinct from all other values s such that there exist some P such that $(P, s, 2)$ is in L_{A}. Finally, it appends $(P_i, \tilde{s}, 2)$ in L_{A}.

Finally, A will output as a solution to the challenge a pair s_q, s_r such that $(Q, s_q, 1), (R, s_r, 2) \in L_{\mathsf{A}}$. Because of the way L_{A} and L_{B} were constructed, there exists some s'_r such that $(Q, s_q, 1), (R, s'_r, 1) \in L_{\mathsf{A}}$. B queries its group oracle for $(R - Q, 1)$ and obtains as a reply some string s_{R-Q}. Finally, it outputs s_{R-Q} as a solution to its challenge. It easily follows that A and B have exactly the same probability of success. □

Finally, we note that the $\mathcal{L}_2$-$\mathsf{SKerMDH}$ assumption is implied by a decisional assumption introduced by Libert et al. [LPJY15b]. The assumption says that, given $([\mathbf{A}]_1, [\mathbf{A}]_2)$, where $\mathbf{A} \leftarrow \mathcal{L}_2$, the vector $([\mathbf{A}]_1\mathbf{w}, [\mathbf{A}]_2\mathbf{w})$, $\mathbf{w} \leftarrow \mathbb{Z}_q^2$, is computationally indistinguishable from $([\mathbf{u}]_1, [\mathbf{u}]_2)$, $\mathbf{u} \leftarrow \mathbb{Z}_q^3$. The proof is analogous to the proof that $\mathcal{D}_{\ell,k}$-$\mathsf{MDDH} \Rightarrow \mathcal{D}_{\ell,k}$-$\mathsf{KerMDH}$. Suppose that $([\mathbf{r}]_1, [\mathbf{s}]_2)$ is a solution to the $\mathcal{L}_2$-$\mathsf{SKerMDH}$ assumption, then $[\mathbf{r}]_1^\top[\mathbf{A}]_2\mathbf{w} - [\mathbf{s}]_2^\top[\mathbf{A}]_1\mathbf{w} = ([\mathbf{r}]_1^\top[\mathbf{A}]_2 - [\mathbf{s}]_2^\top[\mathbf{A}]_1)\mathbf{w} = [0]_T$, while $[\mathbf{r}]_1^\top[\mathbf{u}]_2 - [\mathbf{s}]_2^\top[\mathbf{u}]_1 = [0]_T$ only with negligible probability whenever $\mathbf{r} \neq \mathbf{s}$.

2.5 Non-Interactive Zero-Knowledge Proofs

Zero-Knowledge proofs are proofs that reveal nothing beyond their validity. Since their introduction by Goldreich et al. [GMR89], zero-knowledge proofs have played a central role in cryptography and complexity theory from both the theoretical side –they have been the inspiration of probabilistic checkable proofs and the groundbreaking results on hardness of approximation [GO05]– and the practical side – applications range from multi-party computation [GMW87] to electronic voting [JCJ10] and e-commerce [CHL05].

In a zero-knowledge proof a *prover* P in possession of a secret w wants to convince a *verifier* V that some statement x is true, namely that x belongs to some language $\mathcal{L}$. To do so the prover and the verifier engage on an *interactive protocol*: the prover starts with a message a_1, the verifier answers with b_1, and so on. At the end the verifier outputs a bit $b \in \{0, 1\}$ indicating whether it rejects or accepts the proofs.

There are two basic requirements for a zero-knowledge proof: *completeness*, which says that an honest prover should be successful when convincing the verifier about a true statement, and *soundness*, which says that the verifier should rejects false statements with *high probability.* The third requirement, which gives the name to zero-knowledge proofs, requires that the verifier does not learn nothing beyond the fact that x is true.

This is done by requiring the existence of an efficient algorithm S, the simulator, which, for any true statement, is able to construct a transcript of the interactive execution of P and V even without knowing any secret w.

A weaker variant of a zero-knowledge proof is a *witness-indistinguishable proof*. These proofs are not necessarily simulatable and only guarantee to reveal the same information when using two different secrets w, w'.

The focus of this work are *non-interactive zero-knowledge proofs* (NIZK), where the prover sends a single message, the *proof*, to the verifier. Since their introduction by Blum et al. [BFM88], it was known that a "pre-shared" information, known as the *common reference string* (CRS), allows to construct NIZK proof systems (later it was shown a necessary condition if the statement is not trivial [GO94]). Thereby, the simulator is allowed to simulate the CRS and thus is able to compute trapdoors associated to it. The knowledge of such trapdoors enhances the possibilities of S to successfully simulating proofs.

Syntactically, a NIZK proof system consists of three probabilistic polynomial time algorithms: a CRS generation algorithm K, a prover P, and a verifier V. The CRS generation algorithm takes a group description gk as input and produces a CRS σ (which we assume includes gk). The prover takes as input (σ, x, w) and produces a proof π. The verifier takes as input (σ, x, π) and outputs 1 if the proof is acceptable and 0 if rejecting the proof.

In this work we will consider two particular cases of NIZK: *composable* NIZK [GS08] and *quasi-adaptive* NIZK [JR13]. Both deal with the case of CRS dependent languages, say the language is parameterized by some values which are (randomly) sampled within the CRS. For example, the CRS might contain the group key gk defining a bilinear group and the language might be some set of satisfiable equations over that group. Quasi-adaptive NIZK goes further and the language might also depend on group constants defined in the CRS.

2.5.1 Composable Non-Interactive Zero-Knowledge Proofs

The following definitions are from Groth and Sahai [GS12].

Definition 2.18 (Group dependent languages) *Let $\mathcal{R}$ be an efficiently computable ternary relation. For triplets $(gk, x, w) \in \mathcal{R}$ we call gk the group key, x the statement, and w the witness. Given some gk, we let $\mathcal{L}$ be the language consisting of statements x that have a witness w so $(gk, x, w) \in \mathcal{R}$. For a relation that ignores gk this is, of course, the standard definition of an NP-language. We will be more interested in the case where gk describes a bilinear group, though.*

Definition 2.19 (Composable NIZK proof system) *We say that a non-interactive proof system* $(\mathsf{K}, \mathsf{P}, \mathsf{V})$ *is a composable NIZK proof system with respect to* Gen_a *if*

Perfect Completeness: *For any x, w*

$$\Pr\left[\begin{array}{l} gk \leftarrow \mathsf{Gen}_a(1^\lambda); \sigma \leftarrow \mathsf{K}(gk); \pi \leftarrow \mathsf{P}(\sigma, x, w) : \\ V(\sigma, x, \pi) = 1 \textit{ if } (gk, x, w) \in \mathcal{R} \end{array}\right] = 1.$$

Perfect Soundness: *For any adversary* A

$$\Pr\left[\begin{array}{l} gk \leftarrow \mathsf{Gen}_a(1^\lambda); \sigma \leftarrow \mathsf{K}(gk); (x, \pi) \leftarrow \mathsf{A}(gk, \sigma) : \\ V(\sigma, x, \pi) = 0 \textit{ if } x \notin \mathcal{L} \end{array}\right] = 1.$$

Computational Zero-Knowledge: *There exist efficient algorithms* $\mathsf{S}_1, \mathsf{S}_2$ *such that for any adversaries* $\mathsf{A}_1, \mathsf{A}_2$

$$\Pr\left[gk \leftarrow \mathsf{Gen}_a(1^\lambda); \sigma \leftarrow \mathsf{K}(gk) : \mathsf{A}_1(gk, \sigma) = 1\right] \approx$$
$$\Pr\left[gk \leftarrow \mathsf{Gen}_a(1^\lambda); (\sigma, \tau) \leftarrow \mathsf{S}_1(gk) : \mathsf{A}_1(gk, \sigma) = 1\right]$$

and

$$\Pr\left[\begin{array}{l} gk \leftarrow \mathsf{Gen}_a(1^\lambda); (\sigma, \tau) \leftarrow \mathsf{S}_1(gk); (x, w) \leftarrow \mathsf{A}_2(gk, \sigma, \tau); \\ \pi \leftarrow \mathsf{P}(\sigma, x, w) : \mathsf{A}_2(\pi) = 1 \textit{ if } (gk, x, w) \in \mathcal{R} \end{array}\right] =$$
$$\Pr\left[\begin{array}{l} gk \leftarrow \mathsf{Gen}_a(1^\lambda); (\sigma, \tau) \leftarrow \mathsf{S}_1(gk); (x, w) \leftarrow \mathsf{A}_2(gk, \sigma, \tau); \\ \pi \leftarrow \mathsf{S}_2(\sigma, \tau, x) : \mathsf{A}_2(\pi) = 1 \textit{ if } (gk, x, w) \in \mathcal{R} \end{array}\right].$$

Definition 2.20 (Composable NIWI proof system) *We say that a non-interactive proof system* $(\mathsf{K}, \mathsf{P}, \mathsf{V})$ *is a composable NIWI proof system with respect to* Gen_a *if it have perfect completeness and soundness as defined above and also*

Computational Witness-Indistinguishability: *There exists and efficient algorithm* S_1 *such that for any adversaries* $\mathsf{A}_1, \mathsf{A}_2$

$$\Pr\left[gk \leftarrow \mathsf{Gen}_a(1^\lambda); \sigma \leftarrow \mathsf{K}(gk) : \mathsf{A}_1(gk, \sigma) = 1\right] \approx$$
$$\Pr\left[gk \leftarrow \mathsf{Gen}_a(1^\lambda); (\sigma, \tau) \leftarrow \mathsf{S}_1(gk) : \mathsf{A}_1(gk, \sigma) = 1\right]$$

and

$$\Pr\left[\begin{array}{l} gk \leftarrow \mathsf{Gen}_a(1^\lambda); (\sigma, \tau) \leftarrow \mathsf{S}_1(gk); (x, w, w') \leftarrow \mathsf{A}_2(gk, \sigma, \tau); \\ \pi \leftarrow \mathsf{P}(\sigma, x, w) : \mathsf{A}_2(\pi) = 1 \textit{ if } (gk, x, w), (gk, x, w') \in \mathcal{R} \end{array}\right] \approx$$
$$\Pr\left[\begin{array}{l} gk \leftarrow \mathsf{Gen}_a(1^\lambda); (\sigma, \tau) \leftarrow \mathsf{S}_1(gk); (x, w, w') \leftarrow \mathsf{A}_2(gk, \sigma, \tau); \\ \pi \leftarrow \mathsf{P}(\sigma, x, w') : \mathsf{A}_2(\pi) = 1 \textit{ if } (gk, x, w), (gk, x, w') \in \mathcal{R} \end{array}\right].$$

2.5.2 Quasi-Adaptive Non-Interactive Zero-Knowledge Proofs

A quasi-adaptive NIZK proof system [JR13] enables to prove membership in a language defined by a relation $\mathcal{R}_\rho$, which in turn is completely determined by some parameter ρ sampled from a distribution $\mathcal{D}_{gk}$.

Definition 2.21 (Witness Samplable Distribution) *We say that* $\mathcal{D}_{gk}$ *is* witness samplable *if there exists an efficient algorithm that samples* (ρ, ω) *from a distribution* $\mathcal{D}_{gk}^{\mathsf{par}}$ *such that* ρ *is distributed according to* $\mathcal{D}_{gk}$*, and membership of* ρ *in the parameter language* $\mathcal{L}_{\mathsf{par}}$ *can be efficiently verified with* ω*.*

In a typical scenario, ρ is a matrix of group elements and ω is the matrix of ρ's discrete logarithms.

While the common reference string can be set based on ρ, the zero-knowledge simulator is required to be a single probabilistic polynomial time algorithm that works for the whole collection of relations $\mathcal{R}_{gk} := \{\mathcal{R}_\rho\}_{\rho \in \sup(\mathcal{D}_{gk})}$.

Definition 2.22 (Quasi-Adaptive NIZK (QA-NIZK) proof system) *A non-interactive proof system* $(\mathsf{K}, \mathsf{P}, \mathsf{V})$ *is called a QA-NIZK proof system with respect to* Gen_a *for witness-relations* $\mathcal{R}_{gk} = \{\mathcal{R}_\rho\}_{\rho \in \sup(\mathcal{D}_{gk})}$*, with parameters sampled from a distribution* $\mathcal{D}_{gk}$ *over associated parameter language* $\mathcal{L}_{\mathsf{par}}$*, if there exists a probabilistic polynomial time simulator* $(\mathsf{S}_1, \mathsf{S}_2)$*, such that for all non-uniform PPT adversaries* A_1*,* A_2*,* A_3 *we have:*

Quasi-Adaptive Completeness:

$$\Pr\begin{bmatrix} gk \leftarrow \mathsf{Gen}_a(1^\lambda); \rho \leftarrow \mathcal{D}_{gk}; \psi \leftarrow \mathsf{K}(gk,\rho); (x,w) \leftarrow \mathsf{A}_1(gk,\psi); \\ \pi \leftarrow \mathsf{P}(\psi,x,w) : \mathsf{V}(\psi,x,\pi) = 1 \textit{ if } \mathcal{R}_\rho(x,w) \end{bmatrix} = 1;$$

Computational Quasi-Adaptive Soundness:

$$\Pr\begin{bmatrix} gk \leftarrow \mathsf{Gen}_a(1^\lambda); \rho \leftarrow \mathcal{D}_{gk}; \psi \leftarrow \mathsf{K}(gk,\rho); \\ (x,\pi) \leftarrow \mathsf{A}_2(gk,\psi) : \mathsf{V}(\psi,x,\pi) = 1 \textit{ and } \neg(\exists w : \mathcal{R}_\rho(x,w)) \end{bmatrix} \approx 0; \textit{ and}$$

Perfect Quasi-Adaptive Zero-Knowledge:

$$\Pr[gk \leftarrow \mathsf{Gen}_a(1^\lambda); \rho \leftarrow \mathcal{D}_{gk}; \psi \leftarrow \mathsf{K}(gk,\rho) : \mathsf{A}_3^{\mathsf{P}(\psi,\cdot,\cdot)}(gk,\psi) = 1] =$$
$$\Pr[gk \leftarrow \mathsf{Gen}_a(1^\lambda); \rho \leftarrow \mathcal{D}_{gk}; (\psi,\tau) \leftarrow \mathsf{S}_1(gk,\rho) : \mathsf{A}_3^{\mathsf{S}(\psi,\tau,\cdot,\cdot)}(gk,\psi) = 1]$$

where

- $\mathsf{P}(\psi,\cdot,\cdot)$ *emulates the actual prover. It takes input* (x,w) *and outputs a proof* π *if* $(x,w) \in \mathcal{R}_\rho$. *Otherwise, it outputs* $\perp$.
- $\mathsf{S}(\psi,\tau,\cdot,\cdot)$ *is an oracle that takes input* (x,w). *It outputs a simulated proof* $\mathsf{S}_2(\psi,\tau,x)$ *if* $(x,w) \in \mathcal{R}_\rho$ *and* $\perp$ *if* $(x,w) \notin \mathcal{R}_\rho$.

Note that ψ *is the CRS in the above definitions. We assume that* ψ *contains an encoding of* ρ, *which is thus available to* V.

For witness samplable distributions, we and independently Libert et al., define a stronger notion of soundness where the adversary has also access to a witness of the parameter ρ [GHR15b, LPJY15a].

Computational Quasi-Adaptive Strong Soundness:

$$\Pr\begin{bmatrix} gk \leftarrow \mathsf{Gen}_a(1^\lambda); (\rho,\omega) \leftarrow \mathcal{D}_{gk}^{\mathsf{par}}; \psi \leftarrow \mathsf{K}(gk,\rho); \\ (x,\pi) \leftarrow \mathsf{A}_2(gk,\omega,\psi) : \mathsf{V}(\psi,x,\pi) = 1 \text{ and } \neg(\exists w : \mathcal{R}_\rho(x,w)) \end{bmatrix} \approx 0.$$

2.6 Groth-Sahai Proofs

The GS proof system allows to prove satisfiability of a set of quadratic equations in a bilinear group. In general, the proof is witness-indistinguishable but for most equations it is also (or can be made) zero-knowledge.

The admissible equation types must be in the following form:

$$\sum_{j=1}^{m_y} f(\alpha_j, \mathsf{y}_j) + \sum_{i=1}^{m_x} f(\mathsf{x}_i, \beta_i) + \sum_{i=1}^{m_x}\sum_{j=1}^{m_y} f(\mathsf{x}_i, \gamma_{i,j}\mathsf{y}_j) = t, \tag{2.1}$$

where A_1, A_2, A_T are $\mathbb{Z}_q$-vector spaces equipped with some bilinear map $f : A_1 \times A_2 \to A_T$, $\boldsymbol{\alpha} \in A_1^{m_y}$, $\boldsymbol{\beta} \in A_2^{m_x}$, $\boldsymbol{\Gamma} = (\gamma_{i,j}) \in \mathbb{Z}_q^{m_x \times m_y}$, $t \in A_T$. The vector spaces and the map f can be defined in different ways as:

(a) in pairing-product equations (PPEs), $A_1 = \mathbb{G}_1$, $A_2 = \mathbb{G}_2$, $A_T = \mathbb{G}_T$, $f([x]_1,[y]_2) = [x]_1[y]_2 \in \mathbb{G}_T$,

(b1) in multi-scalar multiplication equations in $\mathbb{G}_1$ (MMEs), $A_1 = \mathbb{G}_1$, $A_2 = \mathbb{Z}_q$, $A_T = \mathbb{G}_1$, $f([x]_1, y) = y[x]_1 \in \mathbb{G}_1$, (b2) MMEs in $\mathbb{G}_2$ (MMEs), $A_1 = \mathbb{Z}_q$, $A_2 = \mathbb{G}_2$, $A_T = \mathbb{G}_2$, $f(x, [y]_2) = x[y]_2 \in \mathbb{G}_2$, and

(c) in quadratic equations in $\mathbb{Z}_q$ (QEs), $A_1 = A_2 = A_T = \mathbb{Z}_q$, $f(x, y) = xy \in \mathbb{Z}_q$.

An equation is linear if $\mathbf{\Gamma} = \mathbf{0}$, it is *two-sided linear* if both $\boldsymbol{\alpha} \neq \mathbf{0}$ and $\boldsymbol{\beta} \neq \mathbf{0}$, and *one-sided* otherwise.

When $t = f(t_1, 1)$ or $t = f(1, t_2)$, for some efficiently computable $t_1 \in A_1$ or $t_2 \in A_2$, we say that the equation allows simulation (see [GS12, Section 11]) and the proof is zero-knowledge (rather than just witness-indistinguishable). Note that this is always the case for equations other than PPEs.

2.6.1 Commit-and-Prove Schemes

The GS proof system works as a commit-and-prove scheme: first the prover commits to all the variables in an equation with the Groth-Sahai commitment scheme, defined in the next section, and then it "proves" that the committed values satisfy the equation. The commitment to an element in the vector space A_i lives in another vector space B_i of larger dimension where interesting decisional assumptions exist. To prove that the equation is satisfied the verifier checks some equations in these larger fields.

2.6.2 Groth-Sahai Commitments

Definition 2.23 *The Groth-Sahai commitment scheme in the group $\mathbb{G}_\gamma$, $\gamma \in \{1, 2\}$, is specified by the following three algorithms* ($\mathsf{GS.K}, \mathsf{GS.Com}, \mathsf{GS.Vrfy}$) *such that:*

- $\mathsf{GS.K}(gk, \mathcal{D}_{2,2})$ *is a randomized algorithm, which on input the group key gk and the description of some matrix distribution $\mathcal{D}_{2,2}$, outputs a commitment key $ck := [\mathbf{U}]_\gamma = [(\mathbf{u}_1|\mathbf{u}_2)]_\gamma \in \mathbb{G}_\gamma^{2\times 2}$, where $\mathbf{U} \leftarrow \mathcal{D}_{2,2}$.*
- $\mathsf{GS.Com}_{ck}(\mathsf{m}; r)$ *is a randomized algorithm which, on input a commitment key $ck = [\mathbf{U}]_\gamma$, and a message m in the message space $\mathcal{M}_{ck} = A_\gamma$, it proceeds as follows. If $\mathsf{m} = m \in \mathbb{Z}_q$, it samples $r \leftarrow \mathbb{Z}_q$ and outputs a commitment $[\mathbf{c}]_\gamma := m[\mathbf{e}_2 + \mathbf{u}_1]_\gamma + r[\mathbf{u}_2]_\gamma$ in the commitment space $\mathcal{C}_{ck} = \mathbb{G}_\gamma^2$ and an opening $Op = r$. If $\mathsf{m} = [m]_\gamma \in \mathbb{G}_\gamma$, it samples $\mathbf{r} \leftarrow \mathbb{Z}_q^2$ and outputs a commitment $[\mathbf{c}]_\gamma := [m]_\gamma \mathbf{e}_2 + [\mathbf{U}]_\gamma \mathbf{r}$ in the commitment space $\mathcal{C}_{ck} = \mathbb{G}_\gamma^2$ and an opening $Op = \mathbf{r}$.*
- $\mathsf{GS.Vrfy}_{ck}([\mathbf{c}]_\gamma, Op)$ *is a deterministic algorithm which, on input the commitment key $ck = [\mathbf{U}]_\gamma$, a commitment $[\mathbf{c}]_\gamma$, a message $m \in \mathcal{M}_{ck}$ and an opening Op, outputs* 1 *if $[\mathbf{c}]_\gamma = \mathsf{GS.Com}_{ck}(m; Op)$ and* 0 *otherwise.*

We will instantiate this commitment scheme with two different matrix distributions which give rise to two different commitment keys: the *perfectly binding* and the *perfectly hiding* commitment keys. The matrix distribution for perfectly binding commitment keys is defined as

$$\mathcal{B} : \mathbf{U} = (\mathbf{u}_1|\mathbf{u}_2), \text{ where } \mathbf{u}_2 \leftarrow \mathcal{L}_1 \text{ and } \mathbf{u}_1 := \mu \mathbf{u}_2, \mu \leftarrow \mathbb{Z}_q,$$

and the matrix distribution for perfectly hiding commitment keys is defined as

$$\mathcal{H} : \mathbf{U} = (\mathbf{u}_1|\mathbf{u}_2), \text{ where } \mathbf{u}_2 \leftarrow \mathcal{L}_1 \text{ and } \mathbf{u}_1 := \mu \mathbf{u}_2 - \mathbf{e}_2, \mu \leftarrow \mathbb{Z}_q.$$

Theorem 2.24 ([GS12]) *If $ck \leftarrow \mathsf{K}(gk, \mathcal{B})$ (resp. $ck \leftarrow \mathsf{K}(gk, \mathcal{H})$), where $gk \leftarrow \mathsf{Gen}_a(1^\lambda)$, the Groth-Sahai commitment scheme is perfectly binding (resp. computationally binding if the DL assumption relative to Gen_a holds) and computationally hiding if the SXDH assumption relative to Gen_a holds (resp. perfectly hiding).*

2.6.3 The Scheme

Next, we give a description of the Groth-Sahai proof system in the SXDH instantiation.

$\mathsf{K}(gk)$**:** On input the group key gk pick $\mathbf{U}, \mathbf{V} \leftarrow \mathcal{B}$ and define $ck_1 := [\mathbf{U}]_1$ and $ck_2 := [\mathbf{V}]_2$. The common reference string is: $\mathsf{crs}_{\mathsf{GS}} := (gk, [\mathbf{u}_1]_1, [\mathbf{u}_2]_1, [\mathbf{v}_1]_2, [\mathbf{v}_2]_2)$ and is known as the *perfectly binding CRS*. The CRS defines some associated maps:

$$\begin{array}{lll}
\iota_1 : \mathbb{G}_1 \cup \mathbb{Z}_q \to \mathbb{G}_1^2, & \iota_1([x]_1) := ([x]_1, [0]_1)^\top, & \iota_1(x) := x[\mathbf{u}_1]_1. \\
\iota_2 : \mathbb{G}_2 \cup \mathbb{Z}_q \to \mathbb{G}_2^2, & \iota_2([y]_2) := ([y]_2, [0]_2)^\top, & \iota_2(y) := y[\mathbf{v}_1]_2. \\
\iota_T : \begin{array}{c}\mathbb{Z}_q \cup \mathbb{G}_1 \cup \\ \mathbb{G}_2 \cup \mathbb{G}_T\end{array} \to \mathbb{G}_T^{2\times 2}, & \iota_T(t) := \begin{pmatrix} t & 0 \\ 0 & 0 \end{pmatrix}, & \iota_T(x) := \iota_1(x)\iota_2(1)^\top, \\
 & \iota_T([x]_1) := \iota_1([x]_1)\iota_2(1)^\top, & \iota_T([y]_2) := \iota_1(1)\iota_2([y]_2)^\top.
\end{array}$$

The maps $\iota_X X \in \{1, 2\}$ can be naturally extended to column vectors of arbitrary length, and we write $\iota_X(\boldsymbol{\delta}^\top)$ for $(\iota_X(\delta_1)| \dots |\iota_X(\delta_r))$.

$\mathsf{P}(\mathsf{crs}_{\mathsf{GS}}, \mathsf{eq}, (\mathsf{x}_1, \dots, \mathsf{x}_{m_x}), (\mathsf{y}_1, \dots, \mathsf{y}_{m_y}))$**:** Given some equation eq of the form 2.1 and solutions to the equation $\mathsf{x}_1, \dots, \mathsf{x}_{m_x}$ and $\mathsf{y}_1, \dots, \mathsf{y}_{m_y}$, the prover proceeds as follows:

- Commit to all $\mathsf{x}_i \in A_1$ computing $([\mathbf{c}_i]_1, \mathbf{r}_i) \leftarrow \mathsf{GS.Com}_{ck_1}(\mathsf{x}_i)$ and commit to all $\mathsf{y}_i \in A_2$ computing $([\mathbf{d}_i]_2, \mathbf{s}_i) \leftarrow \mathsf{GS.Com}_{ck_2}(\mathsf{y}_i)$.

- Let $\mathbf{R} := (\mathbf{r}_1| \dots |\mathbf{r}_{m_x})$ and $\mathbf{S} := (\mathbf{s}_1| \dots |\mathbf{s}_{m_y})$. Compute

$$\begin{array}{rcl}
[\mathbf{\Pi}]_2 & := & \iota_2(\boldsymbol{\beta}^\top)\mathbf{R}^\top + \iota_2(\mathbf{y}^\top)\mathbf{\Gamma}^\top\mathbf{R}^\top + [\mathbf{V}]_2\mathbf{S}\mathbf{\Gamma}^\top\mathbf{R}^\top - [\mathbf{V}]_2\mathbf{T}^\top, \\
[\mathbf{\Theta}]_1 & := & \iota_1(\boldsymbol{\alpha}^\top)\mathbf{S}^\top + \iota_1(\mathbf{x}^\top)\mathbf{\Gamma}\mathbf{S}^\top + [\mathbf{U}]_1\mathbf{T}.
\end{array}$$

$\mathsf{V}(\mathsf{crs}_{\mathsf{GS}}, \mathsf{eq}, \{[\mathbf{c}_i]_1 : i \in [m_x]\}, \{[\mathbf{d}_i]_2 : i \in [m_y]\}, [\mathbf{\Theta}]_1, [\mathbf{\Pi}]_2)$**:** Check if

$$\sum_{i \in m_x} [\mathbf{c}_i]_1 \iota_2(\beta_i)^\top + \sum_{j \in m_y} \iota_1(\alpha_j)[\mathbf{d}_j]_2^\top + \sum_{i \in m_x} \sum_{j \in m_y} \gamma_{i,j}[\mathbf{c}_i]_1[\mathbf{d}_j]_2^\top = \iota_T(t) + [\mathbf{\Theta}]_1[\mathbf{V}]_2^\top + [\mathbf{U}]_1[\mathbf{\Pi}]_2^\top.$$

$\mathsf{S}_1(gk)$**:** On input the group key gk pick $\mathbf{U}, \mathbf{V} \leftarrow \mathcal{H}$ and define $ck_1 := [\mathbf{U}]_1$ and $ck_2 := [\mathbf{V}]_2$. The common reference string is: $\mathsf{crs}_{\mathsf{GS}} := (gk, [\mathbf{u}_1]_1, [\mathbf{u}_2]_1, [\mathbf{v}_1]_2, [\mathbf{v}_2]_2)$ and is known as the *perfectly hiding CRS*. This algorithm also outputs the trapdoor $\tau := (\mathbf{U}, \mathbf{V})$.

$\mathsf{S}_2(\mathsf{crs}_{\mathsf{GS}}, \mathsf{eq}, \tau)$**:** If eq allows simulation, it defines the new equation

$$\mathsf{eq}' := \sum_{j=1}^{m_y} f(\alpha_j, \mathsf{y}_j) + \sum_{i=1}^{m_x} f(\mathsf{x}_i, \beta_i) - f(\mathsf{x}', t) + \sum_{i=1}^{m_x} \sum_{j=1}^{m_y} f(\mathsf{x}_i, \gamma_{i,j}\mathsf{y}_j) = 0, \tag{2.2}$$

and runs the GS prover for equation eq' for solutions $\mathsf{x}_1 = \mathsf{x}_2 = \dots = \mathsf{x}_{m_x} = \mathsf{y}_1 = \dots = \mathsf{y}_{m_y} = 0$ and $\mathsf{x}' = 1$. The simulated proof is $([\mathbf{\Theta}]_1, [\mathbf{\Pi}]_2)$, the proof of the GS prover for the modified equation.

The reference string $\mathsf{crs}_{\mathsf{GS}}$ chosen by algorithm K defines perfectly binding commitments and the proof system has perfect soundness. Furthermore, there exists some extraction trapdoor which allows to compute a function of the witness (this is the perfect *F-Knowledge* property [EG14]). More specifically, the extraction trapdoor allows to compute maps $p_1 : \mathbb{G}_1^2 \to \mathbb{G}_1$, $p_2 : \mathbb{G}_2^2 \to \mathbb{G}_2$, and $p_T : \mathbb{G}_T^{2\times 2} \to \mathbb{G}_T$, such that:

```
$\mathsf{K}(gk, [\mathbf{M}]_1, n)$      $(\mathsf{S}_1(gk, [\mathbf{M}]_1, n))$
    $\mathbf{A} \leftarrow \widetilde{\mathcal{D}_k}, \mathbf{\Delta} \leftarrow \mathbb{Z}_q^{\tilde{k}\times n}$
    $[\mathbf{A}_\Delta]_2 := \mathbf{\Delta}^\top[\mathbf{A}]_2, [\mathbf{M}_\Delta]_1 := \mathbf{\Delta}[\mathbf{M}]_1$
    Return $\mathsf{crs} := ([\mathbf{M}_\Delta]_1, [\mathbf{A}_\Delta]_2, [\mathbf{A}]_2)$
    $(\tau_{sim} := \mathbf{\Delta})$

$\mathsf{P}(\mathsf{crs}, [\mathbf{x}]_1, \mathbf{w})$ \\$[\mathbf{x}]_1 = [\mathbf{M}]_1\mathbf{w}$
    Return $[\boldsymbol{\sigma}]_1 := [\mathbf{M}_\Delta]_1\mathbf{w}$.

$\mathsf{S}_2(\mathsf{crs}, [\mathbf{x}]_1, \tau_{sim})$
    Return $[\boldsymbol{\sigma}]_1 := \mathbf{\Delta}[\mathbf{x}]_1$

$\mathsf{V}(\mathsf{crs}, [\mathbf{x}]_1, [\boldsymbol{\sigma}]_1)$
    Return $([\mathbf{x}]_1^\top[\mathbf{A}_\Delta]_2 = [\boldsymbol{\sigma}]_1^\top[\mathbf{A}]_2)$
```

Figure 2.1: The figure describes $\Psi(\mathcal{D}_k)$ when $\widetilde{\mathcal{D}_k} = \mathcal{D}_k$ and $\tilde{k} = k+1$ and $\Psi(\overline{\mathcal{D}}_k)$ when $\widetilde{\mathcal{D}_k} = \overline{\mathcal{D}}_k$ and $\tilde{k} = k$. Both are QA-NIZK arguments for $\mathcal{L}_{[\mathbf{M}]_1}$. $\Psi(\mathcal{D}_k)$ is the construction of [KW15, Section 3.1], which is a generalization of Libert *et al*'s QA-NIZK [LPJY14] to any $\mathcal{D}_k$-KerMDH$_{\mathbb{G}_2}$ assumption. $\Psi(\overline{\mathcal{D}}_k)$ is the construction of [KW15, Section 3.2.].

(a) for each $X \in \{1, 2, T\}$, $p_X \circ \iota_X$ is the identity map,

(b) for all $\mathsf{x} \in A_1, \mathsf{y} \in A_2$, $\iota_1(\mathsf{x})\iota_2(\mathsf{y})^\top = \iota_T(f(\mathsf{x}, \mathsf{y}))$ and for all $[\mathbf{x}]_1 \in \mathbb{G}_1^2, [\mathbf{y}]_2 \in \mathbb{G}_2^2$, $f(p_1([\mathbf{x}]_1), p_2([\mathbf{y}]_2)) = p_T([\mathbf{x}]_1[\mathbf{y}]_2^\top)$,

(c) for each $i \in [2]$, $p_1([\mathbf{u}_i]_1) = 0$ and $p_2([\mathbf{v}_i]_2) = 0$.

Theorem 2.25 ([GS08]) *If* eq *allows simulation then the Groth-Sahai proof system is a composable zero-knowledge proof system with perfect completeness, perfect soundness, and computational zero-knowledge based on the SXDH assumption. Otherwise, is a composable witness-indistinguishable proof system with perfect completeness, perfect soundness, and computational witness indistinguishability based the SXDH assumption.*

2.7 QA-NIZK Arguments of Membership in Subspaces of $\mathbb{G}_1$ or $\mathbb{G}_2$

In this section we recall the two constructions of QA-NIZK arguments of membership in linear spaces given by Kiltz and Wee [KW15], for the language:

$$\mathcal{L}_{[\mathbf{M}]_1} := \{[\mathbf{x}]_1 \in \mathbb{G}_1^n : \exists \mathbf{w} \in \mathbb{Z}_q^t,\ [\mathbf{x}]_1 = [\mathbf{M}]_1\mathbf{w}\}.$$

The proof system is described in Fig. 2.1.

Theorem 2.26 (Theorem 1 of [KW15]) *If $\widetilde{\mathcal{D}_k} = \mathcal{D}_k$ and $\tilde{k} = k+1$, Fig. 2.1 describes a QA-NIZK proof system with perfect completeness, computational adaptive soundness based on the $\mathcal{D}_k$-*KerMDH$_{\mathbb{G}_2}$ *assumption, perfect zero-knowledge, and proof size $k+1$.*

Theorem 2.27 (Theorem 2 of [KW15]) *If $\widetilde{\mathcal{D}_k} = \overline{\mathcal{D}}_k$ and $\tilde{k} = k$, and $\mathcal{D}_{gk}$ is a witness samplable distribution, Fig. 2.1 describes a QA-NIZK proof system with perfect completeness, computational adaptive soundness based on the $\mathcal{D}_k$-*KerMDH$_{\mathbb{G}_2}$ *assumption, perfect zero-knowledge, and proof size k.*

Chapter 3

QA-NIZK Arguments of Membership in Subspaces of $\mathbb{G}_1 \times \mathbb{G}_2$

In this chapter we construct three QA-NIZK constant-size arguments of membership in different subspaces of $\mathbb{G}_1^m \times \mathbb{G}_2^n$. Their soundness relies on the split kernel assumption. We then show that similar techniques allow to give a constant-size proof of satisfiability of many linear equations (aggregation of Groth-Sahai proofs). Finally, we show that the same techniques also allow to build *structure preserving linearly homomorphic signatures* where messages can be elements of $\mathbb{G}_1^m \times \mathbb{G}_2^n$, an extension of the signature scheme introduced by Libert et al. [LPJY13].

3.1 Introduction

A recent line of work [JR13, JR14, KW15, LPJY14] has succeeded in constructing constant-size arguments for very specific statements, namely, for membership in subspaces of $\mathbb{G}_1^m$, where $\mathbb{G}_1$ is some group equipped with a bilinear map where the discrete logarithm is hard. The soundness of the schemes is based on standard, falsifiable assumptions and the proof size is independent of both m and the witness size. These improvements are in a *quasi-adaptive* model (QA-NIZK, [JR13]). This means that the common reference string of these proof systems is specialized to the linear space where one wants to prove membership.

Interestingly, Jutla and Roy [JR14] also showed that their techniques to construct constant-size NIZK in linear spaces can be used to aggregate the GS proofs of m equations in n variables, that is, the total proof size can be reduced to $\Theta(n)$. Aggregation is also quasi-adaptive, which means that the common reference string depends on the set of equations one wants to aggregate. Further, it is only possible if the equations meet some restrictions. The first one is that only linear equations can be aggregated. The second one is that, in asymmetric bilinear groups, the equations must be one-sided linear, i.e. linear equations which have variables in only one of the $\mathbb{Z}_q$ modules $\mathbb{G}_1, \mathbb{G}_2$, or $\mathbb{Z}_q$.[1]

Thus, it is worth to investigate if we can develop new techniques to aggregate other types of equations (in particular, two-sided linear equations) in asymmetric bilinear groups. The latter (Type III bilinear groups, according to the classification of Glabraith et al. are the most attractive from the perspective of a performance and security trade off [GPS08]),

[1] Jutla and Roy show how to aggregate two-sided linear equations in symmetric bilinear groups. The asymmetric case is not discussed, yet for one-sided linear equations it can be easily derived from their results. This is not the case for two-sided ones, see Section 3.5.2.

specially since the recent attacks on discrete logarithms in finite fields by Joux [Jou14] and subsequent improvements. Considerable research effort (e.g. [AGOT14, Fre10]) has been put into translating pairing-based cryptosystems from a setting with more structure in which design is simpler (e.g. composite-order or symmetric bilinear groups) to a more efficient setting (e.g. prime order or asymmetric bilinear groups). In this line, we aim not only at obtaining new results in the asymmetric setting but also to translate known results and develop new tools specifically designed for it which might be of independent interest.

3.2 Argument of Membership in Subspace Concatenation

Figure 3.1 describes a QA-NIZK argument of membership in the language

$$\mathcal{L}_{[\mathbf{M}]_1,[\mathbf{N}]_2} := \{([\mathbf{x}]_1,[\mathbf{y}]_2) : \exists \mathbf{w} \in \mathbb{Z}_q^t,\ \mathbf{x} = \mathbf{M}\mathbf{w}, \mathbf{y} = \mathbf{N}\mathbf{w}\} \subseteq \mathbb{G}_1^m \times \mathbb{G}_2^n,$$

where $([\mathbf{M}]_1,[\mathbf{N}]_2) \leftarrow \mathcal{D}_{gk}$ for some matrix distribution $\mathcal{D}_{gk}$.

We refer to this as the *concatenation language*, because if we define $\mathbf{P}$ as the concatenation of $[\mathbf{M}]_1, [\mathbf{N}]_2$, that is $\mathbf{P} := \begin{pmatrix} [\mathbf{M}]_1 \\ [\mathbf{N}]_2 \end{pmatrix}$, then $([\mathbf{x}]_1,[\mathbf{y}]_2) \in \mathcal{L}_{[\mathbf{M}]_1,[\mathbf{N}]_2}$ iff $\begin{pmatrix} [\mathbf{x}]_1 \\ [\mathbf{y}]_2 \end{pmatrix}$ is in the span of $\mathbf{P}$.

Soundness Intuition. If we ignore for a moment that $\mathbb{G}_1, \mathbb{G}_2$ are different groups, $\Psi_{\mathsf{spl}}(\mathcal{D}_k)$ (resp. $\Psi_{\mathsf{spl}}(\overline{\mathcal{D}}_k)$) is almost identical to $\Psi(\mathcal{D}_k)$ (resp. to $\Psi(\overline{\mathcal{D}}_k)$), as defined in Section 2.7, for the language $\mathcal{L}_{[\mathbf{P}]_1}$, and $\boldsymbol{\Delta} := (\boldsymbol{\Lambda}|\boldsymbol{\Xi})$, where $\boldsymbol{\Lambda} \in \mathbb{Z}_q^{\tilde{k}\times m}, \boldsymbol{\Xi} \in \mathbb{Z}_q^{\tilde{k}\times n}$. Further, the information that an unbounded adversary can extract from the CRS about $\boldsymbol{\Delta}$ is:

1. $\left\{\mathbf{P}_\Delta = \boldsymbol{\Lambda}\mathbf{M} + \boldsymbol{\Xi}\mathbf{N}, \mathbf{A}_\Delta = \boldsymbol{\Delta}^\top\mathbf{A} = \begin{pmatrix} \boldsymbol{\Lambda}^\top\mathbf{A} \\ \boldsymbol{\Xi}^\top\mathbf{A} \end{pmatrix}\right\}$ from $\mathsf{crs}_{\Psi(\mathcal{D}_k)}$,
2. $\left\{\mathbf{M}_\Lambda = \boldsymbol{\Lambda}\mathbf{M} + \mathbf{Z}, \mathbf{N}_\Xi = \boldsymbol{\Xi}\mathbf{N} - \mathbf{Z}, \begin{pmatrix} \mathbf{A}_\Lambda \\ \mathbf{A}_\Xi \end{pmatrix} = \begin{pmatrix} \boldsymbol{\Lambda}^\top\mathbf{A} \\ \boldsymbol{\Xi}^\top\mathbf{A} \end{pmatrix}\right\}$ from $\mathsf{crs}_{\Psi_{\mathsf{spl}}(\mathcal{D}_k)}$.

Given that the matrix $\mathbf{Z}$ is uniformly random, $\mathsf{crs}_{\Psi(\mathcal{D}_k)}$ and $\mathsf{crs}_{\Psi_{\mathsf{spl}}(\mathcal{D}_k)}$ reveal the same information about $\boldsymbol{\Delta}$ to an unbounded adversary. Therefore, as the proof of soundness is essentially based on the fact that parts of $\boldsymbol{\Delta}$ are information theoretically hidden to the adversary, the original proof of Kiltz and Wee can be easily adapted for the new arguments.

Theorem 3.1 *If $\widetilde{\mathcal{D}_k} = \mathcal{D}_k$ and $\tilde{k} = k + 1$, Fig. 3.1 describes a QA-NIZK proof system with perfect completeness, computational adaptive soundness based on the $\mathcal{D}_k$-*SKerMDH *assumption, and perfect zero-knowledge.*

Proof Through this proof we define $\mathbf{P} := \begin{pmatrix} \mathbf{M} \\ \mathbf{N} \end{pmatrix}$, $\boldsymbol{\Delta} := \begin{pmatrix} \boldsymbol{\Lambda} & \boldsymbol{\Xi} \end{pmatrix}$ and $\tilde{m} := m + n$.

(Completeness.) Follows from the fact that

$$\begin{aligned} \mathbf{x}^\top\mathbf{A}_\Lambda + \mathbf{y}^\top\mathbf{A}_\Xi &= (\mathbf{P}\mathbf{w})^\top \boldsymbol{\Delta}^\top\mathbf{A} \\ &= \left(\begin{pmatrix} \boldsymbol{\Lambda} & \boldsymbol{\Xi} \end{pmatrix} \begin{pmatrix} \mathbf{M} \\ \mathbf{N} \end{pmatrix} \mathbf{w}\right)^\top \mathbf{A} \\ &= \boldsymbol{\rho}^\top\mathbf{A} + \boldsymbol{\sigma}^\top\mathbf{A}. \end{aligned}$$

```
$\underline{\mathsf{K}(gk, [\mathbf{M}]_1, [\mathbf{N}]_2, m, n) \quad (\mathsf{S}_1(gk, [\mathbf{M}]_1, [\mathbf{N}]_1, m, n))}$
$\mathbf{A} \leftarrow \widetilde{\mathcal{D}_k}, \boldsymbol{\Lambda} \leftarrow \mathbb{Z}_q^{\tilde{k}\times m}, \boldsymbol{\Xi} \leftarrow \mathbb{Z}_q^{\tilde{k}\times n}, \mathbf{Z} \leftarrow \mathbb{Z}_q^{\tilde{k}\times t}$
$[\mathbf{A}_\Lambda]_2 := \boldsymbol{\Lambda}^\top[\mathbf{A}]_2, [\mathbf{A}_\Xi]_1 := \boldsymbol{\Xi}^\top[\mathbf{A}]_1$
$[\mathbf{M}_\Lambda]_1 := \boldsymbol{\Lambda}[\mathbf{M}]_1 + [\mathbf{Z}]_1, [\mathbf{N}_\Xi]_2 := \boldsymbol{\Xi}[\mathbf{N}]_2 - [\mathbf{Z}]_2$
Return $\mathsf{crs} := ([\mathbf{M}_\Lambda]_1, [\mathbf{A}_\Lambda]_2, [\mathbf{A}]_2, [\mathbf{N}_\Xi]_2,[\mathbf{A}_\Xi]_1, [\mathbf{A}]_1)$.
$(\tau_{sim} := (\boldsymbol{\Lambda}, \boldsymbol{\Xi}).)$

$\underline{\mathsf{P}(\mathsf{crs}, [\mathbf{x}]_1, [\mathbf{y}]_2, \mathbf{w})}\backslash\backslash([\mathbf{x}]_1 = [\mathbf{M}]_1\mathbf{w}, [\mathbf{y}]_2 = [\mathbf{N}]_2\mathbf{w})$
$\mathbf{z} \leftarrow \mathbb{Z}_q^{\tilde{k}}$
$[\boldsymbol{\rho}]_1 := [\mathbf{M}_\Lambda]_1\mathbf{w} + [\mathbf{z}]_1, [\boldsymbol{\sigma}]_2 := [\mathbf{N}_\Xi]_2\mathbf{w} - [\mathbf{z}]_2$
Return $([\boldsymbol{\rho}]_1, [\boldsymbol{\sigma}]_2)$.

$\underline{\mathsf{V}(\mathsf{crs}, ([\mathbf{x}]_1, [\mathbf{y}]_2), ([\boldsymbol{\rho}]_1, [\boldsymbol{\sigma}]_2))}$
Return $([\mathbf{x}^\top]_1[\mathbf{A}_{\boldsymbol{\Lambda}}]_2 - [\boldsymbol{\rho}^\top]_1[\mathbf{A}]_2 = [\boldsymbol{\sigma}^\top]_2[\mathbf{A}]_1 - [\mathbf{y}^\top]_2[\mathbf{A}_{\boldsymbol{\Xi}}]_1)$.

$\underline{\mathsf{S}_2(\mathsf{crs}, ([\mathbf{x}]_1, [\mathbf{y}]_2), \tau_{sim})}$
$\mathbf{z} \leftarrow \mathbb{Z}_q^{\tilde{k}}$
$[\boldsymbol{\rho}]_1 := \boldsymbol{\Lambda}[\mathbf{x}]_1 + [\mathbf{z}]_1, [\boldsymbol{\sigma}]_2 := \boldsymbol{\Xi}[\mathbf{y}]_2 - [\mathbf{z}]_2$
Return $([\boldsymbol{\rho}]_1, [\boldsymbol{\sigma}]_2)$.
```

Figure 3.1: Two QA-NIZK arguments for $\mathcal{L}_{[\mathbf{M}]_1,[\mathbf{N}]_2}$. $\Psi_{\mathsf{spl}}(\mathcal{D}_k)$ is defined for $\widetilde{\mathcal{D}_k} = \mathcal{D}_k$ and $\tilde{k} = k+1$, and is a generalization of Kiltz and Wee's construction [KW15, Section 3.1] in two groups. The second construction $\Psi_{\mathsf{spl}}(\overline{\mathcal{D}}_k)$ corresponds to $\widetilde{\mathcal{D}_k} = \overline{\mathcal{D}_k}$ and $\tilde{k} = k$, and is a generalization of Kiltz and Wee's contraction [KW15, Section 3.2] in two groups. Computational soundness is based on the $\mathcal{D}_k$-SKerMDH assumption. $\mathbf{M}$ is matrix of size $m\times t$, $\mathbf{N}$ is of size $n\times t$, $\mathbf{A}$ is of size $\tilde{\times}k$, $\boldsymbol{\Lambda}$ is of size $\tilde{k}\times m$, $\boldsymbol{\Xi}$ is of size $\tilde{k}\times n$, $\mathbf{M}_\Lambda$ is of size $\tilde{k}\times t$, $\mathbf{N}_\Xi$ is of size $\tilde{k}\times t$, $\mathbf{A}_\Lambda$ is of size $m\times k$, and $\mathbf{A}_\Xi$ is of size $n\times k$. The CRS size is $(\tilde{k}k+\tilde{k}t+mk)|\mathbb{G}_1|+(\tilde{k}k+\tilde{k}t+nk)|\mathbb{G}_2|$ and the proof size $\tilde{k}(|\mathbb{G}_1| + |\mathbb{G}_2|)$. Verification requires $2\tilde{k}k + (m + n)k$ pairing computations. We denote by Ψ_{spl} the most efficient instantiation of $\Psi_{\mathsf{spl}}(\mathcal{D}_k)$, which happens when $\mathcal{D}_k = \bar{\mathcal{L}}_2$.

(Soundness.) B receives a challenge $([\mathbf{A}]_1, [\mathbf{A}]_2)$, $\mathbf{A} \leftarrow \mathcal{D}_k$, and then it chooses $\boldsymbol{\Lambda} \leftarrow \mathbb{Z}_q^{(k+1)\times m}, \boldsymbol{\Xi} \leftarrow \mathbb{Z}_q^{(k+1)\times n}$, samples $([\mathbf{M}]_1, [\mathbf{N}]_2) \leftarrow \mathcal{D}_{gk}$, $[\mathbf{M}]_1 \in \mathbb{G}_1^{m\times t}, [\mathbf{N}]_2 \in \mathbb{G}_2^{n\times t}$, and computes

$$\begin{aligned}\mathsf{crs} :=&([\mathbf{M}_\Lambda]_1, [\mathbf{A}_\Lambda]_2, [\mathbf{A}]_2, [\mathbf{N}_\Xi]_2, [\mathbf{A}_\Xi]_1, [\mathbf{A}]_1)\\ &\in \mathbb{G}_1^{(k+1)\times t} \times \mathbb{G}_2^{m\times k} \times \mathbb{G}_2^{(k+1)\times k} \times \mathbb{G}_2^{(k+1)\times t} \times \mathbb{G}_1^{n\times k}, \mathbb{G}_1^{(k+1)\times k}\end{aligned}$$

in the natural way. An adversary F against the soundness property outputs a vector $([\mathbf{x}^*]_1, [\mathbf{y}^*]_2) \notin \mathcal{L}_{[\mathbf{M}]_1,[\mathbf{N}]_2}$ and a valid proof $([\boldsymbol{\rho}^*]_1, [\boldsymbol{\sigma}^*]_2)$. At this point, B computes its own proof $([\boldsymbol{\rho}^\dagger]_1, [\boldsymbol{\sigma}^\dagger]_2)$ using $\boldsymbol{\Lambda}$ and $\boldsymbol{\Xi}$. The adversary B will output as a response to the $\mathcal{D}_k$-SKerMDH challenge the pair $([\mathbf{r}]_1, [\mathbf{s}]_2) := ([\boldsymbol{\rho}^*]_1 - [\boldsymbol{\rho}^\dagger]_1, [\boldsymbol{\sigma}^\dagger]_2 - [\boldsymbol{\sigma}^*]_2)$. We now see that with all but probability $1/q$, this is a valid solution. Indeed, if $\mathbf{r} \neq \mathbf{s}$, we are done, because since both are valid proofs, subtraction of the verification equations yields

$$([\boldsymbol{\rho}^*]_1 - [\boldsymbol{\rho}^\dagger]_1)^\top[\mathbf{A}]_2 = ([\boldsymbol{\sigma}^\dagger]_2 - [\boldsymbol{\sigma}^*]_2)^\top[\mathbf{A}]_1.$$

By definition $\mathbf{r} \neq \mathbf{s}$ if and only if $\boldsymbol{\rho}^* + \boldsymbol{\sigma}^* \neq \boldsymbol{\rho}^\dagger + \boldsymbol{\sigma}^\dagger$. Note that

$$\boldsymbol{\rho}^\dagger + \boldsymbol{\sigma}^\dagger = \boldsymbol{\Lambda}\mathbf{x}^* + \boldsymbol{\Xi}\mathbf{y}^* = \boldsymbol{\Delta}\mathbf{t}, \text{ where } \mathbf{t} := \begin{pmatrix}\mathbf{x}^*\\ \mathbf{y}^*\end{pmatrix}.$$

Since $\mathbf{Z}$ is a uniform random value, the CRS reveals (information theoretically) only $\{\boldsymbol{\Delta}\mathbf{P} := \mathbf{P}_\Delta, \boldsymbol{\Delta}^\top\mathbf{A} := \mathbf{A}_\Delta\}$ about $\boldsymbol{\Delta}$. From $\boldsymbol{\Delta}^\top\mathbf{A} = \mathbf{A}_\Delta$, an (unbounded) adversary might only deduce that

$$\mathbf{\Delta}_1 = (\mathbf{A}_1^\top)^{-1}(\mathbf{A}_\Delta^\top - \mathbf{A}_2^\top \mathbf{\Delta}_2),$$

where $\mathbf{\Delta}_1 \in \mathbb{Z}_q^{k\times \tilde{m}}, \mathbf{\Delta}_2 \in \mathbb{Z}_q^{1\times \tilde{m}}, \mathbf{A}_1 \in \mathbb{Z}_q^{k\times k}, \mathbf{A}_2 \in \mathbb{Z}_q^{k+1\times 1}$ and $\mathbf{\Delta} = \begin{pmatrix}\mathbf{\Delta}_1\\ \mathbf{\Delta}_2\end{pmatrix}, \mathbf{A} = (\mathbf{A}_1\mathbf{A}_2)$. Therefore, $\mathbf{\Delta}_2$ remains completely hidden given only $\mathbf{A}_\Delta$. Note also that the first k rows of $\mathbf{P}_{\mathbf{\Delta}}$ (i.e. $\mathbf{\Delta}_1\mathbf{P}$) are completely determined by the last row of $\mathbf{P}_\Delta$ (i.e. $\mathbf{\Delta}_2\mathbf{P}$) and the CRS, since

$$\mathbf{\Delta}_1\mathbf{P} = (\mathbf{A}_0^\top)^{-1}(\mathbf{A}_\Delta^\top\mathbf{P} - \mathbf{A}_1^\top \mathbf{\Delta}_2\mathbf{P}).$$

Let $\mathbf{P}^\perp \in \mathbb{Z}_q^{\tilde{m}\times(\tilde{m}-r)}$, where $r = \mathsf{rank}(\mathbf{P})$, a basis of the kernel of $\mathbf{P}$. The row vector $\mathbf{\Delta}_2$ can be always written as $\mathbf{\Delta}_2^\top = \mathbf{P}\mathbf{w}_1 + \mathbf{P}^\perp\mathbf{w}_2$, where $\mathbf{w}_1 \in \mathbb{Z}_q^t, \mathbf{w}_2 \in \mathbb{Z}_q^{\tilde{m}-r}$ are uniformly random vectors. It follows that $\mathbf{w}_2$ is completely hidden given only the CRS since $\mathbf{\Delta}_2\mathbf{P} = \mathbf{w}_1^\top\mathbf{P}^\top\mathbf{P}$. Since $\mathbf{t} \notin \mathsf{span}(\mathbf{P})$, there exists some $\mathbf{w}_1' \in \mathbb{Z}_q^t, \mathbf{w}_2' \in \mathbb{Z}_q^{\tilde{m}-r}$ such that $\mathbf{w}_2' \neq \mathbf{0}$ and $\mathbf{t} = \mathbf{P}\mathbf{w}_1' + \mathbf{P}^\perp\mathbf{w}_2'$. Finally, note that

$$\begin{aligned}\mathbf{\Delta}_2\mathbf{t} &= (\mathbf{P}\mathbf{w}_1 + \mathbf{P}^\perp\mathbf{w}_2)^\top(\mathbf{P}\mathbf{w}_2' + \mathbf{P}^\perp\mathbf{w}_2')\\ &= \mathbf{w}_1^\top\mathbf{P}^\top\mathbf{P}\mathbf{w}_1' + \mathbf{w}_2^\top(\mathbf{P}^\perp)^\top\mathbf{P}^\perp\mathbf{w}_2'\end{aligned}$$

where the non-zero component of $\mathbf{w}_2'$ is multiplied by a component of (the random vector) $\mathbf{w}_2$ and thus, $\mathbf{\Delta}_2\mathbf{t}$ is uniformly distributed over $\mathbb{Z}_q$. It follows that $\Pr[\mathbf{\Delta}\mathbf{t} \neq \boldsymbol{\rho}^* + \boldsymbol{\rho}^*] \geq 1 - 1/q$.

(Zero-Knowledge.) It is direct from the construction that the simulated proof follows the same distribution as an honestly computed proof. □

Theorem 3.2 *If $\widetilde{\mathcal{D}_k} = \overline{\mathcal{D}}_k$ and $\tilde{k} = k$, and $\mathcal{D}_{gk}$ is a witness samplable distribution, Fig. 3.1 describes a QA-NIZK proof system with perfect completeness, computational adaptive strong soundness based on the $\mathcal{D}_k$-$\mathsf{SKerMDH}$ assumption, and perfect zero-knowledge.*

Proof (Completeness and Zero-Knowledge.) Equal as in Theorem 3.1.

(Soundness.) Define $\tilde{m} := m + n$ and $\mathbf{P} := \left(\begin{smallmatrix}\mathbf{M}\\ \mathbf{N}\end{smallmatrix}\right)$. An adversary B against $\mathcal{D}_k$-$\mathsf{SKerMDH}$ assumption receives a challenge $([\mathbf{A}]_1, [\mathbf{A}]_2)$, $\mathbf{A} \leftarrow \mathcal{D}_k$. It samples $([\mathbf{M}]_1, [\mathbf{N}]_2, \mathbf{M}, \mathbf{N}) \in \mathcal{R}_{par}$ and computes $\mathbf{P}^\perp \in \mathbb{Z}_q^{\tilde{m}\times(\tilde{m}-r)}$, where $r = \mathsf{rank}(\mathbf{P})$, a basis of the kernel of $\mathbf{P}^\top$. By definition, $\mathbf{P}^\top = (\mathbf{M}^\top|\mathbf{N}^\top)$ and $\mathbf{P}^\top\mathbf{P}^\perp = \mathbf{0}$, thus we can write $\mathbf{P}^\perp = \left(\begin{smallmatrix}\mathbf{E}\\ \mathbf{F}\end{smallmatrix}\right)$, for some matrices such that $\mathbf{M}^\top\mathbf{E} = -\mathbf{N}^\top\mathbf{F}$.

Adversary B samples $\mathbf{R} \in \mathbb{Z}_q^{(\tilde{m}-r-1)\times(k+1)}$ and defines

$$[\mathbf{A}']_1 := \begin{pmatrix}[\mathbf{A}]_1\\ \mathbf{R}[\mathbf{A}]_1\end{pmatrix} \in \mathbb{G}_1^{(k+\tilde{m}-r)\times k}, \qquad [\mathbf{A}']_2 := \begin{pmatrix}[\mathbf{A}]_2\\ \mathbf{R}[\mathbf{A}]_2\end{pmatrix} \in \mathbb{G}_2^{(k+\tilde{m}-r)\times k}.$$

Then B samples $(\widetilde{\mathbf{\Lambda}}|\widetilde{\mathbf{\Xi}}) \leftarrow \mathbb{Z}_q^{k\times\tilde{m}}$. Let $\mathbf{A}_0$ be the first k rows of $\mathbf{A}'$ (or $\mathbf{A}$) and $\mathbf{A}_1'$ the rest of the rows, and $\mathbf{T}_{\mathbf{A}'} = \mathbf{A}_1'\mathbf{A}_0^{-1}$. Then B implicitly sets $(\mathbf{\Lambda}|\mathbf{\Xi}) := (\widetilde{\mathbf{\Lambda}}|\widetilde{\mathbf{\Xi}}) + \mathbf{T}_{\mathbf{A}'}^\top(\mathbf{E}^\top|\mathbf{F}^\top)$, and computes:

$$\begin{pmatrix}[\mathbf{A}_\Lambda]_2\\ [\mathbf{A}_\Xi]_1\end{pmatrix} = \begin{pmatrix}\mathbf{\Lambda}^\top[\mathbf{A}_0]_2\\ \mathbf{\Xi}^\top[\mathbf{A}_0]_1\end{pmatrix} := \begin{pmatrix}(\widetilde{\mathbf{\Lambda}}^\top + \mathbf{E}\mathbf{T}_{\mathbf{A}'})[\mathbf{A}_0]_2\\ (\widetilde{\mathbf{\Xi}}^\top + \mathbf{F}\mathbf{T}_{\mathbf{A}'})[\mathbf{A}_0]_1\end{pmatrix} = \begin{pmatrix}(\widetilde{\mathbf{\Lambda}}^\top|\mathbf{E})[\mathbf{A}']_2\\ (\widetilde{\mathbf{\Xi}}^\top|\mathbf{F})[\mathbf{A}']_1\end{pmatrix} \tag{3.1}$$

So far the argument is very similar to Kiltz and Wee's [KW15, Section 3.2], now comes an important difference. Adversary B also needs to compute $\mathbf{\Lambda}[\mathbf{M}]_1 + [\mathbf{Z}]_1$ and $\mathbf{\Xi}[\mathbf{N}]_2 - [\mathbf{Z}]_2$.

Although the adversary B does not know how to compute $\mathbf{\Xi N}$ or $\mathbf{\Lambda M}$, it can compute their sum in $\mathbb{Z}_q$ as:

$$\mathbf{\Xi N} + \mathbf{\Lambda M} = \Big((\widetilde{\mathbf{\Lambda}}|\widetilde{\mathbf{\Xi}}) + \mathbf{T}_{\mathbf{A}'}^\top(\mathbf{E}^\top|\mathbf{F}^\top)\Big)\begin{pmatrix}\mathbf{M}\\ \mathbf{N}\end{pmatrix} = \widetilde{\mathbf{\Lambda}}\mathbf{M} + \widetilde{\mathbf{\Xi}}\mathbf{N} =: \mathbf{T}.$$

Thus, B picks $\mathbf{Z} \leftarrow \mathbb{Z}_q^{k\times t}$ and outputs $[\mathbf{N}_\Xi]_2 := [\mathbf{T}]_2 - [\mathbf{Z}]_2$ and $[\mathbf{M}_\Xi]_1 := [\mathbf{Z}]_1$. Now, when F outputs a valid proof for some $([\mathbf{x}]_1, [\mathbf{y}]_2) \notin \mathcal{L}_{[\mathbf{M}]_1,[\mathbf{N}]_2}$, it holds that:

$$\begin{aligned}
[\mathbf{x}^\top]_1[\mathbf{A}_\Lambda]_2 - [\boldsymbol{\rho}^\top]_1[\mathbf{A}_0]_2 = [\boldsymbol{\sigma}^\top]_2[\mathbf{A}_0]_1 - [\mathbf{y}^\top]_2[\mathbf{A}_\Xi]_1 \iff \\
[\mathbf{x}^\top]_1(\widetilde{\mathbf{\Lambda}}^\top|\mathbf{E})[\mathbf{A}']_2 - ([\boldsymbol{\rho}^\top]_1|[\mathbf{0}_{1\times(\tilde{m}-r)}]_1)^\top[\mathbf{A}']_2 = \\
([\boldsymbol{\sigma}^\top]_2|[\mathbf{0}_{1\times(\tilde{m}-r)}]_2)[\mathbf{A}']_1 - [\mathbf{y}^\top]_2(\widetilde{\mathbf{\Xi}}^\top|\mathbf{F})[\mathbf{A}']_1 \iff \\
[\mathbf{c}^\top]_1[\mathbf{A}']_2 = [\mathbf{d}^\top]_2[\mathbf{A}']_1,
\end{aligned}$$

where $[\mathbf{c}^\top]_1 := ([\mathbf{x}^\top]_1\widetilde{\mathbf{\Lambda}} - [\boldsymbol{\rho}^\top]_1|[\mathbf{x}^\top]_1\mathbf{E})$ and $[\mathbf{d}^\top]_2 := ([\boldsymbol{\sigma}^\top]_2 - [\mathbf{y}^\top]_2\widetilde{\mathbf{\Xi}}| - [\mathbf{y}^\top]_2\mathbf{F})$.

Obviously

$$\mathbf{c} - \mathbf{d} \in \ker((\mathbf{A}')^\top) \iff (\mathbf{c} - \mathbf{d})^\top\mathbf{A}' = 0 \iff (\mathbf{c}_1^\top + \mathbf{c}_2^\top\mathbf{R}) - (\mathbf{d}_1^\top + \mathbf{d}_2^\top\mathbf{R}) \in \ker(\mathbf{A}^\top).$$

while, by assumption, $([\mathbf{x}]_1, [\mathbf{y}]_2) \notin \mathcal{L}_{[\mathbf{M}]_1,[\mathbf{N}]_2}$ and thus $[\mathbf{x}^\top]_1\mathbf{E} \neq -[\mathbf{y}^\top]_2\mathbf{F}$. We conclude with an information-theoretic argument. Because $\mathbf{R}$ is only revealed to B through $\mathbf{A}_\mathbf{R} := \mathbf{RA}$ it holds that

$$\mathbf{R}_0 := \mathbf{A}_0^{-1}(\mathbf{A}_\mathbf{R} - \mathbf{r}_1\mathbf{A}_1),$$

where $\mathbf{R}_0 \in \mathbb{Z}_q^{(\tilde{m}-r-1)\times k}, \mathbf{r}_1 \in \mathbb{Z}_q^{\tilde{m}-r-1}$, $\mathbf{R} = (\mathbf{R}_0|\mathbf{r}_1)$, $\mathbf{A} = \begin{pmatrix}\mathbf{A}_0\\ \mathbf{A}_1\end{pmatrix}$, and $\mathbf{r}_1$ remains completely hidden to the adversary. Therefore,

$$\begin{aligned}
\Pr[\mathbf{c}_1^\top + \mathbf{c}_2^\top\mathbf{R} = \mathbf{d}_1^\top + \mathbf{d}_2^\top\mathbf{R}] &= \Pr[(\mathbf{c}_2^\top - \mathbf{d}_2^\top)\mathbf{R} = \mathbf{d}_1^\top - \mathbf{c}_1^\top] \\
&= \Pr[(\mathbf{c}_2^\top - \mathbf{d}_2^\top)\mathbf{R}_0, (\mathbf{c}_2^\top - \mathbf{d}_2^\top)\mathbf{r}_1) = (\boldsymbol{\alpha}^\top, \beta)] \\
&\leq \Pr[(\mathbf{c}_2^\top - \mathbf{d}_2^\top)\mathbf{r}_1 = \beta] \\
&= 1/q
\end{aligned}$$

where $\boldsymbol{\alpha} \in \mathbb{Z}_q^k, \beta \in \mathbb{Z}_q$, and $(\boldsymbol{\alpha}^\top, \beta) := \mathbf{c}_2^\top - \mathbf{d}_2^\top$.

We conclude that, with high probability, $([\mathbf{c}_1^\top]_1 + [\mathbf{c}_2^\top]_1\mathbf{R}), ([\mathbf{d}_1^\top]_2 + [\mathbf{d}_2^\top]_2\mathbf{R})$ solves $\mathcal{D}_k$-$\mathsf{SKerMDH}$.

This proves standard soundness. Strong soundness follows from the fact that the argument is essentially information theoretic. In particular, the knowledge of $(\mathbf{M}, \mathbf{N})$ does not reveal additional information about $\mathbf{R}$. □

3.3 Argument of Sum in Subspace

We can adapt the previous construction to the *sum in subspace* language,

$$\mathcal{L}_{[\mathbf{M}]_1,[\mathbf{N}]_2,+} := \{([\mathbf{x}]_1, [\mathbf{y}]_2) \in \mathbb{G}_1^m \times \mathbb{G}_2^m : \exists \mathbf{w} \in \mathbb{Z}_q^t,\ \mathbf{x} + \mathbf{y} = (\mathbf{M} + \mathbf{N})\mathbf{w}\}.$$

We define two proof systems $\Psi_{\mathsf{sum}}(\mathcal{D}_k)$, $\Psi_{\mathsf{sum}}(\overline{\mathcal{D}}_k)$ as in Fig. 3.1, but now with $\mathbf{\Lambda} = \mathbf{\Xi}$. Also, we define $\Psi_{\mathsf{sum}} := \Psi_{\mathsf{sum}}(\overline{\mathcal{D}}_k)$ when $\mathcal{D}_k = \mathcal{L}_2$.

Completeness and zero-knowledge are straightforward. Soundness follows from the same argument as before with the following differences. First, note that in the subspace concatenation case the information revealed to the adversary in the CRS was $\mathbf{\Lambda M} + \mathbf{\Xi N}$, $\mathbf{\Lambda}^\top \mathbf{A}$, and $\mathbf{\Xi}^\top \mathbf{A}$, and the information revealed now is $\mathbf{\Lambda}(\mathbf{M}+\mathbf{N}), \mathbf{\Lambda}^\top \mathbf{A}$. In the soundness proof for $\mathcal{D}_k$ the key point was that if $([\mathbf{x}^*]_1, [\mathbf{y}^*]_2) \notin \mathcal{L}_{[\mathbf{M}]_1,[\mathbf{N}]_2,+}$, then $\mathbf{\Delta}\begin{pmatrix}\mathbf{x}^*\\ \mathbf{y}^*\end{pmatrix}$, where $\mathbf{\Delta} = (\mathbf{\Lambda}|\mathbf{\Xi})$, was information theoretically hidden to the adversary. In this case $\mathbf{x}^* + \mathbf{y}^* \notin \mathbf{Span}(\mathbf{M}+\mathbf{N})$ and thus $\mathbf{x}^* + \mathbf{y}^* = (\mathbf{M}+\mathbf{N})\mathbf{w} + \mathbf{P}^\perp \mathbf{w}'$, where $\mathbf{P}^\perp$ is a basis of the kernel of $\mathbf{M}+\mathbf{N}$ and $\mathbf{w}' \neq 0$. Then, $\mathbf{\Delta}\begin{pmatrix}\mathbf{x}^*\\ \mathbf{y}^*\end{pmatrix} = \mathbf{\Lambda}(\mathbf{x}^* + \mathbf{y}^*)$ is information theoretically hidden because $\mathbf{\Lambda P}^\perp$ is information theoretically hidden. In the soundness proof for $\overline{\mathcal{D}}_k$, one needs to compute $\mathbf{P}^\perp$, a basis for the kernel of $\mathbf{M}+\mathbf{N}$, and defines $\mathbf{E} := \mathbf{P}^\perp$ and $\mathbf{F} := \mathbf{P}^\perp$. From these definitions it follows that $\mathbf{\Lambda}(\mathbf{M}+\mathbf{N}) = \widetilde{\mathbf{\Lambda}}(\mathbf{M}+\mathbf{N})$ and that $([\mathbf{x}]_1, [\mathbf{y}]_2) \notin \mathcal{L}_{[\mathbf{M}]_1,[\mathbf{N}]_2,+}$ implies that $\mathbf{x}^\top \mathbf{E} = -\mathbf{y}^\top \mathbf{F}$. Given that the same information is revealed in the CRS, the proof of soundness follows as in Theorem 3.2.

3.4 Argument of Equal Opening in Different Groups

Given $\Psi_{\mathsf{spl}}(\mathcal{D}_k)$ or $\Psi_{\mathsf{spl}}(\overline{\mathcal{D}}_k)$, it is direct to construct constant-size NIZK arguments of membership in:

$$\mathcal{L}_{\mathsf{com},[\mathbf{U}]_1,[\mathbf{V}]_2,\nu} := \left\{ ([\mathbf{c}]_1,[\mathbf{d}]_2) \in \mathbb{G}_1^m \times \mathbb{G}_2^n : \begin{array}{c} \exists(\mathbf{w},\mathbf{r},\mathbf{s}) \text{ s.t.} \\ [\mathbf{c}]_1 = [\mathbf{U}]_1 \begin{pmatrix}\mathbf{w}\\ \mathbf{r}\end{pmatrix} \text{ and} \\ [\mathbf{d}]_2 = [\mathbf{V}]_2 \begin{pmatrix}\mathbf{w}\\ \mathbf{s}\end{pmatrix} \end{array} \right\},$$

where $[\mathbf{U}]_1 \in \mathbb{G}_1^{m\times\tilde{m}}$, $[\mathbf{V}]_2 \in \mathbb{G}_2^{n\times\tilde{n}}$ and $\mathbf{w} \in \mathbb{Z}_q^\nu$. The witness is $(\mathbf{w},\mathbf{r},\mathbf{s}) \in \mathbb{Z}_q^\nu \times \mathbb{Z}_q^{\tilde{m}-\nu} \times \mathbb{Z}_q^{\tilde{n}-\nu}$. This language is interesting because it can express the fact that $([\mathbf{c}]_1, [\mathbf{d}]_2)$ are commitments to the same vector $\mathbf{w} \in \mathbb{Z}_q^\nu$ in different groups.

The construction is an immediate consequence of the observation that $\mathcal{L}_{\mathsf{com},[\mathbf{U}]_1,[\mathbf{V}]_2,\nu}$ can be rewritten as some concatenation language $\mathcal{L}_{[\mathbf{M}]_1,[\mathbf{N}]_2}$. Denote by $\mathbf{U}_1$ the first ν columns of $\mathbf{U}$ and $\mathbf{U}_2$ the remaining ones, and $\mathbf{V}_1$ the first ν columns of $\mathbf{V}$ and $\mathbf{V}_2$ the remaining ones. If we define:

$$\mathbf{M} := (\mathbf{U}_1|\mathbf{U}_2|\mathbf{0}_{m\times(\tilde{n}-\nu)}) \qquad \mathbf{N} := (\mathbf{V}_1|\mathbf{0}_{n\times(\tilde{m}-\nu)}|\mathbf{V}_2).$$

then it is immediate to verify that $\mathcal{L}_{\mathsf{com},[\mathbf{U}]_1,[\mathbf{V}]_2,\nu} = \mathcal{L}_{[\mathbf{M}]_1,[\mathbf{N}]_2}$.

We denote as $\Psi_{\mathsf{com}}(\overline{\mathcal{D}}_k)$ the proof system for $\mathcal{L}_{\mathsf{com},\hat{\mathbf{U}},\check{\mathbf{V}},\nu}$ which corresponds to $\Psi_{\mathsf{spl}}(\overline{\mathcal{D}}_k)$ for $\mathcal{L}_{[\mathbf{M}]_1,[\mathbf{N}]_2}$, where $[\mathbf{M}]_1, [\mathbf{N}]_2$ are the matrices defined above. Also, we denote the proof system as Ψ_{com} when we use Ψ_{spl}. Note that for commitment schemes we can generally assume $[\mathbf{U}]_1, [\mathbf{V}]_2$ to be drawn from some witness samplable distribution. Therefore, it follows from Theorem 3.2 that $\Psi_{\mathsf{com}}(\overline{\mathcal{D}}_k)$ satisfies the notion of strong soundness.

3.5 Aggregation of Groth-Sahai Proofs

In this section we discuss two different ways to aggregate GS equations. The first is a direct application of the proof of equal commitment opening and is only valid for two-sided linear equations in $\mathbb{Z}_q$, the second is an extension of the results of Jutla and Roy for all other types of linear equations.

3.5.1 Aggregating Two-Sided Linear Equations in $\mathbb{Z}_q$

We note that proving that n pairs of GS commitments open (pairwise) to the same elements in $\mathbb{Z}_q$ is simply a special case of the proof of equal commitment opening in Section 3.4. Indeed, the concatenation of n GS commitments is just a commitment to a vector of scalars. In particular, given $\mathsf{crs}_{\mathsf{GS}} = (gk, [\mathbf{u}_1]_1, [\mathbf{u}_2]_1, [\mathbf{v}_1]_2, [\mathbf{v}_2]_2)$, it is easy to see that n commitments to $x_i \in \mathbb{Z}_q$, which are of the form: $[\mathbf{c}_i]_1 = x_i[\mathbf{u}_1]_1 + r_i[\mathbf{u}_2]_1$ for some $r_i \in \mathbb{Z}_q$ (recall that $\iota_1(x_i) = x_i[\mathbf{u}_1]_1$), can be written as

$$\begin{pmatrix} [\mathbf{c}_1]_1 \\ \vdots \\ [\mathbf{c}_n]_1 \end{pmatrix} = \begin{pmatrix} [\mathbf{u}_1]_1 & \dots & [\mathbf{0}]_1 \\ \vdots & \ddots & \vdots \\ [\mathbf{0}]_1 & \dots & [\mathbf{u}_1]_1 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} [\mathbf{u}_2]_1 & \dots & [\mathbf{0}]_1 \\ \vdots & \ddots & \vdots \\ [\mathbf{0}]_1 & \dots & [\mathbf{u}_2]_1 \end{pmatrix} \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix},$$

and similarly the concatenation of n commitments $[\mathbf{d}_i]_2$, $i \in [\ell]$ can be written as $[\mathbf{V}^1]_2\mathbf{y} + [\mathbf{V}^2]_2\mathbf{s}$, where $[\mathbf{V}^i]_2$ is the block-wise concatenation of n copies of $[\mathbf{v}_i]_2$.

In particular, proving that n GS commitments open to the same value can be also seen as the aggregation of the proof of n GS equations of the form $\mathsf{x}_\ell - \mathsf{y}_\ell = 0$. The aggregation of any other set of two-sided linear equations in $\mathbb{Z}_q$ easily reduces to this case using the homomorphic properties of GS commitments. Indeed, given n equations of the form:

$$\boldsymbol{\alpha}_\ell^\top \mathsf{y} + \mathsf{x}^\top \boldsymbol{\beta}_\ell = t_\ell, \ \ell \in [n],$$

and the commitments to a satisfying assignment (where the commitments to every coordinate of x (resp. y) are in $\mathbb{G}_1$ (resp. $\mathbb{G}_2$), it is easy to derive a commitment to $\mathsf{x}^\top \boldsymbol{\beta}_\ell - t_\ell$ in $\mathbb{G}_1$ and a commitment to $\boldsymbol{\alpha}_\ell^\top \mathsf{y}$ in $\mathbb{G}_2$ for all $\ell \in [n]$. Obviously, the equations are satisfied if for each ℓ, these commitments open to the same value.

3.5.2 QA Aggregation of Other Equation Types

Jutla and Roy [JR14] show how to aggregate GS proofs linear equations in symmetric bilinear groups. In the original construction of Jutla and Roy soundness is based on a decisional assumption (a weaker variant of the 2-Lin assumption). Its natural generalization in asymmetric groups (where soundness is based on the SXDH assumption) only enables to aggregate the proofs of one-sided linear equations.

In this section, we revisit their construction. We give an alternative, simpler, proof of soundness under a computational assumption which avoids altogether the “switching lemma" of Jutla and Roy. Further, we extend it to two-sided equations in the asymmetric setting. For one-sided linear equations we can prove soundness under any kernel assumption and for two-sided linear equations, under any split kernel assumption.[2]

Let A_1, A_2, A_T be $\mathbb{Z}_q$-vector spaces compatible with some Groth-Sahai equation as detailed in Section 2.6. Let $\mathcal{D}_{gk}$ be a witness samplable distribution which outputs n pairs of vectors $(\boldsymbol{\alpha}_\ell, \boldsymbol{\beta}_\ell) \in A_1^{m_y} \times A_2^{m_x}$, $\ell \in [n]$, for some $m_x, m_y \in \mathbb{N}$. Given some fixed pairs $(\boldsymbol{\alpha}_\ell, \boldsymbol{\beta}_\ell)$, we define, for each $\tilde{\mathbf{t}} \in A_T^n$, the set of equations $\mathcal{S}_{\tilde{\mathbf{t}}}$ as:

$$\mathcal{S}_{\tilde{\mathbf{t}}} = \left\{ E_\ell(\mathsf{x}, \mathsf{y}) = \tilde{t}_\ell : \ell \in [n] \right\}, \quad E_\ell(\mathsf{x}, \mathsf{y}) := \sum_{j \in [m_y]} f(\alpha_{\ell,j}, \mathsf{y}_j) + \sum_{i \in [m_x]} f(\mathsf{x}_i, \beta_{\ell,i}).$$

[2] The results of Jutla and Roy are based on what they call the “switching lemma". As noted Morillo et al. [MRV15], it is implicit in the proof of this lemma that the same results can be obtained under computational assumptions.

We note that, as in Jutla and Roy's work, we only achieve *quasi-adaptive aggregation*, that is, the common reference string is specific to a particular set of equations. More specifically, it depends on the constants $\boldsymbol{\alpha}_\ell, \boldsymbol{\beta}_\ell$ (but not on $\tilde{t}_\ell$, which can be chosen by the prover) and it can be used to aggregate the proofs of $\mathcal{S}_{\tilde{\mathbf{t}}}$, for any $\tilde{\mathbf{t}}$.

Given the equation types for which we can construct NIZK GS proofs (and not only NIWI proofs), there always exists (1) $t_\ell \in A_1$, such that $\tilde{t}_\ell = f(t_\ell, \mathsf{base}_2)$ or (2) $t_\ell \in A_2$, such that $\tilde{t}_\ell = f(\mathsf{base}_1, t_\ell)$, where $\mathsf{base}_i = 1$ if $A_i = \mathbb{Z}_q$ and $\mathsf{base}_i = \mathcal{P}_i$ if $A_i = \mathbb{G}_i$, $i \in \{1,2\}$ [GS12]. For simplicity, in the construction we assume that (1) is the case, otherwise change $\iota_2(a_{\ell,i}), \iota_1(t_\ell)$ for $\iota_1(a_{\ell,i}), \iota_2(t_\ell)$ in the construction below.

$\mathsf{K}(gk, \mathcal{S}_{\tilde{\mathbf{t}}})$**:** Let $\mathbf{A} = (a_{i,j}) \leftarrow \mathcal{D}_{n,k}$. Define

$$\mathsf{crs} := \left(\mathsf{crs}_{\mathsf{GS}}, \left\{\sum_{\ell\in[n]} \iota_1(a_{\ell,i}\boldsymbol{\alpha}_\ell), \sum_{\ell\in[n]} \iota_2(a_{\ell,i}\boldsymbol{\beta}_\ell), \left\{\iota_2(a_{\ell,i}) : \ell \in [n]\right\} : i \in [k]\right\}\right)$$

$\mathsf{P}(gk, \mathcal{S}_{\tilde{\mathbf{t}}}, \mathbf{x}, \mathbf{y})$**:** Given a solution $\mathsf{x} = \mathbf{x}$, $\mathsf{y} = \mathbf{y}$ to $\mathcal{S}_{\tilde{\mathbf{t}}}$, the prover proceeds as follows:

- Commit to all $x_j \in A_1$ as $[\mathbf{c}_j]_1 \leftarrow \mathsf{GS.Com}(x_j)$, and to all $y_j \in A_2$ as $[\mathbf{d}_j]_2 \leftarrow \mathsf{GS.Com}(y_j)$.
- For each $i \in [k]$, run the GS prover for the equation $\sum_{\ell\in[n]} a_{\ell,i} E_\ell(\mathsf{x}, \mathsf{y}) = \sum_{\ell\in[n]} f(t_\ell, a_{\ell,i})$ to obtain the proof, which is a pair $([\boldsymbol{\Theta}_i]_1, [\boldsymbol{\Pi}_i]_2)$.

Output $(\{[\mathbf{c}_j]_1 : j \in [m_x]\}, \{[\mathbf{d}_j]_2 : j \in [m_y]\}, \{([\boldsymbol{\Pi}_i]_2, [\boldsymbol{\Theta}_i]_1) : i \in [k]\})$.

$\mathsf{V}(\mathsf{crs}, \mathcal{S}_{\tilde{\mathbf{t}}}, \{[\mathbf{c}_j]_1 : j \in [m_x]\}, \{[\mathbf{d}_j]_2 : j \in [m_y]\}, \{[\boldsymbol{\Theta}_i]_1, [\boldsymbol{\Pi}_i]_2 : i \in [k]\})$**:** For each $i \in [k]$, run the GS verifier for equation

$$\sum_{\ell\in[n]} a_{\ell,i} E_\ell(\mathsf{x}, \mathsf{y}) = \sum_{\ell\in[n]} f(t_\ell, a_{\ell,i}).$$

Theorem 3.3 *The above protocol is a QA-NIZK proof system for two-sided linear equations.*

Proof (Completeness.) Observe that for each $i \in [k]$

$$\sum_{\ell\in[n]} a_{\ell,i} E_\ell(\mathsf{x}, \mathsf{y}) = \sum_{\ell\in[n]} a_{\ell,i}\tilde{t}_\ell = \sum_{\ell\in[n]} f(t_\ell, a_{\ell,i}). \tag{3.2}$$

Completeness follows from the observation that to efficiently compute the proof, the GS prover only needs, apart from a satisfying assignment to the equation, the randomness used in the commitments plus a way to compute the inclusion map of all involved constants, in this case $\iota_1(a_{\ell,i}\alpha_{\ell,j})$, $\iota_2(a_{\ell,i}\beta_{\ell,j})$, and the latter is part of the CRS.

(Soundness.) We change to a game Game_1 where we know the discrete logarithm of the GS commitment key, as well as the discrete logarithms of $(\boldsymbol{\alpha}_\ell, \boldsymbol{\beta}_\ell)$, $\ell \in [n]$. This is possible because they are both chosen from a witness samplable distribution.

We now prove that an adversary against the soundness in Game_1 can be used to construct an adversary B against the $\mathcal{D}_{n,k}$-$\mathsf{SKerMDH}$ assumption, where $\mathcal{D}_{n,k}$ is the matrix distribution used in the CRS generation.

B receives a challenge $([\mathbf{A}]_1, [\mathbf{A}]_2) \in \mathbb{G}_1^{n\times k} \times \mathbb{G}_2^{n\times k}$. Given all the discrete logarithms that B knows, it can compute a properly distributed CRS even without knowledge of the discrete logarithm of $[\mathbf{A}]_1$. The soundness adversary outputs commitments $\{[\mathbf{c}_j]_1 : j \in [m_x]\}, \{[\mathbf{d}_j]_2 : j \in [m_y]\}$ together with proofs $\{[\mathbf{\Theta}_i]_1, [\mathbf{\Pi}_i]_2 : i \in [k]\}$, which are accepted by the verifier.

The adversary B can use the discrete logarithm of the commitment keys to compute openings of $\{[\mathbf{c}_j]_1 : j \in [m_x]\}, \{[\mathbf{d}_j]_2 : j \in [m_y]\}$ (or the corresponding translation to $\mathbb{G}_s$ when $A_s = \mathbb{Z}_q, s \in \{1,2\}$). Let $[\mathbf{x}]_1$ and $[\mathbf{y}]_2$ the vectors of these commitments. We claim that the pair $([\boldsymbol{\rho}]_1, [\boldsymbol{\sigma}]_2) \in \mathbb{G}_1^n \times \mathbb{G}_2^n$, $[\boldsymbol{\rho}]_1 := (\boldsymbol{\beta}_1^\top[\mathbf{x}]_1 - [t_1]_1, \ldots, \boldsymbol{\beta}_n^\top[\mathbf{x}]_1 - [t_n]_1), [\boldsymbol{\sigma}]_2 := (\boldsymbol{\alpha}_1^\top[\mathbf{y}]_2, \ldots, \boldsymbol{\alpha}_n^\top[\mathbf{y}]_2)$, solves the $\mathcal{D}_{n,k}$-$\mathsf{SKerMDH}$ challenge and can be efficiently computed by B.

First, observe that if the adversary is successful in breaking the soundness property, then $\boldsymbol{\rho} \neq \boldsymbol{\sigma}$. Indeed, if this is the case there is some index $\ell \in [n]$ such that $E_\ell(\mathbf{x}, \mathbf{y}) \neq \tilde{t}_\ell$, which means that $\sum_{j\in[m_y]} f(\alpha_{\ell,j}, \mathsf{y}_j) \neq \sum_{j\in[m_x]} f(\mathsf{x}_j, \beta_{\ell,j}) - f(t_\ell, \mathsf{base}_2)$. If we take discrete logarithms in each side of the equation, this inequality is exactly equivalent to $\boldsymbol{\rho} \neq \boldsymbol{\sigma}$.

Further, because GS proofs have perfect soundness, $\mathbf{x}$ and $\mathbf{y}$ satisfy the equation $\sum_{\ell\in[n]} a_{\ell,i} E_\ell(\mathsf{x}, \mathsf{y}) = \sum_{\ell\in[n]} f(t_\ell, a_{\ell,i})$, for all $i \in [k]$. Thus, for all $i \in [k]$,

$$\sum_{\ell\in[n]} [a_{\ell,i}]_2 \left(\boldsymbol{\beta}_\ell^\top[\mathbf{x}]_1 - [t_\ell]_1\right) = \sum_{\ell\in[n]} [a_{\ell,i}]_1 \left(\boldsymbol{\alpha}_\ell^\top[\mathbf{y}]_2\right), \tag{3.3}$$

which implies that $[\boldsymbol{\rho}]_1[\mathbf{A}]_2 = [\boldsymbol{\sigma}]_2[\mathbf{A}]_1$.

(Zero-Knowledge.) The same simulator of GS proofs can be used. Specifically the simulated proof corresponds to k simulated GS proofs. □

One-Sided Equations.

In the case when $\boldsymbol{\alpha}_\ell = \mathbf{0}$ and $\tilde{t}_\ell = f(t_\ell, \mathsf{base}_2)$ for some $t_\ell \in A_1$, for all $\ell \in [n]$, proofs can be aggregated under a standard kernel assumption (and thus, in asymmetric bilinear groups we can choose $k = 1$). Indeed, in this case, in the soundness proof, the adversary B receives $[\mathbf{A}]_2 \in \mathbb{G}_2^{n\times k}$, an instance of the $\mathcal{D}_{n,k}$-$\mathsf{KerMDH}_{\mathbb{G}_2}$ problem. The adversary B outputs $[\boldsymbol{\rho}]_1 := (\boldsymbol{\beta}_1^\top[\mathbf{x}]_1 - [t_1]_1, \ldots, \boldsymbol{\beta}_n^\top[\mathbf{x}]_1 - [t_n]_1)$ as a solution to the challenge. To see why this works, note that, when $\boldsymbol{\alpha}_\ell = \mathbf{0}$ for all $\ell \in [n]$, equation (3.3) reads $\sum_{\ell\in[n]} [a_{\ell,i}]_2 \left(\boldsymbol{\beta}_\ell^\top[\mathbf{x}]_1 - [t_\ell]_1\right) = [0]_T$ and thus $[\boldsymbol{\rho}]_1[\mathbf{A}]_2 = [\mathbf{0}]_T$. The case when $\boldsymbol{\beta}_\ell = \mathbf{0}$ and $\tilde{t}_\ell = f(\mathsf{base}_1, t_\ell)$ for some $t_\ell \in A_2$, for all $\ell \in [n]$, is analogous.

Public Parameters.

The size of the CRS of the construction above depends on the number of elements needed to represent $[\mathbf{A}]_2$. In this sense, it is interesting to sample $[\mathbf{A}]_2$ from some family of matrix assumptions with good representation size. As we assume that $n > k$, it is interesting to instantiate this scheme with the *circulant matrix distribution* of Morillo et al. [MRV15], which has a representation size of n — independent of k.

3.6 Structure Preserving Linearly Homomorphic Signatures

Linearly-homomorphic structure preserving signatures [AFG$^+$10, BFKW09] enable to sign group elements in G, where G is a group and to publicly derive signatures of new elements which are a linear combination of other signed messages. We take Libert et al.'s definition

[LPJY13], except that we do not identify the elements of G with vectors in $\mathbb{G}_1^n$, for some group $\mathbb{G}_1$. The reason is that G might be some space of the form $\mathbb{G}_1^m \times \mathbb{G}_2^n$.

Definition 3.4 (SPLHS scheme) *A linearly homomorphic structure-preserving signature scheme over the group G consists of a tuple of efficient algorithms Φ=($\mathsf{SignGen}$, Sign, $\mathsf{SignDerive}$, Verify) for which the message space is $\mathcal{M} := G$, with the following specifications.*

$\mathsf{SignGen}(gk, n)$: *is a randomized algorithm that takes as input a group key gk and an integer n and outputs a key pair (pk, sk). The public key pk specifies a $\mathbb{Z}_q$ vector space G of dimension n.*

$\mathsf{Sign}(sk, \mathbf{m})$**:** *is a possibly probabilistic algorithm that takes as input a private key sk and $\mathbf{m} \in G$. It outputs a signature $\boldsymbol{\sigma} \in G$.*

$\mathsf{SignDerive}(pk, \{\omega_i, \boldsymbol{\sigma}_i, \mathbf{m}_i\}_{i\in[\ell]})$**:** *is a possibly probabilistic signature derivation algorithm. It takes as input a public key pk as well as ℓ pairs $(\omega_i, \boldsymbol{\sigma}_i)$, each of which consists of a weight $\omega_i \in \mathbb{Z}_q$ and a signature $\boldsymbol{\sigma}_i \in G$. The output is a signature $\boldsymbol{\sigma} \in G$ on the vector $\mathbf{m} = \sum_{i\in[\ell]} \omega_i \mathbf{m}_i$.*

$\mathsf{Verify}(pk, \mathbf{m}, \boldsymbol{\sigma})$**:** *is a deterministic algorithm that takes in a public key pk, a signature $\boldsymbol{\sigma}$, and a vector $\mathbf{m}$. It outputs 1 if $\boldsymbol{\sigma}$ is deemed valid and 0 otherwise.*

Correctness is expressed by imposing that, for all security parameters $\lambda \in \mathbb{N}$, all integers $n \in \mathsf{poly}(\lambda)$ and all pairs $(pk, sk) \leftarrow \mathsf{SignGen}(gk, n)$, the following holds:

1. For all $\mathbf{m} \in G$, if $\boldsymbol{\sigma} = \mathsf{Sign}(sk, \mathbf{m})$, then we have $\mathsf{Verify}(pk, \mathbf{m}, \boldsymbol{\sigma}) = 1$.
2. For any $\ell > 0$ and any set of triples $\{(\omega_i, \boldsymbol{\sigma}_i, \mathbf{m}_i)\}_{i\in[\ell]}$, if $\mathsf{Verify}(pk, \mathbf{m}_i, \boldsymbol{\sigma}_i) = 1$ for each $i \in [\ell]$, then $\mathsf{Verify}(pk, \sum_{i\in[\ell]} \omega_i \mathbf{m}_i, \mathsf{SignDerive}(pk, \{(\omega_i, \boldsymbol{\sigma}_i)\})) = 1$

In order to get a uniform definition for different types of forgery, we will say that a pair $(\mathbf{m}^*, \boldsymbol{\sigma}^*)$ is a forgery if $P(\mathbf{m}^*, Q) = 1$, where P is a predicate on $(\mathbf{m}^*, Q)$ and Q is the set of reveal queries made by the adversary. We stress that the predicate P is not always efficiently computable. For instance, for the scheme of Libert *et al.* ([LPJY13]), this predicate is 1 iff $\mathbf{m}^*$ is outside the linear span of previous queries, and this is, in general, hard to decide in the group G (although it might be easy for some set Q).

Definition 3.5 *A SPLHS scheme Φ = ($\mathsf{SignGen}$, Sign, Verify, $\mathsf{SignDerive}$) is secure against type P adversaries if no PPT adversary has non-negligible advantage in the game below:*

1. *The adversary A chooses an integer $n \in \mathbb{N}$ and sends it to the challenger who runs $\mathsf{SignGen}(gk, n)$ and obtains (pk, sk) before sending pk to A.*
2. *On polynomially-many occasions, A can interleave the following kinds of queries.*

   Signing queries: A *chooses a vector $\mathbf{m} \in G^n$. The challenger picks a handle h and computes $\boldsymbol{\sigma} \leftarrow \mathsf{Sign}(sk, \mathbf{m})$. It stores $(h, \mathbf{m}, \boldsymbol{\sigma})$ in a table T and returns h.*

   Derivation queries: A *chooses a vector of handles $\mathbf{h} = (h_1, \ldots, h_\ell)$ and a set of coefficients $\{\omega_i\}_{i\in[\ell]}$. The challenger retrieves the tuples $\{(h_i, \mathbf{m}_i, \boldsymbol{\sigma}_i)\}_{i\in[\ell]}$ from T and returns $\perp$ if one of these does not exist. Otherwise, it computes $\mathbf{m} = \sum_{i\in[\ell]} \omega_i \mathbf{m}_i$ and runs $\boldsymbol{\sigma} \leftarrow \mathsf{SignDerive}(pk, \{(\omega_i, \boldsymbol{\sigma}_i)\}_{i\in[\ell]})$. It also chooses a handle h, stores $(h, \mathbf{m}, \boldsymbol{\sigma})$ in T and returns h to A.*

   Reveal queries: A *chooses a handle h. If no tuple of the form $(h, \mathbf{m}, \boldsymbol{\sigma})$ exists in T, the challenger returns $\perp$. Otherwise, it returns $\boldsymbol{\sigma}$ to A and adds $(\mathbf{m}, \boldsymbol{\sigma})$ to the set Q.*

3. A *outputs a signature* $\boldsymbol{\sigma}^*$ *and a vector* $\mathbf{m}^*$. *The adversary* A *wins if* $P(\mathbf{m}^*, Q) = 1$.

A*'s advantage is its probability of success taken over all coin tosses.*

Libert *et al.* also used a set $\mathcal{T}$ of tags in order to add up many instances of their signature scheme in only one. For simplicity, we omit this parameter.

3.6.1 One-Time LHSPS Signatures in Different Groups

The one-time linearly homomorphic signature of Libert, Peters and Yung [LPJY14] implies a QA-NIZK argument for linear spaces. Similarly, our constructions of QA-NIZK proofs for membership in concatenated subspace and for sum in subspace (in the case where the space is not from a witness samplable distribution) is implied by a one-time structure preserving signature scheme with different security properties.

In particular, for subspace concatenation, "one-time" means that the adversary is unable to sign vectors which are not in the span of previously signed vectors, namely, the adversary cannot output a signature for a pair $([\mathbf{x}]_1^*, [\mathbf{y}]_2^*) \in \mathbb{G}_1^m \times \mathbb{G}_2^n$ if $((\mathbf{x}^*)^\top | (\mathbf{y}^*)^\top)$ is linearly independent from the vectors $(\mathbf{x}_i^\top | \mathbf{y}_i^\top)$, $i \in [q_s]$, (the concatenation of two vectors), where $([\mathbf{x}_i]_1, [\mathbf{y}_i]_2)$ are the signing queries of the adversary. The discussion for the scheme which results from our Sum-in-Subspace QA-NIZK proof, results in a different notion of "one-time" — this is captured in the security definition by a different predicate P —, see discussion below.

In either case, the size of the resulting signatures is $(k+1)(|\mathbb{G}_1|+|\mathbb{G}_2|)$ under the $\mathsf{SKerMDH}$ assumption, but if security against random message attacks is sufficient (meaning that the signatures in the set Q which are seen by the adversary are sampled uniformly at random), the signature size can be reduced to $k(|\mathbb{G}_1| + |\mathbb{G}_2|)$ (essentially, in this case one can sample $\mathbf{A}$ from $\overline{\mathcal{D}}_k$). This is inspired by the one-time constructions of structure-preserving signatures of Kiltz et al. secure against random message attacks[KPW15]. We omit any further discussion of this case, as it is a straightforward generalization of our QA-NIZK proofs in the witness samplable setting using the ideas of Kiltz et al.

Our construction is based on the $\mathsf{SKerMDH}$ assumption introduced in Section 2.4. Following the syntactic definition of Section 2.4, our scheme assumes $G = \mathbb{G}_1^m \times \mathbb{G}_2^n$ and the length of the messages is $n + m$.

- $\mathsf{SignGen}(gk, m, n)$: Choose $\mathbf{A} \leftarrow \mathcal{D}_k$, $\boldsymbol{\Lambda}, \boldsymbol{\Xi} \leftarrow \mathbb{Z}_q^{(k+1)\times m}$, $\mathbf{A}_\Lambda := \boldsymbol{\Lambda}^\top \mathbf{A}$, $\mathbf{A}_\Xi := \boldsymbol{\Xi}^\top \mathbf{A}$ The secret key is $\mathsf{sk} = (\boldsymbol{\Lambda}, \boldsymbol{\Xi})$, while the public key is defined to be
$$\mathsf{pk} = ([\mathbf{A}]_1, [\mathbf{A}_\Xi]_1, [\mathbf{A}]_2, [\mathbf{A}_\Lambda]_2) \in \mathbb{G}_1^{(k+1)\times k} \times \mathbb{G}_1^{m\times k} \times \mathbb{G}_2^{(k+1)\times k} \times \mathbb{G}_2^{m\times k}.$$
- $\mathsf{Sign}(\mathsf{sk}, ([\mathbf{x}]_1, [\mathbf{y}]_2))$: To sign a vector $([\mathbf{x}]_1, [\mathbf{y}]_2) \in \mathbb{G}_1^m \times \mathbb{G}_2^m$, pick $\mathbf{z} \leftarrow \mathbb{Z}_q^{(k+1)}$ and output the pair $([\boldsymbol{\rho}]_1, [\boldsymbol{\sigma}]_2) \in \mathbb{G}_1^{(k+1)} \times \mathbb{G}_2^{(k+1)}$, defined as:
$$[\boldsymbol{\rho}]_1 := \boldsymbol{\Lambda}[\mathbf{x}]_1 + [\mathbf{z}]_1, \qquad [\boldsymbol{\sigma}]_2 := \boldsymbol{\Xi}[\mathbf{y}]_2 - [\mathbf{z}]_2.$$
- $\mathsf{SignDerive}(\mathsf{pk}, \{(\omega_i, [\boldsymbol{\rho}_i]_1, [\boldsymbol{\sigma}_i]_2)\}_{i=1}^{\ell})$: given the public key pk, and ℓ tuples $(\omega_i, [\boldsymbol{\rho}_i]_1, [\boldsymbol{\sigma}_i]_2)$, output the pair $(\sum_{i=1}^{\ell} \omega_i [\boldsymbol{\rho}_i]_1, \sum_{i=1}^{\ell} \omega_i [\boldsymbol{\sigma}_i]_2) \in \mathbb{G}_1^{(k+1)} \times \mathbb{G}_2^{(k+1)}$.
- $\mathsf{Verify}(\mathsf{pk}, ([\mathbf{x}]_1, [\mathbf{y}]_2), ([\boldsymbol{\rho}]_1, [\boldsymbol{\sigma}]_2))$ is a deterministic algorithm, that takes as input a public key pk, a signature $([\boldsymbol{\rho}]_1, [\boldsymbol{\sigma}]_2)$ and returns 1 if and only if $([\boldsymbol{\rho}]_1, [\boldsymbol{\sigma}]_2)$ satisfies
$$[\boldsymbol{\rho}^\top]_1 [\mathbf{A}]_2 + [\boldsymbol{\sigma}^\top]_2 [\mathbf{A}]_1 = [\mathbf{x}^\top]_1 [\mathbf{A}_\Lambda]_2 + [\mathbf{y}^\top]_2 [\mathbf{A}_\Xi]_1.$$

Correctness. If a signature is correctly generated then

$$[\boldsymbol{\rho}^\top]_1[\mathbf{A}]_2 - [\mathbf{x}^\top]_1[\mathbf{A}_\Lambda]_2 = [\mathbf{z}^\top]_1[\mathbf{A}]_2 \qquad [\boldsymbol{\sigma}^\top]_2[\mathbf{A}]_1 - [\mathbf{y}^\top]_2[\mathbf{A}_\Xi]_1 = -[\mathbf{z}^\top]_2[\mathbf{A}]_1.$$

Therefore the verification algorithm outputs 1 on a correctly generated signature. The proof of correctness of the signature derivation algorithm follows a similar argument.

Let $Q = \{([\mathbf{x}_i]_1, [\mathbf{y}_i]_2)\}_{i\in[q_s]}$ be some set of elements of $\mathbb{G}_1^m \times \mathbb{G}_2^n$. We define the predicate P as $P(([\mathbf{x}]_1, [\mathbf{y}]_2), Q) = 1$ iff $(\mathbf{x}^\top|\mathbf{y}^\top) \in \mathbb{Z}_q^{2m}$ is not in the space spanned by $\{(\mathbf{x}_i^\top|\mathbf{y}_i^\top) : i \in [q_s]\}$.

Theorem 3.6 *The signature scheme is type P unforgeable if the* $\mathsf{SKerMDH}$ *assumption holds in* $\mathbb{G}_1, \mathbb{G}_2$*.*

The argument is almost identical to Libert et al.'s [LPJY13].

Proof We show how to construct an algorithm B which takes as input an instance $([\mathbf{A}]_1, [\mathbf{A}]_2)$ of the $\mathsf{SKerMDH}$ assumption and outputs a pair of vectors $([\mathbf{r}]_1, [\mathbf{s}]_2) \in \mathbb{G}_1^3 \times \mathbb{G}_2^3$, $\mathbf{r} \neq \mathbf{s}$, such that $[\mathbf{r}^\top]_1[\mathbf{A}]_2 = [\mathbf{s}^\top]_2[\mathbf{A}]_1$ given oracle access to a forger F against the signature scheme (see Section 3.6).

Algorithm B starts by honestly running the key generation algorithm using a randomly chosen $\mathsf{sk} = (\boldsymbol{\Lambda}, \boldsymbol{\Xi})$. Any signature query of F on a vector $([\mathbf{x}]_1, [\mathbf{y}]_2)$ is honestly answered by B, by running the signing algorithm. The game ends with F outputting a vector $([\mathbf{x}]_1^*, [\mathbf{y}]_2^*)$ with a valid signature $([\boldsymbol{\rho}^*]_1, [\boldsymbol{\sigma}^*]_2)$. At this point, B computes its own signature $([\boldsymbol{\rho}^\dagger]_1, [\boldsymbol{\sigma}^\dagger]_2)$ using the secret key $\mathsf{sk} := (\boldsymbol{\Lambda}, \boldsymbol{\Xi})$. The adversary B will output as a response to the $\mathsf{SKerMDH}$ challenge the pair $([\boldsymbol{\rho}^*]_1 - [\boldsymbol{\rho}^\dagger]_1, [\boldsymbol{\sigma}^\dagger]_2 - [\boldsymbol{\sigma}^*]_2)$.

We now see that, with overwhelming probability, this is a valid answer to the $\mathsf{SKerMDH}$ challenge. Indeed, since both signatures satisfy the verification equation, we can subtract the verification equation of each pair, obtaining:

$$([\boldsymbol{\rho}^*]_1 - [\boldsymbol{\rho}^\dagger]_1)^\top[\mathbf{A}]_2 = ([\boldsymbol{\sigma}^\dagger]_2 - [\boldsymbol{\sigma}^*]_2)^\top[\mathbf{A}]_1$$

Therefore, all we need to argue is that $\boldsymbol{\rho}^* - \boldsymbol{\rho}^\dagger \neq \boldsymbol{\sigma}^\dagger - \boldsymbol{\sigma}^*$ with overwhelming probability. This is equivalent to show that the probability that $\boldsymbol{\rho}^* + \boldsymbol{\sigma}^* = \boldsymbol{\rho}^\dagger + \boldsymbol{\sigma}^\dagger$ is negligible. The key point of the argument is that

$$\boldsymbol{\rho}^\dagger + \boldsymbol{\sigma}^\dagger = \boldsymbol{\Lambda}\mathbf{x}^* + \boldsymbol{\Xi}\mathbf{y}^* = \begin{pmatrix}\boldsymbol{\Lambda} & \boldsymbol{\Xi}\end{pmatrix}\begin{pmatrix}\mathbf{x}^* \\ \mathbf{y}^*\end{pmatrix}$$

is information theoretically hidden to F.

The rest of the argument is identical to Libert et al.'s. The argument goes as follows: since, by assumption, $\begin{pmatrix}\mathbf{x}^* \\ \mathbf{y}^*\end{pmatrix}$ is independent of all previous queries, then there is some information about $\begin{pmatrix}\boldsymbol{\Lambda} & \boldsymbol{\Xi}\end{pmatrix}$ which is information theoretically hidden. Thus, $\boldsymbol{\rho}^\dagger + \boldsymbol{\sigma}^\dagger$ is information theoretically hidden and from the adversary's point of view it is equally likely that it has any out of q potential values. □

Signing the Sum of Two Linear Spaces. When $m = n$, we can adapt the previous construction to a different forgery condition namely, we can prove security against a different type of adversary. Namely, Libert et al.'s scheme is secure against an adversary whose goal is to output a forgery for a message which is linearly independent from all of its signing queries. In our case, we require that the adversary cannot output a signature for a pair $([\mathbf{x}]_1^*, [\mathbf{y}]_2^*) \in \mathbb{G}_1^m \times \mathbb{G}_2^m$ if $\mathbf{x}^* + \mathbf{y}^*$ is linearly independent from the vectors $\mathbf{x}_i + \mathbf{y}_i$, $i \in [q_s]$, where $([\mathbf{x}_i]_1, [\mathbf{y}_i]_2)$ are the signing queries of the adversary.

Our construction is like the previous one taking $\boldsymbol{\Xi} = \boldsymbol{\Lambda}$. Indeed, in this case the adversary only learns $\boldsymbol{\Lambda}\mathbf{x}^* + \boldsymbol{\Xi}\mathbf{y}^* = \boldsymbol{\Lambda}(\mathbf{x}^* + \mathbf{y}^*)$, and identically the same argument follows.

Chapter 4

QA-NIZK Arguments for Bit-Strings

In this chapter construct a constant-size proof that a set of n commitments to elements in some field $\mathbb{Z}_q$ open to 0 or 1. Equivalently, we construct a constant size proof for the satisfiability of the equations $b_1(b_1 - 1) = 0, \ldots, b_n(b_n - 1) = 0$. Although solutions for this problem can be easily derived from general results of constant-size NIZK for any NP language [GGPR13, DFGK14, Gro16], they would rely on strong and controversial assumptions, namely non-falsifiable assumptions. Therefore, it is an open question how to build constant-size proofs for this statement using only standard falsifiable assumptions.

A set of n commitments $\mathbf{c}_1, \ldots, \mathbf{c}_n$ to elements of $\mathbb{Z}_q$, each commitment of size s, defines a single commitment $\mathbf{c} = (\mathbf{c}_1, \ldots, \mathbf{c}_n)$ to an element of $\mathbb{Z}_q^n$, of size $n \cdot s$. Alternatively, one can define the commitment $\mathbf{c}$ so that its size may be $< n \cdot s$ and, depending on the size of $\mathbf{c}$, there may or not be a unique opening. Thereby, we distinguish two different cases:

Perfectly Binding Commitment: The commitment defines a unique vector $\mathbf{x} \in \mathbb{Z}_q^n$. It must hold that $|\mathbf{c}| \geq n \log q = \Omega(n)$.

Computationally Binding Commitment: In this case $\mathbf{c}$ can be opened to many values and it is possible that $|\mathbf{c}| = o(n)$.

In the second case it is not clear what a proof that the openings are in $\{0, 1\}$ means. For example, in the case of perfectly hiding commitments such as multi-Pedersen commitments – where a commitment to $\mathbf{x} \in \mathbb{Z}_q^n$ is $[c]_1 = \sum_{i \in [n]} x_i [g_i]_1 + r[g_{n+1}]_1 \in \mathbb{G}_1$ – each $[c]_1$ can be opened to any $\mathbf{x}' \in \mathbb{Z}_q^n$ since

$$[c]_1 = \sum_{i \in [n]} x'_i [g_i]_1 + \left(\left(c - \sum_{i \in [n]} x'_i g_i \right) g_{n+1}^{-1} \right) [g_{n+1}]_1$$

(in particular to 0 or 1) and thus the proof is trivial. Although it does makes sense to do a *proof of knowledge*, where one can extract a witness, we do not know how construct such proof system using only falsifiable assumptions.

For this reason, in [GHR15a] we first concentrated in the perfectly binding case, specifically Groth-Sahai commitments (and also other related perfectly-binding commitment scheme). We find two interesting applications of this proof system: more efficient signature schemes, with emphasis on the case of ring signatures, and more efficient threshold Groth-Sahai proofs.

Later, in [GR16], we tackle the computationally binding case for a commitment scheme which is an "hybrid" between multi-Pedersen commitments and Groth-Sahai commitments.

We call this commitment scheme *extended multi-Pedersen commitments*. What is interesting about extended multi-Pedersen commitments is that they can be perfectly hiding but they can also be perfectly binding at one (and only one) coordinate, depending on the the commitment key distribution. Furthermore, the different commitment key distributions are computationally indistinguishable and, thereby, one can randomly choose an index which remains hidden to the adversary such that b_i, the opening at coordinate i, is uniquely defined. Unlike the NIZK proof for multi-Pedersen commitment, our NIZK proof for extended multi-Pedersen commitments implies that $b_i \in \{0,1\}$ which is not trivially true.

Extended multi-Pedersen commitments bears some similarities with *somewhere statistically binding hashing* [HW15] and *vector commitments* [CF13]. See Section 4.2.1 for a more detailed comparison.

To exemplify the usefulness of extended multi-Pedersen commitments, we build a proof for the perfectly binding case. Given a perfectly binding commitment $[\mathbf{c}]_1$ to $\mathbf{b} \in \mathbb{Z}_q^n$ compute a proof that $\mathbf{b} \in \{0,1\}^n$ as follows:

1. Compute and extended multi-Pedersen commitment $[\mathbf{c}']_1$ to $(b_1, \ldots, b_n)$.
2. Show that $[\mathbf{c}]_1$ and $[\mathbf{c}']_1$ can be opened to the same value.
3. Show that $[\mathbf{c}']_1$ can be opened to and element from $\{0,1\}^n$.

Soundness follows from soundness of the proof from step 3 as follows. Suppose that $\mathbf{b} \notin \{0,1\}^n$, i.e. there is some i^* such that $b_{i^*} \notin \{0,1\}$. By choosing a random index i from $[n]$ and picking the commitments keys such that the extended multi-Pedersen commitments are perfectly binding at coordinate i, we have that with probability $1/n$, $i^* = i$. Given that $[\mathbf{c}]_1$ and $[\mathbf{c}']_1$ can be opened to the same value and the opening of $[\mathbf{c}']_1$ at coordinate i is uniquely defined, such opening must be equal to $b_{i^*} \notin \{0,1\}$ and we can break soundness of the proof from step 3 with probability at least $1/n$.

While we use essentially the same techniques from the perfectly binding case to build the proof system for the computationally binding case (step 3), this new approach can be applied to more diverse scenarios. Indeed, it is a key ingredient in Chapter 5 where we construct aggregated set-membership proofs and more efficient range proofs and proofs of correctness of a shuffle.

In Section 4.1 we describe our results for the perfectly binding case and the applications, and in Section 4.2 we describe our results for the computationally binding case.

4.1 The Perfectly Binding case

In this section we construct a constant-size proof that a perfectly binding commitment in $\mathbb{G}_1$ opens to an element of $\{0,1\}^n$. Such a construction was unknown even in symmetric bilinear groups (yet, it can be easily generalized to this setting [GHR15b, Appendix C]). More specifically, we prove membership in

$$\mathcal{L}_{ck,\mathsf{bits}} := \{[\mathbf{c}]_1 \in \mathbb{G}_1^{n+m} : \exists \mathbf{b} \in \{0,1\}^n, \mathbf{w} \in \mathbb{Z}_q^m \text{ s.t. } [\mathbf{c}]_1 := \mathsf{Com}_{ck}(\mathbf{b};\mathbf{w})\},$$

where $ck := ([\mathbf{U}_1]_1, [\mathbf{U}_2]_1) \in \mathbb{G}_1^{(n+m)\times n} \times \mathbb{G}_1^{(n+m)\times m}$ define a perfectly binding and computationally hiding commitment to $\mathbf{b}$ which is computed as $\mathsf{Com}_{ck}(\mathbf{b};\mathbf{w}) := [\mathbf{U}_1]_1\mathbf{b} + [\mathbf{U}_2]\mathbf{w}$. Specifically, we give instantiations for $m = 1$ (when $[\mathbf{c}]_1$ is a single commitment to $\mathbf{b}$), and $m = n$ (when $[\mathbf{c}]_1$ is the concatenation of n Groth-Sahai commitments).

We stress that although our proof is constant-size, we need the commitment to be perfectly binding, thus the size of the commitment is linear in n. The common reference string which we need for this construction is quadratic in the size of the bit-string. Our proof is compatible with proving linear statements about the bit-string, for instance, that $\sum_{i\in[n]} b_i = t$ by adding a linear number (in n) of elements to the CRS (see Section 4.1.5). We observe that in the special case where $t = 1$ the common reference string can be linear in n. The costs of our constructions and the cost of GS proofs are summarized in Table 4.1.

Our results rely solely on falsifiable assumptions. More specifically, in the asymmetric case we need some assumptions which are weaker than the symmetric external DH assumption plus the SSDP assumption. Interestingly, the translation of our construction to the symmetric setting relies on assumptions which are all weaker than the 2-Lin assumption [GHR15b, Appendix C].

We combine the QA-NIZK argument for $\mathcal{L}_{[\mathbf{M}]_1,[\mathbf{N}]_2,+}$ from Section 3.3 with decisional assumptions in $\mathbb{G}_1$ and $\mathbb{G}_2$. We do this with the purpose of using QA-NIZK arguments even when $\mathbf{M}+\mathbf{N}$ has full rank. In this case, strictly speaking "proving membership in the space" looses all meaning, as every vector in $\mathbb{G}_1^m \times \mathbb{G}_2^m$ is in the space. However, using decisional assumptions, we can argue that the generating matrix of the space is indistinguishable from a lower rank matrix which spans a subspace in which it is meaningful to prove membership.

Finally, in Section 4.1.6 we discuss some applications of our results. In particular, our results provide shorter signature size of several schemes, more efficient ring signatures, more efficient set membership proofs, and improved threshold GS proofs for pairing product equations.

	Comms	Proof	CK	CRS(ρ)	#Pairings
GS [GS08]	$(2n, 2n)$	$(4n, 4n)$	$(4, 4)$	0	$28n$
GS + $\Psi_{\mathsf{com}}(\overline{\mathcal{D}}_k)$	$(2n, 2n)$	$(2n+2, 2n+2)$	$(4, 4)$	$(10n+4,$ $10n+4)$	$20n+8$
Π_{bit} $m = 1$	$(n+1, 0)$	$(10, 10)$	$(n+1, 0)$	$(6n^2+11n+34,$ $6n^2+11n+34)$	$n+55$
Π_{bit} $m = n$ (i)	$(2n, 0)$	$(10, 10)$	$(4, 0)$	$(12n^2+14n+22,$ $12n^2+13n+24)$	$2n+52$
Π_{bit} $m = n$ (ii)	$(2n, 0)$	$(10, 10)$	$(4, 0)$	$(6n^2+16n+32,$ $6n^2+12n+32)$	$4n+52$
Π_{bit} weight 1, $m = 1$	$(n+1, 0)$	$(10, 10)$	$(n+1, 0)$	$(18n+32,$ $19n+34)$	$n+55$
Π_{bit} weight 1, $m = n$	$(2n, 0)$	$(10, 10)$	$(4, 0)$	$(20n+32,$ $18n+32)$	$4n+52$

Table 4.1: Comparison for proofs of membership in $\mathcal{L}_{ck,\mathsf{bits}}$ between GS proofs and our different constructions. Our NIZK construction for bit-strings is denoted by Π_{bit} and the construction for proving that two sets of commitments open to the same value $\Psi_{\mathsf{com}}(\overline{\mathcal{D}}_k)$. Row "$\Pi_{\mathsf{bit}}$ $m = 1$" is for our construction for a single commitment of size $n+1$ to a bit-string of size n. Rows "Π_{bit} $m = n$ (i)" and "Π_{bit} $m = n$ (ii)" are for our construction for n concatenated GS commitments, using the two different CRS distributions described in Section 4.1.2. Rows "Π_{bit} weight 1, $m = 1$" and "Π_{bit} weight 1, $m = n$" are for our constructions for bit-strings of weight 1 with $m = 1$ and $m = n$, respectively. Column "Comms" contains the size of the commitments, "CK" the size of the commitment keys in the CRS, and "CRS(ρ)" the size of the language dependent part of the CRS. Notation (a, b) means a elements of $\mathbb{G}_1$ and b elements of $\mathbb{G}_2$. The table is computed for $\mathcal{D}_k = \mathcal{L}_2$, the 2-Linear matrix distribution.

4.1.1 Intuition

To prove that a commitment in $\mathbb{G}_1$ opens to a vector of bits $\mathbf{b}$, the usual strategy is to compute another commitment $[\mathbf{d}]_2 \in \mathbb{G}_2^{\bar{n}}$ to a vector $\bar{\mathbf{b}} \in \mathbb{Z}_q^n$ and prove (1) $b_i(\bar{b}_i - 1) = 0$, for all $i \in [n]$, and (2) $b_i - \bar{b}_i = 0$, for all $i \in [n]$. For statement (2), since $[\mathbf{U}]_1$ is witness samplable, we can use our most efficient QA-NIZK from Section 3.4 for equal opening in different groups. Under the SSDP assumption, which is the $\mathsf{SKerMDH}$ assumption of minimal size conjectured to hold in asymmetric groups, the proof is of size $2(|\mathbb{G}_1| + |\mathbb{G}_2|)$. Thus, the challenge is to aggregate n equations of the form $b_i(\bar{b}_i - 1) = 0$. We note that this is a particular case of the problem of aggregating proofs of quadratic equations, which was left open in [JR14].

We finally remark that the proof must include $[\mathbf{d}]_2$ and thus it may be not of size independent of n. However, it turns out that $[\mathbf{d}]_2$ needs not be perfectly binding, in fact $\bar{n} = 2$ suffices.

Our Approach

A prover wanting to show satisfiability of the equation $\mathsf{x}(\mathsf{y} - 1) = 0$ using GS proofs, will commit to a solution $\mathsf{x} = b$ and $\mathsf{y} = \bar{b}$ as $[\mathbf{c}]_1 = b[\mathbf{u}_1]_1 + r[\mathbf{u}_2]_1$ and $[\mathbf{d}]_2 = \bar{b}[\mathbf{v}_1]_2 + s[\mathbf{v}_2]_2$, for $r, s \leftarrow \mathbb{Z}_q$, and then give a pair $([\boldsymbol{\theta}]_1, [\boldsymbol{\pi}]_2) \in \mathbb{G}_1^2 \times \mathbb{G}_2^2$ which satisfies the following verification equation[1]:

$$[\mathbf{c}]_1 \left([\mathbf{d}]_2 - [\mathbf{v}_1]_2\right)^\top = [\mathbf{u}_2]_1[\boldsymbol{\pi}^\top]_2 + [\boldsymbol{\theta}]_1[\mathbf{v}_2^\top]_2. \tag{4.1}$$

The reason why this works is that, if we express both sides of the equation in the basis of $\mathbb{G}_T^{2\times 2}$ given by $\{[\mathbf{u}_1]_1[\mathbf{v}_1^\top]_2, [\mathbf{u}_2]_1[\mathbf{v}_1^\top]_2, [\mathbf{u}_1]_1[\mathbf{v}_2^\top]_2, [\mathbf{u}_2]_1[\mathbf{v}_2^\top]_2\}$, the coefficient of $[\mathbf{u}_1]_1[\mathbf{v}_1^\top]_2$ is $b(\bar{b}-1)$ on the left side and 0 on the right side (regardless of $([\boldsymbol{\theta}]_1, [\boldsymbol{\pi}]_2)$). Our observation is that the verification equation can be abstracted as saying:

$$[\mathbf{c}]_1 \left([\mathbf{d}]_2 - [\mathbf{v}_1]_2\right)^\top \in \mathsf{Span}([\mathbf{u}_2]_1[\mathbf{v}_1^\top]_2, [\mathbf{u}_1]_1[\mathbf{v}_2^\top]_2, [\mathbf{u}_2]_1[\mathbf{v}_2^\top]_2) \subset \mathbb{G}_T^{2\times 2}. \tag{4.2}$$

Now consider commitments to $(b_1, \ldots, b_n)$ and $(\bar{b}_1, \ldots, \bar{b}_n)$ constructed with some commitment key $\{([\mathbf{g}_i]_1, [\mathbf{h}_i]_2) : i \in [n+1]\} \subset \mathbb{G}_1^{\bar{n}} \times \mathbb{G}_2^{\bar{n}}$, for some $\bar{n} \in \mathbb{N}$, to be determined later, and defined as $[\mathbf{c}]_1 := \sum_{i\in[n]} b_i[\mathbf{g}_i]_1 + r[\mathbf{g}_{n+1}]_1$, $[\mathbf{d}]_2 := \sum_{i\in[n]} \bar{b}_i[\mathbf{h}_i]_2 + s[\mathbf{h}_{n+1}]_2$, $r, s \leftarrow \mathbb{Z}_q$. Suppose for a moment that $\{[\mathbf{g}_i]_1[\mathbf{h}_j^\top]_2 : i, j \in [n+1]\}$ is a set of linearly independent vectors. Then,

$$[\mathbf{c}]_1 \left([\mathbf{d}^\top]_2 - \sum_{j\in[n]} [\mathbf{h}_j^\top]_2\right) \in \mathbf{Span}\{[\mathbf{g}_i]_1[\mathbf{h}_j^\top]_2 : i \neq j \text{ when } i, j \neq n+1\} \tag{4.3}$$

if and only if $b_i(\bar{b}_i - 1) = 0$ for all $i \in [n]$, because $b_i(\bar{b}_i - 1)$ is the coordinate of $[\mathbf{g}_i]_1[\mathbf{h}_i^\top]_2$ in the left side of the equation.

Equation 4.3 suggests to use one of the constant-size QA-NIZK arguments for linear spaces to get a constant-size proof that $b_i(\bar{b}_i - 1) = 0$ for all $i \in [n]$. [2]Unfortunately, these arguments are only defined for membership in subspaces in $\mathbb{G}_1^m$ or $\mathbb{G}_2^m$ but not in $\mathbb{G}_T^m$. Our solution is to include information in the CRS to "bring back" this statement from $\mathbb{G}_T$ to $\mathbb{G}_1$, i.e. the matrices $[\mathbf{C}_{i,j}]_1 := [\mathbf{g}_i]_1\mathbf{h}_j^\top$, where $i \neq j$ when $i, j \neq n+1$. We denote this set of matrices as $\mathcal{C} := \{[\mathbf{C}_{i,j}]_1 : i \neq j \text{ when } i, j \neq n+1\}$. Then, to prove that $b_i(\bar{b}_i - 1) = 0$ for all $i \in [n]$, the prover computes $[\boldsymbol{\Theta}]_1$ as a linear combination (with coefficients which

[1] For readers familiar with the Groth-Sahai notation, equation (4.1) corresponds to $\mathbf{c} \bullet (\mathbf{d} - \iota_2(1)) = \mathbf{u}_2 \bullet \boldsymbol{\pi} + \boldsymbol{\theta} \bullet \mathbf{v}_2$.

[2] We identify matrices in $\mathbb{G}_1^{a\times b}$ (resp. in $\mathbb{G}_2^{a\times b}$) with vectors in $\mathbb{G}_1^{ab}$ (resp. in $\mathbb{G}_2^{ab}$).

depend on $\mathbf{b}, \overline{\mathbf{b}}, r, s$) of the matrices in $\mathcal{C}$. Then the verifier checks that

$$[\mathbf{c}]_1 \left([\mathbf{d}]_2 - \sum_{j \in [n]} [\mathbf{h}_j]_2 \right)^\top = [\mathbf{\Theta}]_1 [\mathbf{I}_{\overline{n}}]_2, \tag{4.4}$$

and finally the prover gives a QA-NIZK proof of $[\mathbf{\Theta}]_1 \in \mathsf{Span}(\mathcal{C})$.

This reasoning assumes that $\{[\mathbf{g}_i]_1 \mathbf{h}_j^\top\}$ (or equivalently, $\{[\mathbf{C}_{i,j}]_1\}$) are linearly independent, which can only happen if $\overline{n} \geq n + 1$. If that is the case, the proof size cannot be constant because $[\mathbf{\Theta}]_1 \in \mathbb{G}_1^{\overline{n} \times \overline{n}}$ and this matrix is part of the proof. Instead, we choose $\mathbf{g}_1, \ldots, \mathbf{g}_{n+1} \in \mathbb{G}_1^2$ and $\mathbf{h}_1, \ldots, \mathbf{h}_{n+1} \in \mathbb{G}_2^2$, so that $\{[\mathbf{C}_{i,j}]_1\} \subseteq \mathbb{G}_1^{2\times 2}$. Intuitively, this should still work because the prover receives these vectors as part of the CRS and he does not know their discrete logarithms, so to him, they behave as linearly independent vectors.

Nevertheless, the statement $[\mathbf{\Theta}]_1 \in \mathbf{Span}(\mathcal{C})$ seems no longer meaningful, as $\mathbf{Span}(\mathcal{C})$ is all of $\mathbb{G}_1^{2\times 2}$ with overwhelming probability. But this is not the case, because by means of decisional assumptions in $\mathbb{G}_1$ and in $\mathbb{G}_2$, we switch to a game where the matrices $[\mathbf{C}_{i,j}]_1$ span a non-trivial space of $\mathbb{G}_1^{2\times 2}$. Specifically, to a game where $[\mathbf{C}_{i^*,i^*}]_1 \notin \mathbf{Span}(\mathcal{C})$, were i^* is a random integer in $[n]$ which remains hidden to the adversary. Once we are in such a game, perfect soundness is guaranteed for equation $b_{i^*}(\bar{b}_{i^*} - 1) = 0$ and a cheating adversary is caught with probability at least $1/n$. We think this technique might be of independent interest.

The last obstacle is that, using decisional assumptions on the set of vectors $\{[\mathbf{h}_j]_2\}_{j \in [n+1]}$ is incompatible with using the discrete logarithms of $[\mathbf{h}_j]_2$ to compute the matrices $[\mathbf{C}]_{1_{i,j}} := [\mathbf{g}_i]_1 \mathbf{h}_j^\top$ given in the CRS. To account for the fact that, in some games, we only know $\mathbf{g}_i \in \mathbb{Z}_q$ and, in some others, only $\mathbf{h}_j \in \mathbb{Z}_q$, we replace each matrix $[\mathbf{C}_{i,j}]_1$ by a pair $([\mathbf{C}_{i,j}]_1, [\mathbf{D}_{i,j}]_2)$ which is uniformly distributed conditioned on $\mathbf{C}_{i,j} + \mathbf{D}_{i,j} = \mathbf{g}_i \mathbf{h}_j^\top$. This randomization completely hides the group in which we can compute $\mathbf{g}_i \mathbf{h}_j^\top$. Finally, we use our QA-NIZK argument for sum in a subspace (Section 3.3) to prove membership in this space.

4.1.2 Instantiations

We discuss in detail two particular cases of languages $\mathcal{L}_{ck,\mathsf{bits}}$. First, in Section 4.1.3 we discuss the case when

(a) $[\mathbf{c}]_1$ is a vector in $\mathbb{G}_1^{n+1}$, $\mathbf{u}_{n+1} \leftarrow \mathcal{L}_{n+1,1}$ and $\mathbf{U}_1 := \begin{pmatrix} \mathbf{I}_{n\times n} \\ \mathbf{0}_{1\times n} \end{pmatrix} \in \mathbb{Z}_q^{(n+1)\times n}, \mathbf{U}_2 := \mathbf{u}_{n+1} \in \mathbb{Z}_q^{n+1}$, $\mathbf{U} := (\mathbf{U}_1 | \mathbf{U}_2)$.

In this case, the vectors $[\mathbf{g}_i]_1$ in the intuition are defined as $[\mathbf{g}_i]_1 = \mathbf{\Delta}[\mathbf{u}_i]_1$, where $\mathbf{\Delta} \leftarrow \mathbb{Z}_q^{2\times(n+1)}$, and the commitment to $\mathbf{b}$ is computed as $[\mathbf{c}]_1 := \sum_{i\in[n]} b_i [\mathbf{u}_i]_1 + w[\mathbf{u}_{n+1}]_1$. Then in Section 4.1.5 we discuss how to generalize the construction for a) to

(b) $[\mathbf{c}]_1$ is the concatenation of n GS commitments. That is, given the GS CRS $\mathsf{crs}_{\mathsf{GS}} = (gk, [\mathbf{u}_1]_1, [\mathbf{u}_2]_1, [\mathbf{v}_1]_2, [\mathbf{v}_2]_2)$, we define,

$$\mathbf{U}_1 := \begin{pmatrix} \mathbf{u}_1 & \ldots & \mathbf{0} \\ \vdots & \ddots & \vdots \\ \mathbf{0} & \ldots & \mathbf{u}_1 \end{pmatrix} \in \mathbb{Z}_q^{2n\times n}, \mathbf{U}_2 := \begin{pmatrix} \mathbf{u}_2 & \ldots & \mathbf{0} \\ \vdots & \ddots & \vdots \\ \mathbf{0} & \ldots & \mathbf{u}_2 \end{pmatrix} \in \mathbb{Z}_q^{2n\times n}.$$

Although the proof size is constant, in both of our instantiations the commitment size is $\Theta(n)$. Specifically, $(n+1)|\mathbb{G}_1|$ for case a) and $2n|\mathbb{G}_1|$ for case b).

4.1.3 The Scheme

$\mathsf{K}(gk, [\mathbf{U}]_1)$**:** Let $\mathbf{h}_{n+1} \leftarrow \mathbb{Z}_q^2$ and for all $i \in [n]$, $\mathbf{h}_i := \epsilon_i \mathbf{h}_{n+1}$, where $\epsilon_i \leftarrow \mathbb{Z}_q$. Define $[\mathbf{H}]_2 := ([\mathbf{h}_1]_2 | \dots | [\mathbf{h}_{n+1}]_2)$. Choose $\mathbf{\Delta} \leftarrow \mathbb{Z}_q^{2\times(n+1)}$, define $[\mathbf{G}]_1 := \mathbf{\Delta}[\mathbf{U}]_1$ and $[\mathbf{g}_i]_1 := \mathbf{\Delta}[\mathbf{u}_i]_1 \in \mathbb{G}_1^2$, for all $i \in [n+1]$. Let $\mathbf{a} \leftarrow \mathcal{L}_1$ and define $[\mathbf{a}_\Delta]_2 := \mathbf{\Delta}^\top [\mathbf{a}]_2 \in \mathbb{G}_2^{n+1}$. For any pair $(i,j) \in \mathcal{I}_{n,1}$ (as defined in Section 2.1), let $\mathbf{T}_{i,j} \leftarrow \mathbb{Z}_q^{2\times 2}$ and set:

$$[\mathbf{C}_{i,j}]_1 := [\mathbf{g}_i]_1 \mathbf{h}_j^\top - [\mathbf{T}_{i,j}]_1 \in \mathbb{G}_1^{2\times 2}, \qquad [\mathbf{D}_{i,j}]_2 := [\mathbf{T}_{i,j}]_2 \in \mathbb{G}_2^{2\times 2}.$$

Note that $[\mathbf{C}_{i,j}]_1$ can be efficiently computed as $\mathbf{h}_j \in \mathbb{Z}_q^2$ is the vector of discrete logarithms of $[\mathbf{h}_j]_1$.

Let Ψ_{sum} be the proof system for sum in subspace (Section 3.3) and Ψ_{com} be an instance of the proof system for equal opening (Section 3.4).

Let $\mathsf{crs}_{\Psi_{\mathsf{sum}}} \leftarrow \mathsf{K}_1(gk, \{[\mathbf{C}_{i,j}]_1, [\mathbf{D}_{i,j}]_2 : (i,j) \in \mathcal{I}_{n,1}\})$ and $\mathsf{crs}_{\Psi_{\mathsf{com}}} \leftarrow \mathsf{K}_1(gk, [\mathbf{G}]_1, [\mathbf{H}]_2, n)$. The common reference string is given by:

$$\begin{aligned} \mathsf{crs}_P &:= \left([\mathbf{U}]_1, [\mathbf{G}]_1, [\mathbf{H}]_1, \{[\mathbf{C}_{i,j}]_1, [\mathbf{D}_{i,j}]_2 : (i,j) \in \mathcal{I}_{n,1}\}, \mathsf{crs}_{\Psi_{\mathsf{sum}}}, \mathsf{crs}_{\Psi_{\mathsf{com}}}\right), \\ \mathsf{crs}_V &:= \left([\mathbf{a}]_2, [\mathbf{a}_\Delta]_2, \mathsf{crs}_{\Psi_{\mathsf{sum}}}, \mathsf{crs}_{\Psi_{\mathsf{com}}}\right). \end{aligned}$$

$\mathsf{P}(\mathsf{crs}_P, [\mathbf{c}]_1, \langle \mathbf{b}, w_g \rangle)$**:** Pick $w_h \leftarrow \mathbb{Z}_q$, $\mathbf{R} \leftarrow \mathbb{Z}_q^{2\times 2}$ and then:

1. Define
$$[\mathbf{c}_\Delta]_1 := [\mathbf{G}]_1 \begin{pmatrix} \mathbf{b} \\ w_g \end{pmatrix}, \qquad [\mathbf{d}]_2 := [\mathbf{H}]_2 \begin{pmatrix} \mathbf{b} \\ w_h \end{pmatrix}.$$

2. Compute $([\mathbf{\Theta}]_1, [\mathbf{\Pi}]_2) :=$
$$\begin{aligned} &\sum_{i\in[n]} \left(b_i w_h([\mathbf{C}_{i,n+1}]_1, [\mathbf{D}_{i,n+1}]_2) + w_g(b_i - 1)([\mathbf{C}_{n+1,i}]_1, [\mathbf{D}_{n+1,i}]_2)\right) \\ &+ \sum_{i\in[n]} \sum_{\substack{j\in[n] \\ j\neq i}} b_i(b_j - 1)([\mathbf{C}_{i,j}]_1, [\mathbf{D}_{i,j}]_2) \\ &+ w_g w_h([\mathbf{C}_{n+1,n+1}]_1, [\mathbf{D}_{n+1,n+1}]_2) + ([\mathbf{R}]_1, -[\mathbf{R}]_2). \end{aligned} \tag{4.5}$$

3. Compute a proof π_{sum} that $\mathbf{\Theta} + \mathbf{\Pi}$ belongs to the space spanned by $\{\mathbf{C}_{i,j} + \mathbf{D}_{i,j} : (i,j) \in \mathcal{I}_{n,1}\}$, and a proof π_{com} that $([\mathbf{c}_\Delta]_1, [\mathbf{d}]_2)$ open to the same value, using $\mathbf{b}, w_g$, and w_h.

$\mathsf{V}(\mathsf{crs}_V, [\mathbf{c}]_1, [\mathbf{c}_\Delta]_1, [\mathbf{d}]_2, ([\mathbf{\Theta}]_1, [\mathbf{\Pi}]_2), \pi_{\mathsf{sum}}, \pi_{\mathsf{com}})$**:**

1. Check if $[\mathbf{c}]_1^\top [\mathbf{a}_\Delta]_2 = [\mathbf{c}_\Delta]_1^\top [\mathbf{a}]_2$.

2. Check if
$$[\mathbf{c}_\Delta]_1 \left([\mathbf{d}]_2 - \sum_{j\in[n]} [\mathbf{h}_j]_2 \right)^\top = [\mathbf{\Theta}]_1 [\mathbf{I}_{2\times 2}]_2 + [\mathbf{I}_{2\times 2}]_1 [\mathbf{\Pi}]_2. \tag{4.6}$$

3. Verify that $\pi_{\mathsf{sum}}, \pi_{\mathsf{com}}$ are valid proofs for $([\mathbf{\Theta}]_1, [\mathbf{\Pi}]_2)$ and $([\mathbf{c}_\Delta]_1, [\mathbf{d}]_2)$ using Ψ_{sum} and Ψ_{com} respectively.

If any of these checks fails, the verifier outputs 0, else it outputs 1.

$\mathsf{S}_1(gk, [\mathbf{U}]_1)$: The simulator receives as input a description of an asymmetric bilinear group gk and a matrix $[\mathbf{U}]_1 \in \mathbb{G}_1^{(n+1)\times(n+1)}$ sampled according to distribution $\mathcal{D}_{gk}$. It generates and outputs the CRS in the same way as K_1, but additionally it also outputs the simulation trapdoor

$$\tau = (\mathbf{H}, \mathbf{\Delta}, \tau_{\Psi_{\mathsf{sum}}}, \tau_{\Psi_{\mathsf{com}}}),$$

where $\tau_{\Psi_{\mathsf{sum}}}$ and $\tau_{\Psi_{\mathsf{com}}}$ are, respectively, Ψ_{sum}'s and Ψ_{com}'s simulation trapdoors.

$\mathsf{S}_2(\mathsf{crs}_P, [\mathbf{c}]_1, \tau)$: Compute $[\mathbf{c}_\Delta]_1 := \mathbf{\Delta}[\mathbf{c}]_1$. Then pick random $\overline{w}_h \leftarrow \mathbb{Z}_q$, $\mathbf{R} \leftarrow \mathbb{Z}_q^{2\times 2}$ and define $\mathbf{d} := \overline{w}_h \mathbf{h}_{n+1}$. Then set:

$$[\mathbf{\Theta}]_1 := [\mathbf{c}_\Delta]_1 \left(\mathbf{d} - \sum_{i\in[n]} \mathbf{h}_i\right)^\top + [\mathbf{R}]_1, \qquad [\mathbf{\Pi}]_2 := -[\mathbf{R}]_2.$$

Finally, simulate proofs $\pi_{\mathsf{sum}}, \pi_{\mathsf{com}}$ using $\tau_{\Psi_{\mathsf{sum}}}$ and $\tau_{\Psi_{\mathsf{com}}}$.

4.1.4 Proof of Security

Theorem 4.1 *The proof system from Section 4.1.3 is QA-NIZK proof system for the language $\mathcal{L}_{ck,\mathsf{bits}}$ with perfect completeness, computational soundness, and perfect zero-knowledge*

Proof (Completeness.) It is obvious by definition that for any $[\mathbf{c}]_1 \in \mathcal{L}_{ck,\mathsf{bits}}$ the vector $[\mathbf{c}_\Delta]_1$ generated by an honest prover passes the verification test described in 1).

Note that, by definition of $[\mathbf{C}_{i,j}]_1$ and $[\mathbf{D}_{i,j}]_2$, $[\mathbf{C}_{i,j}]_1[\mathbf{I}_{2\times2}]_2 + [\mathbf{I}_{2\times2}]_1[\mathbf{D}_{i,j}]_2 = [\mathbf{g}_i]_1[\mathbf{h}_j^\top]_2$. Since $b_i(b_i-1) = 0$ for each $i \in [n]$,

$$\begin{aligned}
&[\mathbf{c}_\Delta]_1 \left([\mathbf{d}]_2 - \sum_{i\in[n]} [\mathbf{h}_i]_2\right)^\top \\
=&\sum_{i\in[n]} \left(b_i w_h [\mathbf{g}_i]_1[\mathbf{h}_{n+1}^\top]_2 + w_g(b_i-1)[\mathbf{g}_{n+1}]_1[\mathbf{h}_i^\top]_2 + \sum_{j\in[n]} b_i(b_j-1)[\mathbf{g}_i]_1[\mathbf{h}_j^\top]_2 \right) + \\
&w_g w_h [\mathbf{g}_{n+1}][\mathbf{h}_{n+1}^\top]_2 \\
=&\sum_{i\in[n]} \left(b_i w_h [\mathbf{g}_i]_1[\mathbf{h}_{n+1}^\top]_2 + w_g(b_i-1)[\mathbf{g}_{n+1}]_1[\mathbf{h}_i^\top]_2 + \sum_{\substack{j\in[n]\\ j\neq i}} b_i(b_j-1)[\mathbf{g}_i]_1[\mathbf{h}_j^\top]_2 \right) \\
&+ w_g w_h [\mathbf{g}_{n+1}]_1[\mathbf{h}_{n+1}^\top]_2 + [\mathbf{R}]_1[\mathbf{I}_{2\times2}]_2 - [\mathbf{I}_{2\times2}]_1[\mathbf{R}]_2 \\
=&[\mathbf{\Theta}]_1[\mathbf{I}_{2\times2}]_2 + [\mathbf{I}_{2\times2}]_1[\mathbf{\Pi}]_2.
\end{aligned}$$

Finally, the rest of the proof follows from completeness of Ψ_{com} and Ψ_{sum}.

(Soundness.) Soundness is proven in Theorem 4.2.

(Zero-Knowledge.) First, note that the vector $[\mathbf{d}]_2 \in \mathbb{G}_2^2$ output by the prover and the vector output by S_2 follow exactly the same distribution. This is because the rank of $[\mathbf{H}]_2$ is 1. In particular, although the simulator S_2 does not know the opening of $[\mathbf{c}]_1$, which is some $\mathbf{b} \in \{0,1\}^n$, there exists $w_h \in \mathbb{Z}_q$ such that $[\mathbf{d}]_2 = [\mathbf{H}]_2 \binom{\mathbf{b}}{w_h}$. Since $\mathbf{R}$ is chosen uniformly at random in $\mathbb{Z}_q^{2\times 2}$, the proof $([\mathbf{\Theta}]_1, [\mathbf{\Pi}]_2)$ is uniformly distributed conditioned on satisfying check 2) of algorithm V. Therefore, these elements of the simulated proof have the same distribution as in a real proof. This fact combined with the perfect zero-knowledge property of Ψ_{sum} and Ψ_{com} concludes the proof. □

Theorem 4.2 *Let $\mathsf{Adv}_{\mathcal{PS}}(\mathsf{A})$ be the advantage of an adversary A against the soundness of the proof system described above. There exist PPT adversaries $\mathsf{B}_1, \mathsf{B}_2, \mathsf{B}_3, \mathsf{P}_1^*, \mathsf{P}_2^*$ such that*

$$\begin{aligned}\mathsf{Adv}_{\mathcal{PS}}(\mathsf{A}) \quad \leq n \quad \big(6/q + \mathsf{Adv}_{\mathcal{U}_1,\mathbb{G}_1}(\mathsf{B}_1) + \mathsf{Adv}_{\mathcal{U}_1,\mathbb{G}_2}(\mathsf{B}_2) + \mathsf{Adv}_{\mathsf{SP}_{\mathbb{G}_2}}(\mathsf{B}_3) \\ + \mathsf{Adv}_{\Psi_{\mathsf{sum}}}(\mathsf{P}_1^*) + \mathsf{Adv}_{\Psi_{\mathsf{com}}}(\mathsf{P}_2^*)\big) .\end{aligned}$$

The proof follows from the indistinguishability of the following games:

Real This is the real soundness game. The output is 1 if the adversary breaks the soundness, i.e. the adversary submits some $[\mathbf{c}]_1 = [\mathbf{U}]_1 \left(\begin{smallmatrix}\mathbf{b}\\ wg\end{smallmatrix}\right)$, for some $\mathbf{b} \notin \{0,1\}^n$ and $w \in \mathbb{Z}_q$, and the corresponding proof which is accepted by the verifier.

Game_0 This game is identical to Real except that algorithm K does not receive $[\mathbf{U}]_1$ as a input but it samples $([\mathbf{U}]_1, \mathbf{U}) \in \mathcal{R}_{par}$ itself according to $\mathcal{D}_{gk}$.

Game_1 This game is identical to Game_0 except that the simulator picks a random $i^* \in [n]$, and uses $\mathbf{U}$ to check if the output of the adversary A is such that $b_{i^*} \in \{0,1\}$. It aborts if $b_{i^*} \in \{0,1\}$.

Game_2 This game is identical to Game_1 except that now the vectors $[\mathbf{g}_i]_1$, $i \in [n]$ and $i \neq i^*$, are uniform vectors in the space spanned by $[\mathbf{g}_{n+1}]_1$.

Game_3 This game is identical to Game_2 except that now the vector $[\mathbf{h}_{i^*}]_2$ is a uniform vector in $\mathbb{G}_2^2$, sampled independently of $[\mathbf{h}_{n+1}]_2$.

It is obvious that the first two games are indistinguishable. The rest of the argument goes as follows.

Lemma 4.3 $\Pr[\mathsf{Game}_1(\mathsf{A}) = 1] \geq \dfrac{1}{n} \Pr[\mathsf{Game}_0(\mathsf{A}) = 1]$.

Proof The probability that $\mathsf{Game}_1(\mathsf{A}) = 1$ is the probability that a) $\mathsf{Game}_0(\mathsf{A}) = 1$ and b) $b_{i^*} \notin \{0,1\}$. The view of adversary A is independent of i^*, while, if $\mathsf{Game}_0(\mathsf{A}) = 1$, then there is at least one index $\ell \in [n]$ such that such that $b_\ell \notin \{0,1\}$. Thus, the probability that the event described in b) occurs conditioned on $\mathsf{Game}_0(\mathsf{A}) = 1$, is greater than or equal to $1/n$ and the lemma follows. □

Lemma 4.4 *There exists a $\mathcal{U}_1$-$\mathsf{MDDH}_{\mathbb{G}_1}$ adversary B such that* $|\Pr[\mathsf{Game}_1(\mathsf{A}) = 1] - \Pr[\mathsf{Game}_2(\mathsf{A}) = 1]| \leq \mathsf{Adv}_{\mathcal{U}_1,\mathbb{G}_1}(\mathsf{B}) + 2/q$.

Proof The adversary B receives $([\mathbf{s}]_1, [\mathbf{t}]_1)$ an instance of the $\mathcal{U}_1$-$\mathsf{MDDH}_{\mathbb{G}_1}$ problem. B defines all the parameters honestly except that it embeds the $\mathcal{U}_1$-$\mathsf{MDDH}_{\mathbb{G}_1}$ challenge in the matrix $[\mathbf{G}]_1$.

Let $[\mathbf{E}]_1 := ([\mathbf{s}]_1 | [\mathbf{t}]_1)$. B picks $i^* \leftarrow [n]$, $\mathbf{W}_0 \leftarrow \mathbb{Z}_q^{2\times(i^*-1)}$, $\mathbf{W}_1 \leftarrow \mathbb{Z}_q^{2\times(n-i^*)}$, $[\mathbf{g}_{i^*}]_1 \leftarrow \mathbb{G}_1^2$, and defines $[\mathbf{G}]_1 := ([\mathbf{E}]_1\mathbf{W}_0 | [\mathbf{g}_{i^*}]_1 | [\mathbf{E}]_1\mathbf{W}_1 | [\mathbf{s}]_1)$. In the real algorithm K, the generator picks the matrix $\mathbf{\Delta} \in \mathbb{Z}_q^{2\times(n+1)}$. Although B does not know $\mathbf{\Delta}$, it can compute $[\mathbf{\Delta}]_1$ as $[\mathbf{\Delta}]_1 = [\mathbf{G}]_1\mathbf{U}^{-1}$, given that $\mathbf{U}$ is full rank and was sampled by B, so it can compute the rest of the elements of the common reference string using the discrete logarithms of $[\mathbf{U}]_1$, $[\mathbf{H}]_2$ and $[\mathbf{a}]_2$.

In case $[\mathbf{t}]_1$ is uniform over $\mathbb{G}_1^2$, by the Schwartz-Zippel lemma $\det([\mathbf{E}]_1) = 0$ with probability at most $2/q$. Thus, with probability at least $1 - 2/q$, the matrix $[\mathbf{E}]_1$ is full-rank and $[\mathbf{G}]_1$ is uniform over $\mathbb{G}_1^{2\times(n+1)}$ as in Game_1. On the other hand, in case $[\mathbf{t}]_1 = \gamma[\mathbf{s}]_1$, all of $[\mathbf{g}_i]_1$, $i \neq i^*$, are in the space spanned by $[\mathbf{g}_{n+1}]_1$ as in Game_2. □

Lemma 4.5 *There exists a $\mathcal{U}_1$-$\mathsf{MDDH}_{\mathbb{G}_2}$ adversary B such that* $|\Pr[\mathsf{Game}_2(\mathsf{A}) = 1] - \Pr[\mathsf{Game}_3(\mathsf{A}) = 1]| \leq \mathsf{Adv}_{\mathcal{U}_1,\mathbb{G}_2}(\mathsf{B})$.

Proof The adversary B receives an instance of the $\mathcal{U}_1$-$\mathsf{MDDH}_{\mathbb{G}_2}$ problem, which is a pair $([\mathbf{s}]_2, [\mathbf{t}]_2)$, where $[\mathbf{s}]_2$ is a uniform vector of $\mathbb{G}_2^2$ and $[\mathbf{t}]_2$ is either a uniform vector in $\mathbb{G}_2^2$ or $[\mathbf{t}]_2 = \gamma[\mathbf{s}]_2$, for random $\gamma \in \mathbb{Z}_q$.

Adversary B samples $\mu_i \leftarrow \mathbb{Z}_q, \mathbf{g}_{i^*}, \mathbf{g}_{n+1} \leftarrow \mathbb{Z}_q^2$ and defines $\mathbf{g}_i = \mu_i \mathbf{g}_{n+1}$, $i \neq i^*$. Then, defines $[\mathbf{h}_{n+1}]_2 := [\mathbf{s}]_2$ and honestly samples the rest of the columns of $[\mathbf{H}]_2$ with the sole exception of $[\mathbf{h}_{i^*}]_2$, which is set to $[\mathbf{t}]_2$.

Given that adversary B can only compute $\mathbf{g}_i[\mathbf{h}_j^\top]_2 \in \mathbb{G}_2^{2\times 2}$, it defines $[\mathbf{D}_{i,j}]_2 := \mathbf{g}_i[\mathbf{h}_j^\top]_2 - [\mathbf{T}_{i,j}]_2$ and $[\mathbf{C}_{i,j}]_1 := [\mathbf{T}_{i,j}]_1$, for $\mathbf{T}_{i,j} \leftarrow \mathbb{Z}_q^{2\times 2}$ and $(i, j) \in \mathcal{I}_{n,1}$. Note that this does not change the distribution of $([\mathbf{D}_{i,j}]_2, [\mathbf{C}_{i,j}]_1)$, which is the uniform one conditioned on $\mathbf{C}_{i,j} + \mathbf{D}_{i,j} = \mathbf{g}_i\mathbf{h}_j^\top$.

The rest of the parameters are computed using $\mathbf{a} \leftarrow \mathcal{L}_1$, the matrix $\mathbf{\Delta} \in \mathbb{Z}_q^{2\times(n+1)}$ and the discrete logarithms of $[\mathbf{G}]_1$. It is immediate to see that adversary B perfectly simulates Game_2 when $[\mathbf{t}]_2 = \gamma[\mathbf{s}]_2$ and Game_3 when $[\mathbf{t}]_2$ is uniform. □

Lemma 4.6 *There exists a $\mathsf{SP}_{\mathbb{G}_2}$ adversary B, a soundness adversary P_1^* for Ψ_{sum} and a strong soundness adversary P_2^* for Ψ_{com} such that*

$$\Pr[\mathsf{Game}_3(\mathsf{A}) = 1] \leq 4/q + \mathbf{Adv}_{\mathsf{SP}_{\mathbb{G}_2}}(\mathsf{B}) + \mathbf{Adv}_{\Psi_{\mathsf{sum}}}(\mathsf{P}_1^*) + \mathbf{Adv}_{\Psi_{\mathsf{com}}}(\mathsf{P}_2^*).$$

Proof $\Pr[\det((\mathbf{g}_{i^*}|\mathbf{g}_{n+1})) = 0] = \Pr[\det((\mathbf{h}_{i^*}|\mathbf{h}_{n+1})) = 0] \leq 2/q$, by the Schwartz-Zippel lemma. Then, with probability at least $1 - 4/q$, $\mathbf{g}_{i^*}\mathbf{h}_{i^*}^\top$ is linearly independent from $\{\mathbf{g}_i\mathbf{h}_j^\top : (i, j) \in [n+1]^2 \setminus \{(i^*, i^*)\}\}$ which implies that $\mathbf{g}_{i^*}\mathbf{h}_{i^*}^\top \notin \mathbf{Span}(\{\mathbf{C}_{i,j} + \mathbf{D}_{i,j} : (i, j) \in \mathcal{I}_{n,1}\})$. Additionally $\mathsf{Game}_3(\mathsf{A}) = 1$ implies that $b_{i^*} \notin \{0, 1\}$ while the verifier accepts the proof produced by A, which is $([\mathbf{c}_\Delta]_1, [\mathbf{d}]_2, ([\mathbf{\Theta}]_1, [\mathbf{\Pi}]_2), \pi_{\mathsf{sum}}, \pi_{\mathsf{com}})$. Since $\{[\mathbf{h}_{i^*}]_2, [\mathbf{h}_{n+1}]_2\}$ is a basis of $\mathbb{G}_2^2$, we can define $\overline{w}_h, \overline{b}_{i^*}$ as the unique coefficients in $\mathbb{Z}_q$ such that $[\mathbf{d}]_2 = \overline{b}_{i^*}[\mathbf{h}_{i^*}]_2 + \overline{w}_h[\mathbf{h}_{n+1}]_2$. We distinguish three cases:

1) If $[\mathbf{c}_\Delta]_1 \neq \mathbf{\Delta}[\mathbf{c}]_1$, we can construct an adversary B against the $\mathsf{SP}_{\mathbb{G}_2}$ assumption that outputs $[\mathbf{c}_\Delta]_1 - \mathbf{\Delta}[\mathbf{c}]_1 \in \ker([\mathbf{a}]_2^\top)$.

2) If $[\mathbf{c}_\Delta]_1 = \mathbf{\Delta}[\mathbf{c}]_1$ but $b_{i^*} \neq \overline{b}_{i^*}$. Given that $[\mathbf{c}]_1$ is perfectly binding and that $\overline{b}_{i^*} \neq b_{i^*}$ is the unique opening of $[\mathbf{c}_\Delta]_1$ at coordinate i^*, both commitments can not be opened to the same value. Therefore, the adversary P_2^* against the strong soundness of Ψ_{com} outputs π_{com} which is a fake proof for $([\mathbf{c}_\Delta]_1, [\mathbf{d}]_2)$. Note that strong soundness is required since, in order to compute $\{[\mathbf{C}_{i,j}]_1, [\mathbf{D}_{i,j}]_2 : (i, j) \in \mathcal{I}_{n,1}\}$, P_2^* requires the discrete logs of either $[\mathbf{G}]_1$ or $[\mathbf{D}]_2$.

3) If $[\mathbf{c}_\Delta]_1 = \mathbf{\Delta}[\mathbf{c}]_1$ and $b_{i^*} = \overline{b}_{i^*}$, then $b_{i^*}(\overline{b}_{i^*} - 1) \neq 0$. If we express $\mathbf{\Theta} + \mathbf{\Pi}$ as a linear combination of $\mathbf{g}_i\mathbf{h}_j^\top$, the coordinate of $\mathbf{g}_{i^*}\mathbf{h}_{i^*}^\top$ is $b_{i^*}(\overline{b}_{i^*} - 1) \neq 0$ and thus

$\boldsymbol{\Theta} + \boldsymbol{\Pi} \notin \mathbf{Span}(\{\mathbf{C}_{i,j} + \mathbf{D}_{i,j} : (i,j) \in \mathcal{I}_{n,1}\})$. The adversary P_1^* against Ψ_{sum} outputs π_{sum} which is a fake proof for $([\boldsymbol{\Theta}]_1, [\boldsymbol{\Pi}]_2)$. [3] □

4.1.5 Extensions

CRS Generation for Individual Commitments.

A natural way to extend our construction to individual commitments (distribution (b) from Section 4.1.2) is the following. The only change is that the matrix $\boldsymbol{\Delta}$ is sampled uniformly from $\mathbb{Z}_q^{2\times 2n}$ (the distribution of $[\mathbf{H}]_2$ is not changed). Thus, the matrix $[\mathbf{G}]_1 := \boldsymbol{\Delta}[\mathbf{U}]_1$ has $2n$ columns instead of $n+1$ and $[\mathbf{c}_\Delta]_1 := [\mathbf{G}]_1 \begin{pmatrix} \mathbf{b} \\ \mathbf{w}_g \end{pmatrix}$ for some $\mathbf{w}_g \in \mathbb{Z}_q^n$. In the soundness proof, the only change is that in Game_2, the extra columns are also changed to span a one-dimensional space, *i.e.* in this game $[\mathbf{g}_i]_1$, $i \in [2n-1]$ and $i \neq i^*$, are uniform vectors in the space spanned by $[\mathbf{g}_{2n}]_1$. With this approach, the proof size is still constant and the changes to the original construction are minimal but the CRS is considerably larger. Further, we do not know how to make the CRS linear for bit-strings of weight 1.

Therefore, we propose an alternative way to extend our result to individual commitments. In this new construction, the matrix $[\mathbf{G}]_1$ is independent from $[\mathbf{U}]_1$ and for all $i \in [n]$, $[\mathbf{g}_i]_1 = \mu_i[\mathbf{g}_{n+1}]_1$, $\mu_i \leftarrow \mathbb{Z}_q$ and $[\mathbf{g}_{n+1}]_1 \leftarrow \mathbb{Z}_q^2$.

The proof is defined in a slightly different way. Now one computes $[\mathbf{c}_\Delta]_1 := [\mathbf{G}]_1 \begin{pmatrix} \mathbf{b} \\ w'_g \end{pmatrix}$, $w'_g \leftarrow \mathbb{Z}_q$, and one proves that the three commitments, $[\mathbf{c}]_1, [\mathbf{c}_\Delta]_1, [\mathbf{d}]_2$ open to the same value. Intuitively, this replaces in the original construction the proofs that $\boldsymbol{\Delta}[\mathbf{c}]_1 = [\mathbf{c}_\Delta]_1$ and that $\boldsymbol{\Delta}[\mathbf{c}]_1$ and $[\mathbf{d}]_2$ open to the same value. More specifically, this is proven by showing that $(\begin{pmatrix} [\mathbf{c}]_1 \\ [\mathbf{c}_\Delta]_1 \end{pmatrix}, [\mathbf{d}]_2) \in \mathcal{L}_{[\mathbf{M}]_1,[\mathbf{N}]_2}$, where.

$$\mathbf{M} := \begin{pmatrix} \mathbf{U}_1 & \mathbf{U}_2 & \mathbf{0}_{2n\times 1} & \mathbf{0}_{2n\times 1} \\ \mathbf{G}_1 & \mathbf{0}_{2\times n} & \mathbf{g}_{n+1} & \mathbf{0}_{2\times 1} \end{pmatrix} \text{ and } \mathbf{N} := \begin{pmatrix} \mathbf{H}_1 & \mathbf{0}_{2\times n} & \mathbf{0}_{2\times 1} & \mathbf{h}_{n+1} \end{pmatrix}.$$

The advantage of this alternative approach is that the matrix $[\mathbf{G}]_1$ has now $n+1$ columns as in the original construction as opposed to $2n$ in the first extension to individual commitments.

The proof of soundness must be modified in the following way. In the proof of Lemma 7.7 one sets $[\mathbf{g}_{n+1}]_1 := [\mathbf{s}]_1$ and $[\mathbf{g}_{i^*}]_1 := [\mathbf{t}]_1$, similarly as done in Lemma 4.5. This guarantees that, as in the original construction, in the last game $[\mathbf{g}_{i^*}]_1$ (resp. $[\mathbf{h}_{i^*}]_2$) is linearly independent of the rest of columns of $[\mathbf{G}]_1$ (resp. $[\mathbf{H}]_2$). In the last game we need to show that $[\mathbf{c}_\Delta]_1 = b_{i^*}[\mathbf{g}_{i^*}]_1 + \tilde{w}_g[\mathbf{g}_{n+1}]_1$ and $[\mathbf{d}]_2 = b_{i^*}[\mathbf{h}_{i^*}]_2 + \tilde{w}_h[\mathbf{h}_{n+1}]_2$, for some $\tilde{w}_g, \tilde{w}_h \in \mathbb{Z}_q$ and that $b_{i^*} \in \{0,1\}$. Note that the fact that $(\begin{pmatrix} [\mathbf{c}]_1 \\ [\mathbf{c}_\Delta]_1 \end{pmatrix}, [\mathbf{d}]_2) \in \mathcal{L}_{[\mathbf{M}]_1,[\mathbf{N}]_2}$ implies that there is some $\boldsymbol{\gamma} \in \mathbb{Z}_q^{2n+2}$ such that $\begin{pmatrix} [\mathbf{c}]_1 \\ [\mathbf{c}_\Delta]_1 \\ [\mathbf{d}]_2 \end{pmatrix} = \begin{pmatrix} [\mathbf{M}]_1 \\ [\mathbf{N}]_2 \end{pmatrix} \boldsymbol{\gamma}$, and the fact that $[\mathbf{c}]_1$ is perfectly binding together with the form of $[\mathbf{M}]_1, [\mathbf{N}]_2$ implies that $\boldsymbol{\gamma} = \begin{pmatrix} \mathbf{b} \\ \gamma' \end{pmatrix}$. In particular, $[\mathbf{c}_\Delta]_1 = [\mathbf{G}]_1 \begin{pmatrix} \mathbf{b} \\ \gamma_{2n+1} \end{pmatrix} = b_{i^*} + \tilde{w}_g[\mathbf{g}_{n+1}]_1$ and $[\mathbf{d}]_2 = [\mathbf{H}]_2 \begin{pmatrix} \mathbf{b} \\ \gamma_{2n+2} \end{pmatrix} = b_{i^*}[\mathbf{h}_{i^*}]_2 + \tilde{w}_h[\mathbf{h}_{n+1}]_2$ for some

[3] The proof system Ψ_{sum} is constructed for matrices $\{(\mathbf{C}_{i,j}, \mathbf{D}_{i,j}) : (i,j) \in \mathcal{I}_{n,1}\}$ sampled from some distribution $\mathcal{D}_{gk}$, which in this case depends on the distribution of $\mathbf{G}$ and $\mathbf{H}$. We assume that the adversary P_2^* against Ψ_{sum} receives the common reference string of Ψ_{sum} as described in Section 3.3 and additionally the matrices $[\mathbf{G}]_1$ and $[\mathbf{H}]_2$ which defines the language, i.e. the distribution of $\mathbf{C}_{i,j}$, $\mathbf{D}_{i,j}$ (this is necessary so that P_2^* can simulate the crs for adversary A). We stress this additional information to describe the language does not affect the soundness proof for Theorem 3.1 (in particular, $[\mathbf{G}]_1$ and $[\mathbf{H}]_2$ are independent of $(\boldsymbol{\Lambda}, \boldsymbol{\Xi})$).

unique b_{i^*}. To conclude the proof of soundness we just need to argue that $b_{i^*} \neq \{0,1\}$, leads to a contradiction. This follows from the same argument as the original proof.

For zero-knowledge, observe that $[\mathbf{c}_\Delta]_1$ is just a uniform vector in $\mathbf{Span}([\mathbf{g}_{n+1}]_1)$. The simulator just picks a random $[\mathbf{c}_\Delta]_1$ and simulates the proof that $\left(\left(\begin{smallmatrix}[\mathbf{c}]_1\\ [\mathbf{c}_\Delta]_1\end{smallmatrix}\right), [\mathbf{d}]_2\right) \in \mathcal{L}_{[\mathbf{M}]_1,[\mathbf{N}]_2}$ with the appropriate trapdoor. The rest of the proof is identical to the simulated proof in the original construction.

Linear Equations Satisfied by Bit-Strings

Because of the homomorphic properties of the commitments, we can easily extend it to prove that the bit-string $\mathbf{b}$ satisfies $\sum_{i\in[n]} \beta_i b_i = t$, for some $\boldsymbol{\beta} \in \mathbb{Z}_q^n, t \in \mathbb{Z}_q$. If the commitment $[\mathbf{c}]_1$ is a concatenation of GS commitments to b_i, this can be done in the usual way with GS proofs. But if $\mathbf{U}$ is drawn from distribution (a) (see Section 4.1.2) this can also be done as follows. Define $\mathbf{B} := \left(\begin{smallmatrix}\beta_1 & \dots & \beta_n & 0\\ 0 & \dots & 0 & 1\end{smallmatrix}\right) \in \mathbb{Z}_q^{2\times(n+1)}$. We claim the following:

$$\mathbf{B}[\mathbf{c}]_1 - t[\mathbf{e}_1^2] \in \mathbf{Span}\left(\mathbf{B}[\mathbf{u}_{n+1}]_1\right) \Leftrightarrow \sum_{i\in[n]} \beta_i b_i = t.$$

This is justified because $\mathbf{B}\mathbf{u}_i = \mathbf{B}\mathbf{e}_i^{n+1} = \beta_i \mathbf{e}_1^2$, and then $\mathbf{B}\mathbf{c} - t\mathbf{e}_1^2 = w\mathbf{B}\mathbf{u}_{n+1} + \sum_{i\in[n]} b_i \mathbf{B}\mathbf{u}_i - t\mathbf{e}_1^2 = w\mathbf{B}\mathbf{u}_{n+1} + \left(\sum_{i\in[n]} \beta_i b_i - t\right)\mathbf{e}_1^2$. So to be able to prove that $\sum_{i\in[n]} \beta_i b_i = t$, we just need to add to the CRS the necessary elements to prove membership in $\mathcal{L}_{B[\mathbf{u}_{n+1}]_1} := \{[\mathbf{x}]_1 \in \mathbb{G}_1^2 : \exists w \in \mathbb{Z}_q, \mathbf{x} = w\mathbf{B}\mathbf{u}_{n+1}\}$ using one of the constructions of Section 2.7.

Bit-Strings of Weight 1

In the special case when the bit-string has only one 1 (this case is useful in some applications, see Section 4.1.6), the size of the CRS can be made linear in n, instead of quadratic. To prove this statement we would combine our proof system for bit-strings of Section 4.1.3 and a proof that $\sum_{i\in[n]} b_i = 1$ as described above when $m = 1$ or using GS-proofs when $m = n$. In the definition of $(\boldsymbol{\Theta}, \boldsymbol{\Pi})$ in Eq. 4.5, one sees that for all pairs $(i,j) \in [n] \times [n]$, the coefficient of $(\mathbf{C}_{i,j}, \mathbf{D}_{i,j})$ is $b_i(b_j - 1)$. If i^* is the only index such that $b_{i^*} = 1$, then we have:

$$\sum_{i\in[n]}\sum_{j\in[n]} b_i(b_j-1)(\mathbf{C}_{i,j}, \mathbf{D}_{i,j}) = \sum_{j\neq i^*}(\mathbf{C}_{i^*,j}, \mathbf{D}_{i^*,j}) =: (\mathbf{C}_{i^*,\neq}, \mathbf{D}_{i^*,\neq}).$$

Therefore, one can replace in the CRS the pairs of matrices $(\mathbf{C}_{i,j}, \mathbf{D}_{i,j})$ by $(\mathbf{C}_{i,\neq}, \mathbf{D}_{i,\neq})$, $i \in [n]$. The resulting CRS is linear in n.

4.1.6 Applications

Many protocols use proofs that a commitment opens to a bit-string as a building block. Since our commitments are still of size $\Theta(n)$, our results may not apply to some of these protocols. Yet, there are several applications where bits need to be used independently and our results provide significant improvements. Table 4.2 summarizes them.

Signatures

There are many signature schemes where a proof that some vector of integers is a bit-string is useful [BFPV11, BPV12, Cam13, EHM11]. For example, in the revocable attribute-based signature scheme of Escala *et. al* [EHM11], every signature includes a proof that a set of GS commitments, whose size is the number of attributes, opens to a bit-string.

Further, the set membership proof discussed below can also be used to reduce the size of the ring signature scheme of Chandran et al. [CGS07], which is the most efficient ring signature in the standard model. Indeed, to sign a message m, among other things, the signer picks a one-time signature key and certifies the one-time verification key by signing it with a Boneh-Boyen signature under vk_α. Then, the signer commits to vk_α and shows that vk_α belongs to the set of Boneh-Boyen verification keys $(vk_1, \ldots, vk_n)$ of the parties in the ring R.

Proof System	Author	Proof Size
Threshold GS	Ràfols [Ràf15] (1)	$(m_x + 3(n-t) + 2\bar{n}, 0)$
	Ràfols [Ràf15] (2)	$2(n-t+1, n)$
	This work	$(2n+12, 10)$
Set-Membership proof (Ring Signature)	Chandran et al. [CGS07]	$(16\sqrt{n}+4, 16\sqrt{n}+4)$
	Ràfols [Ràf15]	$(8\sqrt{n}+6, 12\sqrt{n})$
	This work	$(4\sqrt{n}+14, 8\sqrt{n}+14)$
Set-Membership proof (fixed set)	This work (first scheme)	$(4\sqrt{n}+16, 2\sqrt{n}+22)$
	This work (second scheme)	$(6\sqrt[3]{n}+36, 6\sqrt[3]{n}+60)$

Table 4.2: Comparison of the application of our techniques and results from the literature. Notation (a, b) means a elements of $\mathbb{G}_1$ and b elements of $\mathbb{G}_2$. In rows labeled as "Threshold GS" we give the size of the proof of satisfiability of t-out-of-n sets $\mathcal{S}_i$, where m_x is the sum of the number of variables in $\mathbb{G}_1$ in each set $\mathcal{S}_i$, and $\bar{n}$ is the total number of two-sided and quadratic equations in $\bigcup_{i\in[n]} \mathcal{S}_i$. For all rows, we must add to the proof size the cost of a GS proof of each equation in one of the sets $\mathcal{S}_i$. In the other rows n is the size of the set.

Threshold GS Proofs for PPEs

There are two approaches to construct threshold GS proofs for PPEs, i.e. proofs of satisfiability of t-out-of-n equations. One is due to Groth [Gro06] and consists in compiling the n equations into a single equation which is satisfied only if t of the original equations are satisfied. For the case of PPEs, this method adds new variables and proves that each of them opens to a bit. Our result reduces the cost of this approach, but we omit any further discussion as it is quite inefficient because the number of additional variables is $\Theta(m_{var} + n)$, where m_{var} is the total number of variables in the original n equations.

The second approach is due to Ràfols [Ràf15]. The basic idea behind Ràfols's work, which extends Groth et al.'s work [GOS06a], follows from the observation that for each GS equation type tp, the CRS space $\mathcal{K}$ is partitioned into a perfectly sound CRS space $\mathcal{K}^b_{\mathsf{tp}}$ and a perfectly witness indistinguishable CRS space $\mathcal{K}^h_{\mathsf{tp}}$.

In particular, to prove satisfiability of t-out-of-n sets of equations from $\{\mathcal{S}_i : i \in [n]\}$ of type tp, it suffices to construct an algorithm $\mathsf{K}_{\mathsf{corr}}$ which on input $\mathsf{crs}_{\mathsf{GS}}$ and some set of indexes $A \subset [n]$, $|A| = t$, generates n GS common reference strings $\{\mathsf{crs}_i, i \in [n]\}$ and simulation trapdoors $\tau_{i,sim}$, $i \in A^c$, in a such a way that[4]:

a) it can be publicly verified the set of perfectly sound keys, $\{\mathsf{crs}_i : \mathsf{crs}_i \in \mathcal{K}^b_{\mathsf{tp}}\}$ is of size at least t,

b) there exists a simulator $\mathsf{S}_{\mathsf{corr}}$ who outputs $(\mathsf{crs}_i, \tau_{i,sim})$ for all $i \in [n]$, and the distribution of $\{\mathsf{crs}_i : i \in [n]\}$ is the same as the one of the keys output by $\mathsf{K}_{\mathsf{corr}}$ when $\mathsf{crs}_{\mathsf{GS}}$ is the perfectly witness-indistinguishable CRS.

[4] More technically, this is the notion of *simulatable verifiable correlated key generation* of Ràfols, which extends the definition of verifiable correlated key generation of Groth et al. [GOS06a].

The prover of t-out-of-n satisfiability can run $\mathsf{K}_{\mathsf{corr}}$ and, for all $i \in [n]$, compute a real (resp. simulated) proof for $\mathcal{S}_i$ with respect to crs_i when $i \in A$ (resp. when $i \in A^c$).

Ràfols gives two constructions for PPEs, the first one can be found in Appendix C and the other follows from Section 7[5]. Our algorithm $\mathsf{K}_{\mathsf{corr}}$ for PPEs[6] goes as follows:

- Define $(b_1, \ldots, b_n)$ as $b_i = 1$ if $i \in A$ and $b_i = 0$ if $i \in A^c$. For all $i \in [n]$, let $[\mathbf{z}_i]_1 := \mathsf{GS.Comm}_{ck}(b_i) = b_i[\mathbf{u}_1]_1 + r_i[\mathbf{u}_2]_1$, $r_i \in \mathbb{Z}_q$, and define $\tau_{sim,i} = r_i$, for all $i \in A^c$. Define $\mathsf{crs}_i := (\Gamma, [\mathbf{z}_i]_1, [\mathbf{u}_2]_1, [\mathbf{v}_1]_2, [\mathbf{v}_2]_2)$.
- Prove that $([\mathbf{c}_1]_1, \ldots, [\mathbf{c}_n]_1)$ opens to $\mathbf{b} \in \{0,1\}^n$ and that $\sum_{i \in [n]} b_i = t$.

The simulator just defines $\mathbf{b} = \mathbf{0}$. The reason why this works is that when $b_i = 1$, $([\mathbf{z}_i]_1 - [\mathbf{u}_1]_1) \in \mathsf{Span}([\mathbf{u}_2]_1)$, therefore $\mathsf{crs}_i \in \mathcal{K}^b_{PPE}$ and when $b_i = 0$, $([\mathbf{z}_i]_1 - [\mathbf{u}_1]_1) \notin \mathsf{Span}([\mathbf{u}_2]_1)$ so $\mathsf{crs}_i \in \mathcal{K}^h_{PPE}$.

More Efficient Set-Membership Proofs

Chandran *et al.* construct a ring signature of size $\Theta(\sqrt{n})$ [CGS07], which is the most efficient ring signature in the standard model. Their construction uses as a subroutine a non-interactive proof of membership in some set $S = ([s_1]_1, \ldots, [s_n]_1)$ which is of size $\Theta(\sqrt{n})$. The trick of Chandran *et al.* to achieve this asymptotic complexity is to view S as a matrix $[\mathbf{S}]_1 \in \mathbb{G}_1^{m \times m}$, for $m = \sqrt{n}$, where the i, j th element of $[\mathbf{S}]_1$ is $[s_{i,j}]_1 := [s_{(i,j)}]_1$ and $(i,j) := (i-1)m + j$. Given a commitment $[\mathbf{c}]_1$ to some element $[s_\alpha]_1$, where $\alpha = (i_\alpha, j_\alpha)$, their construction in asymmetric bilinear groups works as follows :

1. Compute GS commitments in $\mathbb{G}_2$ to $b_1 \ldots, b_m$ and $b'_1, \ldots, b'_m$, where $b_i = 1$ if $i = i_\alpha$ and 0 otherwise, and $b'_j = 1$ if $j = j_\alpha$, and 0 otherwise.
2. Compute a GS proof that $b_i \in \{0,1\}$ and $b'_j \in \{0,1\}$ for all $i, j \in [m]$, and that $\sum_{i \in [m]} b_i = 1$, and $\sum_{j \in [m]} b'_j = 1$.
3. Compute GS commitments to $[x_1]_1 := [s_{(i_\alpha,1)}]_1, \ldots, [x_m]_1 := [s_{(i_\alpha,m)}]_1$.
4. Compute a GS proof that $[x_j]_1 = \sum_{i \in [m]} b_i[s_{(i,j)}]_1$, for all $j \in [m]$, is satisfied.
5. Compute a GS proof that $[s_\alpha]_1 = \sum_{j \in [m]} b'_j[x_j]_1$ is satisfied.

With respect to the naive use of GS proofs, Step 2 was improved by Ràfols [Ràf15]. Using our proofs for bit-strings of weight 1 from Section 4.1.5, we can further reduce the size of the proof in step 2, see table.

We note that although in step 4 the equations are all two-sided linear equations, proofs can only be aggregated if the set comes from a witness samplable distribution and the CRS is set to depend on that specific set. This is not useful for the application to ring signatures, since the CRS should be independent of the ring R (which defines the set). If aggregation is possible then the size of the proof in step 4 is reduced from $(2|\mathbb{G}_1| + 4|\mathbb{G}_2|)\sqrt{n}$ to $4|\mathbb{G}_1| + 8|\mathbb{G}_2|$.

Next we describe the construction generalized to vectors (which will be useful in the next construction) and then we show that, when the CRS depends on the set and the set is witness samplable, the proof can be further reduced to $\Theta(\sqrt[3]{n})$.

[5] The construction in [Ràf15, Section 7] is for other equation types but can be used to prove that t-out-of-n of $\mathsf{crs}_1, \ldots, \mathsf{crs}_n$ are perfectly binding for PPEs.

[6] Properly speaking the construction is for PPEs which are left-simulatable in Ràfols's terminology.

More Efficient Set-Membership proof for a Set of Vectors

Here we describe a more efficient version of Chandran's *et al.* set-membership proof, which is also extended to vectors –i.e. to the case where $S = ([\mathbf{s}_1]_1, \ldots, [\mathbf{s}_n]_1)$ is a set of vectors of length ℓ. In such a proof, we show that some commitment $[\mathbf{c}]_1$ opens to a vector $[\mathbf{s}_\alpha]_1$, where $\alpha = (i_\alpha, j_\alpha)$ (recall that $(i, j) = \sqrt{n}(i-1) + j$).

1. Compute GS commitments in $\mathbb{G}_2$ to $b_1 \ldots, b_m$ and $b'_1, \ldots, b'_m$, where $b_i = 1$ if $i = i_\alpha$ and 0 otherwise, and $b'_j = 1$ if $j = j_\alpha$, and 0 otherwise.
2. Compute a proof that $b_i \in \{0, 1\}$ and $b'_j \in \{0, 1\}$ for all $i, j \in [m]$, using the proof system of Section 4.1.3.
3. Compute GS proofs that $\sum_{i \in [m]} b_i = 1$ and $\sum_{j \in [m]} b'_j = 1$.
4. Compute GS commitments to each coordinate of $[\mathbf{x}_1]_1 := [\mathbf{s}_{(i_\alpha,1)}]_1, \ldots, [\mathbf{x}_m]_1 := [\mathbf{s}_{(i_\alpha,m)}]_1$.
5. Compute an aggregated GS proof that the equations $[\mathbf{x}_j]_1 = \sum_{i \in [m]} b_i [\mathbf{s}_{(i,j)}]_1$, for all $j \in [m]$, are satisfied, as detailed in Section 3.4.
6. Compute a GS proof that $[\mathbf{s}_\alpha]_1 = \sum_{j \in [m]} b'_j [\mathbf{x}_j]_1$ is satisfied.

We emphasize that the CRS depends on the set S. This is necessary to aggregate the proofs as in step 5. More specifically, to aggregate the proof of the equations $[\mathbf{x}_j]_1 = \sum_{i \in [m]} b_i [\mathbf{s}_{(i,j)}]_1$, $j \in [m]$ (that is, a total of ℓk equations), we need to include in the CRS some information which depends on the coordinates of $[\mathbf{s}_{(i,j)}]_1$.

In Section 6 we require a CRS independent of the set and thus step 5 is proven using GS proofs without aggregation. While this require $\Theta(\sqrt{n})$ additional elements, the proof size is still $\Theta(\sqrt{n})$.

Theorem 4.7 *If S is witness samplable, the above protocol is a perfectly complete, computationally sound, and computationally zero-knowledge proof system for the language of commitments to elements from the set S.*

Proof Completeness follows directly from the completeness of the building blocks. Soundness follows directly from the perfect soundness of GS proofs together with the computational soundness of aggregation of GS proofs. For computational zero-knowledge, if $\mathsf{crs}_{\mathsf{GS}} := (\Gamma, [\mathbf{u}_1]_1, [\mathbf{u}_2]_1, [\mathbf{v}_1]_2, [\mathbf{v}_2]_2)$ is the GS common reference string in the soundness setting as defined in Section 2.6, switch to a game where $[\mathbf{v}_1]_2 = \epsilon[\mathbf{v}_2]_2$. Under the DDH assumption in $\mathbb{G}_2$, the new CRS is computationally indistinguishable from the original CRS. In a simulated proof, commit to $b_i = 0$, $b'_j = 0$ for all $i, j \in [m]$. In step 2, simply compute a real proof. In step 3, use the GS simulation algorithm (with trapdoor ϵ) to simulate the proof. In Step 4, set $[\mathbf{x}_j]_1 = [\mathbf{0}]_1$. Finally, in step 6, simulate a proof using ϵ. It is not hard to see that such a proof can be simulated even without knowledge of an opening of $[\mathbf{c}]_1$. □

A $\Theta(\sqrt[3]{n})$ Set-Membership proof for Witness Samplable Fixed Sets

We give set-membership proof with improved asymptotic proof size when the set is drawn from a witness samplable distribution and the CRS depends on the set (two different sets require two different CRS).

The main idea is to combine the previous set-membership proof with a split kernel assumption. Specifically, the CRS includes a matrix $[\mathbf{A}]_2$, $\mathbf{A} \leftarrow \mathcal{D}_{m,2}$, whose rows are denoted

$[\boldsymbol{a}_1]_2, \ldots, [\boldsymbol{a}_m]_2$ and a set

$$S' := \left(\sum_{i\in[m]} \boldsymbol{a}_i [s_{(i,1,1)}]_1, \sum_{i\in[m]} \boldsymbol{a}_i [s_{(i,1,2)}]_1, \ldots, \sum_{i\in[m]} \boldsymbol{a}_i [s_{(i,m,m)}]_1 \right) \in \mathbb{G}_1^{2\times m^2},$$

where $m := \sqrt[3]{n}$, $(i,j,k) = m^2(i-1) + m(j-1) + k \in [n]$. As before, the goal to prove is that a commitment $[\mathbf{c}]_1$ opens to some $[s_\alpha]_1 \in S = \{[s_1]_1, \ldots, [s_n]_1\}$ and $(i_\alpha, j_\alpha, k_\alpha)$ are such that $\alpha = (i_\alpha, j_\alpha, k_\alpha)$.

1. Commit to $[\mathbf{y}]_1 := \sum_{i\in[m]} \boldsymbol{a}_i [s_{(i,j_\alpha,k_\alpha)}]_1$ such that $\alpha = (i_\alpha, j_\alpha, k_\alpha)$.
2. Using the set-membership proof for vectors to show that $[\mathbf{y}]_1$ is an element of S'.
3. Compute commitments to $[z_i]_1 := [s_{(i,j_\alpha,k_\alpha)}]_1$, for each $i \in [m]$.
4. Compute a GS proof for the equations $[\mathbf{y}]_1[h]_2 = \sum_{i\in[n]} [\boldsymbol{a}_i]_2 [z_i]_1$.
5. Compute GS commitments in $\mathbb{G}_2$ to $b_1 \ldots, b_m \in \{0,1\}$, where $b_i = 1$ if $i = i_\alpha$ and 0 otherwise.
6. Using our proof system from Section 4.1.3 prove that $b_i \in \{0,1\}$ for all $i \in [m]$.
7. Compute GS proofs for the satisfiability of equations $\sum_{i\in[m]} b_i = 1$ and $[s_\alpha]_1 = \sum_{i\in[m]} b_i [z_i]_1$.

The first step is to commit to $[\mathbf{y}]_1 := \sum_{i\in[m]} \boldsymbol{a}_i [s_{(i,j_\alpha,k_\alpha)}]_1$ and use the previous proof system to prove $[\mathbf{y}]_1 \in S'$. The next step is to commit to $[z_i]_1 := [s_{(i,j_\alpha,k_\alpha)}]_1$ and prove that $\sum_{i\in[m]} [\boldsymbol{a}_i]_2 [z_i]_1 = [h]_2 [\mathbf{y}]_1$ holds. Finally, steps 5 and 6 prove that $[s_\alpha]_1$ is an element of the set $([z_1]_1, \ldots, [z_m]_1)$. For the last statement, compute GS commitments to b_i, $i \in [m]$, and prove that $\sum_{i\in[m]} b_i [z_i]_1 = [s_\alpha]_1$, $\sum_{i\in[m]} b_i = 1$ and $b_i \in \{0,1\}$.[7]

Theorem 4.8 *If S is witness samplable, the above protocol is a perfectly complete, computationally sound, and computationally zero-knowledge proof system for the language of commitments to elements from the set S.*

Proof Completeness follows directly from the completeness of the building blocks. Soundness can be argued as follows. If the set is witness samplable, the CRS can be generated given an instance of the $\mathcal{D}_{m,2}$-$\mathsf{SKerMDH}$ assumption, $([\mathbf{A}]_1, [\mathbf{A}]_2)$. By the soundness of the extension to vectors of the proof of Chandran *et al.*, it holds that $[\mathbf{y}]_1 = \sum_{i\in[m]} \boldsymbol{a}_i [s_{(i,j,k)}]_1$ for some $j, k \in [m]$. Because of the perfect soundness of GS proofs it must hold that $\sum_{i\in[m]} [\boldsymbol{a}_i]_2 [z_i]_1 = [\mathbf{y}]_1 [h]_2 = \sum_{i\in[m]} [\boldsymbol{a}_i]_2 [s_{(i,j,k)}]_1$. It must also be the case that $[z_1]_1 = [s_{(1,j,k)}]_1, \ldots, [z_m]_1 = [s_{(m,j,k)}]_1$, because otherwise the pair $([\boldsymbol{\rho}]_1, [\mathbf{0}]_2)$, where $[\boldsymbol{\rho}]_1 := ([z_1]_1 - [s_{(1,j,k)}]_1, \ldots, [z_m]_1 - [s_{(m,j,k)}]_1)$ is a solution to the $\mathcal{D}_{m,2}$-$\mathsf{SKerMDH}$ challenge, as $[\boldsymbol{\rho}]_1 [\mathbf{A}]_2 = [\mathbf{0}]_2 [\mathbf{A}]_1$. Soundness of the last step implies that $b_i \in \{0,1\}$, for all $i \in [m]$, and that $\sum_{i\in[m]} b_i = 1$. Therefore, there exists a unique $i \in [m]$ such that $b_i = 1$. Finally, $[s_\alpha]_1 = \sum_{i\in[m]} b_i [z_i]_1$ implies that $[\mathbf{c}]_1$ opens to $[s_\alpha]_1 = [z_i]_1 = [s_{(i,j,k)}]_1$. Zero-knowledge follows from the same argument as in the proof of Theorem 4.7. □

[7] Such statement can also be proven using again the set-membership proof, and the proof will be of size $\Theta(\sqrt[6]{n})$. Note this is not exactly a set-membership proof, since only the commitments to the elements in the set are public. However, it is not hard to construct a proof system for that statement using the same ideas as Chandran *et al.*

4.2 The Computationally Binding Case

In this section we construct a constant-size proof that a computationally binding commitment to a vector from $\mathbb{Z}_q^n$ opens to an element from $\{0,1\}^n$. In this case the size of the commitment is independent of n.

In Section 4.2.1 we introduce a new commitment scheme, *extended multi-Pedersen commitments*, which is an "hybrid" between Groth-Sahai commitments and multi-Pedersen commitments. Then, in Section 4.2.2, we construct a QA-NIZK argument that an extended multi-Pedersen commitment opens to an element from $\{0,1\}^n$. Finally, in Section 4.2.3 we show how to give a constant-size proof that many multi-Pedersen commitments open to bit-strings. Using this last proof system one can derive our construction for the perfectly-binding case as a simple corollary and, further, it helps to construct the efficient constructions from Chapter 5.

4.2.1 Extended Multi-Pedersen Commitments

In this section we introduce a new commitment scheme which is a generalization of multi-Pedersen commitments and which was implicitly used in Section 4.1.3.

Given a vector $\mathbf{m} \in \mathbb{Z}_q^m$, the multi-Pedersen commitment in $\mathbb{G}_\gamma$ is a single group element $[c]_\gamma := \sum_{i\in[m]} m_i[g_i]_\gamma + r[g_{m+1}]_\gamma \in \mathbb{G}_\gamma$, where $[g_i]_\gamma \in \mathbb{G}_\gamma$, $i \in [m+1]$, and $r \leftarrow \mathbb{Z}_q$. [8] The $(k+1)$-dimensional multi-Pedersen commitments differs only in that the keys and the resulting commitments are in $\mathbb{G}_\gamma^{k+1}$, for $k \geq 1$.

While the original MP commitments are perfectly hiding, the interest of the new commitments is that, if the keys come from the distribution $\mathcal{D}_k^{m,i}$ defined in Section 2.4, they are perfectly binding at coordinate i. Intuitively, the new commitment is defined in a larger space so that not all the information about the witness is destroyed (in an information-theoretic sense).

Definition 4.9 *The $(k+1)$-dimensional multi-Pedersen commitment scheme in the group $\mathbb{G}_\gamma$ is specified by the following three algorithms* $\mathsf{MP} = (\mathsf{MP.K}, \mathsf{MP.Com}, \mathsf{MP.Vrfy})$*:*

- $\mathsf{MP.K}$ *is a randomized algorithm, which on input the group key gk, a natural number $m \in \mathbb{N}$, and the description of some matrix distribution $\mathcal{D}_{k+1,m+k}$, outputs a commitment key $ck := [\mathbf{G}]_\gamma$, where $\mathbf{G} \leftarrow \mathcal{D}_{k+1,m+k}$.*
- $\mathsf{MP.Com}$ *is a randomized algorithm which, om input a commitment key $ck = [\mathbf{G}]_\gamma$, and a message $\mathbf{m}$ in the message space $\mathcal{M}_{ck} = \mathbb{Z}_q^m$, samples $\mathbf{r} \leftarrow \mathbb{Z}_q^k$ and outputs a commitment $[\mathbf{c}]_\gamma := [\mathbf{G}]_\gamma \binom{\mathbf{m}}{\mathbf{r}}$ in the commitment space $\mathcal{C}_{ck} = \mathbb{G}_\gamma^{k+1}$ and an opening $Op = \mathbf{r}$,*
- $\mathsf{MP.Vrfy}$ *is a deterministic algorithm which, on input the commitment key $ck = [\mathbf{G}]_\gamma$, a commitment $[\mathbf{c}]_\gamma$, a message $\mathbf{m} \in \mathbb{Z}_q^m$ and an opening $Op = \mathbf{r} \in \mathbb{Z}_q^k$, outputs 1 if $[\mathbf{c}]_\gamma = [\mathbf{G}]_\gamma \binom{\mathbf{m}}{\mathbf{r}}$ and 0 otherwise.*

Theorem 4.10 *The* MP *scheme is computationally binding if the discrete logarithm assumption holds in $\mathbb{G}_\gamma$. Further, if $\mathcal{D}_{k+1,m+k} = \mathcal{D}_k^{m,i}$, it holds that:*

- *If $i = 0$, then* MP *is perfectly hiding,*
- *If $i \in [m]$, then* MP *is statistically binding at coordinate i, which means that for each $[\mathbf{c}]_\gamma \in \mathbb{G}_\gamma^{k+1}$, there exists a unique $\tilde{m}_i \in \mathbb{Z}_q$ such that for all $\mathbf{m} \in \mathbb{Z}_q^m, \mathbf{r} \in \mathbb{Z}_q^k$*

[8] Written in the usual multiplicative notation $c = \prod_{i\in[m]} g_i^{m_i} \cdot g_{m+1}^r$.

such that $[\mathbf{c}]_\gamma = [\mathbf{G}]_\gamma \left(\begin{smallmatrix}\mathbf{m}\\ \mathbf{r}\end{smallmatrix}\right)$*,* $m_i = \tilde{m}_i$*. Further, the scheme is perfectly hiding at the rest of coordinates.*

Proof (Computationally binding.) (This follows a proof due to Jorge Villar). Let $[a]_\gamma \in \mathbb{G}_\gamma$ be the discrete logarithm challenge. To sample the commitment key according to $\mathcal{D}_k^{m,i}$, choose $\mathbf{G}_2 \leftarrow \mathcal{D}_k$, and define the last k columns of $[\mathbf{G}]_\gamma$ as $[\mathbf{G}_2]_\gamma$. For the rest of the columns of $[\mathbf{G}]_\gamma$, independently for each $j \in [m]$, $i \neq j$, sample a pair α_j, β_j and define $[\mathbf{g}_j]_\gamma = [\mathbf{G}_2(a\alpha_j + \beta_j)]_\gamma$, which can be computed as $[a]_\gamma \mathbf{G}_2 \alpha_j + [\mathbf{G}_2\beta_j]_\gamma$. If $i \neq 0$, set $\mathbf{g}_i \leftarrow \mathbb{Z}_q^{k+1}$. In this case, with overwhelming probability, $\mathbf{g}_i$ is linearly independent of the rest of the columns and we will assume so in the following. The commitment key is then given to the adversary against the binding property of the scheme, and it outputs a commitment $[\mathbf{c}]_\gamma$, together with two valid openings $(\mathbf{m}, \mathbf{r}), (\mathbf{m}', \mathbf{r}')$ such that $\mathbf{m} \neq \mathbf{m}'$. It follows that $[\mathbf{c}]_\gamma = [\mathbf{G}]_\gamma \left(\begin{smallmatrix}\mathbf{m}\\ \mathbf{r}\end{smallmatrix}\right) = [\mathbf{G}]_\gamma \left(\begin{smallmatrix}\mathbf{m}'\\ \mathbf{r}'\end{smallmatrix}\right)$, which implies that $[\mathbf{0}]_\gamma = [\mathbf{G}]_\gamma \left(\begin{smallmatrix}\mathbf{m}-\mathbf{m}'\\ \mathbf{r}-\mathbf{r}'\end{smallmatrix}\right)$. Further, because $\mathbf{g}_i$ is linearly independent of the rest of the columns, it holds that:

$$a \left(\mathbf{G}_2 (\sum_{j \neq i} (m'_j - m_j)\boldsymbol{\alpha}_j) \right) = \left(\mathbf{G}_2(\mathbf{r} - \mathbf{r}' + \sum_{j \neq i} \boldsymbol{\beta}_j (m_j - m'_j)) \right). \tag{4.7}$$

W.l.o.g we can assume that $\mathbf{G}_2$ has full rank (it can be shown that if $\mathcal{D}_k$-MDDH is a generically hard assumption in k-linear groups, then matrices sampled from $\mathcal{D}_k$ have full rank with overwhelming probability). Then, we can recover $a \in \mathbb{Z}_q$ from equation 4.7 except if $\sum_{j \neq i}(m'_j - m_j)\boldsymbol{\alpha}_j = \mathbf{0}$. But since, for all j, $\boldsymbol{\alpha}_j$ is information theoretically hidden from the adversary, the probability of this event is at most $1/q^k$.

(Perfectly binding at coordinate i.) With overwhelming probability, $\mathbf{g}_i$ is linearly independent of the rest of the columns of $\mathbf{G}$. Therefore, given any $[\mathbf{c}]_\gamma \in \mathbb{G}_\gamma^{k+1}$, if $\mathbf{m} \in \mathbb{Z}_q^m, \mathbf{r} \in \mathbb{Z}_q^k$ are such that $\mathbf{c} = \mathbf{G} \left(\begin{smallmatrix}\mathbf{m}\\ \mathbf{r}\end{smallmatrix}\right)$, there exists a unique $\tilde{m}_i \in \mathbb{Z}_q$ such that $m_i = \tilde{m}_i$.

(Perfectly hiding at coordinate j, $j \neq i$.) This follows immediately from the fact that $\mathbf{g}_j$ is in the image of $\mathbf{G}_2$. □

Comparison with other Primitives

Somewhere Statistically Hashing. The idea of primitives being binding at only one coordinate have been used before in the context of *somewhere statistically binding hash functions* (SSB hashing) [HW15, OPWW15]. SSB hashing formalize the notion of being binding at only one coordinate and of indistinguishability of the different keys (called *index hiding*). In addition, SSB hashing should have a *local opening* property which means that there is a short proof that certifies the i th opening. Unlike multi-Pedersen commitments, SSB lacks of a (computational) "everywhere binding" property nor a hiding property. While the former property can be easily shown to hold from the somewhere statistically binding and index hiding properties (with a security loss of $1/n$), they totally lack of a hiding property.

Okamoto et al. constructed a "two-to-one" SSB hash function under the DDH assumption – i.e. a vector of size $2n$ is hashed into a digest which uniquely defines one of the halves of the original vector – which bears some similarities with extended multi-Pedersen commitments [OPWW15]. Using our notation, Okamoto et al. compute the hash of $(\mathbf{x}, \mathbf{y}) \in \mathbb{Z}_q^{2n}$ [9,10]

$$H_{hk}(\mathbf{x}, \mathbf{y}) = [\mathbf{A}]_1\mathbf{x} + [\mathbf{B}]_1\mathbf{y} \in \mathbb{G}_1^{n+1},$$

[9] In fact, Okamoto et al. considered that $\mathbf{x} \in \{0,1\}^s$ and then they "parsed" $\mathbf{x}$ as a vector in $\mathbb{Z}_q^n$, for $n = s/t$, where each coordinate is the integer in $[0, 2^t - 1]$ corresponding to the respective block of size t of $\mathbf{x}$.

[10] Okamoto et al. considered a transposed version of what is written here.

where $hk = ([\mathbf{A}]_1 \in \mathbb{G}_1^{(n+1)\times n}, [\mathbf{B}]_1 \in \mathbb{G}_1^{(n+1)\times n})$. $\mathbf{A}$ and $\mathbf{B}$ can be sampled in such a way that either $\mathbf{A}$ or $\mathbf{B}$ is full rank and their columns are linearly independent from the columns of the other matrix ($\mathbf{B}$ and $\mathbf{A}$ respectively). The size of the digest is $\Theta(n)$ group elements.

Okamoto et al.'s construction can be viewed as variant of extended multi-Pedersen commitment where the commitment key is a matrix of size $(n+1)\times 2n$ and the first (or last) columns are linearly independent from the other columns. However, with standard extended multi-Pedersen commitments, one can construct a SSB hash function $H_{hk}(\mathbf{x}) := \mathsf{MP.Com}_{ck}(\mathbf{x}; 0)$, $hk := ck$, where digests consist of only 2 group elements. Further, one can have the local opening property by attaching a QA-NIZK proof that

$$\mathsf{MP.Com}_{ck}(\mathbf{x}; 0) - x_i[\mathbf{g}_i]_1 \in \mathbf{Span}(\{[\mathbf{g}_j]_1 : j \neq i\}),$$

while Okamoto et al.'s "two-to-one" construction lacks of this property.

Vector Commitments. Extended multi-Pedersen commitments bear some similarities with vector commitments, introduced by Catalano and Fiore [CF13]. Using extended multi-Pedersen commitments, one can commit to a vector $\mathbf{m} \in \mathbb{Z}_q^n$ and show the so called *position binding* property, that is, show that it opens to m_i at coordinate i. Indeed, we can compute a proof that $(\mathsf{MP.Com}_{ck}(\mathbf{x}_i; 0) - m_i[\mathbf{g}_i]_1) \in \mathbf{Span}(\{[\mathbf{g}_j]_1 : j \neq i\})$. However, we do not elaborate more on this application since Catalano and Fiore's construction is (by a constant factor) more efficient in terms of CRS size and commitment size, and also relies on weaker assumptions.

4.2.2 The Scheme

We construct a QA-NIZK argument of membership in the language

$$\mathcal{L}_{ck,\mathsf{bits}} := \{[\mathbf{c}]_1 \in \mathbb{G}_1^{k+1} : \exists \mathbf{b} \in \{0,1\}^m, \mathbf{r} \in \mathbb{Z}_q^k \text{ s.t. } [\mathbf{c}]_1 = \mathsf{MP.Com}_{ck}(\mathbf{b}; \mathbf{r})\},$$

where $ck := [\mathbf{G}]_1$ and $\mathbf{G}$ is a matrix sampled from some distribution $\mathcal{D}_k^{m,i}$ (as defined on Section 2.4). For simplicity, in the exposition we restrict ourselves to the case $\mathcal{D}_k = \mathcal{L}_1$ so $\mathbf{G}$ is sampled from $\mathcal{L}_1^{m,i}$, for some $0 \leq i \leq m$.

It is important to note that, as an extended MP commitment is at best only binding at one coordinate, a priori showing that it opens to $\mathbf{b} \in \{0,1\}^m$ is not very meaningful, as it does open to other values as well. However, when combined with external protocols that unequivocally define $\mathbf{b}$, it becomes a key building block to obtain the the results of Chapter 5.

The argument is implicit in Section 4.1, where we construct a QA-NIZK argument for proving that a perfectly binding commitment opens to a bit-string. More technically, to prove that a perfectly binding commitment $[\mathbf{c}']_1$ opens to a bit-string $\mathbf{b}$, the argument in Section 4.1 takes the following steps:

1. Construct two MP commitments $[\mathbf{c}]_1$, $[\mathbf{d}]_2$ to $\mathbf{b}$.
2. Prove that $[\mathbf{c}]_1$ and $[\mathbf{c}']_1$ open to the same value.
3. Prove that the two MP commitments $[\mathbf{c}]_1$ and $[\mathbf{d}]_2$ open to the same value.
4. Prove that $\mathbf{c}(\mathbf{d} - \sum_{j\in[m]} \mathbf{h}_j)^\top \in \mathbf{Span}(\{\mathbf{g}_i\mathbf{h}_j^\top : i, j \in [m+1]\} \setminus \{\mathbf{g}_i\mathbf{h}_i^\top : i \in [m]\})$, where $ck := [(\mathbf{g}_1, \ldots, \mathbf{g}_{m+1})]_1$ and $ck' := [(\mathbf{h}_1, \ldots, \mathbf{h}_{m+1})]_2$.

The argument we need for our results eliminates the perfectly binding commitment, which of course also means that step 2 disappears. Additionally, in the original scheme from Section 4.1, the distribution of $ck = [\mathbf{G}]_1$ is uniform over $\mathbb{G}_1^{2\times(n+1)}$, while in our argument of membership in $\mathcal{L}_{ck,\mathsf{bits}}$, $\mathbf{G}$ can follow any distribution $\mathcal{L}_1^{m,i}$ for some $0 \le i \le m$. However, it is not hard to adapt the original proof to these distributions (in fact, in the soundness proof of Lemma 4.3, there is a game where the distribution of $\mathbf{G}$ is changed to $\mathcal{L}_1^{m,i}$, for some $i \leftarrow [m]$). The proof that $\mathcal{L}_{ck,\mathsf{bits}}$ admits a constant-size QA-NIZK argument essentially reuses parts of the proof of Theorem 7.3. For completeness, we give a full description of the scheme for the computationally binding case below.

Detailed Description

$\mathsf{K}(gk, [\mathbf{G}]_1)$**:** Pick $\mathbf{H} \leftarrow \mathcal{L}_1^{m,0}$, and denote by $\mathbf{h}_j$ the j th column of $\mathbf{H}$. Pick $\mathbf{T} \leftarrow \mathbb{Z}_q^{2\times 2}$ and for each $(i,j) \in \mathcal{I}_{m,1}$ define matrices

$$([\mathbf{C}_{i,j}]_1, [\mathbf{D}_{i,j}]_2) := ([\mathbf{g}_i\mathbf{h}_j^\top + \mathbf{T}]_1, [-\mathbf{T}]_2).$$

Let Π_{sum} be the proof system for sum in subspace (Section 3.3) and Π_{com} be an instance of the proof system for equal commitment opening (Section 3.4). Let $\mathsf{crs}_{\mathsf{sum}} \leftarrow \Pi_{\mathsf{sum}}.\mathsf{K}(gk, \{([\mathbf{C}_{i,j}]_1, [\mathbf{D}_{i,j}]_2) : (i,j) \in \mathcal{I}_{m,1}\})$ and let $\mathsf{crs}_{\mathsf{com}} \leftarrow \Pi_{\mathsf{com}}.\mathsf{K}(gk, [\mathbf{G}]_1, [\mathbf{H}]_2, m)$.

The common reference string is given by:

$$\mathsf{crs} \;:=\; (gk, [\mathbf{G}]_1, [\mathbf{H}]_2, \{([\mathbf{C}_{i,j}]_1, [\mathbf{D}_{i,j}]_2) : (i,j) \in \mathcal{I}_{m,1}\}, \mathsf{crs}_{\mathsf{sum}}, \mathsf{crs}_{\mathsf{com}}).$$

$\mathsf{P}(\mathsf{crs}, [\mathbf{c}]_1, \langle \mathbf{b}, r\rangle)$**:** The proof $([\mathbf{d}]_1, ([\mathbf{\Theta}]_1, [\mathbf{\Pi}]_2), \pi_{\mathsf{com}}, \pi_{\mathsf{sum}})$ is computed as follows:

1. $[\mathbf{d}]_2 := \mathsf{MP.Com}_{[\mathbf{H}]_2}(\mathbf{b}; s)$, $s \leftarrow \mathbb{Z}_q$.

2. Pick $\mathbf{R} \leftarrow \mathbb{Z}_q^{2\times 2}$ and compute:

$$\begin{aligned}([\mathbf{\Theta}]_1, [\mathbf{\Pi}]_2) \;:=\; & ([\mathbf{R}]_1, [-\mathbf{R}]_2) + \sum_{i\in[m]}\sum_{j\in[m]} b_i(b_j - 1)([\mathbf{C}_{i,j}]_1, [\mathbf{D}_{i,j}]_2) + \\ & rs([\mathbf{C}_{m+1,m+1}]_1, [\mathbf{D}_{m+1,m+1}]_2) + \\ & \sum_{i\in[m]} (b_i s([\mathbf{C}_{i,m+1}]_1, [\mathbf{D}_{i,m+1}]_2) + \\ & r(b_i - 1)([\mathbf{C}_{m+1,i}]_1, [\mathbf{D}_{m+1,i}]_2)).\end{aligned}$$

3. Compute a proof π_{sum} that $\mathbf{\Theta} + \mathbf{\Pi}$ is in the span of $\{\mathbf{C}_{i,j} + \mathbf{D}_{i,j}\}_{(i,j)\in\mathcal{I}_{m,1}}$ and a proof π_{com} that $([\mathbf{c}]_1, [\mathbf{d}]_2)$ open to the same value, using $\mathbf{b}, r$, and s.

$\mathsf{V}(\mathsf{crs}, [\mathbf{c}]_1, [\mathbf{d}]_2, ([\mathbf{\Theta}]_1, [\mathbf{\Pi}]_2), \pi_{\mathsf{com}}, \pi_{\mathsf{sum}})$**:** If any of the following checks fails, the verifier outputs 0, else it outputs 1:

1. $[\mathbf{c}]_1 \left([\mathbf{d}]_2^\top - \sum_{j\in[m]}[\mathbf{h}_j]_2^\top\right) = [\mathbf{\Theta}]_1[\mathbf{I}]_2 + [\mathbf{I}]_1[\mathbf{\Pi}]_2.$

2. $\Pi_{\mathsf{sum}}.\mathsf{V}(\mathsf{crs}_{\mathsf{sum}}, ([\mathbf{\Theta}]_1, [\mathbf{\Pi}]_2), \pi_{\mathsf{sum}})) = 1$ and $\Pi_{\mathsf{com}}.\mathsf{V}(\mathsf{crs}_{\mathsf{com}}, ([\mathbf{c}]_1, [\mathbf{d}]_2), \pi_{\mathsf{com}}) = 1$.

$\mathsf{S}_1(gk, [\mathbf{G}]_1)$**:** It generates and outputs the CRS in the same way as K and additionally outputs the simulation trapdoor $\tau = (\mathbf{H}, \tau_{\mathsf{sum}}, \tau_{\mathsf{com}})$, where τ_{sum} and τ_{com} are, respectively, Π_{sum}'s and Π_{com}'s simulation trapdoors.

$\mathsf{S}_2(\mathsf{crs}, [\mathbf{c}]_1, (\mathbf{H}, \tau_{\mathsf{sum}}, \tau_{\mathsf{com}}))$**:** The proof $([\mathbf{d}]_1, ([\mathbf{\Theta}]_1, [\mathbf{\Pi}]_2), \pi_{\mathsf{com}}, \pi_{\mathsf{sum}})$ is simulated as follows:

1. $\mathbf{d} := \mathsf{MP.Com}_{[\mathbf{H}]_2}(\mathbf{0}_{n\times 1}, \overline{w}_h)$, $\overline{w}_h \leftarrow \mathbb{Z}_q$.

2. Pick $\mathbf{R} \leftarrow \mathbb{Z}_q^{2\times 2}$ and define:
$$[\mathbf{\Theta}]_1 := [\mathbf{c}]_1 \left(\mathbf{d} - \sum_{i\in[m]} \mathbf{h}_i\right)^\top + [\mathbf{R}]_1, \qquad\qquad [\mathbf{\Pi}]_2 := -[\mathbf{R}]_2.$$

3. $\pi_{\mathsf{sum}} \leftarrow \Pi_{\mathsf{sum}}.\mathsf{S}_2(\mathsf{crs}_{\mathsf{sum}}, ([\mathbf{\Theta}]_1, [\mathbf{\Pi}]_2), \tau_{\mathsf{sum}})$ and $\pi_{\mathsf{com}} \leftarrow \Pi_{\mathsf{com}}.\mathsf{S}_2(\mathsf{crs}_{\mathsf{com}}, ([\mathbf{c}]_1, [\mathbf{d}]_2), \tau_{\mathsf{com}})$.

Security Proof

Theorem 4.11 *The proof system described above is a QA-NIZK proof system with perfect completeness, computational soundness, and perfect zero-knowledge.*

Proof We remark that proof of completeness and zero-knowledge is the same for any distribution $\mathcal{L}_1^{m,i}$.

Perfect Completeness: Note that, by definition of $\mathbf{C}_{i,j}$ and $\mathbf{D}_{i,j}$, $[\mathbf{C}_{i,j}]_1[\mathbf{I}]_2+[\mathbf{I}]_1[\mathbf{D}_{i,j}]_2 = [\mathbf{g}_i]_1[\mathbf{h}_j]_2^\top$. Since $b_i(b_i-1) = 0$ for each $i \in [m]$,

$$\begin{aligned}
&[\mathbf{c}]_1 \left([\mathbf{d}]_2 - \sum_{i\in[m]} [\mathbf{h}_i]_2\right)^\top \\
&= \sum_{i\in[m]} \left(b_i s[\mathbf{g}_i]_1[\mathbf{h}_{m+1}]_2^\top + r(b_i-1)[\mathbf{g}_{m+1}]_1[\mathbf{h}_i]_2^\top + \sum_{j\in[m]} b_i(b_j-1)[\mathbf{g}_i]_1[\mathbf{h}_j]_2^\top \right) \\
&\quad + rs[\mathbf{g}_{m+1}]_1[\mathbf{h}_{m+1}]_2^\top \\
&= \left(\sum_{i\in[m]} b_i s[\mathbf{g}_i]_1\mathbf{h}_{m+1}^\top + r(b_i-1)[\mathbf{g}_{m+1}]_1\mathbf{h}_i^\top + \sum_{\substack{j\in[m]\\ j\neq i}} b_i(b_j-1)[\mathbf{g}_i]_1\mathbf{h}_j^\top \right)[\mathbf{I}]_2 \\
&\quad + rs[\mathbf{g}_{m+1}]_1\mathbf{h}_{m+1}^\top[\mathbf{I}]_2 + [\mathbf{R}]_1[\mathbf{I}]_2 + [\mathbf{I}]_1[-\mathbf{R}]_2 \\
&= [\mathbf{\Theta}]_1[\mathbf{I}]_2 + [\mathbf{I}]_1[\mathbf{\Pi}]_2.
\end{aligned}$$

Finally, the rest of the proof follows from completeness of Π_{sum} and Π_{com}.

Soundness: When $\mathbf{G}$ is sampled from $\mathcal{L}_1^{m,0}$ it suffices to prove that the commitment $[\mathbf{c}]_1$ output by the adversary is in $\mathbf{Span}([\mathbf{G}]_1)$ since, by the perfect hiding property, $[\mathbf{c}]_1$ can be opened to any $\mathbf{b} \in \{0,1\}^m$ thus $[\mathbf{c}]_1 \in \mathcal{L}_{ck,\mathsf{bits}}$. If $[\mathbf{c}]_1 \notin \mathbf{Span}([\mathbf{G}]_1)$, then we can break the (strong) soundness of the proof that $[\mathbf{c}]_1$ and $[\mathbf{d}]_2$ open to the same value, since that proof implies that there exist $\mathbf{x}, r, s$ such that $[\mathbf{c}]_1 = [\mathbf{G}]_1 \left(\begin{smallmatrix}\mathbf{x}\\ r\end{smallmatrix}\right)$ and $[\mathbf{d}]_2 = [\mathbf{H}]_2 \left(\begin{smallmatrix}\mathbf{x}\\ s\end{smallmatrix}\right)$. Therefore, we construct an adversary B against the strong soundness of Π_{com} that simulates A until it halts and outputs $([\mathbf{c}]_1, [\mathbf{d}]_2, \pi_{\mathsf{com}})$. Note that, in order to simulate the CRS B requires $\mathbf{H}$, but this is not a problem since it is part of the input in the strong soundness game.

When $\mathbf{G}$ is sampled from $\mathcal{L}_1^{m,i^*}$, $i^* > 0$, the proof follows from the indistinguishability of the following three games:

Real: This is the real soundness game. The output is 1 if the adversary submits some $[\mathbf{c}]_1 \notin \mathcal{L}_{ck,\mathsf{bits}}$ and the corresponding proof which is accepted by the verifier.

Game_0: This identical to Real, except that K does not receive $[\mathbf{G}]_1$ as a input but it samples $\mathbf{G}$ itself according to $\mathcal{L}_1^{m,i^*}$.

Game_1: This game is identical to Game_0 except that now $\mathbf{H} \leftarrow \mathcal{L}_1^{m,i^*}$.

It is obvious that the first two games are indistinguishable. The rest of the argument goes as follows.

Lemma 4.12 *There exists a* $\mathcal{L}_1$-$\mathsf{MDDH}_{\mathbb{G}_2}$ *adversary* D *such that* $|\Pr[\mathsf{Game}_0(\mathsf{A}) = 1] - \Pr[\mathsf{Game}_1(\mathsf{A}) = 1]| \leq \mathsf{Adv}_{\mathcal{L}_1,\mathsf{Gen}_a}(\mathsf{D})$.

Proof We construct an adversary D that receives a challenge $([\mathbf{A}]_2, [\mathbf{u}]_2)$ of the $\mathcal{L}_1$-$\mathsf{MDDH}_{\mathbb{G}_2}$ assumption. From this challenge, D just defines the matrix $[\mathbf{H}]_2 \in \mathbb{G}_2^{2\times(m+1)}$ as the matrix whose last column consists of $[\mathbf{A}]_2$, the ith column consists of $[\mathbf{u}]_2$ and the rest of the columns are random vectors in the image of $[\mathbf{A}]_2$. Obviously, when $[\mathbf{u}]_2$ is sampled from the image of $[\mathbf{A}]_2, \mathbf{H}$ follows the distribution $\mathcal{L}_1^{m,0}$, while if $[\mathbf{u}]_2$ is a uniform element of $\mathbb{G}^2$, $\mathbf{H}$ follows the distribution $\mathcal{L}_1^{m,i^*}$.

Adversary D samples $\mathbf{G} \leftarrow \mathcal{L}_1^{m,i^*}$. Given that D does not know the discrete logarithms of $[\mathbf{H}]_2$, it cannot compute the pairs $(\mathbf{C}_{i,j}, \mathbf{D}_{i,j})$ exactly as in Game_0. Nevertheless, for each $(i,j) \in \mathcal{I}_{m,1}$ it can compute identically distributed pairs by picking $\mathbf{T} \leftarrow \mathbb{Z}_q^{2\times 2}$ and defining

$$([\mathbf{C}_{i,j}]_1, [\mathbf{D}_{i,j}]_2) := ([\mathbf{T}]_1, \mathbf{g}_i[\mathbf{h}_j]_2^\top - [\mathbf{T}]_2).$$

The rest of the elements of the CRS, namely $\mathsf{crs}_{\mathsf{com}}$ and $\mathsf{crs}_{\mathsf{sum}}$, are honestly computed. When $\mathbf{H} \leftarrow \mathcal{L}_1^{m,0}$, D perfectly simulates Game_0, and when $\mathbf{H} \leftarrow \mathcal{L}_1^{m,i^*}$, D perfectly simulates Game_1, which concludes the proof. □

Lemma 4.13 *There exist adversaries* B_1*, against the strong soundness of* Π_{com}*, and* B_2*, against the soundness of* Π_{sum}*, such that* $\Pr[\mathsf{Game}_1(\mathsf{A}) = 1] \leq 4/q + \mathbf{Adv}_{\Pi_{\mathsf{com}}}(\mathsf{B}_1) + \mathbf{Adv}_{\Pi_{\mathsf{sum}}}(\mathsf{B}_2)$.

Proof With probability $1 - 4/q$, $\{\mathbf{g}_{i^*}, \mathbf{g}_{m+1}\}$ and $\{\mathbf{h}_{i^*}, \mathbf{h}_{m+1}\}$ are both bases of $\mathbb{Z}_q^2$, we can define $b_{i^*}, \overline{w}_g, \overline{w}_h, \overline{b}_{i^*}$ as the unique coefficients in $\mathbb{Z}_q$ such that $\mathbf{c} = b_{i^*}\mathbf{g}_{i^*} + \overline{w}_g\mathbf{g}_{m+1}$ and $\mathbf{d} = \overline{b}_{i^*}\mathbf{h}_{i^*} + \overline{w}_h\mathbf{h}_{m+1}$.

In particular, if A breaks soundness, this implies that $b_{i^*} \notin \{0,1\}$ (since for $i \neq i^*$, $\mathbf{c}$ can always be opened to choose $b_i = 0$). Further, the verifier accepts the proof proof: $([\mathbf{d}]_2, ([\boldsymbol{\Theta}]_1, [\boldsymbol{\Pi}]_2), \pi_{\mathsf{com}}, \pi_{\mathsf{sum}})$ produced by A. We distinguish two cases:

$b_{i^*} \neq \overline{b}_{i^*}$**:** Given that $[\mathbf{c}]_1$ and $[\mathbf{d}]_2$ are perfectly binding at coordinate i^*, if $b_{i^*} \neq \overline{b}_{i^*}$ it is not possible that $[\mathbf{c}]_1$ and $[\mathbf{d}]_2$ open to the same value. We construct an adversary B_1 against the strong soundness of Π_{com} that simulates game Game_1 with A (using $\mathbf{H}$ to simulate the CRS) until it halts and outputs $([\mathbf{c}]_1, [\mathbf{d}]_2, \pi_{\mathsf{com}})$. If $b_{i^*} \neq \overline{b}_{i^*}$, π_{com} is a fake proof for $([\mathbf{c}]_1, [\mathbf{d}]_2)$ opening to the same value and then B_1 breaks the strong soundness of Π_{com}.

$b_{i^*} = \overline{b}_{i^*}$**,** $b_{i^*}(\overline{b}_{i^*} - 1) \neq 0$**:** If we express $\boldsymbol{\Theta} + \boldsymbol{\Pi}$ as a linear combination of $\{\mathbf{g}_i\mathbf{h}_j^\top : i,j \in [n+1]\}$, the coordinate of $\mathbf{g}_{i^*}\mathbf{h}_{i^*}^\top$ is $b_{i^*}(\overline{b}_{i^*} - 1) \neq 0$ and thus $\boldsymbol{\Theta} + \boldsymbol{\Pi} \notin \mathbf{Span}(\{\mathbf{C}_{i,j} + \mathbf{D}_{i,j} : (i,j) \in \mathcal{I}_{m,1}\})$. We construct an adversary B_2 against the soundness of Π_{sum} that simulates game Game_1 with A until it halts and outputs $([\mathbf{\Theta}]_1, [\mathbf{\Pi}]_2, \pi_{\mathsf{sum}})$. If $b_{i^*} = \overline{b}_{i^*}$ but $b_{i^*}(\overline{b}_{i^*} - 1) \neq 0$, π_{sum} is a fake proof for $([\mathbf{\Theta}]_1, [\mathbf{\Pi}]_2)$ and then B_2 breaks the soundness of Π_{sum}. □

Perfect Zero-Knowledge: First, note that the vector $[\mathbf{d}]_2 \in \mathbb{G}_2^2$ output by the prover and the vector output by S_2 follow exactly the same distribution. This is because $\mathbf{H} \leftarrow \mathcal{L}_1^{m,0}$ defines perfectly hiding commitments. In particular, although the simulator S_2 does not know $\mathbf{b} \in \{0,1\}^m$ such that $[\mathbf{c}]_1 = [\mathbf{G}]_1 \left(\begin{smallmatrix} \mathbf{b} \\ r \end{smallmatrix}\right)$, for some $r \in \mathbb{Z}_q$, there exists $s \in \mathbb{Z}_q$ such that $[\mathbf{d}]_2 = [\mathbf{H}]_2 \left(\begin{smallmatrix} \mathbf{b} \\ s \end{smallmatrix}\right)$.

Since $\mathbf{R}$ is chosen uniformly at random in $\mathbb{Z}_q^{2\times 2}$, the proof $([\mathbf{\Theta}]_1, [\mathbf{\Pi}]_2)$ is uniformly distributed conditioned on satisfying check 1) of algorithm V. Finally, the rest of the proof follows from zero-knowledge of Π_{sum} and Π_{com}. □

4.2.3 Constant-Size Argument for $\mathcal{L}^n_{ck,\mathsf{bits}}$

We give a QA-NIZK argument of membership in the language $\mathcal{L}^n_{ck,\mathsf{bits}} = \mathcal{L}_{ck,\mathsf{bits}} \times \ldots \times \mathcal{L}_{ck,\mathsf{bits}}$ with a proof size which is independent of n (but with a loss factor of n in the proof of soundness). The result will be crucial to get improved proof sizes for more complex statements. For example, note that the language for the perfectly binding case with GS commitments is $\mathcal{L}^n_{ck,\mathsf{bits}}$, where $ck := [\mathbf{U}]_1$ and $\mathbf{U} \leftarrow \mathcal{L}_1^{1,1}$. [11]

Intuition

We would like to prove that some tuple $([\mathbf{c}_1]_1, \ldots, [\mathbf{c}_n]_1) \in \mathcal{L}^n_{ck,\mathsf{bits}}$, where $[\mathbf{c}_j]_1 = \mathsf{MP.Com}_{ck}(\mathbf{b}_j; \mathbf{r}_j)$, $j \in [n]$, $ck := [\mathbf{G}]_1$, and $\mathbf{G} \leftarrow \mathcal{D}_k^{m,i}$, for some $0 \leq i \leq n$. Denote $\mathbf{c} = \mathbf{c}_1/\ldots/\mathbf{c}_n$, $\mathbf{b} = \mathbf{b}_1/\ldots/\mathbf{b}_n$ and $\mathbf{r} = \mathbf{r}_1/\ldots/\mathbf{r}_n$ (concatenation of column vectors as defined in Section 2.1). The proof system works as follows:

1. It defines $\overline{ck} := [\overline{\mathbf{G}}]_1 \leftarrow \mathsf{MP.K}(gk, mn, \mathcal{L}_1^{mn,0})$ for computing multi-Pedersen commitments to vectors of size mn
2. it computes $[\overline{\mathbf{c}}]_1 \leftarrow \mathsf{MP.Com}_{\overline{ck}}(\mathbf{b}; \mathbf{s})$ for some randomness $\mathbf{s}$, and proves that $[\overline{\mathbf{c}}]_1 \in \mathcal{L}_{\overline{ck},\mathsf{bits}}$ with the proof system Π_{bits},
3. it proves that there exists an equal opening of $[\mathbf{c}]_1$ and $[\overline{\mathbf{c}}]_1$ with Π_{com}.

First, note that in step 3, we can use the proof system Π_{com}, as both $[\mathbf{c}]_1$ and $[\overline{\mathbf{c}}]_1$ are commitments of the required form, as if $\mathbf{G}_2$ denotes the last k columns of $\mathbf{G}$ and $\mathbf{G}_1$ the rest, $\mathbf{c} = \mathrm{diag}(\mathbf{G}_1, n)\mathbf{b} + \mathrm{diag}(\mathbf{G}_2, n)\mathbf{r}$. We give some intuition on why is the above scheme sound. For the case $\mathbf{G} \leftarrow \mathcal{D}_k^{m,0}$ it suffices to note that the proof that $[\mathbf{c}]_1$ and $[\overline{\mathbf{c}}]_1$ share an opening implies in particular that they are both valid commitments. But if $[\overline{\mathbf{c}}]_1$ is a valid commitment then $([\mathbf{c}_1]_1, \ldots, [\mathbf{c}_n]_1) \in \mathcal{L}^n_{ck,\mathsf{bits}}$ because for this distribution the commitments are perfectly hiding.

For the case where $\mathbf{G} \leftarrow \mathcal{D}_k^{m,i}$, $i > 0$, recall that the MP commitment with this key is perfectly binding at coordinate i. In particular, this implies that if some $[\mathbf{c}_j]_1 \notin \mathcal{L}_{ck,\mathsf{bits}}$, the ith coordinate of $\mathbf{b}_j$, denoted $b_{i,j}$, satisfies that $b_{i,j} \notin \{0,1\}$. Therefore, given some $j^* \leftarrow [n]$, if the adversary breaks soundness, then, with probability at least $1/n$, $b_{i,j^*} \notin \{0,1\}$. In the soundness proof, we switch to a game where the distribution of $\overline{\mathbf{G}}$ is changed so that now $\mathsf{MP.Com}_{\overline{ck}}$ is perfectly binding for b_{i,j^*}. Now it is easy to prove that if $b_{i,j^*} \notin \{0,1\}$, the soundness of Π_{bits} or of Π_{com} is broken, because this is incompatible with $[\mathbf{c}]_1$ and $[\overline{\mathbf{c}}]_1$ sharing an opening and $[\overline{\mathbf{c}}]_1 \in \mathcal{L}_{\overline{ck},\mathsf{bits}}$.

[11] Note that $\mathcal{L}_1^{1,1} \equiv \mathcal{B}$, where $\mathcal{B}$ is the perfectly binding distribution defined in Section 2.6.2. The perfectly hiding case corresponds to $\mathbf{U} \leftarrow \mathcal{L}_1^{1,0} \equiv \mathcal{H}$.

```
$\mathsf{K}(gk, [\mathbf{G}]_1, n) \quad (\mathsf{S}_1(gk, [\mathbf{G}]_1, n))$
$[\overline{\mathbf{G}}]_1 \leftarrow \mathsf{MP.K}(gk, mn, \mathcal{L}_1^{mn,0})$
$\mathsf{crs}_{\mathsf{com}} \leftarrow \Pi_{\mathsf{com}}.\mathsf{K}(gk, [\mathrm{diag}(\mathbf{G}_1, n)|\mathrm{diag}(\mathbf{g}_{n+1}, n)]_1, [\overline{\mathbf{G}}]_1, mn)$
$\mathsf{crs}_{\mathsf{bits}} \leftarrow \Pi_{\mathsf{bits}}.\mathsf{K}(gk, [\overline{\mathbf{G}}]_1)$
Return $\mathsf{crs} := (\mathsf{crs}_{\mathsf{com}}, \mathsf{crs}_{\mathsf{bits}})$.
$(\tau_{\mathsf{com}} \leftarrow \Pi_{\mathsf{com}}.\mathsf{S}_1(gk, [\mathrm{diag}(\mathbf{G}, n)]_1, [\overline{\mathbf{G}}]_1, mn)$
$\tau_{\mathsf{bits}} \leftarrow \Pi_{\mathsf{bits}}.\mathsf{S}_1(gk, [\overline{\mathbf{G}}]_1)$.
$\tau := (\mathbf{a}, \tau_{\mathsf{lin}}, \tau_{\mathsf{bits}}))$.

$\mathsf{P}(\mathsf{crs}, ([\mathbf{c}]_1, \ldots, [\mathbf{c}_n]_1), \langle(\mathbf{b}_1, \ldots, \mathbf{b}_n), \mathbf{w}\rangle)$
$[\overline{\mathbf{c}}]_1 := \mathsf{MP.Com}_{[\overline{\mathbf{G}}]_1}(\mathbf{b}; \overline{w}), \overline{w} \leftarrow \mathbb{Z}_q$
$\pi_{\mathsf{com}} \leftarrow \Pi_{\mathsf{com}}.\mathsf{P}(\mathsf{crs}_{\mathsf{com}}, [\mathbf{c}]_1, [\overline{\mathbf{c}}]_1, \langle\mathbf{b}, \mathbf{w}, \overline{w}\rangle)$
$\pi_{\mathsf{bits}} \leftarrow \Pi_{\mathsf{bits}}.\mathsf{P}(\mathsf{crs}_{\mathsf{bits}}, [\overline{\mathbf{c}}]_1, \langle\mathbf{b}, \overline{w}\rangle)$
Return $([\overline{\mathbf{c}}]_1, \pi_{\mathsf{com}}, \pi_{\mathsf{bits}})$.

$\mathsf{V}(\mathsf{crs}, ([\mathbf{c}_1]_1, \ldots, [\mathbf{c}_n]_1), ([\overline{\mathbf{c}}]_1, \pi_{\mathsf{com}}, \pi_{\mathsf{bits}}))$
$\mathsf{ans}_1 \leftarrow \Pi_{\mathsf{com}}.\mathsf{V}(\mathsf{crs}_{\mathsf{com}}, [\mathbf{c}]_1, [\overline{\mathbf{c}}]_1, \pi_{\mathsf{com}})$
$\mathsf{ans}_2 \leftarrow \Pi_{\mathsf{bits}}.\mathsf{V}(\mathsf{crs}_{\mathsf{bits}}, [\overline{\mathbf{c}}]_1, \pi_{\mathsf{bits}})$
Return $\mathsf{ans}_1 \wedge \mathsf{ans}_2$.

$\mathsf{S}_2(\mathsf{crs}, ([\mathbf{c}_1]_1, \ldots, [\mathbf{c}_n]_1), [\mathbf{D}]_1, \tau)$
$[\overline{\mathbf{c}}]_1 \leftarrow \mathsf{MP.Com}_{[\overline{\mathbf{G}}]_1}(\mathbf{0}_{mn\times 1})$
$\pi_{\mathsf{com}} \leftarrow \Pi_{\mathsf{com}}.\mathsf{S}_2(\mathsf{crs}_{\mathsf{com}}, [\mathbf{c}]_1, [\overline{\mathbf{c}}]_1, \tau_{\mathsf{com}})$
$\pi_{\mathsf{bits}} \leftarrow \Pi_{\mathsf{bits}}.\mathsf{S}_2(\mathsf{crs}_{\mathsf{bits}}, [\overline{\mathbf{c}}]_1, \tau_{\mathsf{bits}})$
Return $([\overline{\mathbf{c}}]_1, \pi_{\mathsf{com}}, \pi_{\mathsf{bits}})$.
```

Figure 4.1: The proof system for the language $\mathcal{L}^n_{[\mathbf{G}]_1,\mathsf{bits}}$. Π_{bits} is the proof system from Section 4.1.3. The matrix $\mathbf{G}$ is parsed as $\mathbf{G} = (\mathbf{G}_1|\mathbf{g}_{n+1})$, and $\mathbf{c} := \mathbf{c}_1/\ldots/\mathbf{c}_n$ and $\mathbf{b} := \mathbf{b}_1/\ldots/\mathbf{b}$. The size of $[\overline{\mathbf{c}}_1]$ is 2 elements of $\mathbb{G}_1$, the size of π_{com} is 1 element of $\mathbb{G}_1$, and π_{bits} requires 10 elements of $\mathbb{G}_1$ and 10 elements of $\mathbb{G}_2$, respectively. The total proof size is 13 elements of $\mathbb{G}_1$ and 10 elements of $\mathbb{G}_2$.

The scheme

The description of the protocol is in Fig. 4.1 and we prove that:

Theorem 4.14 *The proof system from Fig. 4.1 is a QA-NIZK proof system for the language $\mathcal{L}^n_{ck,\mathsf{bits}}$ with proof size $10|\mathbb{G}_1| + 10|\mathbb{G}_2|$, perfect completeness, perfect-zero knowledge, and computational soundness.*

Proof (Completeness.) Follows from the fact that $([\mathbf{c}]_1, [\overline{\mathbf{c}}]_1) \in \mathcal{L}_{\mathsf{com},[\mathrm{diag}(\mathbf{G},n)]_1,[\overline{\mathbf{G}}]_1,mn}$ and that $[\overline{\mathbf{c}}]_1 \in \mathcal{L}_{[\overline{\mathbf{G}}]_1,\mathsf{bits}}$.

(Soundness.) When $\mathbf{G} \leftarrow \mathcal{L}_1^{m,0}$ the proof follows from the proof that $[\mathbf{c}]_1$ and $[\overline{\mathbf{c}}]_1$ open to the same value. When $\mathbf{G} \leftarrow \mathcal{L}_1^{m,i^*}$, the proof follows from the indistinguishability of the following games.

Real: This is the real soundness game. The adversary wins if it outputs $([\mathbf{c}_1]_1, \ldots, [\mathbf{c}_n]_1) \notin \mathcal{L}^n_{ck,\mathsf{bits}}$ and the corresponding proof which is accepted by the verifier.

Game_0: This game is exactly as Real except that K_1 does not receive $[\mathbf{G}]_1$ as a input but it samples $\mathbf{G}$ itself according to $\mathcal{L}_1^{m,i^*}$.

Game_1**:** This game is exactly as Game_0 except that the simulator picks a random $j^* \in [n]$ and uses $\mathbf{G}$ to check whether $\mathbf{c}_{j^*} = b_{i^*,j^*}\mathbf{g}_{i^*} + \tilde{w}\mathbf{g}_{n+1}$ such that $b_{i^*,j^*} \notin \{0,1\}$. It aborts if this is not the case.

Game_2**:** This game is exactly as Game_1 except that $\overline{\mathbf{G}} \leftarrow \mathcal{L}_1^{mn,m(i^*-1)+j^*}$.

It is obvious that the first two games are indistinguishable. The rest of the argument goes as follows.

Lemma 4.15 $\Pr\left[\mathsf{Game}_1(\mathsf{A}) = 1\right] \geq \dfrac{1}{n} \Pr\left[\mathsf{Game}_0(\mathsf{A}) = 1\right].$

Proof The probability that $\mathsf{Game}_1(\mathsf{A}) = 1$ is the probability that a) $\mathsf{Game}_0(\mathsf{A}) = 1$ and b) $b_{i^*,j^*} \notin \{0,1\}$. The view of adversary A is independent of j^*, while, if $\mathsf{Game}_0(\mathsf{A}) = 1$, then there is at least one index $\ell \in [n]$ such that $[\mathbf{c}_\ell]_1 \notin \mathcal{L}_{[\mathbf{G}]_1,\mathsf{bits}} \Longrightarrow b_{i^*,\ell} \notin \{0,1\}$. Thus, the probability that the event described in b) occurs conditioned on $\mathsf{Game}_0(\mathsf{A}) = 1$, is greater than or equal to $1/n$ and the lemma follows. □

Lemma 4.16 *There exists a* $\mathcal{D}_1$-$\mathsf{MDDH}_{\mathbb{G}_1}$ *adversary* D *such that* $|\Pr\left[\mathsf{Game}_1(\mathsf{A}) = 1\right] - \Pr\left[\mathsf{Game}_2(\mathsf{A}) = 1\right]| \leq \mathsf{Adv}_{\mathcal{L}_1,\mathsf{Gen}_a}(\mathsf{D})$.

Proof We construct an adversary D that receives a challenge $([\mathbf{A}]_1, [\mathbf{u}]_1)$ of the $\mathcal{L}_1$-$\mathsf{MDDH}_{\mathbb{G}_1}$ assumption. From this challenge, D just defines the matrix $[\overline{\mathbf{G}}]_1 \in \mathbb{G}_1^{2\times(mn+1)}$ as the matrix whose last column consists of $[\mathbf{A}]_1$, the ith column consists of $[\mathbf{u}]_1$ and the rest of the columns are random vectors in the image of $[\mathbf{A}]_1$. Then D honestly simulates the rest of the CRS, gives it as input to A, and outputs whatever A outputs.

Obviously, when $[\mathbf{u}]_1$ is sampled from the image of $[\mathbf{A}]_1, \overline{\mathbf{G}}$ follows the distribution $\mathcal{L}_1^{m,0}$ and D perfectly simulates Game_1, while if $[\mathbf{u}]_1$ is a uniform element of $\mathbb{G}_1^2$, $\overline{\mathbf{G}}$ follows the distribution $\mathcal{L}_1^{m,i^*}$ and D perfectly simulates Game_2. □

Lemma 4.17 *There exists adversaries* $\mathsf{B}_1, \mathsf{B}_2$ *such that* $\Pr[\mathsf{Game}_2(\mathsf{A}) = 1] \leq \mathbf{Adv}_{\Pi_{\mathsf{com}}}(\mathsf{B}_1) + \mathbf{Adv}_{\Pi_{\mathsf{bits}}}(\mathsf{B}_2)$.

Proof If $\mathsf{Game}(\mathsf{A}) = 1$, then $b_{i^*,j^*} \notin \{0,1\}$ while all the verification equations are accepted. Given that $\overline{\mathbf{g}}_{m(i^*-1)+j^*}$ is linearly independent from $\{\overline{\mathbf{g}}_j : j \neq m(i^*-1)+j^*\}$, it holds that $\{\overline{\mathbf{g}}_{m(i^*-1)+j^*}, \overline{\mathbf{g}}_{mn+1}\}$ is a basis for $\mathbb{Z}_q^2$ and thus we can define $\overline{b}_{i^*,j^*}, \overline{w}_{h,i}$ as the unique coefficients in $\mathbb{Z}_q$ such that $\overline{\mathbf{c}} = \overline{b}_{i^*,j^*}\overline{\mathbf{g}}_{m(i^*-1)+j^*} + \overline{w}_{h,i}\overline{\mathbf{g}}_{mn+1}$. If $b_{i^*,j^*} \neq \overline{b}_{i^*,j^*}$, then $([\mathbf{c}]_1, [\overline{\mathbf{c}}]_1)$ can not open to the same value and we can construct an adversary B_1 against Π_{com}. Else, it must be the case that $\overline{b}_{i^*,j^*} = b_{i^*,j^*} \notin \{0,1\}$. Therefore, if an adversary B_2 simulates Game_2 until A halts and outputs $([\overline{\mathbf{c}}]_1, \pi_{\mathsf{bits}})$, then B_2 breaks soundness of Π_{bits}.□

(Zero-Knowledge.) Given that $\overline{\mathbf{G}}$ defines perfectly hiding commitments, $[\overline{\mathbf{c}}]_1$ can be opened to any value. Therefore $[\overline{\mathbf{c}}]_1$ and $[\mathbf{c}]_1$ share a common opening and $[\overline{\mathbf{c}}]_1 \in \mathcal{L}_{\overline{ck},\mathsf{bits}}$, and thus π_{com} and π_{bits} are correctly distributed. □

Chapter 5

New Techniques for Non-Interactive Shuffle and Range Arguments

This chapter focuses on obtaining efficiency improvements for two non-interactive arguments, namely *range proofs* and *proof of correctness of a shuffle*, based only on falsifiable assumptions. To derive efficiency improvements for these arguments we develop a new cryptographic primitive which we call *aggregated zero-knowledge set-membership proof* (aZKSMP). A zero-knowledge set-membership proof allows to show, in zero-knowledge, that the openings of many commitments belong to a public set. We say that the proof is aggregated when the size of the proof does not depend on the number of commitments.

Our resulting proofs are more efficient in terms of proof size and are based on more standard assumptions, but they have a rather large common reference string. They build on the recent arguments for membership in linear spaces [LPJY14, JR14, KW15], arguments of membership in linear spaces of Chapter 3, and the argument for proving that some commitment to a vector of integers in $\mathbb{Z}_q^n$ opens to $\{0,1\}^n$ from Section 4.2.

5.1 Related Work

Zero Knowledge Set Membership Arguments.

Camenisch et al. constructed $\Theta(1)$ interactive zero-knowledge set membership arguments using Boneh-Boyen Signatures, and they prove them secure under the q-SDH assumption [CCs08]. Bayer and Groth constructed $\Theta(\log |S|)$ interactive zero-knowledge arguments for polynomial evaluation, which can be used to construct set membership arguments, relying only on the discrete logarithm assumption [BG13]. However, none of the previous constructions has addressed the problem of aggregating many proofs, and a direct use of them will end up with a proof of size $\Omega(n)$.

NIZK Shuffle and Range Arguments.

The most efficient NIZK shuffle argument under falsifiable assumptions is the one from Groth and Lu [GL07], which works for BBS ciphertexts. The proof size is linear in the number of ciphertexts, specifically $15n+120$ group elements in type I groups. The security of their construction relies on two assumptions: the *pairing product assumption* and the *permutation pairing assumption.* The first assumption is a $\mathcal{D}_{n,2}$-KerMDH assumption, when $\mathbf{M} \leftarrow \mathcal{D}_{n,2}$ is of the form $\mathbf{M}^\top := \begin{pmatrix} x_1, \ldots, x_n \\ x_1^2, \ldots, x_n^2 \end{pmatrix}$ for $x_i \leftarrow \mathbb{Z}_q$, $i \in [n]$. The second assumption is proven generically secure by Groth and Lu, but it seems to be unrelated with any other assumption.

Using non-falsifiable assumptions (i.e. knowledge of exponent type of assumptions), Lipmaa and Zhang [LZ12] constructed a shuffle argument with communication $6n|\mathbb{G}_1|+11|\mathbb{G}_2|$, and recently Fauzi and Lipmaa [FL15] constructed a shuffle argument with communication $(5n+2)|\mathbb{G}_1|+2n|\mathbb{G}_2|$.

Rial, Kohlweiss, and Preneel constructed a range argument in $[0, 2^n-1]$ with communication $\Theta(\frac{n}{\log n - \log\log n})$ and prove it secure under the q-HSDH assumption [RKP09]. One might get rid of the q-HSDH assumption replacing the *P-signature* with any *structure preserving signature*, but, since the proof requires $\frac{n}{\log n - \log\log n}$ Groth-Sahai proofs of satisfiability of the signature's verification equation and the signature's size is at least 6 group elements [JR17], the resulting protocol is far less efficient. Using non-falsifiable assumptions, Chaabouni, Lipmaa, and Zhang constructed a range argument with constant communication [CLZ12].

A detailed comparison of our shuffle and range arguments with the most efficient constructions under falsifiable assumptions is depicted in Table 5.1.

	Shuffle Argument		Range Argument	
	[GL07]	Π_{shuffle}	[RKP09]	$\Pi_{\mathsf{range\text{-}proof}}$
CRS size	$2n+8$	$(n^2+24n+36, 23n+37)$	$\Theta(\frac{n}{\log n - \log\log n})$	$(6n^2, 6n^2)$
Proof size	$15n+120$	$(4n+17, 14)$	$\Theta(\frac{n}{\log n - \log\log n})$	$(\frac{2n}{k\log n}, 10)$
P's comp.	$51n+246$	$11n+17$	$\Theta(\frac{n}{\log n - \log\log n})$	$2n$
V's comp.	$75n+282$	$13n+55$	$\Theta(\frac{n}{\log n - \log\log n})$	$\frac{4n}{k\log n}$
Assumption	PP	SXDH+SSDP	q-HSDH	SXDH+SSDP

Table 5.1: Comparison of our shuffle, Π_{shuffle}, and range, $\Pi_{\mathsf{range\text{-}proof}}$, arguments with the literature. To increase readability, for $\Pi_{\mathsf{range\text{-}proof}}$ we include only the leading part of the sizes, that is, we write $f(n)$ and we mean $f(n)+o(f(n))$. Notation (x, y) means x elements of $\mathbb{G}_1$ and y elements of $\mathbb{G}_2$. "PP" stands for the permutation pairing assumption. The prover's computation is measured by the number of exponentiations (i.e. $z[x]_i$) and the verifier's computation is measured by the number of pairings.

5.2 Overview

Our starting point is the observation that range and shuffle proofs can be constructed using an aZKSMP as a common building block by slightly modifying some previous strategies used for shuffle and range proofs. Before moving to shuffles and range proofs, we need to define in more detail what an aZKSMP is.

Given some publicly known set S, an aZKSMP allows to prove that n commitments $c_1, \ldots, c_n$ open to values $x_1, \ldots, x_n \in S$. The set S is of polynomial size and is either $[0, d-1] \subset \mathbb{Z}_q$ or a subset of $\mathbb{G}_\gamma$, $\gamma \in \{1, 2\}$. In other words, an aggregated set membership argument proves that each $c_1, \ldots, c_n$ is in the language

$$\mathcal{L}_{ck,S} := \{c : \exists x \in S, \mathbf{w} \in \mathbb{Z}_q^r \text{ s.t. } c = \mathsf{Com}_{ck}(x; \mathbf{w})\}, \text{ where } ck \leftarrow \mathcal{K},$$

and $c = \mathsf{Com}_{ck}(x; \mathbf{w})$ is a Groth-Sahai commitment to x with randomness $\mathbf{w}$.

The proof that we construct in Section 5.3 is quasi-adaptive, in the sense that the language and the common reference string depends on ck and S. Further, the marginal distribution of ck is witness samplable, that is, it can be sampled along with its discrete logarithms. The argument is *aggregated* because the size of the proof is independent of n ($\Theta(\log d)$

when $S = [0, d-1]$ and $\Theta(|S|)$ when $S \subset \mathbb{G}_\gamma$). However, in the soundness proof we will loose a factor of n in the reduction.

5.2.1 Range Argument

A range argument is a tool often required in e-voting and e-cash scenarios, with the purpose of showing that the opening y of some commitment c is an integer in some interval $[A, B]$. For simplicity, the range considered is usually $[0, 2^n - 1]$ since a proof in any interval can be reduced to a proof in this interval.

Let $n, d \in \mathbb{N}$, $m := \log d$, and $\ell := n/m$. A commitment c opens to a integer x in the range $[0, 2^n - 1]$ if $\exists x_1, \ldots, x_\ell \in [0, d-1]$ and $x = \sum_{i\in[\ell]} x_i d^{i-1}$. Indeed, since $x_i \in [0, d-1]$

$$x \;=\; \sum_{i\in[\ell]} x_i d^{i-1} \in [0, d^\ell - 1] = [0, (d^{1/\log d})^n - 1] = [0, 2^n - 1].$$

The statement $\exists x_1, \ldots, x_\ell \in [0, d-1]$ can be proven by showing that $(c_1, \ldots, c_n) \in \mathcal{L}^\ell_{ck,[0,d-1]}$, where $c_i = \mathsf{Com}_{ck}(x_i)$, with an aggregated set membership proof, and the statement $x = \sum_{i\in[\ell]} d^{i-1} x_i$ can be proven using standard techniques.

While this way of constructing range arguments has been widely used in the literature [CCs08, RKP09], with the addition of our techniques we get a smaller proof size. Indeed, the total cost of the range proof is $\Theta(\ell + m)$ (ℓ is due to the size of the commitments $c_1, \ldots, c_\ell$ and m to the size of an aggregated proof of membership in $\mathcal{L}^\ell_{ck,[0,d-1]}$). Setting $d = n^k$ for arbitrary k leads to a proof size of $\Theta(\frac{n}{k \log n})$. Compared to previous approaches, the novelty of ours is that the cost of proving that $x_1, \ldots, x_\ell \in [0, d-1]$ is significantly reduced.

5.2.2 Shuffle Argument

An argument of correctness of a shuffle is an essential tool in the construction of *mix-nets* [Cha81]. A mix-net, in turn, is a distributed protocol between many mixers, where each mixer receives as input a set of n ciphertexts and outputs a shuffle of the input ciphertexts. That is, a re-randomization of the set of ciphertexts obtained after applying a random permutation to the input set of ciphertexts. To enforce the honest behavior of mixers they are required to produce a zero-knowledge argument that the shuffle was correctly computed.

Our proof is partially inspired by the non-interactive shuffle of Groth and Lu [GL07]. The statement we want to prove in a correctness of a shuffle argument is : "Given two vectors of ciphertexts which open, respectively, to vectors of plaintexts $[\mathbf{m}_1]_2, [\mathbf{m}_2]_2$, prove that $[\mathbf{m}_2]_2$ is a permutation of $[\mathbf{m}_1]_2$". Roughly, our strategy is the following:

1) Publish some vector of group elements $[\mathbf{s}]_1 = ([s_1]_1, \ldots, [s_n]_1)^\top$ (which we identify with the set S of its components) in the common reference string, where $\mathbf{s}$ is sampled from some distribution $\mathcal{D}_{n,1}$.

2) The prover commits to $[\mathbf{x}]_1 = ([x_1]_1, \ldots, [x_n]_1)^\top$, a permutation of the set S and proves that the commitments to $[\mathbf{x}]_1$ are in $\mathcal{L}^n_{ck,S}$.

3) The prover proves that $\sum_{i\in[n]} [x_i]_1 = \sum_{i\in[n]} [s_i]_1$.

4) Finally, the prover outputs a proof that:[1]

$$[\mathbf{s}^\top]_1[\mathbf{m}_1]_2 = [\mathbf{x}^\top]_1[\mathbf{m}_2]_2. \tag{5.1}$$

The underlying computational assumption is that it is infeasible to find a non-trivial combination of elements of S which adds to 0, that is, given $[\mathbf{s}]_1$ it is infeasible to find $[\mathbf{k}]_2 \neq [\mathbf{0}]_2$ such that $\mathbf{s}^\top\mathbf{k} = \mathbf{0}$ (this is the $\mathcal{D}_{n,1}$-KerMDH assumption from Section 2.4).

Soundness goes as follows. First, by the soundness of the aggregated set membership proof, $[\mathbf{x}]_1 \in S^n$ and from the fact that $\sum_{i\in[n]} x_i = \sum_{i\in[n]} s_i$, it holds that if $\mathbf{x}$ is not a permutation of $\mathbf{s}$, then one can extract in the soundness game (assuming the extractor knows ck) a non-trivial linear combination of elements of S which adds to 0, which contradicts the security assumption. Finally, if $\mathbf{x}$ is a permutation of $\mathbf{s}$, then equation (5.1) implies that the shuffle is correct, or, again, one can extract from $[\mathbf{m}_1]_2, [\mathbf{m}_2]_2$ the coefficients of some non-trivial combination of elements of S which is equal to 0 (breaking the $\mathcal{D}_{n,1}$-KerMDH assumption).

This soundness argument is an augmentation and translation into asymmetric groups of the argument of Groth and Lu [GL07]. Essentially, the argument there also consists of two parts: one devoted to proving that some GS commitments open to a permutation of some set in the CRS (Groth and Lu prove this using the (non-standard) pairing permutation assumption), while the second part (Step 4) is proven very similarly (in particular, its soundness also follows from some kernel assumption secure in symmetric bilinear groups).

We note that it is crucial for our soundness argument that it is possible to decrypt the ciphertexts (otherwise we cannot extract solutions to the kernel problems). This is possible in our case because public key for encryption is assumed to be witness-samplable and the argument is quasi-adaptive. This explains why we do not refer to the notion of culpable soundness, as done by Groth and Lu [GL07] and by Fauzi and Lipmaa [FL15].

5.3 Aggregated NIZK Set Membership Arguments

In this section we construct a QA-NIZK argument that many commitments open to elements in a set $[0, d-1] \subset \mathbb{Z}_q$ or $S \subset \mathbb{G}_\gamma$. We say that the argument is aggregated because the size of the proof does not depend on the number of commitments.

Before we move to the aggregated case, we study the case of a single set membership proof.

5.3.1 Set Membership Proofs

We want to show that a single commitment belongs to the language

$$\mathcal{L}_{ck,S} := \{c : \exists x \in S, \mathbf{w} \in \mathbb{Z}_q^r \text{ s.t. } c = \mathsf{Com}_{ck}(x; \mathbf{w})\}, \text{ where } ck \leftarrow \mathcal{K},$$

and $c = \mathsf{Com}_{ck}(x; \mathbf{w})$ is a Groth-Sahai commitment to x with randomness $\mathbf{w}$.

We observe that membership in S can be written as:

- If $S \subset \mathbb{G}_\gamma$, and we identify S with $[\mathbf{s}]_\gamma = ([s_1]_\gamma, \dots, [s_m]_\gamma)^\top$ then, $c \in \mathcal{L}_{ck,S}$ if and only if $\exists \mathbf{b}, \in \mathbb{Z}_q^m$ and $\mathbf{w} \in \mathbb{Z}_q^2$ such that:

[1] This is a slightly oversimplified explanation. Actually, a prover (a mixer) does not know the randomness nor the decryptions of the ciphertexts but only the randomness of the re-encryptions, so it cannot prove exactly this statement.

   1. $\mathbf{b} \in \{0,1\}^m$,

   2. $c = \mathsf{GS.Com}_{ck}(x; \mathbf{w})$,

   3. $x = \mathbf{s}^\top \mathbf{b}$,

   4. $\sum_{i \in [m]} b_i = 1$.

- If $S = [0, d-1]$ and $m := \log d$, then $c \in \mathcal{L}_{ck,S}$ if and only if $\exists \mathbf{b} \in \mathbb{Z}_q^m$ and $w \in \mathbb{Z}_q$ such that:

   1. $\mathbf{b} \in \{0,1\}^m$,

   2. $c = \mathsf{GS.Com}_{ck}(x; w)$,

   3. $x = (1, 2, \ldots, 2^{m-1})\mathbf{b}$.

That is, both languages can be written in a similar way, except that when $S \subset \mathbb{G}_\gamma$ there is an additional linear constraint that $\mathbf{b}$ must satisfy (condition 4)).

To avoid distinguishing all the time between both types of subsets, we note that both languages can be seen as special case of the language $\mathcal{L}_{[\mathbf{M}]_1,[\mathbf{N}]_1,\mathbf{\Lambda},\boldsymbol{\alpha}} \subseteq \mathbb{G}_1^{\ell_1}$, as defined below.

Definition 5.1 *Denote by* $\mathcal{L}_{[\mathbf{M}]_1,[\mathbf{N}]_1,\mathbf{\Lambda},\boldsymbol{\alpha}} \subseteq \mathbb{G}_1^{\ell_1}$ *the language parameterized by* $[\mathbf{M}]_1 \in \mathbb{G}_1^{\ell_1 \times m}, \mathbf{N} \in \mathbb{G}_1^{\ell_1 \times \ell_2}, \mathbf{\Lambda} \in \mathbb{Z}_q^{\ell_3 \times m}$*, and* $\boldsymbol{\alpha} \in \mathbb{Z}_q^{\ell_3}$ *such that*

$$[\mathbf{c}]_1 \in \mathcal{L}_{[\mathbf{M}]_1,[\mathbf{N}]_1,\mathbf{\Lambda},\boldsymbol{\alpha}} \iff \exists \mathbf{b} \in \{0,1\}^m, \mathbf{w} \in \mathbb{Z}_q^{\ell_2} \text{ s.t. } \begin{pmatrix} \mathbf{c} \\ \boldsymbol{\alpha} \end{pmatrix} = \begin{pmatrix} \mathbf{M} & \mathbf{N} \\ \mathbf{\Lambda} & \mathbf{0}_{\ell_3 \times \ell_2} \end{pmatrix} \begin{pmatrix} \mathbf{b} \\ \mathbf{w} \end{pmatrix}. \quad (5.2)$$

Additionally, we require $(\mathbf{N}, [\mathbf{N}]_1)$ *to be efficiently samplable and that membership in* $\mathcal{L}_{[\mathbf{M}]_1,[\mathbf{N}]_1,\mathbf{\Lambda},\boldsymbol{\alpha}}$ *is efficiently testable with the trapdoor* $\mathbf{N}$*, that is, that there exists an efficient algorithm* F *such that* $\mathsf{F}([\mathbf{M}]_1, \mathbf{N}, [\mathbf{c}]_1) = 1 \iff [\mathbf{c}]_1 \in \mathcal{L}_{\mathbf{M},\mathbf{N},\mathbf{\Lambda},\boldsymbol{\alpha}}$.

The additional condition is key in the proof of soundness and allows telling apart fake from honest proofs.

Example 5.2 *The language of GS commitments to group elements in the set* $S := \{[s_1]_1, \ldots, [s_m]_1\} \subset \mathbb{G}_1$, $\mathcal{L}_{ck,S}$*, where* $ck := ([\mathbf{u}_1]_1|[\mathbf{u}_2]_1)$*, is equal to* $\mathcal{L}_{[\mathbf{M}]_1,[\mathbf{N}]_1,\mathbf{\Lambda},\boldsymbol{\alpha}}$*, where* $\mathbf{M} := \left(\begin{smallmatrix} s_1 & \cdots & s_m \\ 0 & \cdots & 0 \end{smallmatrix}\right)$*,* $\mathbf{N} := (\mathbf{u}_1 - \mathbf{e}_1|\mathbf{u}_2)$*,* $\alpha = 1$*, and* $\mathbf{\Lambda} = (1, \ldots, 1)$*. Membership in* S *is efficiently testable given* $\mathbf{u}_1, \mathbf{u}_2 \in \mathbb{Z}_q^2$ *and assuming* $|S| \in \mathsf{poly}(\lambda)$*.*

Example 5.3 *The language of GS commitments to integers in the range* $[0, d-1]$*,* $\mathcal{L}_{ck,[0,d-1]}$*, where* $ck := ([\mathbf{u}_1]_1|[\mathbf{u}_2]_1)$*, is equal to* $\mathcal{L}_{[\mathbf{M}]_1,[\mathbf{N}]_1,\mathbf{\Lambda},\boldsymbol{\alpha}}$*, where* $\mathbf{M} := \mathbf{u}_1(2^0, 2^1, \ldots, 2^{\log d - 1}) \in \mathbb{Z}_q^{2 \times \log d}$*,* $\mathbf{N} := \mathbf{u}_2 \in \mathbb{Z}_q^2$*, and* $\ell_3 := 0$*. Membership in* $\mathcal{L}_{ck,[0,d-1]}$ *is easily testable given* $\mathbf{u}_2 \in \mathbb{Z}_q^2$ *and assuming* $d \in \mathsf{poly}(\lambda)$*.*

Proof Strategy

The most efficient strategy we are aware of for proving membership in $\mathcal{L}_{[\mathbf{M}]_1,\mathbf{N},\mathbf{\Lambda},\boldsymbol{\alpha}}$ follows a commit-and-prove approach. Namely, to prove that $\mathbf{b}, \mathbf{w}$ exist, one computes GS commitments $[\mathbf{d}_i]_1$, $i \in [m]$, to all coordinates of $\mathbf{b}$ and then it proves two independent statements, namely that:

1. $\exists \mathbf{b} \in \mathbb{Z}_q^m, \mathbf{r} \in \mathbb{Z}_q^m$ such that

   a) $\mathbf{b} \in \{0,1\}^m$ and

b) $\forall i \in [m], \mathbf{d}_i = \begin{pmatrix}\mathbf{u}_1 & \mathbf{u}_2\end{pmatrix} \binom{b_i}{r_i}$.

2. $\exists \widetilde{\mathbf{b}} \in \mathbb{Z}_q^m, \widetilde{\mathbf{r}} \in \mathbb{Z}_q^m, \mathbf{w} \in \mathbb{Z}_q^{\ell_2}$ such that

    a) $\binom{\mathbf{c}}{\boldsymbol{\alpha}} = \begin{pmatrix}\mathbf{M} & \mathbf{N} \\ \boldsymbol{\Lambda} & \mathbf{0}_{\ell_3 \times \ell_2}\end{pmatrix} \binom{\widetilde{\mathbf{b}}}{\mathbf{w}}$ and

    b) $\forall i \in [m], \mathbf{d}_i = \begin{pmatrix}\mathbf{u}_1 & \mathbf{u}_2\end{pmatrix} \binom{\widetilde{b}_i}{r_i}$.

For the first statement, one can use the QA-NIZK argument for bit-strings of Section 4.2, and for the second, the QA-NIZK argument for linear spaces of [JR14, KW15] (for the latter, note that conditions 2.a) and 2.b) can be written down as a single system of equations with a large matrix $\widetilde{\mathbf{M}}$ and then satisfiability of 2.a) and 2.b) is equivalent to $(\mathbf{c}^\top, \boldsymbol{\alpha}^\top, \mathbf{d}_1^\top, \ldots, \mathbf{d}_m^\top)^\top$ being in the span of this matrix $\widetilde{\mathbf{M}}$).

Since both proofs are constant-size, the resulting proof size is dominated by the cost of the commitments to b_i, which is $\Theta(m)$. For soundness, the important point here is that we never prove that $\mathbf{b} = \widetilde{\mathbf{b}}$, but, since GS commitments are perfectly binding (or, said otherwise, because $\begin{pmatrix}\mathbf{u}_1 & \mathbf{u}_2\end{pmatrix}$ has full rank), equality holds. This immediately proves that the statement is in the language.

5.3.2 Aggregated set membership proofs

An aggregated set membership proof amounts to proving membership in $\mathcal{L}^n_{[\mathbf{M}]_1,[\mathbf{N}]_1,\boldsymbol{\Lambda},\boldsymbol{\alpha}}$. By definition, $([\mathbf{c}_1]_1, \ldots, [\mathbf{c}_n]_1) \in \mathcal{L}^n_{[\mathbf{M}]_1,[\mathbf{N}]_1,\boldsymbol{\Lambda},\boldsymbol{\alpha}}$ if and only if $\forall j \in [n], \exists \mathbf{b}_j \in \mathbb{Z}_q^m, \mathbf{w}_j \in \mathbb{Z}_q^{\ell_2}$ such that

$$1)\mathbf{b}_j \in \{0,1\}^m \wedge\ 2) \binom{\mathbf{c}_j}{\boldsymbol{\alpha}} = \begin{pmatrix}\mathbf{M} & \mathbf{N} \\ \boldsymbol{\Lambda} & \mathbf{0}_{\ell_3 \times \ell_2}\end{pmatrix} \binom{\mathbf{b}_j}{\mathbf{w}_j}.$$

Recall that we want a proof size independent of n. This rules out the naive approach of computing GS commitments to all the coordinates of $\mathbf{b}_j$, for all $j \in [n]$, as the cost is $\Theta(nm)$. Therefore, to improve on the asymptotic size of the proof, we are forced to use shrinking commitments to $b_{i,j}$. We stress that it is far from clear how to do this, as it might break down the soundness argument completely (e.g. in the single proof, we used in a fundamental way the uniqueness of the commitment openings). In fact, overcoming this problem is one of the main technical contributions of this chapter.

Our idea is to use as a shrinking commitment a two-dimensional multi-Pedersen commitment, as defined on Section 4.2.1, to commit to $\mathbf{b}_1^*, \ldots, \mathbf{b}_m^*$, where $\mathbf{b}_i^* = (b_{i,1}, \ldots, b_{i,n})^\top$ is the vector of the i th bits of all witness $\mathbf{b}_1, \ldots, \mathbf{b}_n$. Thereby, we use only $2m$ group elements and, carefully using the QA-NIZK proof systems from Sections 3 and 4, we construct a proof whose total proof size is linear in m and independent of n.

Given some matrix $\mathbf{G} \in \mathbb{Z}_q^{2\times(n+1)}$ sampled from some distribution $\mathcal{D}_{2,n+1}$, recall that the multi-Pedersen commitment to $\mathbf{y} \in \mathbb{Z}_q^n$ using randomness $r \in \mathbb{Z}_q$ is computed as $\mathsf{MP.Com}(\mathbf{y}; r) := [\mathbf{G}]_1 \binom{\mathbf{y}}{r}$. The special thing about these commitments is that one can set a "hidden" linearly independent column of $\mathbf{G}$, and thus commitments are perfectly binding at some coordinate $j^* \in [n]$ which is computationally hidden to the adversary.

Define the matrix $\mathbf{B} = (\mathbf{b}_1 | \ldots | \mathbf{b}_n) \in \{0,1\}^{m\times n}$ and let $\mathbf{b}_i^*$ be the ith row of $\mathbf{B}$. To prove $([\mathbf{c}_1]_1, \ldots, [\mathbf{c}_n]_1) \in \mathcal{L}^n_{[\mathbf{M}]_1,[\mathbf{N}]_1,\boldsymbol{\Lambda},\boldsymbol{\alpha}}$, we first compute MP commitments $[\mathbf{d}_i]_1$, $i \in [m]$, to $\mathbf{b}_i^*$. As before, the proof actually consists of two independent statements:

1. $\exists \mathbf{r} \in \mathbb{Z}_q^m, \mathbf{B} \in \mathbb{Z}_q^{m\times n}$ such that

    a) $\mathbf{B} \in \{0,1\}^{m\times n}$ and

    b) $\forall i \in [m], \mathbf{d}_i = \mathbf{G} \binom{\mathbf{b}_i^*}{r_i}$,

2. $\exists \widetilde{\mathbf{r}} \in \mathbb{Z}_q^m, \mathbf{w}_1, \ldots, \mathbf{w}_n \in \mathbb{Z}_q^{\ell_2}, \widetilde{\mathbf{B}} \in \mathbb{Z}_q^{m \times n}$, (whose rows are denoted as $\widetilde{\mathbf{b}}_i^*$, $i \in [m]$, and the columns $\widetilde{\mathbf{b}}_j$, $j \in [n]$), such that

   a) $\forall i \in [n], \left(\begin{smallmatrix} \mathbf{c}_j \\ \boldsymbol{\alpha} \end{smallmatrix}\right) = \left(\begin{smallmatrix} \mathbf{M} & \mathbf{N} \\ \boldsymbol{\Lambda} & \mathbf{0}_{\ell_3 \times \ell_2} \end{smallmatrix}\right) \left(\begin{smallmatrix} \mathbf{b}_j \\ \mathbf{w}_j \end{smallmatrix}\right)$ and

   b) $\forall i \in [m], \mathbf{d}_i = \mathbf{G} \left(\begin{smallmatrix} \widetilde{\mathbf{b}}_i^* \\ \widetilde{r}_i \end{smallmatrix}\right)$.

For the first statement we use our aggregated proof that many commitments opens to bitstrings from Section 4.2.3 and for the second, (after rewriting the equations) a QA-NIZK argument for linear spaces. With this approach, the proof remains of size $\Theta(m)$, the size of the commitments, while the rest of the proof is constant.

The interesting part is the soundness argument. The previous reasoning for the non-aggregated case (when $n = 1$) fails here because now there is no guarantee that $\mathbf{B} = \widetilde{\mathbf{B}}$ (as the openings of $[\mathbf{d}_i]_1$ are not unique). However, as we said, the distribution of the MP commitment key can be chosen so that it is binding at some coordinate j^*. This implies that for all i, the j^*th coordinate of $\mathbf{b}_i^*$ and $\widetilde{\mathbf{b}}_i^*$ is equal, i.e. the j^*th column of $\mathbf{B}$ and $\widetilde{\mathbf{B}}$ must be equal.

Thus, we have that for the coordinate j^*, the proof is sound (because $\mathbf{b}_j^*$ is uniquely determined, which was the uniqueness of openings which was necessary to prove soundness for $n = 1$). That is, the adversary cannot break soundness for any tuple $([\mathbf{c}_1]_1, \ldots, [\mathbf{c}_n]_1)$ such that $[\mathbf{c}_{j^*}]_1 \notin \mathcal{L}_{[\mathbf{M}]_1,[\mathbf{N}]_1,\boldsymbol{\Lambda},\boldsymbol{\alpha}}$. But since j^* is computationally hidden from the adversary, we can prove soundness with a loss in the reduction of $1/n$.

5.3.3 QA-NIZK Argument of Membership in $\mathcal{L}^n_{[\mathbf{M}]_1,[\mathbf{N}]_1,\boldsymbol{\Lambda},\boldsymbol{\alpha}}$

As announced in the previous section, our construction proves two different statements. For the second statement, conditions 2.a), 2.b) are written as a single system of equations with a single matrix Ξ and use Π_{lin} to prove that certain vector of $\mathbb{G}_1$ is in the span of Ξ.

This matrix is defined as:

$$\Xi(\mathbf{M}, \mathbf{N}, \boldsymbol{\Lambda}, \mathbf{G}) := \left(\begin{array}{ccc|c} \boldsymbol{\Sigma} & \cdots & \mathbf{0} & \mathbf{0} \\ \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \cdots & \boldsymbol{\Sigma} & \mathbf{0} \\ \hline \mathbf{G}_1 & \cdots & \mathbf{G}_n & \mathbf{G}_{n+1} \end{array}\right),$$

where $\boldsymbol{\Sigma} := \begin{pmatrix} \mathbf{M} & \mathbf{N} \\ \boldsymbol{\Lambda} & \mathbf{0} \end{pmatrix}$, $\mathbf{G}_i = \mathrm{diag}(\mathbf{g}_i, m)|\mathbf{0}$, $i \in [n]$, $\mathbf{G}_{n+1} := \mathrm{diag}(\mathbf{g}_{n+1}, m)$, and $\mathbf{g}_i$ is the i th column of $\mathbf{G}$.

Define $\mathbf{y} := \mathbf{c}_1/\boldsymbol{\alpha}/\ldots/\mathbf{c}_n/\boldsymbol{\alpha}/\mathbf{d}_1/\ldots/\mathbf{d}_m$ and $\mathbf{v} := \mathbf{b}_1/\mathbf{w}_1/\ldots/\mathbf{b}_n/\mathbf{w}_n/r_1/\ldots/r_n$. The statement we want to prove is that $[\mathbf{y}]_1 \in \mathbf{Im}([\Xi]_1)$, and the witness is $\mathbf{v}$. The upper left block of the matrix guarantees condition 2.a), while the two lower blocks guarantee condition 2.b). Note that Ξ has $n(\ell_1 + \ell_3) + 2m$ rows and $n(m + \ell_2) + m$, the vector $\mathbf{v}$ is of size $n(\ell_1 + \ell_3) + 2m$, and that $\mathbf{v}$ is of size $n(m + \ell_2) + m$.

The full description of the proof system is in Fig. 5.1 and security follows from Theorem 5.4.

Theorem 5.4 *There exists a QA-NIZK argument Π_{set} for membership in the language $\mathcal{L}^n_{[\mathbf{M}]_1,[\mathbf{N}]_1,\boldsymbol{\Lambda},\boldsymbol{\alpha}}$ with proof size $(2m + 11)|\mathbb{G}_1| + 10|\mathbb{G}_2|$, perfect completeness, perfect-zero knowledge and computational soundness.*

```
$\mathsf{K}(gk, [\mathbf{M}]_1, [\mathbf{N}]_1, n) \quad (\mathsf{S}_1(gk, [\mathbf{M}]_1, [\mathbf{N}]_1, n))$
$[\mathbf{G}]_1 \leftarrow \mathsf{MP.K}(1^\lambda, n)$
$[\boldsymbol{\Xi}]_1 := [\boldsymbol{\Xi}(\mathbf{M}, \mathbf{N}, \boldsymbol{\Lambda}, \mathbf{G})]_1$
$\mathsf{crs}_{\mathsf{lin}} \leftarrow \Pi_{\mathsf{lin}}.\mathsf{K}(gk, [\boldsymbol{\Xi}]_1)$
$\mathsf{crs}_{\mathsf{bits}} \leftarrow \Pi_{\mathsf{bits}}.\mathsf{K}(gk, [\mathbf{G}]_1, m)$
Return $\mathsf{crs} := (\mathsf{crs}_{\mathsf{lin}}, \mathsf{crs}_{\mathsf{bits}})$.
$(\tau_{\mathsf{lin}} \leftarrow \Pi_{\mathsf{lin}}.\mathsf{S}_1(gk, [\boldsymbol{\Xi}]_1)$
$\tau_{\mathsf{bits}} \leftarrow \Pi_{\mathsf{bits}}.\mathsf{S}_1(gk, [\mathbf{G}]_1, m)$.
$\tau := (\tau_{\mathsf{lin}}, \tau_{\mathsf{bits}}))$.
```

```
$\mathsf{P}(\mathsf{crs}, \{[\mathbf{c}_j]_1, \langle \mathbf{b}_j, \mathbf{w}_j \rangle : j \in [n]\})$
$[\mathbf{d}_i]_1 := \mathsf{MP.Com}_{[\mathbf{G}]_1}(\mathbf{b}_i^*; r_i)$,
$r_i \leftarrow \mathbb{Z}_q, \forall i \in [m]$
$\pi_{\mathsf{lin}} \leftarrow \Pi_{\mathsf{lin}}.\mathsf{P}(\mathsf{crs}_{\mathsf{lin}}, [\mathbf{y}]_1, \mathbf{v})$
$\pi_{\mathsf{bits}} \leftarrow \Pi_{\mathsf{bits}}.\mathsf{P}(\mathsf{crs}_{\mathsf{bits}}, \{[\mathbf{d}_i]_1, \langle \mathbf{b}_i^*, r_i \rangle : i \in [m]\})$
Return $([\mathbf{d}]_1, \pi_{\mathsf{lin}}, \pi_{\mathsf{bits}})$.
```

```
$\mathsf{V}(\mathsf{crs}, \{[\mathbf{c}_j]_1 : j \in [n]\}, ([\mathbf{d}]_1, \pi_{\mathsf{lin}}, \pi_{\mathsf{bits}}))$
$\mathsf{ans}_1 \leftarrow \Pi_{\mathsf{lin}}.\mathsf{V}(\mathsf{crs}_{\mathsf{lin}}, [\mathbf{y}]_1, \pi_{\mathsf{lin}})$
$\mathsf{ans}_2 \leftarrow \Pi_{\mathsf{bits}}.\mathsf{V}(\mathsf{crs}_{\mathsf{bits}}, \{[\mathbf{d}_i]_1 : i \in [m]\}, \pi_{\mathsf{bits}})$
Return $\mathsf{ans}_1 \wedge \mathsf{ans}_2$.
```

```
$\mathsf{S}_2(\mathsf{crs}, [\mathbf{c}]_1, \tau)$
$[\mathbf{d}_i]_1 := \mathsf{MP.Com}_{[\mathbf{G}]_1}(\mathbf{0}_{n \times 1}; \tilde{r}_i)$
$\tilde{r}_i \leftarrow \mathbb{Z}_q, \forall i \in [m]$
$\pi_{\mathsf{lin}} \leftarrow \Pi_{\mathsf{lin}}.\mathsf{S}(\mathsf{crs}_{\mathsf{lin}}, [\mathbf{y}]_1, \tau_{\mathsf{lin}})$
$\pi_{\mathsf{bits}} \leftarrow \Pi_{\mathsf{bits}}.\mathsf{S}(\mathsf{crs}_{\mathsf{bits}}, \{[\mathbf{d}_i]_1 : i \in [m]\}, \tau_{\mathsf{bits}})$
Return $([\mathbf{d}]_1, \pi_{\mathsf{lin}}, \pi_{\mathsf{bits}})$.
```

Figure 5.1: Proof system for the language $\mathcal{L}^n_{\mathbf{M},\mathbf{N},\boldsymbol{\Lambda},\boldsymbol{\alpha}}$, where Π_{bits} is the proof system for $\mathcal{L}^m_{ck,\mathsf{bits}}$ from Section 4.2.3, $\mathbf{d} := \mathbf{d}_1/\ldots/\mathbf{d}_m$, and $\mathbf{c} := \mathbf{c}_1/\ldots/\mathbf{c}_n$. The proof size is $(2m+11)|\mathbb{G}_1| + 10|\mathbb{G}_2|$.

Completeness. If $([\mathbf{c}_1]_1, \ldots, [\mathbf{c}_n]_1) \in \mathcal{L}^n_{[\mathbf{M}]_1,[\mathbf{N}]_1,\boldsymbol{\Lambda},\boldsymbol{\alpha}}$, then for every $j \in [m]$ there exists $\mathbf{b}_j \in \{0,1\}^m, \mathbf{w}_j \in \mathbb{Z}_q^{\ell_2}$ such that

$$\begin{pmatrix} \mathbf{c}_j \\ \boldsymbol{\alpha} \end{pmatrix} = \begin{pmatrix} \mathbf{M} & \mathbf{N} \\ \boldsymbol{\Lambda} & \mathbf{0}_{\ell_3 \times \ell_2} \end{pmatrix} \begin{pmatrix} \mathbf{b}_j \\ \mathbf{w}_j \end{pmatrix}.$$

Given that $[\mathbf{d}_i]_1 = \mathsf{MP.Com}_{[\mathbf{G}]_1}(\mathbf{b}_i^*; r_i) = \sum_{j \in [n]} b_{i,j}[\mathbf{g}_j]_1 + r_i[\mathbf{g}_{n+1}]_1$,

$$\begin{aligned} \mathbf{d}_1/\ldots/\mathbf{d}_m &= \sum_{j \in [n]} \begin{pmatrix} \mathbf{g}_j & \cdots & \mathbf{0} \\ \vdots & \ddots & \vdots \\ \mathbf{0} & \cdots & \mathbf{g}_j \end{pmatrix} \begin{pmatrix} b_{1,j} \\ \vdots \\ b_{m,j} \end{pmatrix} + \begin{pmatrix} \mathbf{g}_{n+1} & \cdots & \mathbf{0} \\ \vdots & \ddots & \vdots \\ \mathbf{0} & \cdots & \mathbf{g}_{n+1} \end{pmatrix} \begin{pmatrix} r_1 \\ \vdots \\ r_m \end{pmatrix} \\ &= (\mathbf{G}_1|\cdots|\mathbf{G}_n|\mathbf{G}_{n+1})(\mathbf{b}_1/\mathbf{w}_1/\ldots/\mathbf{b}_n/\mathbf{w}_n/\mathbf{r}). \end{aligned}$$

Combining these two facts we conclude that $[\mathbf{y}]_1 = [\boldsymbol{\Xi}]_1\mathbf{v}$, which implies that $\mathsf{ans}_1 = 1$. On the other hand, $\mathbf{b}_1^*, \ldots, \mathbf{b}_m^* \in \{0,1\}^n$ implies that $\mathsf{ans}_2 = 1$.

Soundness.

Theorem 5.5 *Let $\mathbf{Adv}_{\mathcal{PS}}(\mathsf{A})$ be the advantage of an adversary A against the soundness of the proof system described in Fig. 5.1. There exist PPT adversaries D, against $\mathcal{L}_1$-*MDDH *in* $\mathbb{G}_1$*,* B_1 *against the soundness of* Π_{lin}*, and* B_2*, against the soundness of* Π_{bits}*, such that*

$$\mathbf{Adv}_{\mathcal{PS}}(\mathsf{A}) \leq n\left(2/q + \mathbf{Adv}_{\mathcal{L}_1,\mathbb{G}_1}(\mathsf{D}) + \mathbf{Adv}_{\Pi_{\mathsf{lin}}}(\mathsf{B}_1) + \mathbf{Adv}_{\Pi_{\mathsf{bits}}}(\mathsf{B}_2)\right).$$

The proof follows from the indistinguishability of the following games:

Real This is the real soundness game. The output is 1 if the adversary breaks soundness, that is, if the adversary submits $([\mathbf{c}_1]_1, \ldots, [\mathbf{c}_n]_1) \notin \mathcal{L}^n_{[\mathbf{M}]_1,[\mathbf{N}]_1,\mathbf{\Lambda},\boldsymbol{\alpha}}$ and the corresponding proof which is accepted by the verifier.

Game_0 This is identical as Real except that algorithm K_1 does not receive $[\mathbf{N}]_1$ as input but it samples $\mathbf{N}$ itself.

Game_1 This game is identical to Game_0 except that the simulator picks a random $j^* \in [n]$, and aborts if $\mathsf{F}([\mathbf{M}]_1, \mathbf{N}, [\mathbf{c}_{j^*}]_1) = 1$ (that is to say if $[\mathbf{c}_{j^*}]_1 \in \mathcal{L}_{[\mathbf{M}]_1,[\mathbf{N}]_1,\mathbf{\Lambda},\boldsymbol{\alpha}}$.)

Game_2 This game is identical to Game_1 but now $\mathbf{G} \leftarrow \mathcal{L}_1^{n,j^*}$.

It is obvious that the first two games are indistinguishable. The rest of the argument goes as follows.

Lemma 5.6 $\Pr\left[\mathsf{Game}_1(\mathsf{A}) = 1\right] \geq \dfrac{1}{n} \Pr\left[\mathsf{Game}_0(\mathsf{A}) = 1\right].$

Proof The probability that $\mathsf{Game}_1(\mathsf{A}) = 1$ is the probability that a) $\mathsf{Game}_0(\mathsf{A}) = 1$ and b) $[\mathbf{c}_{j^*}]_1 \notin \mathcal{L}_{\mathbf{M},\mathbf{N},\mathbf{\Lambda},\boldsymbol{\alpha}}$. The view of adversary A is independent of j^*, while, if $\mathsf{Game}_0(\mathsf{A}) = 1$, then there is at least one index $j \in [n]$ such that $[\mathbf{c}_j]_1 \notin \mathcal{L}_{[\mathbf{M}]_1,[\mathbf{N}]_1,\mathbf{\Lambda},\boldsymbol{\alpha}}$. Thus, the probability that the event described in b) occurs conditioned on $\mathsf{Game}_0(\mathsf{A}) = 1$, is greater than or equal to $1/n$ and the lemma follows. □

Lemma 5.7 *There exists a* $\mathcal{L}_1$-$\mathsf{MDDH}_{\mathbb{G}_1}$ *adversary* D' *such that* $\left|\Pr\left[\mathsf{Game}_1(\mathsf{A}) = 1\right] - \Pr\left[\mathsf{Game}_2(\mathsf{A}) = 1\right]\right| \leq \mathsf{Adv}_{\mathcal{L}_1,\mathsf{Gen}_a}(\mathsf{D}')$.

The proof is obvious in the light of lemma 2.13.

Lemma 5.8 *There exist adversaries* $\mathsf{B}_1, \mathsf{B}_2$ *such that* $\Pr[\mathsf{Game}_2(\mathsf{A}) = 1] \leq \mathbf{Adv}_{\mathsf{lin}}(\mathsf{B}_1) + \mathbf{Adv}_{\mathsf{bits}}(\mathsf{B}_2)$.

Proof Let E the event where $\mathbf{y} \notin \mathbf{Im}(\Xi)$, and let B_1 the adversary against Π_{lin} that outputs $[\tilde{\mathbf{x}}]_1/[\mathbf{d}]_1$ and π_{lin}. Obviously, $\Pr[\mathsf{Game}_2(\mathsf{A}) = 1] \leq \mathbf{Adv}_{\Pi_{\mathsf{lin}}}(\mathsf{B}_1) + \Pr[\mathsf{Game}_2(\mathsf{A}) = 1 | \neg E]$, because if E occurs the adversary breaks the soundness of Π_{lin}. To prove the lemma, there is only left to bound this last probability.

If $\mathsf{Game}(\mathsf{A}) = 1$, then $[\mathbf{c}_{j^*}]_1 \notin \mathcal{L}_{[\mathbf{M}]_1,[\mathbf{N}]_1,\mathbf{\Lambda},\boldsymbol{\alpha}}$ while all the verification equations are accepted. $\neg E$ implies that there exists $\mathbf{v}$, which uniquely defines some $(\widetilde{\mathbf{b}}_{j^*}, \mathbf{w}_{j^*})$ and some $\widetilde{\mathbf{b}}_i^*$ such that:

$$\mathbf{y} = \Xi\mathbf{v} \Longrightarrow \begin{pmatrix} \mathbf{c}_{j^*} \\ \boldsymbol{\alpha} \end{pmatrix} = \begin{pmatrix} \mathbf{M} & \mathbf{N} \\ \mathbf{\Lambda} & \mathbf{0} \end{pmatrix} \begin{pmatrix} \widetilde{\mathbf{b}}_{j^*} \\ \mathbf{w}_{j^*} \end{pmatrix}$$

and $[\mathbf{d}_i]_1 = \mathsf{MP.Com}_{[\mathbf{G}]_1}(\widetilde{\mathbf{b}}_i^*; r), \forall i \in [m]$. Since in this game $[\mathbf{c}_{j^*}]_1 \notin \mathcal{L}_{\mathbf{M},\mathbf{N},\mathbf{\Lambda},\boldsymbol{\alpha}}$ (otherwise the game aborts), then $\widetilde{\mathbf{b}}_{j^*} \notin \{0,1\}^m$.

Since the MP commitment is perfectly binding at coordinate j^*, this implies that $([\mathbf{d}_1]_1, \ldots, [\mathbf{d}_m]_1) \notin \mathcal{L}^m_{[\mathbf{G}]_1,\mathsf{bits}}$. Therefore, an adversary B_2 that simulates A and outputs $(([\mathbf{d}_1]_1 \ldots, [\mathbf{d}_m]_1), \pi_{\mathsf{bits}})$ violates soundness of Π_{bits} with probability at least $\Pr[\mathsf{Game}_2(\mathsf{A}) = 1 | \neg E]$.□

Zero-Knowledge.

Theorem 5.9 *The proof system is perfect quasi-adaptive zero-knowledge.*

Proof Recall that $([\mathbf{c}_1]_1, \ldots, [\mathbf{c}_n]_1) \in \mathcal{L}^n_{[\mathbf{M}]_1,[\mathbf{N}]_1,\boldsymbol{\Lambda},\boldsymbol{\alpha}}$ implies that $\tilde{\mathbf{x}} = \mathrm{diag}(\boldsymbol{\Sigma}, n)\tilde{\mathbf{b}}$ and, given that $\mathcal{L}^{n,0}_1$ defines perfectly hiding commitments, for all $i \in [m]$ there is some $r_i \in \mathbb{Z}_q$ such that $[\mathbf{d}_i]_1 = \mathsf{MP.Com}(\mathbf{0}_{n\times 1}; \tilde{r}_i) = \mathsf{MP.Com}(\mathbf{b}^*_i; r_i)$. Then $\mathbf{y} \in \mathbf{Im}(\boldsymbol{\Xi})$ and thus perfect zero-knowledge of Π_{lin} and Π_{bits} implies that π_{lin} and π_{bits} are correctly distributed. □

5.4 Proof of Correctness of a Shuffle

In a NIZK shuffle argument one wants to prove that two lists of ciphertexts open to the same values when second list is permuted under some hidden permutation. We represent each list of ciphertexts as a matrix in $\mathbb{G}_2^{2\times n}$ where each column is an El-Gamal ciphertext under public key $pk := [\mathbf{v}]_2 \in \mathbb{G}_2^2$ and we write $\mathsf{Enc}_{pk}([\mathbf{m}^\top]_2; \mathbf{r}^\top) := (\mathsf{Enc}_{pk}([m_1]_2; r_1)|\cdots|\mathsf{Enc}_{pk}([m_n]_2; r_n))$, where $[\mathbf{m}]_2 \in \mathbb{G}_2^n$, $\mathbf{r} \in \mathbb{Z}_q^n$, and $\mathsf{Enc}_{pk}([m]_2; r) := [m]_2\mathbf{e}_2 + r[\mathbf{v}]_2$. Similarly, through this section we will sometimes write $\mathsf{GS.Com}_{ck}([\mathbf{x}^\top]_\gamma; \mathbf{R}) := (\mathsf{GS.Com}_{ck}([x_1]_\gamma; \mathbf{r}_1)|\cdots|\mathsf{GS.Com}_{ck}([x_n]_\gamma;\mathbf{r}_n))$, where $\mathbf{R} = (\mathbf{r}_1|\cdots|\mathbf{r}_n) \in \mathbb{Z}_q^{2\times n}$.

The language of correct shuffles under public key $pk := [\mathbf{v}]_2 \in \mathbb{G}_2^2$ can be defined as

$$\begin{aligned}\mathcal{L}_{pk,n,\mathsf{shuffle}} := \{([\mathbf{C}]_2,[\mathbf{D}]_2) \in \mathbb{G}_2^{2\times n} \times \mathbb{G}_2^{2\times n} :\\ \exists \mathbf{P} \in \mathcal{S}_n, \boldsymbol{\delta} \in \mathbb{Z}_q^n \text{ s.t. } [\mathbf{C}]_2\mathbf{P} - [\mathbf{D}]_2 = \mathsf{Enc}_{pk}([\mathbf{0}_{1\times n}]_2; \boldsymbol{\delta}^\top)\},\end{aligned}$$

where $\mathcal{S}_n$ is the set of permutation matrices of size $n\times n$. This definition can be generalized for any "El-Gamal like" encryption scheme as, for example, the BBS encryption scheme [BBS04].

5.4.1 Our construction

Our proof system builds on a proof that a set of GS commitments open to elements in the set $S = \{[s_1]_1, \ldots, [s_n]_1\}$, where $\mathbf{s} := (s_1, \ldots, s_n)^\top \leftarrow \mathcal{D}_{n,1}$ and the $\mathcal{D}_{n,1}$-KerMDH assumption holds in $\mathbb{G}_1$. Given $[\mathbf{F}]_1 \in \mathbb{G}_1^{2\times n}$, where the i th column is $[\mathbf{f}_i]_1 \leftarrow \mathsf{GS.Com}([x_i]_1)$, let $\mathbf{x} := (x_1, \ldots, x_n)^\top = \mathbf{P}\mathbf{s}$, for some permutation matrix $\mathbf{P}$, and given a commitment to $[y]_1 := [\mathbf{s}^\top]_1\boldsymbol{\delta}$, we prove that $([\mathbf{C}]_2, [\mathbf{D}]_2) \in \mathcal{L}_{pk,n,\mathsf{shuffle}}$ as follows:

a) Show that $[\mathbf{F}]_1 \in \mathcal{L}^n_{ck,S}$, where $ck \leftarrow \mathsf{GS.K}(gk)$.

b) Give a GS proof for the satisfiability of $\sum_{i\in[n]}[s_i]_1 - \sum_{j\in[n]}[x_j]_1 = [0]_1$.

c) Give a GS proof for the satisfiability of $[\mathbf{x}^\top]_1[\mathbf{C}^\top]_2 - [\mathbf{s}^\top]_1[\mathbf{D}^\top]_2 = [y]_1[\mathbf{v}^\top]_2$.

Soundness Intuition.

Conditions a) and b) implies that $\mathbf{x}$ is a permutation of $\mathbf{s}$ or equivalently, $\mathbf{x} = \mathbf{P}\mathbf{s}$ and $\mathbf{P}$ is a permutation matrix. Note that $\mathbf{P}$ is a permutation matrix iff $\mathbf{P}$ is a binary matrix and for each row and column there is at most one 1. Let's see in more detail why $\mathbf{x}$ is a permutation of $\mathbf{s}$. Condition a) implies that each x_i is an element from $\{s_1, \ldots, s_n\}$, which can be written as $\mathbf{x} = \mathbf{P}\mathbf{s}$, $\mathbf{P} \in \{0,1\}^{n\times n}$, where each row of $\mathbf{P}$ has at most one 1. But, given that there might be repeated elements, there might be also more than one 1 in some column of $\mathbf{P}$. For example, if $S = \{s_1, s_2, s_3\}$, it may be that $\mathbf{x} = \left(\begin{smallmatrix} s_2 \\ s_3 \\ s_1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} s_1 \\ s_2 \\ s_3 \end{smallmatrix}\right)$ but also $\mathbf{x} = \left(\begin{smallmatrix} s_2 \\ s_3 \\ s_3 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} s_1 \\ s_2 \\ s_3 \end{smallmatrix}\right)$. Condition b) implies that there are no repeated x_is unless one can break the $\mathcal{D}_{n,1}$-KerMDH assumption. Indeed, there are repeated x_is iff $(1,\ldots,1)\mathbf{P}$ (the row vector of "frequencies" of $\mathbf{x}$, which in the first example is $(1,1,1)$ and in the second $(0,1,2)$) is not equal to $(1,\ldots,1)$. Given that b) is equivalent to $((1,\ldots,1)-(1,\ldots,1)\mathbf{P})[\mathbf{s}]_1 = [0]_1$, then $((1,\ldots,1)-(1,\ldots,1)\mathbf{P})^\top$ is solution to the $\mathcal{D}_{n,1}$-KerMDH problem. We conclude that $\mathbf{P}$ is a permutation matrix and thus $\mathbf{x}$ is a permutation of $\mathbf{s}$.

The remainder of the proof follows essentially Groth and Lu's proof. Suppose that $[\mathbf{C}]_2 = \mathsf{Enc}_{[\mathbf{v}]_2}([\mathbf{m}^\top]_2)$ and $[\mathbf{C}]_2 = \mathsf{Enc}_{[\mathbf{v}]_2}([\mathbf{n}^\top]_2)$. Let $\mathbf{k} = (-v_2/v_1, 1)^\top$ the "decryption key" (i.e. $\mathbf{v}^\top\mathbf{k} = 0$ and $(0,1)\mathbf{k} = 1$)[2], we multiply by $\mathbf{k}$, on the right, the equation from condition c) to "decrypt" $[\mathbf{C}]_2$ and $[\mathbf{D}]_2$. We get that $[\mathbf{s}^\top]_1\mathbf{P}^\top[\mathbf{m}]_2 - [\mathbf{s}^\top]_1[\mathbf{n}]_2 = [0]_T$, which implies that $\mathbf{P}^\top[\mathbf{m}]_2 = [\mathbf{n}]_2$ unless $\mathbf{P}^\top[\mathbf{m}]_2 - [\mathbf{n}]_2$ is a solution to the $\mathcal{D}_{n,1}$-KerMDH. Finally this implies that $[\mathbf{C}]_2\mathbf{P} - [\mathbf{D}]_2$ is an encryption of $[\mathbf{0}_{n\times 1}]_2$ and thus $([\mathbf{C}]_2, [\mathbf{D}]_2) \in \mathcal{L}_{pk,n,\mathsf{shuffle}}$.

A detailed description of our construction is in Fig. 5.2 and the proof of security follows from Theorem 5.10

Theorem 5.10 *The proof system from Fig. 5.2 is a QA-NIZK proof system for the language $\mathcal{L}_{pk,n,\mathsf{shuffle}}$ with perfect completeness, computational soundness, and computational zero-knowledge.*

Proof (Completeness.) If $\mathbf{P}$ is a permutation matrix and $\mathbf{x} = \mathbf{P}\mathbf{s}$, then $\mathsf{GS.Com}(\mathbf{x}^\top) \in \mathcal{L}^n_{S,\mathbf{u}_1,\mathbf{u}_2}$ and $\sum_{i\in[n]}[s_i]_1 - \sum_{j\in[n]}[x_j]_1 = [0]_1$. If $[y]_1 = [\mathbf{s}^\top]_1\boldsymbol{\delta}$ then

$$[\mathbf{x}^\top]_1[\mathbf{C}^\top]_2 - [\mathbf{s}^\top]_1[\mathbf{D}^\top]_2 = [\mathbf{s}^\top]_1([\mathbf{C}]_2\mathbf{P} - [\mathbf{D}]_2)^\top = [\mathbf{s}^\top]_1([\mathbf{v}]_2\boldsymbol{\delta}^\top)^\top = [y]_1[\mathbf{v}^\top]_2.$$

(Soundness.) We will show that for any adversary A against the soundness of the proof system from Figure 5.2, there exist an adversary B_1 against soundness of Π_{set} and an adversary B_2 against the $\mathcal{D}_{n,1}$-KerMDH assumption such that

$$\mathbf{Adv}(\mathsf{A}) \leq \mathbf{Adv}_{\Pi_{\mathsf{set}}}(\mathsf{B}_1) + \mathbf{Adv}_{\mathcal{D}_{n,1}\text{-}\mathsf{KerMDH}}(\mathsf{B}_2).$$

The adversary B_1 receives as input $\mathsf{crs}_{\mathsf{set}}$ and honestly samples the rest of the CRS. Then B_1 runs A until it halts and outputs $[\mathbf{F}]_1$ with the proof π_{set}.

The adversary B_2 receives as input $[\mathbf{s}]_1 \in \mathbb{G}_1^n$, samples $\mathbf{u}_1, \mathbf{u}_2, \mathbf{v} \leftarrow \mathbb{Z}_q^2$, honestly simulates the rest of the CRS, and runs A until it halts. It extracts $[\mathbf{x}^\top]_1$, the opening of $[\mathbf{F}]_1$, using $\mathbf{u}_1, \mathbf{u}_2$, and aborts if $[\mathbf{F}]_1 \notin \mathcal{L}^n_{\mathbf{u}_1,\mathbf{u}_2,S}$. Else $[\mathbf{x}]_1 = \mathbf{B}[\mathbf{s}]_1$, where $\mathbf{B} \in \{0,1\}^{n\times n}$ and $\mathbf{B}\mathbf{1}_{n\times 1} = \mathbf{1}_{n\times 1}$. If there are repeated x_is, B outputs $(\mathbf{1}_{1\times n} - \mathbf{1}_{1\times n}\mathbf{B})^\top$. Else, using $\mathbf{v}$, B_2 decrypts $[\mathbf{C}]_2$ and $[\mathbf{D}]_2$ obtaining $[\mathbf{m}^\top]_2 \in \mathbb{G}_2^{1\times n}$ and $[\mathbf{n}^\top]_2 \in \mathbb{G}_2^{1\times n}$, respectively, and returns $\mathbf{B}^\top[\mathbf{m}]_2 - [\mathbf{n}]_2$.

Let E_1 the event where $([\mathbf{C}]_2, [\mathbf{D}]_2) \in \mathcal{L}_{pk,n,\mathsf{shuffle}}$, E_2 the event where $[\mathbf{F}]_1 \in \mathcal{L}^n_{\mathbf{u}_1,\mathbf{u}_2,S}$, and E_3 the event where $\mathbf{1}_{1\times n} = \mathbf{1}_{1\times n}\mathbf{B} \wedge \mathbf{B}^\top[\mathbf{m}]_2 - [\mathbf{n}]_2 = 0$. Note that $E_2 \wedge E_3 \implies E_1$ since E_2 implies that $\mathbf{x} = \mathbf{B}\mathbf{s}$, where $\mathbf{B} \in \{0,1\}^{n\times n}$ and $\mathbf{B}\mathbf{1}_{n\times 1} = \mathbf{1}_{n\times 1}$, and together with E_3 implies that $\mathbf{B}$ is a permutation. Note also that $\mathsf{eq}_1 \wedge \mathsf{eq}_2 \wedge \neg E_3$ implies that

[2] The availability of the decryption key $\mathbf{k}$ in the soundness reduction is possible since the reduction samples by itself the language parameter $\mathbf{v}$. Correspondingly Groth and Lu [GL07] proved *culpable soundness* (also called co-soundness), which essentially requires the soundness adversary to produce the decryption key.

```
$\mathsf{K}(gk, [\mathbf{v}]_2, n) \quad (\mathsf{S}_1(gk, [\mathbf{v}]_2, n))$
$S := \{[s_1]_1, \ldots, [s_n]_1\}, \mathbf{s}^\top \leftarrow \mathcal{L}_{1,n}$
$\mathsf{crs}_{\mathsf{GS}} \leftarrow \mathsf{GS.K}(gk)$
$\mathsf{crs}_{\mathsf{set}} \leftarrow \Pi_{\mathsf{set}}.\mathsf{K}(gk, [\mathbf{M}]_1, [\mathbf{N}]_1, [\mathbf{\Lambda}]_1, n)$
Return $\mathsf{crs} := ([\mathbf{v}]_2, \mathsf{crs}_{\mathsf{GS}}, \mathsf{crs}_{\mathsf{set}})$.
$(\tau_{\mathsf{GS}} \leftarrow \mathsf{GS.S}_1(gk)$
$\tau_{\mathsf{set}} \leftarrow \Pi_{\mathsf{set}}.\mathsf{S}_1(gk, L, [\mathbf{M}]_1, [\mathbf{N}]_1, [\mathbf{\Lambda}]_1, n)$.
$\tau := (\mathbf{s}, \tau_{\mathsf{GS}}, \tau_{\mathsf{set}}))$.

$\mathsf{P}(\mathsf{crs}, [\mathbf{C}]_2, [\mathbf{D}]_2, \langle \mathbf{P}, \boldsymbol{\delta} \rangle)$
$[\mathbf{x}]_1 := \mathbf{P}[\mathbf{s}]_1, [y]_1 := [\mathbf{s}^\top]_1 \boldsymbol{\delta}$
$\pi_{\mathsf{GS}} \leftarrow \mathsf{GS.P}(\mathsf{crs}_{\mathsf{GS}}, \{\mathsf{eq}_1, \mathsf{eq}_2\}, \langle [\mathbf{x}]_1, [y]_1 \rangle)$
$\pi_{\mathsf{set}} \leftarrow \Pi_{\mathsf{set}}.\mathsf{P}(\mathsf{crs}_{\mathsf{set}}, [\mathbf{F}]_1, \langle \mathbf{P}^\top, \mathbf{R} \rangle)$
$//[\mathbf{F}]_1 = \mathsf{GS.Com}_{\mathsf{crs}_{\mathsf{GS}}}([\mathbf{x}^\top]_1; \mathbf{R})$
Return $(\pi_{\mathsf{GS}}, \pi_{\mathsf{set}})$.

$\mathsf{V}(\mathsf{crs}, [\mathbf{C}]_2, [\mathbf{D}]_2, (\pi_{\mathsf{GS}}, \pi_{\mathsf{set}}))$
$\mathsf{ans}_1 \leftarrow \mathsf{GS.V}(\mathsf{crs}_{\mathsf{GS}}, \{\mathsf{eq}_1, \mathsf{eq}_2\}, \pi_{\mathsf{GS}})$
$\mathsf{ans}_2 \leftarrow \Pi_{\mathsf{set}}.\mathsf{V}(\mathsf{crs}_{\mathsf{set}}, [\mathbf{F}]_1, \pi_{\mathsf{set}})$
Return $\mathsf{ans}_1 \wedge \mathsf{ans}_2$.

$\mathsf{S}_2(\mathsf{crs}, [\mathbf{C}]_1, [\mathbf{D}]_1, \tau)$
$\pi_{\mathsf{GS}} \leftarrow \mathsf{GS.S}_2(\mathsf{crs}_{\mathsf{GS}}, \{\mathsf{eq}_1, \mathsf{eq}'_2\}, \tau_{\mathsf{GS}})$
$\pi_{\mathsf{set}} \leftarrow \Pi_{\mathsf{set}}.\mathsf{S}_2(\mathsf{crs}_{\mathsf{set}}, [\mathbf{F}]_1, \tau_{\mathsf{set}})$
Return $(\pi_{\mathsf{GS}}, \pi_{\mathsf{set}})$.
```

Figure 5.2: The proof system Π_{shuffle} for the language $\mathcal{L}_{[\mathbf{v}]_2,n,\mathsf{shuffle}}$. Π_{set} is the proof system from Section 5.3.3. The matrices $\mathbf{M}, \mathbf{N}, \mathbf{\Lambda}$ are defined as $\mathbf{M} := \binom{\mathbf{s}^\top}{\mathbf{0}_{1\times n}}$, $\mathbf{N} := (\mathbf{u}_1|\mathbf{u}_2), \mathbf{\Lambda} := (1, \ldots, 1)$, where $\mathbf{u}_1, \mathbf{u}_2$ are the GS commitment keys from $\mathsf{crs}_{\mathsf{GS}}$, and the equations are defined as $\mathsf{eq}_1 := \sum_{i\in[n]}[s_i]_1 - \sum_{j\in[n]}[x_i]_1 = [0]_1$, $\mathsf{eq}_2 := [\mathbf{x}^\top]_1[\mathbf{C}^\top]_2 - [\mathbf{s}^\top]_1[\mathbf{D}^\top]_2 = [y]_1[\mathbf{v}^\top]_2$, and $\mathsf{eq}'_2 := [\mathbf{x}^\top]_1[\mathbf{C}^\top]_2 - [1]_1[\mathbf{s}^\top\mathbf{D}^\top]_2 = [y]_1[\mathbf{v}^\top]_2$. The proof size is $(4n + 17)|\mathbb{G}_1| + 14|\mathbb{G}_2| + 1|\mathbb{Z}_q|$

$(\mathbf{1}_{1\times n} - \mathbf{B}\mathbf{1}_{1\times n})^\top$ or $\mathbf{B}^\top[\mathbf{m}]_1 - [\mathbf{n}]_2$ are solutions to the $\mathcal{D}_{1,n}$-KerMDH. Then it holds that

$$\begin{aligned}
\mathbf{Adv}(\mathsf{A}) &= \Pr[\neg E_1 \wedge \mathsf{V}(\mathsf{crs}, ([\mathbf{C}]_2, [\mathbf{D}]_2), \pi) = 1] \\
&= \Pr[\neg E_1 \wedge \mathsf{V}(\mathsf{crs}, ([\mathbf{C}]_2, [\mathbf{D}]_2), \pi) = 1 \wedge \neg E_2] + \\
&\quad\ \Pr[\neg E_1 \wedge \mathsf{V}(\mathsf{crs}, ([\mathbf{C}]_2, [\mathbf{D}]_2), \pi) = 1 \wedge E_2] \\
&\leq \Pr[\neg E_2 \wedge \Pi_{\mathsf{set}}.\mathsf{V}(\mathsf{crs}_{\mathsf{set}}, [\mathbf{F}]_2, \pi_{\mathsf{set}}) = 1] + \Pr[\neg E_1 \wedge \mathsf{eq}_1 \wedge \mathsf{eq}_2 \wedge E_2] \\
&\leq \mathbf{Adv}_{\Pi_{\mathsf{set}}}(\mathsf{B}_1) + \Pr[\neg E_1 \wedge \mathsf{eq}_1 \wedge \mathsf{eq}_2 \wedge E_2 \wedge E_3] + \\
&\quad\ \Pr[\neg E_1 \wedge \mathsf{eq}_1 \wedge \mathsf{eq}_2 \wedge E_2 \wedge \neg E_3] \\
&\leq \mathbf{Adv}_{\Pi_{\mathsf{set}}}(\mathsf{B}_1) + \Pr[\neg E_1 \wedge E_2 \wedge E_3] + \Pr[\mathsf{eq}_1 \wedge \mathsf{eq}_2 \wedge \neg E_3] \\
&= \mathbf{Adv}_{\Pi_{\mathsf{set}}}(\mathsf{B}_1) + 0 + \mathbf{Adv}_{\mathcal{D}_{1,n}\text{-}\mathsf{KerMDH}}(\mathsf{B}_2).
\end{aligned}$$

(Zero-Knowledge.) We need to check that the inputs to the simulators are true statements and, for the GS simulator, that the equations allow simulation. This is certainly true for eq_1 and, if $([\mathbf{C}]_1, [\mathbf{D}]_1) \in \mathcal{L}_{pk,n,\mathsf{shuffle}}$, then is also true for eq'_2. Furthermore, it is guaranteed that π_{GS} is computationally indistinguishable from a real proof for $\{\mathsf{eq}_1, \mathsf{eq}'_2\}$, which is identically distributed to a real proof for $\{\mathsf{eq}_1, \mathsf{eq}_2\}$ since eq'_2 and eq_2 accepts the same set of solutions. Finally, since the perfectly hiding $\mathsf{crs}_{\mathsf{GS}}$ is such that $\mathbf{rank}(\mathbf{u}_1|\mathbf{u}_2) = 2$, then $\mathcal{L}^n_{\mathbf{u}_1,\mathbf{u}_2,S} = \mathbb{G}_1^{2\times n}$ and thus $[\mathbf{F}]_1 \in \mathcal{L}^n_{\mathbf{u}_1,\mathbf{u}_2,S}$ is always true. □

5.5 Range Argument

We want to prove that a GS commitment $[\mathbf{c}]_1$ opens to some integer y in the range $[0, 2^n - 1]$. That is, construct a NIZK proof system for the language

$$\mathcal{L}_{ck,[0,2^n-1]} := \{[\mathbf{c}]_1 \in \mathbb{G}_1^2 : \exists y, r \in \mathbb{Z}_q \text{ s.t. } [\mathbf{c}]_1 = \mathsf{GS.Com}(y; r) \wedge y \in [0, 2^n - 1]\},$$

where $ck := ([\mathbf{u}_1]_1, [\mathbf{u}_2]_1) \leftarrow \mathsf{GS.K}(1^\lambda)$. Our proof is as follows:

a) Commit to $y_1, \dots y_\ell$.

b) Show that $y_i \in [0, d-1]$, for each $i \in [\ell]$.

c) Show that $y = \sum_{i\in[\ell]} y_i d^{i-1}$.

Given that it must hold that $\ell = n/\log d$, the total size of the proof is $\mathsf{S}_{[0,d-1]}(\ell) + \Theta(\ell)$, where $\mathsf{S}_{[0,d-1]}(\ell)$ is the size of ℓ range proofs in the interval $[0, d-1]$.

5.5.1 Our Construction

Note that b) is equivalent to show that $(\mathsf{GS.Com}(y_1)|\cdots|\mathsf{GS.Com}(y_\ell)) \in \mathcal{L}^\ell_{ck,[0,d-1]}$. Thus, using the proof system from Section 5.3 we are able to aggregate ℓ range proofs in the interval $[0, d-1]$ into a single proof of size $\Theta(\log d)$. Choosing $d = n^k$ we get that $\mathsf{S}_{[0,d-1]}(\ell) = \Theta(k \log n)$ and $\ell = n/\log n^k = \frac{n}{k\log n}$, and thus the size of our range proof is $\Theta(\frac{n}{k \log n})$ for an arbitrarily chosen $k \in \mathbb{N}$. One would be tempted to choose $d = 2^{\sqrt{n}}$ to obtain a proof of size $\Theta(\sqrt{n})$. However, the proof system from Section 5.3 requires membership in $\mathcal{L}_{ck,[0,d-1]}$ to be efficiently testable, which seems to be infeasible as when $d = 2^{\sqrt{n}}$.

A detailed description of our proof system is in Fig. 5.3 and security follows from Theorem 5.11

Theorem 5.11 *The proof system from Fig. 5.3 is a QA-NIZK proof system for the language $\mathcal{L}_{ck,[0,2^n-1]}$ with perfect completeness, computational soundness, and computational zero-knowledge.*

Proof (Completeness.) If $[\mathbf{c}]_1 = \mathsf{GS.Com}(y; r)$ and $y \in [0, 2^n - 1]$, then there exists $y_1, \dots, y_\ell \in [0, d-1]$ such that $y = \sum_{i\in[\ell]} y_i d^{i-1}$. Therefore $\mathbf{y} = (y_1, \dots, y_\ell)^\top$ and r are solutions to eq and $[\mathbf{X}]_1 = \mathsf{GS.Com}(\mathbf{y}^\top) \in \mathcal{L}^\ell_{\mathbf{u}_1',\mathbf{u}_2',d}$.

(Soundness.) Given an adversary A against the soundness of the proof system from Fig. 5.3, we construct an adversary B against the soundness of Π_{bin}. If $y \notin [0, 2^n - 1]$, then the perfect soundness of GS proofs implies that there is some $y_i \notin [0, d-1]$. Therefore $[\mathbf{X}]_1 = \mathsf{GS.Com}(\mathbf{y}^\top) \notin \mathcal{L}^\ell_{\mathbf{u}_1',\mathbf{u}_2',d}$ and $\mathbf{Adv}_{\Pi_{\mathsf{range-proof}}}(\mathsf{A}) \leq \mathbf{Adv}_{\Pi_{\mathsf{bin}}}(\mathsf{B})$.

(Zero-Knowledge.) Follows directly from zero-knowledge of GS proofs, the fact that eq allows simulation, and the fact that $[\mathbf{X}]_1 = \mathsf{GS.Com}(\mathbf{0}_{1\times n}) \in \mathcal{L}^\ell_{d,\mathbf{u}_1',\mathbf{u}_2'}$. □

```
$\mathsf{K}_1(gk, [\mathbf{u}]_1, [\mathbf{u}_2]_1, n) \quad (\mathsf{S}_1(gk, [\mathbf{u}_1]_1, [\mathbf{u}_2]_1, n))$
$d := n^k, m := \log d, \ell := n/m$
$\mathsf{crs}_{\mathsf{GS}} \leftarrow \mathsf{GS}.\mathsf{K}_1(gk)$
$\mathsf{crs}_{\mathsf{set}} \leftarrow \Pi_{\mathsf{set}}.\mathsf{K}_1(gk, [\mathbf{M}]_1, [\mathbf{N}]_1, n)$
Return $\mathsf{crs} := ([\mathbf{u}_1]_1, [\mathbf{u}_2]_1, \mathsf{crs}_{\mathsf{GS}}, \mathsf{crs}_{\mathsf{set}})$.
$(\tau_{\mathsf{GS}} \leftarrow \mathsf{GS}.\mathsf{S}_1(gk)$
$\tau_{\mathsf{set}} \leftarrow \Pi_{\mathsf{set}}.\mathsf{S}_1(gk, [\mathbf{M}]_1, [\mathbf{N}]_1, n)$.
$\tau := (\tau_{\mathsf{GS}}, \tau_{\mathsf{set}}))$.
```

```
$\mathsf{P}(\mathsf{crs}, [\mathbf{c}]_1, \langle y, r \rangle)$
$\mathbf{y} \in \mathbb{Z}_q^\ell$ is s.t. $y = \sum_{i \in [\ell]} y_i d^{i-1}$
$\mathbf{B} \in \{0,1\}^{m \times \ell}$ is s.t.
    $\mathbf{y}^\top = (2^0, \ldots, 2^{m-1})\mathbf{B}$
$\pi_{\mathsf{GS}} \leftarrow \mathsf{GS}.\mathsf{P}(\mathsf{crs}_{\mathsf{GS}}, \mathsf{eq}, \langle \mathbf{y}, r \rangle)$
$\pi_{\mathsf{set}} \leftarrow \Pi_{\mathsf{set}}.\mathsf{P}(\mathsf{crs}_{\mathsf{set}}, [\mathbf{X}]_1, \langle \mathbf{B}, \mathbf{R} \rangle)$
$//[\mathbf{X}]_1 = \mathsf{GS}.\mathsf{Com}_{\mathsf{crs}_{\mathsf{GS}}}(\mathbf{y}^\top; \mathbf{R})$
Return $(\pi_{\mathsf{GS}}, \pi_{\mathsf{set}})$.
```

```
$\mathsf{V}(\mathsf{crs}, [\mathbf{c}]_1, (\pi_{\mathsf{GS}}, \pi_{\mathsf{set}}))$
$\mathsf{ans}_1 \leftarrow \mathsf{GS}.\mathsf{V}(\mathsf{crs}_{\mathsf{GS}}, \mathsf{eq}, \pi_{\mathsf{GS}})$
$\mathsf{ans}_2 \leftarrow \Pi_{\mathsf{set}}.\mathsf{V}(\mathsf{crs}_{\mathsf{set}}, [\mathbf{X}]_1, \pi_{\mathsf{set}})$
Return $\mathsf{ans}_1 \wedge \mathsf{ans}_2$.
```

```
$\mathsf{S}_2(\mathsf{crs}, [\mathbf{c}]_1, \tau)$
$\pi_{\mathsf{GS}} \leftarrow \mathsf{GS}.\mathsf{S}_2(\mathsf{crs}_{\mathsf{GS}}, \mathsf{eq}, \tau_{\mathsf{GS}})$
$\pi_{\mathsf{set}} \leftarrow \Pi_{\mathsf{set}}.\mathsf{S}_2(\mathsf{crs}_{\mathsf{set}}, [\mathbf{X}]_1, \tau_{\mathsf{set}})$
$//[\mathbf{X}]_1 = \mathsf{GS}.\mathsf{Com}_{\mathsf{crs}_{\mathsf{GS}}}(\mathsf{Y}; \mathbf{R})$
Return $(\pi_{\mathsf{GS}}, \pi_{\mathsf{set}})$.
```

Figure 5.3: The proof system $\Pi_{\mathsf{range\text{-}proof}}$ for the language $\mathcal{L}_{ck,[0,2^n-1]}$. Π_{set} is the proof system from Section 5.3.3. The matrices $\mathbf{M}, \mathbf{N}$ are defined as $\mathbf{M} := \mathbf{u}_1'(2^0, 2^1, \ldots, 2^{m-1}), \mathbf{N} := \mathbf{u}_2'$, where $\mathbf{u}_1', \mathbf{u}_2'$ are the GS commitment keys from $\mathsf{crs}_{\mathsf{GS}}$. The equation eq is defined as $[\mathbf{c}]_1 - \sum_{i \in [\ell]} y_i d^{i-1}[\mathbf{u}_1]_1 = r[\mathbf{u}_2]_1$.

Chapter 6

Ring Signature of Size $\Theta(\sqrt[3]{n})$ without Random Oracles

Ring signatures, introduced by Rivest, Shamir and Tauman, [RST01], allow to anonymously sign a message on behalf of a *ring* of users $P_1, \dots, P_n$, only if the signer belongs to the ring. Although there are other cryptographic schemes that provides similar guarantees (e.g. group signatures [Cv91]), ring signatures are not coordinated: each user generates secret/public keys on his own – i.e. no central authorities – and might sign on behalf of a ring without the approval or assistance of the other members.

The literature on ring signatures is vast, and, while there exist even logarithmic size solutions [GK15, LLNW16], most of them rely on the random oracle model (ROM). The ROM idealizes the behavior of hash functions and proofs of security in the ROM model are considered only heuristic arguments, since there are protocols secure in the ROM but insecure using any real hash functions [CGH98]. Without random oracles all the constructions have signatures of size linear in the size of the ring, being the the sole exception the $\Theta(\sqrt{n})$ ring signature of Chandran et al. [CGS07] (already discussed, and optimized, in Section 4.1.6). We remark that no asymptotic improvements to Chandran et al.'s construction have been made since their introduction (only improvements in the constants by Ràfols [Ràf15] and the improvements from Section 4.1.6). We note that although some previous works claim to construct signatures of constant [BDR15] or logarithmic [GSP16] size, they are either in a weaker security model or we can identify a flaw in the construction (see Section 6.2.2).

In this section we present the first ring signature whose signature size is asymptotically smaller than Chandran et al.'s. Specifically, our ring signature is of size $\Theta(\sqrt[3]{n})$. Interestingly, the security of our construction relies on a security assumption – the permutation pairing assumption – introduced by Groth and Lu [GL07] in an unrelated setting: proofs of correctness of a shuffle. While the assumption is "non-standard", in the sense that is not a "DDH like" assumption, it is a falsifiable assumption and it was proven to be generically hard by Groth and Lu. For simplicity, we work on symmetric groups ($\mathbb{G}_1 = \mathbb{G}_2$), but our techniques should be easily extended to asymmetric groups if a natural translation to asymmetric groups of the Groth and Lu's assumption is given.

6.1 High Level Description

Our scheme follows the ring signature of Chandran et al. Given a Boneh-Boyen signature scheme (Section 6.2.4), where the secret/verification keys are of the form $(sk, [vk])$ and

$sk = vk \in \mathbb{Z}_q$, and given a one-time signature scheme (Section 2.2.4), the signature of the message m for a ring $R = \{[vk_1], \ldots, [vk_n]\}$ is computed as follows:[1]

a) pick a one-time signature key $(sk_{\mathsf{ot}}, vk_{\mathsf{ot}})$, sign m with the one-time signature, and sign the one-time verification key with sk,

b) commit to the signature of the one-time verification key and to $[vk]$ and show that it is a valid signature key using GS proofs,

c) show that $[vk] \in R$.

The most costly part is c) and our contribution is a proof of size $\Theta(\sqrt[3]{n})$ of c).

Our construction is similar to the proof system for set membership with proof size $\Theta(\sqrt[3]{n})$ from Section 4.1.6. However, note that the proof system from Section 4.1.6 does not suffice for constructing a ring signature because the CRS is fixed to a specific set and thus, the resulting ring signature will be fixed to a specific ring.

In our scheme the secret/verification keys of party P are $(sk, \mathbf{vk})$, where $\mathbf{vk} = ([vk], [\mathbf{a}], \mathbf{a}[vk])$, $(sk, [vk])$ are secret/verification keys of the Boneh-Boyen signature scheme, and $\mathbf{a} \in \mathbb{Z}_q^2$ is chosen independently for each key from some distribution $\mathcal{Q}$ to be specified later. Suppose that $\mathbf{vk}$ is the α th element in the ring $R = \{\mathbf{vk}_{(1,1,1)}, \ldots, \mathbf{vk}_{(m,m,m)}\}$, where $\alpha = (i_\alpha, j_\alpha, k_\alpha) := (i_\alpha - 1)m^2 + (j_\alpha - 1)m + k_\alpha$ for $i_\alpha, j_\alpha, k_\alpha \in [m], m := \sqrt[3]{n}$. The prover commits to $[\mathbf{x}] = [\mathbf{s}_\mu]$ and $[\mathbf{y}] = [\mathbf{s}'_{\mu'}]$, for $\mu = \mu' = (j_\alpha - 1)m + k_\alpha$, and shows, using the set-membership proof from Section 4.1.6 (which is the proof from Chandran et al. adapted to work with vectors), that $[\mathbf{x}] \in S$ and that $[\mathbf{y}] \in S'$, where

$$S := \{[\mathbf{s}_1], \ldots, [\mathbf{s}_{n^{2/3}}]\} := \left\{ \sum_{i \in [m]} [\mathbf{a}_{(i,1,1)}], \ldots, \sum_{i \in [m]} [\mathbf{a}_{(i,m,m)}] \right\} \text{ and}$$

$$S' := \{[\mathbf{s}'_1], \ldots, [\mathbf{s}'_{n^{2/3}}]\} := \left\{ \sum_{i \in [m]} \mathbf{a}_{(i,1,1)}[vk_{(i,1,1)}], \ldots, \sum_{i \in [m]} \mathbf{a}_{(i,m,m)}[vk_{(i,m,m)}] \right\}.$$

The prover also needs to assure that $\mu = \mu'$, which can be done reutilizing the commitment to μ (in fact to its m-ary representation) used in the proof that $[\mathbf{x}] \in S$ in the proof that $[\mathbf{y}] \in S'$. Since both sets are of size $n^{2/3}$, the two set membership proofs are of size $\Theta(\sqrt[3]{n})$.

Now that the prover has commited to elements

$$[\mathbf{x}] = \sum_{i \in [m]} [\mathbf{a}_{(i,j_\alpha,k_\alpha)}] \text{ and } [\mathbf{y}] = \sum_{i \in [m]} \mathbf{a}_{(i,j_\alpha,k_\alpha)}[vk_{(i,j_\alpha,k_\alpha)}],$$

it additionally commits to $[\kappa_1] := [vk_{(1,j_\alpha,k_\alpha)}], \ldots, [\kappa_m] := [vk_{(m,j_\alpha,k_\alpha)}]$ and $[\mathbf{z}_1] := [\mathbf{a}_{(1,j_\alpha,k_\alpha)}]$, $\ldots, [\mathbf{z}_m] := [\mathbf{a}_{(m,j_\alpha,k_\alpha)}]$. The prover now gives a proof that

$$\sum_{i \in [m]} [\mathbf{z}_i][\kappa_i] = [\mathbf{y}][1]. \tag{6.1}$$

Provided that $\mathbf{z}_1, \ldots, \mathbf{z}_m$ is a permutation of $\mathbf{a}_{(1,j_\alpha,k_\alpha)}, \ldots, \mathbf{a}_{(m,j_\alpha,k_\alpha)}$, we can show that if $[\kappa_1], \ldots, [\kappa_m]$ is not a permutation of $[vk_{(1,j_\alpha,k_\alpha)}], \ldots, [vk_{(m,j_\alpha,k_\alpha)}]$, then we can extract

[1] We could replace the Boneh-Boyen signature scheme with any structure preserving signature scheme secure under milder assumptions (e.g. [JR17]). We rather keep it simple and stick to Boneh-Boyen signature which, since the verification key is just one group element, simplifies the notation and reduces the size of the final signature.

an element from the kernel of the matrix $([\mathbf{a}_{1,j_\alpha,k_\alpha}]\cdots[\mathbf{a}_{m,j_\alpha,k_\alpha}])$. Thereby, provided the corresponding kernel assumption holds, the prover can simply select the i_α th element from $[\kappa_1],\ldots,[\kappa_m]$ which is guaranteed to be an element from the ring.

Therefore, it is only left the to show that $\mathbf{z}_1,\ldots,\mathbf{z}_m$ is a permutation of $\mathbf{a}_{(1,j_\alpha,k_\alpha)},\ldots,\mathbf{a}_{(m,j_\alpha,k_\alpha)}$. To do so we will use the following assumption introduced by Groth and Lu [GL07].

Definition 6.1 (Permutation Pairing Assumption) *Let $\mathcal{Q}_m = \underbrace{\mathcal{Q}|\ldots|\mathcal{Q}}_{m \text{ times}}$, where concatenation of matrix distributions is defined in the natural way and*

$$\mathcal{Q} : \mathbf{a} = \begin{pmatrix} x \\ x^2 \end{pmatrix}, \quad x \leftarrow \mathbb{Z}_q.$$

We say that the m-permutation pairing assumption holds relative to Gen_s if for any adversary A

$$\Pr\left[\begin{array}{l} gk \leftarrow \mathsf{Gen}_s(1^k); \mathbf{A} \leftarrow \mathcal{Q}_m; [\mathbf{Z}] \leftarrow \mathsf{A}(gk,[\mathbf{A}]) : \\ \text{(i)} \sum_{i\in[m]}[\mathbf{z}_i] = \sum_{i\in[m]}[\mathbf{a}_i], \text{(ii)} \ \forall i \in [m] \ [z_{2,i}][1] = [z_{1,i}][z_{1,i}], \\ \quad \textit{and } \mathbf{Z} \textit{ is not a permutation of the columns of } \mathbf{A} \end{array}\right],$$

where $[\mathbf{Z}] = [(\mathbf{z}_1,\ldots,\mathbf{z}_m)], [\mathbf{A}] = [(\mathbf{a}_1,\ldots,\mathbf{a}_m)] \in \mathbb{G}^{2\times m}$, is negligible in k.

If the prover additionally proves that equations (i) and (ii) are satisfied for $\mathbf{A} := (\mathbf{a}_{(1,j_\alpha,k_\alpha)}, \ldots, \mathbf{a}_{(m,j_\alpha,k_\alpha)})$, which can be done with $\Theta(m)$ group elements using Groth-Sahai proofs, the assumption is guaranteeing that the columns of $\mathbf{Z}$ are a permutation of the columns of $\mathbf{A}$, for some permutation $\pi \in S_m$. Therefore, equation (6.1) implies that

$$\begin{aligned} \sum_{i\in[m]}[\mathbf{z}_i][\kappa_i] &= \sum_{i\in[m]}[\mathbf{a}_{(\pi(i),j_\alpha,k_\alpha)}][\kappa_i] = \sum_{i\in[m]}[\mathbf{a}_{(i,j_\alpha,k_\alpha)}][\kappa_{\pi^{-1}(i)}] \\ &= \sum_{i\in[m]}[\mathbf{a}_{(i,j_\alpha,k_\alpha)}][vk_{(i,j_\alpha,k_\alpha)}]. \end{aligned}$$

Then $\kappa_1,\ldots,\kappa_m$ is a permutation of $\mathbf{a}_{(1,j_\alpha,k_\alpha)},\ldots,\mathbf{a}_{(m,j_\alpha,k_\alpha)}$ (the same defined by $\mathbf{z}_1,\ldots,\mathbf{z}_m$), unless $(\kappa_{\pi^{-1}(1)} - vk_{(1,j_\alpha,k_\alpha)}),\ldots,\kappa_{\pi^{-1}(m)} - vk_{(m,j_\alpha,k_\alpha)}))^\top$ is in the kernel of $\mathbf{A}$. Groth and Lu showed the hardness of finding an element from $\ker(\mathbf{A})$, when $\mathbf{A}$ is sampled from $\mathcal{Q}_m$, in the generic group model. They called this assumption the *simultaneous pairing assumption* and it corresponds to the $\mathcal{Q}_m^\top$-KerMDH assumption.

Remark. A natural question is if this technique can be applied once again. That is, to compute a $\Theta(\sqrt[4]{n})$ proof, compute commitments to an element from

$$S = \left\{\sum_{i\in[m]}\mathbf{a}_{(i,1,1,1)}[vk_{(i,1,1,1)}],\ldots,\sum_{i\in[m]}\mathbf{a}_{(i,m,m,m)}[vk_{(i,m,m,m)}]\right\} \text{ and}$$

$$S' = \left\{\sum_{i\in[m]}[\mathbf{a}_{(i,1,1,1)}],\ldots,\sum_{i\in[m]}[\mathbf{a}_{(i,m,m,m)}]\right\},$$

and then prove that they belong to the respective sets with the proof of size $\Theta(\sqrt[3]{n})$. Since $|S| = |S'| = n^{3/4}$, proof will be of size $\Theta(\sqrt[3]{n^{3/4}}) = \Theta(\sqrt[4]{n})$. However, this is not possible since the $\Theta(\sqrt[3]{n})$ proof is not a set membership proof for arbitrary sets, but only for sets where each element is of the form $([vk], \mathbf{a}[vk], [\mathbf{a}])$.

6.2 Preliminaries

6.2.1 Groth-Sahai Proofs in the 2-Lin Instantiation

In our ring signature we use as primitive Groth-Sahai proofs, which we have only instantiated in the SXDH setting. Since the SXDH (and DDH) is false in symmetric groups, in order to use Groth-Sahai proofs in symmetric groups one usually instantiates them using the 2-Lin assumption. Following Groth and Sahai's work [GS08], in symmetric groups and using the 2-Lin assumption, GS commitments are vectors in $\mathbb{G}^3$ of the form

$$\mathsf{GS.Com}_{ck}([x];\mathbf{r}) = \begin{pmatrix}[0]\\ [0]\\ [x]\end{pmatrix} + r_1[\mathbf{u}_1] + r_2[\mathbf{u}_2] + r_3[\mathbf{u}_3]$$

where $ck := ([\mathbf{u}_1]|[\mathbf{u}_2][\mathbf{u}_3])$, $(\mathbf{u}_2|\mathbf{u}_3) \leftarrow \mathcal{L}_2$ and $\mathbf{u}_1 := w_1\mathbf{u}_2 + w_2\mathbf{u}_3$ in the perfectly binding setting, and $\mathbf{u}_1 := w_1\mathbf{u}_2 + w_2\mathbf{u}_3 - \mathbf{e}_3$ in the perfectly hiding setting, for $w_1, w_2 \leftarrow \mathbb{Z}_q$. Security of GS commitments follows from the hardness of the 2-Lin assumption in symmetric groups.

As consequence of the enlargement of commitments, proofs are also larger (for example, 9 group elements for pairing product equations). The form of the proofs is similar to the asymmetric case (see Section 2.6.3), but we do not give the full detail since it does not help for understanding our ring signature nor for proving its security.

6.2.2 Flawed or Weaker Ring Signatures

Bose et al. claim to construct a constant-size ring signature in the standard model [BDR15]. However, they construct a weak ring signature where: a) the public keys are generated all at once in a correlated way; b) the set of parties which are able to participate in a ring is fixed as well as the maximum ring size; and c) the key size is linear in the maximum ring size. In the work of Chandran et al. and also in our setting: a) the key generation is independently run by the user using only the CRS as input; b) any party can be member of the ring as long as she has a verification key, and the maximum ring size is unbounded; and c) the key size is constant. These stronger requirements are in line with the original spirit of non-coordination of Rivest et al. [RST01].

Gritti et al. claim to construct a logarithmic ring signature in the standard model [GSP16]. However, their construction is completely flawed as explained below. In page 12, Gritti et al. define $v_{b_i} := v_{b_1\cdots b_i *}$, where $b_1 \cdots b_i *$ is the set of all bit-strings of size $d := \log n$ whose prefix is $b_1 \cdots b_i$. From this, one has to conclude that v_{b_i} is a set (or vector) of group elements of size 2^{d-i}. In the same page they define the commitment $D_{b_i} := v_{b_i} h^{s_{b_i}}$, for random $s_{b_i} \in \mathbb{Z}_q$, which, according to the previous observation, is the multiplication of a set (or vector) of group elements with a group element. Given that length reducing group to group commitments are known to not exist [AHO12], its representation requires at least 2^{d-i} group elements . Since commitments $D_{b_0}, \ldots, D_{b_d}$ are part of the signature, the actual signature size is $\Theta(2^d) = \Theta(n)$, rather than $\Theta(d) = \Theta(\log n)$ as claimed by Gritti et al.[2]

6.2.3 Definition

We follow Chandran et al.'s definitions [CGS07] described below, which extends the original definition of Bender et al. [BKM06] in order to include a CRS and perfect anonymity.

[2] We used multiplicative notation for the group operations to keep the expressions as they appear in the original work.

Definition 6.2 (Ring Signature) *A ring signature scheme consists of a quadruple of PPT algorithms* $(\mathsf{CRSGen}, \mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$ *that respectively, generate the common reference string, generate keys for a user, sign a message, and verify the signature of a message. More formally:*

- $\mathsf{CRSGen}(gk)$*, where* gk *is the group key, outputs the common reference string* ρ*.*
- $\mathsf{KeyGen}(\rho)$ *is run by the user. It outputs a public verification key* vk *and a private signing key* sk*.*
- $\mathsf{Sign}_{\rho,sk}(m, R)$ *outputs a signature* σ *on the message* m *with respect to the ring* $R = \{vk_1, \ldots, vk_n\}$*. We require that* (vk, sk) *is a valid key-pair output by* KeyGen *and that* $vk \in R$*.*
- $\mathsf{Verify}_{\rho,R}(m, \sigma)$ *verifies a purported signature* σ *on a message* m *with respect to the ring of public keys* R*.*

The quadruple $(\mathsf{CRSGen}, \mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$ *is a ring signature with perfect anonymity if it has perfect correctness, computational unforgeability and perfect anonymity as defined below.*

Definition 6.3 (Perfect Correctness) *We require that a user can sign any message on behalf of a ring where she is a member. A ring signature* $(\mathsf{CRSGen}, \mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$ *has perfect correctness if for all adversaries* A *we have:*

$$\Pr\left[\begin{array}{l} gk \leftarrow \mathsf{Gen}(1^\lambda); \rho \leftarrow \mathsf{CRSGen}(gk); (vk, sk) \leftarrow \mathsf{KeyGen}(\rho); \\ (m, R) \leftarrow \mathsf{A}(\rho, vk, sk); \sigma \leftarrow \mathsf{Sign}_{\rho,sk}(m; R) : \\ \mathsf{Verify}_{\rho,R}(m, \sigma) \text{ or } vk \notin R \end{array}\right] = 1$$

Definition 6.4 (Computational Unforgeability) *A ring signature scheme* $(\mathsf{CRSGen}, \mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$ *is unforgeable if it is infeasible to forge a ring signature on a message without controlling one of the members in the ring. Formally, it is unforgeable when for any non-uniform polynomial time adversaries* A *we have that*

$$\Pr\left[\begin{array}{l} gk \leftarrow \mathsf{Gen}(1^\lambda); \rho \leftarrow \mathsf{CRSGen}(gk); (m, R, \sigma) \leftarrow \mathsf{A}^{\mathsf{VKGen},\mathsf{Sign},\mathsf{Corrupt}}(\rho) : \\ \mathsf{Verify}_{\rho,R}(m, \sigma) = 1 \end{array}\right]$$

is negligible in th security parameter, where

- VKGen *on query number* i *selects randomness* w_i*, computes* $(vk_i, sk_i) := \mathsf{KeyGen}(\rho; w_i)$ *and returns* vk_i*.*
- $\mathsf{Sign}(i, m, R)$ *returns* $\sigma \leftarrow \mathsf{Sign}_{\rho,sk_i}(m, R)$*, provided* (vk_i, sk_i) *has been generated by* VKGen *and* $vk_i \in R$*.*
- $\mathsf{Corrupt}(i)$ *returns* w_i *(from which* sk_i *can be computed) provided* (vk_i, sk_i) *has been generated by* VKGen*.*
- A *outputs* (m, R, σ) *such that* Sign *has not been queried with* $(*, m, R)$ *and* R *only contains keys* vk_i *generated by* VKGen *where* i *has not been corrupted.*

Definition 6.5 (Perfect Anonymity) *A ring signature scheme* $(\mathsf{CRSGen}, \mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$ *has perfect anonymity, if a signature on a message* m *under a ring* R *and key* vk_{i_0} *looks exactly the same as a signature on the message* m *under the ring* R *and key* vk_{i_1}*, where* $vk_{i_0}, vk_{i_1} \in R$*. This means that the signer's key is hidden among all the honestly* *generated keys in the ring. Formally, we require that for any unbounded adversary* A*:*

$$\Pr\left[\begin{array}{l} gk \leftarrow \mathsf{Gen}(1^\lambda); \rho \leftarrow \mathsf{CRSGen}(gk); \\ (m, i_0, i_1, R) \leftarrow \mathsf{A}^{\mathsf{KeyGen}(\rho)}(\rho); \sigma \leftarrow \mathsf{Sign}_{\rho, sk_{i_0}}(m, R) : \\ \mathsf{A}(\sigma) = 1 \end{array}\right] =$$

$$\Pr\left[\begin{array}{l} gk \leftarrow \mathsf{Gen}(1^\lambda); \rho \leftarrow \mathsf{CRSGen}(gk); \\ (m, i_0, i_1, R) \leftarrow \mathsf{A}^{\mathsf{KeyGen}(\rho)}(\rho); \sigma \leftarrow \mathsf{Sign}_{\rho, sk_{i_1}}(m, R) : \\ \mathsf{A}(\sigma) = 1 \end{array}\right]$$

where A *chooses* i_0, i_1 *such that* $(vk_{i_0}, sk_{i_0}), (vk_{i_1}, sk_{i_1})$ *have been generated by the oracle* $\mathsf{KeyGen}(\rho)$*.*

6.2.4 Boneh-Boyen Signatures

Boneh and Boyen described a short signature – each signature consists of only one group element – which is UF-CMA without random oracles [BB04]. Interestingly, the verification of the validity of any signature-message pair can be written as a set of pairing product equations. Thereby, using Groth-Sahai proofs one can show the possession of a valid signature without revealing the actual signature (as done in Chandran et al.'s ring signature and our ring signature).

The Boneh-Boyen signature is proven UF-CMA secure under the *m-strong Diffie-Hellman* assumption, which is described below.

Definition 6.6 (*m-SDH* assumption) *For any adversary* A

$$\Pr\left[gk \leftarrow \mathsf{Gen}_s(1^\lambda), x \leftarrow \mathbb{Z}_q : \mathsf{A}(gk, [x], [x^2], \ldots, [x^m]) = (c, \left[\frac{1}{x+c}\right])\right]$$

is negligible in λ*.*

The Boneh-Boyen signature scheme is described below.

$\mathsf{BB.KeyGen}$**:** Given a group key gk, pick $vk \leftarrow \mathbb{Z}_q$. The secret/public key pair is defined as $(sk, [vk]) := (vk, [vk])$.

$\mathsf{BB.Sign}$**:** Given a secret key $sk \in \mathbb{Z}_q$ and a message $m \in \mathbb{Z}_q$, output the signature $[\sigma] := \left[\frac{1}{sk+m}\right]$. In the unlikely case that $sk + m = 0$ we let $[\sigma] := [0]$.

$\mathsf{BB.Ver}$**:** On input the verification key $[vk]$, a message $m \in \mathbb{Z}_q$, and a signature $[\sigma]$, verify that $[m + vk][\sigma] = [1]_T$.

6.3 Our Construction

$\mathsf{CRSGen}(gk)$**:** Pick a perfectly hiding CRS for the Groth-Sahai proof system $\mathsf{crs}_{\mathsf{GS}}$, and a CRS for the proof of the $\Theta(\sqrt{n})$ proof of membership in a set $\mathsf{crs}_{\mathsf{set}}$ (Section 4.1.6), and output $\rho := (gk, \mathsf{crs}_{\mathsf{GS}}, \mathsf{crs}_{\mathsf{set}})$.

$\mathsf{KeyGen}(\rho)$**:** Pick $\mathbf{a} \leftarrow \mathcal{Q}$ and $(sk, [vk]) \leftarrow \mathsf{BB.KeyGen}(gk)$, compute $[\mathbf{a}]$ and then erase $\mathbf{a}$. The secret key is sk and the verification key is $\mathbf{vk} := ([vk], [\mathbf{a}], \mathbf{a}[vk])$.

$\mathsf{Sign}_{\rho,sk}(m, R)$**:**

1. Compute $(sk_{\mathsf{ot}}, vk_{\mathsf{ot}}) \leftarrow \mathsf{OT.KeyGen}(gk)$ and $\sigma_{\mathsf{ot}} \leftarrow \mathsf{OT.Sign}_{sk_{\mathsf{ot}}}(m, R)$.
2. Compute $[\mathbf{c}] := \mathsf{GS.Com}_{ck}([vk]; r)$, $r \leftarrow \mathbb{Z}_q$, $[\sigma] \leftarrow \mathsf{BB.Sign}_{sk}(vk_{\mathsf{ot}})$, $[\mathbf{d}] := \mathsf{GS.Com}_{ck}([\sigma]; s)$, $s \leftarrow \mathbb{Z}_q$, and a GS proof π_{GS} that $\mathsf{BB.Ver}_{[vk]}([\sigma], [vk_{\mathsf{ot}}]) = 1$ (which can be expressed as a set of pairing product equations).

3. Parse R as $\{\mathbf{vk}_{(1,1,1)},\ldots,\mathbf{vk}_{(m,m,m)}\}$, where $m := \sqrt[3]{n}$, $n := |R|$, and let $\alpha = (i_\alpha, j_\alpha, k_\alpha)$ the index of $\mathbf{vk}$ in R. Define the sets $S = \{\sum_{i\in[m]}[\mathbf{a}_{(i,1,1)}], \ldots, \sum_{i\in[m]}[\mathbf{a}_{(i,m,m)}]\}$ and
$S' = \{\sum_{i\in[m]} \mathbf{a}_{(i,1,1)}[vk_{(i,1,1)}], \ldots, \sum_{i\in[m]} \mathbf{a}_{(i,m,m)}[vk_{(i,m,m)}]\}$.

4. Let $[\mathbf{x}] := \sum_{i\in[m]}[\mathbf{a}_{(i,j_\alpha,k_\alpha)}]$ and $[\mathbf{y}] = \sum_{i\in[m]} \mathbf{a}_{(i,j_\alpha,k_\alpha)}[vk_{(i,j_\alpha,k_\alpha)}]$. Compute GS commitments to $[\mathbf{x}]$ and $[\mathbf{y}]$, and compute proofs π_1 and π_2 that they belong to S and S', respectively. It is also proven that they appear in the same positions reusing the commitments to $b_1,\ldots,b_m$ and $b'_1,\ldots,b'_m$, used in the set-membership proof from Section 4.1.6), which define $[\mathbf{x}]$'s and $[\mathbf{y}]$'s position in S and S' respectively.

5. Let $[\kappa_1] := [vk_{(1,j_\alpha,k_\alpha)}],\ldots,[\kappa_m] := [vk_{(m,j_\alpha,k_\alpha)}]$ and $[\mathbf{z}_1] := [\mathbf{a}_{(1,j_\alpha,k_\alpha)}],\ldots,[\mathbf{z}_m] := [\mathbf{a}_{(m,j_\alpha,k_\alpha)}]$. Compute GS commitments to $[\kappa_1],\ldots,[\kappa_m]$ and $[\mathbf{z}_1],\ldots,[\mathbf{z}_m]$, and GS proof π_κ that $\sum_{i\in[m]}[\kappa_i][\mathbf{z}_i] = [\mathbf{y}][1]$ and a GS proof π_z that $\sum_{i\in[m]}[\mathbf{z}_i] = [\mathbf{x}]$ and $[z_{2,i}][1] = [z_{1,i}][z_{1,i}]$ for each $i \in [m]$.

6. Compute a proof π_3 that $[vk]$ belongs to $S_3 = \{[\kappa_1],\ldots,[\kappa_m]\}$.

7. Return the signature $\boldsymbol{\sigma} := (vk_{\mathsf{ot}}, \sigma_{\mathsf{ot}}, [\mathbf{c}], [\mathbf{d}], \pi_1, \pi_2, \pi_3, \pi_\kappa, \pi_z)$. (GS proofs include commitments to variables).

$\mathsf{Verify}_{\rho,R}(m,\boldsymbol{\sigma})$**:** Verify the validity of the one-time signature and of all the proofs. Return 0 if any of these checks fails and 1 otherwise.

Theorem 6.7 *The scheme presented in this section is a ring signature scheme with perfect correctness, perfect anonymity and computational unforgeability under the m-permutation pairing assumption, the $\mathcal{Q}_m^\top$-KerMDH assumption, the 2-Lin assumption, and the assumption that the one-time signature and the Boneh-Boyen signature are unforgeable. Concretely, for any adversary* A *against the unforgeability of the scheme, there exist adversaries* $\mathsf{B}_1, \mathsf{B}_2, \mathsf{B}_3, \mathsf{B}_4, \mathsf{B}_5$ *such that*

$$\begin{aligned}\mathbf{Adv}(\mathsf{A}) \leq & \mathbf{Adv}_{\mathcal{L}_2\text{-}\mathsf{MDDH}}(\mathsf{B}_1) + \mathbf{Adv}_{q_{\mathsf{gen}}\text{-}PPA}(\mathsf{B}_2) + \mathbf{Adv}_{\mathcal{Q}^\top_{q_{\mathsf{gen}}}\text{-}\mathsf{KerMDH}}(\mathsf{B}_3) + \\ & q_{\mathsf{gen}}(q_{\mathsf{sig}}\mathbf{Adv}_{\mathsf{OT}}(\mathsf{B}_4) + \mathbf{Adv}_{\mathsf{BB}}(\mathsf{B}_5)),\end{aligned}$$

where q_{gen} *and* q_{sign} *are, respectively, upper bounds for the number of queries that* A *makes to its* VKGen *and* Sign *oracles.*

Proof Perfect correctness follows directly from the definitions. Perfect anonymity follows from the fact that the perfectly hiding Groth-Sahai CRS defines perfectly hiding and perfect zero-knowledge proofs, information theoretically hiding any information about $\mathbf{vk}$.

We say that an unforgeability adversary is "eager" if makes all its queries to the VKGen oracle at the beginning. Note that any non-eager adversary A' can be perfectly simulated by an eager adversary that makes q_{gen} queries to VKGen and answers A' queries to VKGen "on demand".

W.l.o.g. we assume that A is an eager adversary. Computational unforgeability follows from the indistinguishability of the following games

Game_0: This is the real unforgeability experiment. Game_0 returns 1 if the adversary A produces a valid forgery and 0 if not.

Game_1: This is game exactly as Game_0 with the following differences:

- The Groth-Sahai CRS is sampled together with its discrete logarithms from the perfectly binding distribution.
- At the beginning, variables err_2 and err_3 are initialized to 0, and a random index i^* is chosen from $[q_{\mathsf{gen}}]$.
- On a query to $\mathsf{Corrupt}$ with argument i, if $i = i^*$ set $\mathsf{err}_3 \leftarrow 1$ and proceed as in Game_2.
- Let (m, R, σ) the purported forgery output by A. If $[vk]$, the opening of commitment $[\mathbf{c}]$ from σ, is not equal to $[vk_{i^*}]$, set $\mathsf{err}_3 \leftarrow 1$. If $[vk] \notin R$, then set $\mathsf{err}_2 = 1$.

Game_2: This is game exactly as Game_1 except that, if err_2 is set to 1, Game_2 aborts.

Game_3: This is game exactly as Game_2 except that, if err_3 is set to 1, Game_3 aborts.

Since variables err_2 and err_3 are just dummy variables, the only difference between Game_0 and Game_1 comes from the Groth-Sahai CRS distribution. It follows that there is an adversary B_1 against DLin such that $|\Pr[\mathsf{Game}_0 = 1] - \Pr[\mathsf{Game}_1 = 1]| \leq \mathbf{Adv}_{\mathcal{L}_2\text{-}\mathsf{MDDH}}(\mathsf{B}_1)$.

Lemma 6.8 *There exist adversaries B_2 and B_3 against the q_{gen}-permutation pairing assumption and against the $\mathcal{Q}_{q_{\mathsf{gen}}}^{\top}$-$\mathsf{KerMDH}$ assumption, respectively, such that*

$$|\Pr[\mathsf{Game}_2 = 1] - \Pr[\mathsf{Game}_1 = 1]| \leq \mathbf{Adv}_{q_{\mathsf{gen}}\text{-PPA}}(\mathsf{B}_2) + \mathbf{Adv}_{\mathcal{Q}_{q_{\mathsf{gen}}}^{\top}\text{-}\mathsf{KerMDH}}(\mathsf{B}_3).$$

Proof Note that

$$\begin{aligned}\Pr[\mathsf{Game}_1 = 1] =& \Pr[\mathsf{Game}_1 = 1|\mathsf{err}_2 = 0]\Pr[\mathsf{err}_2 = 0] + \\ & \Pr[\mathsf{Game}_1 = 1|\mathsf{err}_2 = 1]\Pr[\mathsf{err}_2 = 1] \\ \leq & \Pr[\mathsf{Game}_2 = 1] + \Pr[\mathsf{Game}_1 = 1]\mathsf{err}_2 = 0] \\ \Longrightarrow & |\Pr[\mathsf{Game}_2 = 1] - \Pr[\mathsf{Game}_1 = 1]| \leq \Pr[\mathsf{Game}_1 = 1|\mathsf{err}_2 = 1].\end{aligned}$$

We proceed to bound this last probability.

We construct an adversary B_2 against the q_{gen}-permutation pairing assumption as follows. B_2 receives as challenge $[\mathbf{A}'] \in \mathbb{G}^{2\times q_{\mathsf{gen}}}$ and honestly simulates Game_2 with the following exception. On the i th query of A to VKGen sets $[\mathbf{a}_i]$ as the i th column of $[\mathbf{A}']$. When A outputs $\mathsf{GS.Com}_{ck_{\mathsf{GS}}}([\mathbf{z}_1]), \ldots, \mathsf{GS.Com}_{ck_{\mathsf{GS}}}([\mathbf{z}_m])$, as part of π_z, B_2 extract $[\mathbf{z}_1], \ldots, [\mathbf{z}_m]$. Let $j_\alpha, k_\alpha \in [m]$ the indices defined by π_1 and π_2, B returns $([\mathbf{z}_1], \ldots, [\mathbf{z}_m], [\tilde{\mathbf{a}}_1], \ldots, [\tilde{\mathbf{a}}_{q_{\mathsf{gen}}-m}])$, where $[\tilde{\mathbf{a}}_1], \ldots, [\tilde{\mathbf{a}}_{q_{\mathsf{gen}}-m}]$ are the columns of $[\mathbf{A}']$ which are different from $[\mathbf{a}'_{(1,j_\alpha,k_\alpha)}], \ldots, [\mathbf{a}'_{(m,j_\alpha,k_\alpha)}]$.

We construct an adversary B_3 against the $\mathcal{Q}_{q_{\mathsf{gen}}}^{\top}$-$\mathsf{KerMDH}$ assumption as follows. B receives as challenge $[\mathbf{A}'] \in \mathbb{G}^{2\times q_{\mathsf{gen}}}$ and honestly simulates Game_2 embedding $[\mathbf{A}']$ in the user keys (in the same way as B_2). When A outputs $\mathsf{GS.Com}_{ck_{\mathsf{GS}}}([\kappa_1]), \ldots, \mathsf{GS.Com}_{ck_{\mathsf{GS}}}([\kappa_m])$, as part of π_κ, B_3 extract $[\kappa_1], \ldots, [\kappa_m]$. B_3 attempts to extract a permutation π such that $[\mathbf{z}_i] = [\mathbf{a}'_{(\pi(i),j_\alpha,k_\alpha)}]$ for each $i \in [m]$. If there is no such permutation, B_3 aborts. Finally, B_3 returns $([0], \ldots, [0], [\kappa_{\pi^{-1}(1)}] - [vk_{(1,j_\alpha,k_\alpha)}], \ldots, [\kappa_{\pi^{-1}(m)}] - [vk_{(m,j_\alpha,k_\alpha)}], [0], \ldots)^\top \in \mathbb{G}^{q_{\mathsf{gen}}}$.

Let E the event where $[\mathbf{z}_1], \ldots, [\mathbf{z}_m]$ is a permutation of $[\mathbf{a}'_{(1,j_\alpha,k_\alpha)}], \ldots, [\mathbf{a}'_{(m,j_\alpha,k_\alpha)}]$, and assume that we are in the case $\neg E$. Soundness of proof π_κ implies that

$$\sum_{i\in[m]} [\kappa_i][\mathbf{z}_i] = [\mathbf{y}].$$

Soundness of proof π_z implies that

$$\begin{aligned}&\sum_{i\in[m]}[\mathbf{z}_i]=[\mathbf{x}] \text{ and}\\ &[z_{i,2}][1]=[z_{i,1}][z_{i,1}] \text{ for all } i\in[m]. \end{aligned} \tag{6.2}$$

Soundness of proofs π_1,π_2,π_3 implies, respectively, that there exist $j_\alpha, k_\alpha \in [m]$ such that

$$\sum_{i\in[m]}[\kappa_i][\mathbf{z}_i]=\sum_{i\in[m]}\mathbf{a}'_{(i,j_\alpha,k_\alpha)}[vk_{(i,j_\alpha,k_\alpha)}], \tag{6.3}$$

$$\sum_{i\in[m]}[\mathbf{z}_i]=\sum_{i\in[m]}[\mathbf{a}'_{(i,j_\alpha,k_\alpha)}],, \tag{6.4}$$

and that $[vk]=[\kappa_{i^*}]$, for some $i^*\in[m]$.

Equation (6.4) and imply that

$$\sum_{i\in[q_{\mathsf{gen}}-m]}[\tilde{\mathbf{a}}_i]+\sum_{i\in[m]}[\mathbf{z}_i]=\sum_{i\in[q_{\mathsf{gen}}]}[\mathbf{a}'_i]$$

and together with equation (6.2), the fact that $[\tilde{a}_{i,2}][1]=[\tilde{a}_{i,1}][\tilde{a}_{i,1}]$, and that we assume $\neg E$, implies that B_2 breaks the q_{gen}-permutation pairing assumption. Therefore

$$\Pr[\mathsf{Game}_2=1|\mathsf{err}_2=1\wedge\neg E]\leq\mathbf{Adv}_{q_{\mathsf{gen}}\text{-}PPA}(\mathsf{B}_2).$$

Assume now that we are in the case E. Therefore, equation (6.3) implies that

$$\sum_{i\in[m]}(\kappa_i-vk_{(\pi(i),j_\alpha,k_\alpha)})\mathbf{a}_{(\pi(i),j_\alpha,k_\alpha)}=0.$$

Since $[vk]=[\kappa_{i^*}]\notin R$, then $[\kappa_{i^*}]\neq vk_{(i,j_\alpha,k_\alpha)}$ for all $i\in[m]$. Therefore $([0],\ldots,[0],[\kappa_{\pi^{-1}(1)}]-[vk_{(1,j_\alpha,k_\alpha)}],\ldots,[\kappa_{\pi^{-1}(m)}]-[vk_{(m,j_\alpha,k_\alpha)}])\neq[\mathbf{0}]$ and B_3 breaks the $\mathcal{Q}_{q_{\mathsf{gen}}}^{\top}$-$\mathsf{KerMDH}$ assumption. We conclude that

$$\Pr[\mathsf{Game}_2=1|\mathsf{err}_2=1\wedge E]\leq\mathbf{Adv}_{\mathcal{Q}_{q_{\mathsf{gen}}}^{\top}\text{-}\mathsf{KerMDH}}(\mathsf{B}_3)$$

The lemma follows from the fact that

$$\begin{aligned}\Pr[\mathsf{Game}_1=1|\mathsf{err}_2=1]=&\Pr[\mathsf{Game}_1=1|\mathsf{err}_2=1\wedge\neg E]\Pr[\neg E]+\\ &\Pr[\mathsf{Game}_1=1|\mathsf{err}_2=1\wedge E_1]\Pr[E_1]\\ \leq&\Pr[\mathsf{Game}_1=1|\mathsf{err}_2=1\wedge\neg E]+\\ &\Pr[\mathsf{Game}_1=1|\mathsf{err}_2=1\wedge E_1]\\ \leq&\mathbf{Adv}_{q_{\mathsf{gen}}\text{-}PPA}(\mathsf{B}_2)+\mathbf{Adv}_{\mathcal{Q}_{q_{\mathsf{gen}}}^{\top}\text{-}\mathsf{KerMDH}}(\mathsf{B}_3)\end{aligned} \qquad \square$$

Lemma 6.9

$$\Pr[\mathsf{Game}_3=1]\geq\frac{1}{q_{\mathsf{gen}}}\Pr[\mathsf{Game}_2=1].$$

Proof It holds that

$$\begin{aligned}\Pr[\mathsf{Game}_3=1]&=\Pr[\mathsf{Game}_3=1|\mathsf{err}_3=0]\Pr[\mathsf{err}_3=0]\\ &=\Pr[\mathsf{Game}_2=1|\mathsf{err}_3=0]\Pr[\mathsf{err}_3=0]\\ &=\Pr[\mathsf{err}_3=0|\mathsf{Game}_2=1]\Pr[\mathsf{Game}_2=1].\end{aligned} \qquad \square$$

The probability that $\mathsf{err}_2 = 0$ given $\mathsf{Game}_2 = 1$ is the probability that the q_{cor} calls to $\mathsf{Corrupt}$ do not abort and that $[vk] = [vk_{i^*}]$. Since A is an eager adversary, at the i th call to $\mathsf{Corrupt}$ the index i^* is uniformly distributed over the $q_{\mathsf{gen}} - i + 1$ indices of uncorrupted users. Similarly, when A outputs its purported forgery, the probability that $[vk] = [vk_{i^*}]$ is $1/(q_{\mathsf{gen}} - q_{\mathsf{cor}})$, since $[vk] \in R$ (or otherwise Game_2 would have aborted). Therefore

$$\Pr[\mathsf{err}_2 = 1 | \mathsf{Game}_2 = 1] = \frac{q_{\mathsf{gen}} - 1}{q_{\mathsf{gen}}} \frac{q_{\mathsf{gen}} - 2}{q_{\mathsf{gen}} - 1} \cdots \frac{q_{\mathsf{gen}} - q_{\mathsf{cor}}}{q_{\mathsf{gen}} - q_{\mathsf{cor}} + 1} \frac{1}{q_{\mathsf{gen}} - q_{\mathsf{cor}}} = \frac{1}{q_{\mathsf{gen}}}.$$

Lemma 6.10 *There exist adversaries* B_4 *and* B_5 *against the unforgeability of the one-time signature scheme and the weak unforgeability of the Boneh-Boyen signature scheme such that*

$$\Pr[\mathsf{Game}_3 = 1] \leq q_{\mathsf{sig}} \mathbf{Adv}_{\mathsf{OT}}(\mathsf{B}_4) + \mathbf{Adv}_{\mathsf{BB}}(\mathsf{B}_5)$$

Proof We construct adversaries B_4 and B_5 as follows.

B_4 receives $vk^{\dagger}_{\mathsf{ot}}$ and simulates Game_3 honestly but with the following differences. It chooses a random $j^* \in [q_{\mathsf{sig}}]$ and answer the j^* th query to $\mathsf{Sign}(i, m^{\dagger}, R^{\dagger})$ honestly but computing $\sigma^{\dagger}_{\mathsf{ot}}$ querying on $(m^{\dagger}, R^{\dagger})$ its oracle and setting $vk^{\dagger}_{\mathsf{ot}}$ as the corresponding one-time signature. Finally, when A outputs its purported forgery $(m, R, (\sigma_{\mathsf{ot}}, vk_{\mathsf{ot}}, \ldots))$, B_4 it outputs the corresponding one-time signature.

B_5 receives $[vk]$ and simulates Game_3 honestly but with the following differences. Let $i := 0$. B_5 computes $(sk^i_{\mathsf{ot}}, vk^i_{\mathsf{ot}}) \leftarrow \mathsf{OT.KeyGen}(gk)$, for each $i \in [q_{\mathsf{sig}}]$ and queries its signing oracle on $(vk^1_{\mathsf{ot}}, \ldots, vk^{q_{\mathsf{sig}}}_{\mathsf{ot}})$ obtaining $[\sigma_1], \ldots, [\sigma_{q_{\mathsf{sig}}}]$. When A queries the signing oracle on input (i^*, m, R), B_5 computes an honest signature but replaces vk_{ot} with vk^i_{ot} and $[\sigma]$ with $[\sigma_i]$, and then adds 1 to i. Finally, when A outputs its purported forgery $(m, R, (\sigma_{\mathsf{ot}}, vk_{\mathsf{ot}}, [\mathbf{c}], [\mathbf{d}], \ldots))$, it extracts $[\sigma]$ from $[\mathbf{d}]$ as its forgery for vk_{ot}.

Let E be the event where vk_{ot}, from the purported forgery of A, has been previously output by Sign. We have that

$$\Pr[\mathsf{Game}_3 = 1] \leq \Pr[\mathsf{Game}_3 = 1 | E] + \Pr[\mathsf{Game}_3 = 1 | \neg E].$$

Since (m, R) has never been signed by a one-time signatures and that, conditioned on E, the probability of $vk_{\mathsf{ot}} = vk^{\dagger}_{\mathsf{ot}}$ is $1/q_{\mathsf{sig}}$, then

$$q_{\mathsf{sig}} \mathbf{Adv}_{\mathsf{OT}}(\mathsf{B}_4) \geq \Pr[\mathsf{Game}_3 = 1 | E] \qquad \square$$

Finally, if $\neg E$ holds, then $[\sigma]$ is a forgery for vk_{ot} and thus

$$\mathbf{Adv}_{\mathsf{BB}}(\mathsf{B}_5) \geq \Pr[\mathsf{Game}_3 = 1 | \neg E]$$

Chapter 7

Improved Aggregated Zero-Knowledge Set-Membership Proofs

In this chapter we construct a QA-NIZK proof system for the language

$$\mathcal{L}^n_{ck,\mathsf{set}} := \left\{ \begin{array}{c} ([\boldsymbol{\zeta}_1]_1, \ldots, [\boldsymbol{\zeta}_n]_1, S) : \exists w_1, \ldots, w_n \in \mathbb{Z}_q \text{ s.t. } S \subset \mathbb{Z}_q \\ \text{and } \forall i \in [n]\ [\boldsymbol{\zeta}_i]_1 = \mathsf{GS.Com}_{ck}(x_i; w_i) \wedge x_i \in S \end{array} \right\},$$

with proof size $\Theta(\log |S|)$. In Section 7.2.1 we show how to extend these ideas to show membership in the language

$$\mathcal{L}^n_{ck,S} := \left\{ \begin{array}{c} ([\boldsymbol{\zeta}_1]_1, \ldots, [\boldsymbol{\zeta}_n]_1) : \exists w_1, \ldots, w_n \in \mathbb{Z}_q \text{ s.t. } S \subset \mathbb{G}_1 \\ \text{and } \forall i \in [n]\ [\boldsymbol{\zeta}_i]_1 = \mathsf{GS.Com}_{ck}([x_i]_1; w_i) \wedge [x_i]_1 \in S \end{array} \right\},$$

with proof size $\Theta(\log |S|)$, for any $S \subset \mathbb{G}_1$.

The first case is the more general form of a set-membership proof where the set is dynamically chosen. In the second case each instance of the proof system is fixed to a specific set (encoded in the CRS) and is the same notion of the proofs for "fixed sets" from Section 4.1.6. We note that the aggregated set-membership proofs for $S \subset \mathbb{G}_s$ from Chapter 5 are proofs of membership in $\mathcal{L}^n_{ck,S}$.

In Section 7.1, we start with an intuitive description for the case $S \subset \mathbb{Z}_q$ without aggregation. We note that even in this simpler case, to the best of our knowledge, the shortest non-interactive proof, under falsifiable assumptions and without assuming anything about S,[1] that exists in the literature is the one of Chandran et al. of size $\Theta(\sqrt{|S|})$. Our approach is to commit to the binary representation $(b_1, \ldots, b_{\log t}) \in \{0,1\}^{\log t}$ of the index of the purported $x \in S$, for $S = \{s_1, \ldots, s_t\}$ and where b_1 is the least significant bit, to select the the leaves under the paths $(b_{\log t}), (b_{\log t}, b_{\log t-1}), \ldots, (b_{\log t}, \ldots, b_1)$ in the binary tree whose leaves are (from left to right) $s_1, \ldots, s_t$. In order to keep a logarithmic proof, we commit to the selected leaves using MP commitments from Section 4.2.1 and show, for each $\ell \in [\log t]$, that the leaves under the path $(b_m, \cdots, b_\ell)$ are equal the leftmost or rightmost, depending of b_ℓ, leaves under the path $(b_{\log t}, \cdots, b_{\ell-1})$. We use these ideas together with a clever usage of QA-NIZK proofs of membership in linear subspaces, Groth-Sahai proofs, and the proof systems from Chapters 3 and 4.

In Section 7.2 we give a full description of the non-aggregated case and then we show how to extend this result to the case $S \subset \mathbb{G}_s$. We use the ideas from Section 7.1 and aggregate

[1] If $S = [a, b] \subset \mathbb{Z}_q$ and $a < b$ we can use range proofs.

many instances using similar techniques to those from Chapter 4. We note that, to the best of our knowledge, there is no aggregated proof in the literature (i.e. all proofs are of size $\Omega(n)$) with the sole exception of our proof from Section 5 which is of size $\Theta(|S|)$. Our proof bears some similarities with the work of Groth and Kohlweiss [GK15] – both allow to construct proofs of membership in a set of logarithmic size using the binary encoding of the element index – but they are in general incomparable. Indeed, Groth and Kohlweiss's construction is on a different setting (interactive, without pairings) and does not support aggregation of many proofs.

There is a straightforward application of the improved aZKSMP. In the proof of a shuffle from Section 5.4, the size of the proof that $[\mathbf{F}] \in \mathcal{L}^n_{ck,S}$ can be reduced from $2n + \Theta(1)$ to $\Theta(\log n)$ and thus the total proof size is reduced from $4n + o(n)$ to $2n + o(n)$.

7.1 Intuition

For simplicity, we will restrict to the case $S = \{s_1, \ldots, s_t\} \subset \mathbb{Z}_q$ without aggregation, that is, there is a single commitment $[\mathbf{c}]_1 = \mathsf{GS.Com}_{ck_{\mathsf{GS}}}(x; r)$ and we want to show that $x = s_\alpha$, for some $\alpha \in [t]$. In Section 7.2 we will show how to aggregate many proofs.

The (non-aggregated) proof from Section 5.3 essentially codifies the position α as a weight 1 binary vector $\mathbf{b}$ of size t such that $x = \sum_{i\in[t]} b_i s_i$ and $b_i = 1$ if $i = \alpha$ and 0 if not.[2] A step further in efficiency was given by Chandran et al. [CGS07] (already discussed in Section 4.1.6). There the position α is codified as two weight 1 binary vectors $\mathbf{b}$ and $\mathbf{b}'$ of size $\sqrt{t}$ such that

$$\begin{pmatrix} x_1 \\ \vdots \\ x_{\sqrt{t}} \end{pmatrix} = \sum_{i=1}^{\sqrt{t}} b_i \begin{pmatrix} s_{(i-1)\sqrt{t}+1} \\ \vdots \\ s_{(i-1)\sqrt{t}+\sqrt{t}} \end{pmatrix}, \quad x = \sum_{i=1}^{\sqrt{t}} b'_i x_i,$$

and $b_i = 1$ iff $i = i_\alpha$ and $b'_j = 1$ iff $j = j_\alpha$, where $\alpha = (i_\alpha - 1)\sqrt{t} + j_\alpha$. Since $\sqrt{t}$ new variables are added (variables $x_1, \ldots, x_{\sqrt{t}}$), the proof must contain $\sqrt{t}$ new commitments to these variables. However, this does not not affect the asymptotic size of the proof, which is $\Theta(\sqrt{t})$ anyway.

Let $m := \log t$.[3] The natural next step is to codify α as m weight 1 binary vectors of size 2 (note that a weight 1 binary vector of size 2 can be always written as $(1 - b, b)$, $b \in \{0, 1\}$) such that

$$\begin{pmatrix} x_{\ell,1} \\ \vdots \\ x_{\ell,2^{\ell-1}} \end{pmatrix} = (1 - b_\ell) \begin{pmatrix} x_{\ell+1,1} \\ \vdots \\ x_{\ell+1,2^{\ell-1}} \end{pmatrix} + b_\ell \begin{pmatrix} x_{\ell+1,2^{\ell-1}+1} \\ \vdots \\ x_{\ell+1,2^\ell} \end{pmatrix} \text{ if } \ell \in [m], \tag{7.1}$$

$$x = x_{1,1}, \tag{7.2}$$

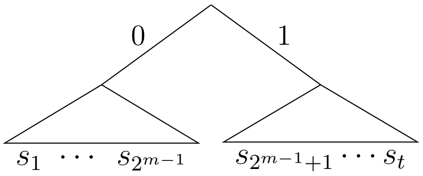
where $x_{m+1,i} := s_i$, $i \in [t]$, and $\alpha = \sum_{i=1}^m b_i 2^{i-1} + 1$. Note that we have added the additional variables $x_{\ell,i}$, $\ell \in [m]$ and $i \in [2^\ell]$.

Consider the binary tree whose leaves are $x_{m+1,1} = s_1, \ldots, x_{m+1,t} = s_t$, where the leftmost leaf is s_1 and the rightmost leaf is $s_{2^m} = s_t$. Intuitively, equation (7.1) for $\ell = m$ says that

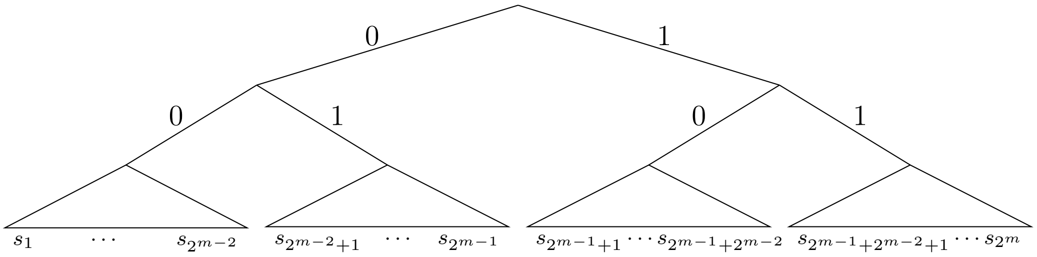
[2] The case $S \subset \mathbb{Z}_q$ is not really discussed in Section 5.3, but it is straightforward that the same techniques from the case $S \subset \mathbb{G}_s$ apply.

[3] W.l.o.g. we assume that $\log t \in \mathbb{N}$, because we can always prove membership in the (multi-)set $S' = S \biguplus_{i=1}^{2^{\lceil \log t \rceil}-t} \{s_t\}$ and it holds that $|S'| = 2^{\lceil \log t \rceil}$ and that $x \in S \iff x \in S'$.

variables $x_{m,1},\ldots,x_{m,2^{m-1}}$ are the leaves of the subtree under the path (b_m). For example, if $b_m=1$, the variables $x_{m,1},\ldots,x_{m,2^{m-1}}$ are equal to $s_{2^{m-1}+1},\ldots,s_t$, which are the leaves of the subtree under the path (1) as depicted below.



Similarly, equation (7.1) for $\ell=m-1$ says that variables $x_{m-1,1},\ldots,x_{m-1,2^{m-2}}$ are the leaves of the subtree under the path (b_m,b_{m-1}). For example, if $(b_m,b_{m-1})=(1,0)$, the variables $x_{m-1,1},\ldots,x_{m-1,2^{m-2}}$ are equal to $x_{m,1}=s_{2^{m-1}+1},\ldots,x_{m,2^{m-2}}=s_{2^{m-1}+2^{m-2}}$, which are the leaves of the subtree under the path (1,0) as depicted below.


0
1
0
1
0
1
s_1 ··· $s_{2^{m-2}}$
$s_{2^{m-2}+1}$ ··· $s_{2^{m-1}}$
$s_{2^{m-1}+1}$ ··· $s_{2^{m-1}+2^{m-2}}$
$s_{2^{m-1}+2^{m-2}+1}$ ··· s_{2^m}

In general, the variables $x_{\ell,1},\ldots,x_{\ell,2^{\ell-1}}$ are equal to the leaves $s_{\mathsf{left}},\ldots,s_{\mathsf{right}}$ under the path $(b_m,\ldots,b_\ell)$, where $\mathsf{left}=\sum_{i=\ell}^{m}b_i2^{i-1}+1$ and $\mathsf{right}=\mathsf{left}+2^{\ell-1}-1$. Therefore, for $\ell=1$ equation (7.1) says that the variable $x_{1,1}$ is equal to the leaf $s_{\mathsf{left}}=s_{\mathsf{right}}=s_\alpha$, since $\mathsf{left}=\mathsf{right}=\sum_{i=1}^{m}b_i2^{i-1}+1=\alpha$, which is the unique leaf (and the unique node) in the subtree under the path $(b_m,\ldots,b_1)$.

Similarly as in Chandran et al.'s proof, for each new variable a new commitment must be added to the proof. But, in contrast with Chandran et al.'s proof, in this case the additional commitments do increase the asymptotic size of the proof. Indeed, the total number of new variables is $2^{m-1}+2^{m-2}+\ldots+1=2^m-1=t-1$, and thus $t-1$ new commitments must be added.

One can reduce the total size of the commitments using the length reducing multi-Pedersen commitments from Section 4.2.1. However, this must be done carefully in order to be able to express equation (7.1) with a Groth-Sahai proof of an equation that involves the MP commitments and the variables $b_1,\ldots,b_m$. For example, if one computes a single commitment to all variables $\mathsf{MP.Com}_{ck}((x_{1,1},\ldots,x_{m,2^{m-1}})^\top;r)$ it is not clear how to use it to express equation (7.1), because not all the variables appear at once in this equation (but all the variables appear in the previous commitment). Our solution is to compute a single MP commitment to each vector that appears in equation (7.1) in order to show with Groth-Sahai proofs that

$$\begin{aligned}\mathsf{MP.Com}_{ck_\ell}\left(\begin{pmatrix}x_{\ell,1}\\ \vdots\\ x_{\ell,2^{\ell-1}}\end{pmatrix};r_\ell\right)=(1-b_\ell)\mathsf{MP.Com}_{ck_\ell}&\left(\begin{pmatrix}x_{\ell+1,1}\\ \vdots\\ x_{\ell+1,2^{\ell-1}}\end{pmatrix};r_{\ell,1}\right)+\\ b_\ell\mathsf{MP.Com}_{ck_\ell}&\left(\begin{pmatrix}x_{\ell+1,2^{\ell-1}+1}\\ \vdots\\ x_{\ell+1,2^{\ell}}\end{pmatrix};r_{\ell,2}\right)+\\ \mathsf{MP.Com}_{ck_\ell}&(\mathbf{0};y_\ell),\end{aligned}$$

$$\iff$$

$$\mathsf{MP.Com}_{ck_\ell}\left(\begin{array}{c}\begin{pmatrix} x_{\ell,1} \\ \vdots \\ x_{\ell,2^{\ell-1}}\end{pmatrix} - (1-b_\ell)\begin{pmatrix} x_{\ell+1,1} \\ \vdots \\ x_{\ell+1,2^{\ell-1}}\end{pmatrix} - b_\ell\begin{pmatrix} x_{\ell+1,2^{\ell-1}+1} \\ \vdots \\ x_{\ell+1,2^\ell}\end{pmatrix}; \\ r_\ell - (1-b_\ell)r_{\ell,1} - b_\ell r_{\ell,2}\end{array}\right)$$
$$= \mathsf{MP.Com}_{ck_\ell}(\mathbf{0}; y_\ell)$$

for each $\ell \in [m]$ and some $y_\ell \in \mathbb{Z}_q$. In this way, we only need $3m = 3\log t$ additional commitments. The reason for using different commitment keys for each $\ell \in [m]$ will be clear when we explain soundness.

Concretely, the prover computes

$$[\mathbf{c}_\ell]_1 = \mathsf{MP.Com}_{ck_\ell}((x_{\ell,1},\dots,x_{\ell,2^{\ell-1}})^\top; r_\ell),$$

for random $r_\ell \in \mathbb{Z}_q$ and $\ell \in [m]$, and

$$[\mathbf{c}_{\ell,1}]_1 = \mathsf{MP.Com}_{ck_\ell}((x_{\ell+1,1},\dots,x_{\ell+1,2^{\ell-1}})^\top; r_{\ell,1}),$$
$$[\mathbf{c}_{\ell,2}]_1 = \mathsf{MP.Com}_{ck_\ell}((x_{\ell+1,2^{m-1}+1},\dots,x_{\ell+1,2^{\ell}})^\top; r_{\ell,2}),$$

for random $r_{\ell,1}, r_{\ell,2} \in \mathbb{Z}_q$ and $\ell \in [m-1]$. Note that the prover does not need to compute commitments to $(x_{m+1,1},\dots,x_{m+1,t})^\top$ since $x_{m+1,i} = s_i$, $i \in [t]$, and thus they can be computed by the verifier.

Then, the prover shows that equation (7.1) holds with a GS proof of the satisfiability of

$$[\mathbf{c}_\ell]_1 - (1-b_\ell)[\mathbf{c}_{\ell,1}]_1 - b_\ell[\mathbf{c}_{\ell,2}]_1 = \mathsf{MP.Com}_{ck_\ell}(\mathbf{0}; y_\ell), \text{ for } \ell \in [m], \tag{7.3}$$

where $[\mathbf{c}_{m,1}] := \mathsf{MP.Com}_{ck_m}((s_1,\dots,s_{2^{m-1}})^\top; 0)$ and $[\mathbf{c}_{m,2}] := \mathsf{MP.Com}_{ck_m}((s_{2^{m-1}+1},\dots, s_t)^\top; 0)$ can be directly computed by the verifier, and $y_\ell := r_\ell - (1-b_\ell)r_{\ell,1} - b_\ell r_{\ell,2}$. It also computes Groth-Sahai proofs that

$$b_\ell(b_\ell - 1) = 0 \tag{7.4}$$

for each $\ell \in [m]$ (or equivalently a proof that $b_\ell \in \{0,1\}$).

The prover also shows that equation (7.2) is satisfied with a QA-NIZK proof that

$$[\mathbf{c}]_1 \text{ and } [\mathbf{c}_1]_1 \text{ open to the same value,} \tag{7.5}$$

using the proof system from Section 3.4.

Note that variables $x_{\ell+1,1},\dots,x_{\ell+1,2^{\ell-1}}$ appear in both $[\mathbf{c}_{\ell,1}]_1$ and $[\mathbf{c}_{\ell+1}]_1$, as well as $x_{\ell+1,2^{\ell-1}+1},\dots,x_{\ell+1,2^\ell}$ appear in both $[\mathbf{c}_{\ell,2}]_1$ and $[\mathbf{c}_{\ell+1}]_1$. To get a sound proof, the prover needs to show that this redundancy is consistent. That is, the prover needs to show that $[\mathbf{c}_{\ell,1}]_1$ and $[\mathbf{c}_{\ell,2}]_1$ are commitments to the first and last halves of the opening of $[\mathbf{c}_{\ell+1}]_1$.

For $\ell \in [m]$, let $ck_\ell := ([\mathbf{G}_\ell]_1, [\mathbf{g}_{\ell,2^{\ell-1}+1}]_1) \in \mathbb{G}_1^{2\times 2^{\ell-1}+1}$ the commitment key of a MP commitment scheme and let

$$\mathbf{G}_{\ell,1} := \begin{pmatrix}\mathbf{g}_{\ell,1} & \cdots & \mathbf{g}_{\ell,2^{\ell-2}}\end{pmatrix}, \qquad \mathbf{G}_{\ell,2} := \begin{pmatrix}\mathbf{g}_{\ell,2^{\ell-2}+1} & \cdots & \mathbf{g}_{\ell,2^{\ell-1}}\end{pmatrix}$$
$$\mathbf{G}_\ell := \mathbf{G}_{\ell,1}|\mathbf{G}_{\ell,2}$$

To prove consistency the prover will show that, for each $\ell \in [m-1]$, the following linear system is satisfied

$$\begin{pmatrix} \mathbf{c}_{\ell+1} \\ \mathbf{c}_{\ell,1} \\ \mathbf{c}_{\ell,2} \end{pmatrix} = \left(\begin{array}{cc|ccc} \mathbf{G}_{\ell+1,1} & \mathbf{G}_{\ell+1,2} & \mathbf{g}_{\ell+1,2^\ell+1} & \mathbf{0} & \mathbf{0} \\ \mathbf{G}_\ell & \mathbf{0}_{2\times 2^{\ell-1}} & \mathbf{0} & \mathbf{g}_{\ell,2^{\ell-1}+1} & \mathbf{0} \\ \mathbf{0}_{2\times 2^{\ell-1}} & \mathbf{G}_\ell & \mathbf{0} & \mathbf{0} & \mathbf{g}_{\ell,2^{\ell-1}+1} \end{array}\right) \mathbf{w}, \tag{7.6}$$

for some $\mathbf{w} \in \mathbb{Z}_q^{2^\ell+3}$, which can be proven using the proof system from Section 3.2.

Intuitively, $\mathbf{w}$ should be equal to $(x_{\ell+1,1}, \ldots, x_{\ell+1,2^\ell}, r_{\ell+1}, r_{\ell,1}, r_{\ell,2})$ and thus

$$[\mathbf{c}_{\ell,1}]_1 = \mathsf{MP.Com}_{ck_\ell}((x_{\ell+1,1}, \ldots, x_{\ell+1,2^{\ell-1}})^\top; r_{\ell,1}) \text{ and}$$
$$[\mathbf{c}_{\ell,2}]_1 = \mathsf{MP.Com}_{ck_\ell}((x_{\ell+1,2^{\ell-1}+1}, \ldots, x_{\ell+1,2^\ell})^\top; r_{\ell,2}).$$

However, since multi-Pedersen commitments have multiple openings it might be the case that the satisfying witness of the proof is different from $(x_{\ell+1,1}, \ldots, x_{\ell+1,2^\ell}, r_{\ell+1}, r_{\ell,1}, r_{\ell,2})$ and thus the intuitive reasoning is invalid.

Despite this flawed reasoning, we will show that the proof system is still sound.

Soundness Intuition

Suppose that an adversary against soundness outputs GS commitments to $b_1, \ldots, b_m \in \mathbb{Z}_q$, outputs commitments $[\mathbf{c}_\ell]_1$, $\ell \in [m]$, and $[\mathbf{c}_{\ell,1}]_1, [\mathbf{c}_{\ell,2}]$, $\ell \in [m-1]$, a GS proofs of the satisfiability of equation (7.3), and QA-NIZK proofs of (7.5) and (7.6) for each $\ell \in [m-1]$. Note that perfect soundness of Groth-Sahai proofs for equation (7.4) imply that $b_1, \ldots, b_m \in \{0,1\}$.

For $\ell \in [m]$, define α_ℓ as the position of s_α respective to the leaves under the path $(b_m, \ldots, b_\ell)$, that is $\alpha_\ell := \alpha - \mathsf{left} + 1$. Note that $\alpha_\ell \in [1, 2^{\ell-1}]$ since

$$1 \le \alpha_\ell = \sum_{i=1}^{m} b_i 2^{i-1} - \sum_{i=\ell}^{m} b_i 2^{i-1} + 1 = \sum_{i=1}^{\ell-1} b_i 2^{i-1} + 1 \le 2^{\ell-1}.$$

The key observation is that, for a fixed $\alpha \in [m]$, even if in equation (7.1) $x_{\ell,j}$ is not correctly computed for $j \neq \alpha_\ell$, it holds that $x_{m,1} = s_\alpha$ anyway. We will take advantage of this observation and the fact that the adversary commits to a fixed $\alpha = \sum_{i=1}^n b_i 2^{i-1} + 1$ to guarantee perfect soundness of equation (7.1) at least for coordinate α_ℓ for each $\ell \in [m]$. We do so by picking the commitment key ck_ℓ in such a way that its α_ℓ th column is linearly independent from the other columns. Although we will not be able to guarantee that $x_{\ell,j}$ is correctly computed if $j \neq \alpha_\ell$, at least we will be able to do so for x_{ℓ,α_ℓ}.

In the reduction we will guess the (sub-)path $(b_{m-1}, \ldots, b_1)$ (it will be not necessary to guess first the edge of the path) chosen by the adversary. While in the real scheme $\mathrm{rank}(\mathbf{G}_\ell) = 1$, for each $\ell \in [m]$, we jump to a game where $\mathbf{g}_{\ell,\alpha_\ell}$ is linearly independent from the other $2^{\ell-1}$ vectors in ck_ℓ. This can be done choosing random $b'_{m-1}, \ldots, b'_1 \in \{0,1\}$ and aborting if $(b'_{m-1}, \ldots, b'_1) \neq (b_{m-1}, \cdots, b_1)$. Therefore, our security reduction will have a security loss factor of $1/2^{m-1} = 2/t$. We sample $ck_\ell \leftarrow \mathcal{L}_1^{2^{\ell-1},\alpha_\ell}$, as defined on Section 2.4, which implies that for every $\ell \in [m]$ there exists unique $\tilde{x}_\ell, \tilde{r}_\ell \in \mathbb{Z}_q$ such that $\mathbf{c}_\ell := \tilde{x}_\ell \mathbf{g}_{\ell,\alpha_\ell} + \tilde{r}_\ell \mathbf{g}_{\ell,2^{\ell-1}+1}$.

We prove by induction on ℓ that $\mathbf{c}_\ell = s_\alpha \mathbf{g}_{\ell,\alpha_\ell} + \tilde{r}_\ell \mathbf{g}_{\ell,2^{\ell-1}+1}$, for some $\tilde{r}_\ell \in \mathbb{Z}_q$. If this is the case $\mathbf{c}_1 = s_\alpha \mathbf{g}_{1,1} + \tilde{r}_1 \mathbf{g}_{1,2}$. Soundness of proof for equation (7.5) together with the fact that ck_1 is perfectly binding implies that $x = \tilde{x}_1 = s_\alpha \in S$ which proves soundness.

First, it will be useful to prove the next lemma about α_ℓ.

Lemma 7.1 *Let $b_m, \ldots, b_1 \in \{0,1\}$. For all $\ell \in [m-1]$, $\alpha_{\ell+1} = \alpha_\ell + b_\ell 2^{\ell-1}$.*

Proof To avoid confusion, define here $\mathsf{left}_\ell := \sum_{i=\ell}^{m} b_i 2^{i-1} + 1$ (previously simply defined as left, the index of the leftmost leaf under the path $(b_m, \cdots, b_\ell)$). It holds that

$$\begin{aligned}
\alpha_{\ell+1} &= \alpha - \mathsf{left}_{\ell+1} + 1 \\
&= \sum_{i=1}^{m} b_i 2^{i-1} - \sum_{i=\ell+1}^{m} b_i 2^{i-1} + 1 \\
&= \sum_{i=1}^{m} b_i 2^{i-1} - \sum_{i=\ell}^{m} b_i 2^{i-1} + 1 + b_\ell 2^{\ell-1} \\
&= \alpha - \mathsf{left}_\ell + 1 + b_\ell 2^{\ell-1} \\
&= \alpha_\ell + b_\ell 2^{\ell-1}
\end{aligned}$$

□

Now we prove that, for all $\ell \in [m]$, $\mathbf{c}_\ell = s_\alpha \mathbf{g}_{\ell,\alpha_\ell} + \tilde{r}_\ell \mathbf{g}_{\ell,2^{\ell-1}+1}$. In the base case ($\ell = m$) the fact that $\mathbf{g}_{m,i} \in \mathbf{Span}(\mathbf{g}_{m,2^{m-1}+1})$ if $i \neq \alpha_m$ together with Lemma 7.1 implies that

$$\begin{aligned}
\mathbf{c}_m &= (1-b_m)\sum_{i=1}^{2^{m-1}} s_i \mathbf{g}_{m,i} + b_m \sum_{i=1}^{2^{m-1}} s_{i+2^{m-1}} \mathbf{g}_{m,i} \\
&= (1-b_m) s_{\alpha_m} \mathbf{g}_{m,\alpha_m} + b_m s_{\alpha_m + 2^{m-1}} \mathbf{g}_{m,\alpha_m} + \tilde{r}_1 \mathbf{g}_{m,2^{m-1}+1} \\
&= (1-b_m) s_{\alpha - \mathsf{left}+1} \mathbf{g}_{m,\alpha_m} + b_m s_{\alpha-\mathsf{left}+1+2^{m-1}} \mathbf{g}_{m,\alpha_m} + \tilde{r}_1 \mathbf{g}_{m,2^{m-1}+1} \\
&= \begin{cases} s_{\alpha-1+1} \mathbf{g}_{m,\alpha_m} + \tilde{r}_1 \mathbf{g}_{m,t/2} & \text{if } b_m = 0 \text{ (and thus } \mathsf{left} = 1) \\ s_{\alpha-(2^{m-1}+1)+1+2^{m-1}} \mathbf{g}_{m,\alpha_m} + \tilde{r}_1 \mathbf{g}_{m,t/2} & \text{if } b_m = 1 \text{ (and thus } \mathsf{left} = 2^{m-1}+1) \end{cases}
\end{aligned}$$

for some $\tilde{r}_1 \in \mathbb{Z}_q$. In both cases $\mathbf{c}_m = s_\alpha \mathbf{g}_{1,\alpha_m} + \tilde{r}_1 \mathbf{g}_{m,t/2}$.

In the inductive case we assume that $\mathbf{c}_{\ell+1} = s_\alpha \mathbf{g}_{\ell+1,\alpha_{\ell+1}} + \tilde{r}_{\ell+1} \mathbf{g}_{\ell+1,2^\ell+1}$ and we want to show that $\mathbf{c}_\ell = s_\alpha \mathbf{g}_{\ell,\alpha_\ell} + \tilde{r}_\ell \mathbf{g}_{\ell,2^{\ell-1}+1}$. Since $\mathbf{g}_{\ell+1,\alpha_{\ell+1}}$ is linearly independent from the rest of vectors in $ck_{\ell+1}$, any solution to equation (7.6) is equal to s_α at position $\alpha_{\ell+1} = \alpha_\ell + b_\ell 2^{\ell-1}$ as depicted below.

$$\begin{pmatrix} \mathbf{c}_{\ell+1} \\ \mathbf{c}_{\ell,1} \\ \mathbf{c}_{\ell,2} \end{pmatrix} = \begin{pmatrix} \cdots & \mathbf{g}_{\ell+1,\alpha_\ell} & \cdots & \mathbf{g}_{\ell+1,\alpha_\ell+2^{\ell-1}} & \cdots \\ \cdots & \mathbf{g}_{\ell,\alpha_\ell} & \cdots & \mathbf{0} & \cdots \\ \cdots & \mathbf{0} & \cdots & \mathbf{g}_{\ell,\alpha_\ell} & \cdots \end{pmatrix} \begin{pmatrix} \vdots \\ s_\alpha \\ \vdots \end{pmatrix}$$

If $b_\ell = 0$, by Lemma 7.1, $\alpha_{\ell+1} = \alpha_\ell$. Therefore, any solution to equation (7.6) is equal to s_α at position α_ℓ and thus $\mathbf{c}_{\ell,1} = s_\alpha \mathbf{g}_{\ell,\alpha_\ell} + \tilde{r}_{\ell,1} \mathbf{g}_{\ell,2^{\ell-1}+1}$. Equation (7.3) implies that

$$\begin{aligned}
\mathbf{c}_\ell =& (1-b_\ell)(s_\alpha \mathbf{g}_{\ell,\alpha_\ell} + \tilde{r}_{\ell,1} \mathbf{g}_{\ell,2^{\ell-1}+1}) + b_\ell \mathbf{c}_{\ell,2} + y_\ell \mathbf{g}_{\ell,2^{\ell-1}+1} \\
=& s_\alpha \mathbf{g}_{\ell,\alpha_\ell} + (\tilde{r}_{\ell,1} + y_\ell) \mathbf{g}_{\ell,2^{\ell-1}+1}.
\end{aligned}$$

If $b_\ell = 1$, then $\alpha_{\ell+1} = \alpha_\ell + 2^{\ell-1}$ and similarly, $\mathbf{c}_\ell = s_\alpha \mathbf{g}_{\ell,\alpha_\ell} + (\tilde{r}_{\ell,2} + y_\ell) \mathbf{g}_{\ell,2^{\ell-1}+1}$.

7.2 The Aggregated Case

Let $t := |S|$ and $m := \log t$. The statement is now $[\boldsymbol{\zeta}_1] = \mathsf{GS.Com}_{ck_{\mathsf{GS}}}(x_1; r_1), \ldots, [\boldsymbol{\zeta}_n]_1 = \mathsf{GS.Com}_{ck_{\mathsf{GS}}}(x_n; r_n)$, for some $n \in \mathbb{N}$, and the prover wants to show that $x_i = s_{\alpha_i}$, for all

$i \in [n]$ and $\alpha_i = \sum_{j=1}^{m} b_{i,j}2^{j-1} + 1$, for some $b_{i,1}, \ldots, b_{i,m} \in \{0,1\}$. We need to reformulate equations (7.1) and (7.2) to take in count new variables. For $\ell \in [m], i \in [n]$, define

$$\mathbf{x}_\ell^i := \begin{pmatrix} \mathbf{x}_{\ell,1}^i \\ \hline \mathbf{x}_{\ell,2}^i \end{pmatrix} := \begin{pmatrix} x_{\ell,1}^i \\ \vdots \\ x_{\ell,2^{\ell-2}}^i \\ \hline x_{\ell,2^{\ell-2}+1}^i \\ \vdots \\ x_{\ell,2^{\ell-1}}^i \end{pmatrix}, \qquad \mathbf{x}_{m+1,1}^i := \begin{pmatrix} s_1 \\ \vdots \\ s_{t/2} \end{pmatrix}, \text{ and } \mathbf{x}_{m+1,2}^i := \begin{pmatrix} s_{t/2+1} \\ \vdots \\ s_t \end{pmatrix},$$

and define new equations for each $\ell \in [m], i \in [n]$

$$\mathbf{x}_\ell^i = (1 - b_{i,\ell})\mathbf{x}_{\ell+1,1}^i + b_{i,\ell}\mathbf{x}_{\ell+1,2}^i, \tag{7.7}$$

$$x_i = \mathbf{x}_1^i \tag{7.8}$$

Next, we construct an aZKSMP for $S \subset \mathbb{Z}_q$ and in Section 7.2.1 we show how to extend these ideas for the case of fixed $S \subset \mathbb{G}_1$. The construction follows the intuition outlined before but it "aggregates" many instances on a single $\Theta(\log t)$ proof. From a high level this is done as follows.

We will rewrite equation (7.7), which is a system of mn equations, as m equations of the form

$$\mathbf{x}\mathbf{y}^\top = \begin{pmatrix} 0 & x_1y_2 & \cdots & x_1y_n \\ x_2y_1 & 0 & \cdots & x_2y_n \\ \vdots & \vdots & \ddots & \vdots \\ x_my_1 & x_my_2 & \cdots & 0 \end{pmatrix}, \tag{7.9}$$

where $\mathbf{x} \in \mathbb{Z}_q^m, \mathbf{y} \in \mathbb{Z}_q^n$ (i.e. the diagonal of the matrix $\mathbf{x}\mathbf{y}^\top$ is $\mathbf{0}$). We will use similar techniques to those of Chapter 4 to give a constant size proof for the satisfiability of each of these equations. Therefore, to prove m of these equations we will require $\Theta(m) = \Theta(\log t)$ group elements.

We can compute $\mathbf{x}\mathbf{y}^\top$ in the "commitment space" by means of $[\mathbf{c}]_1[\mathbf{d}^\top]_2$, where $[\mathbf{c}]_1 := \mathsf{MP.Com}_{ck_1}(\mathbf{x}; r_1)$ and $[\mathbf{d}]_2 := \mathsf{MP.Com}_{ck_2}(\mathbf{y}; r_2)$. Indeed, by the definition of MP commitments it holds that

$$\begin{aligned}[\mathbf{c}]_1[\mathbf{d}^\top]_2 &= \left(\sum_{i=1}^{m} x_i[\mathbf{g}_i]_1 + r_1[\mathbf{g}_{m+1}]_1\right)\left(\sum_{j=1}^{n} y_j[\mathbf{h}_j^\top]_2 + r_2[\mathbf{h}_{n+1}^\top]_2\right) \\ &= \sum_{i=1}^{m}\sum_{j=1}^{n} x_iy_j[\mathbf{g}_i\mathbf{h}_j^\top]_T + \sum_{i=1}^{m} x_ir_2[\mathbf{g}_i\mathbf{h}_{n+1}^\top]_T + \sum_{j=1}^{n+1} r_1y_j[\mathbf{g}_{m+1}\mathbf{h}_j^\top]_T\end{aligned}$$

Therefore, if the diagonal of $\mathbf{x}\mathbf{y}^\top$ is $\mathbf{0}$, then $[\mathbf{c}]_1[\mathbf{d}^\top]_2$ is in the space spanned by $\{[\mathbf{g}_i\mathbf{h}_j^\top]_T : i \neq j \text{ or } i = m+1 \text{ or } j = n+1\}$. Similarly as done in Section 4.1.1, equation (7.9) can be proven computing two matrices $[\mathbf{\Theta}]_1 \in \mathbb{G}_1^{2\times 2}$ and $[\mathbf{\Pi}]_2 \in \mathbb{G}_2^{2\times 2}$ and showing that $[\mathbf{c}]_1[\mathbf{d}^\top]_2 = [\mathbf{\Theta}]_1[\mathbf{I}]_2 + [\mathbf{I}]_1[\mathbf{\Pi}]_2$ and $\mathbf{\Theta} + \mathbf{\Pi} \in \mathbf{Span}(\{\mathbf{g}_i\mathbf{h}_j^\top : i = m+1 \text{ or } j = n+1\})$.

For each $\ell \in [m]$, to rewrite the right side of equation (7.7) in the $\mathbf{x}\mathbf{y}^\top$ form, we observe that

$$\begin{pmatrix}\mathbf{x}^1_{\ell+1,1}\\ \vdots \\ \mathbf{x}^n_{\ell+1,1}\end{pmatrix}\left(\begin{pmatrix}b_{1,\ell}\\ \vdots \\ b_{n,\ell}\end{pmatrix} - \begin{pmatrix}1\\ \vdots \\ 1\end{pmatrix}\right)^\top + \begin{pmatrix}\mathbf{x}^1_{\ell+1,1}\\ \vdots \\ \mathbf{x}^n_{\ell+1,2}\end{pmatrix}\begin{pmatrix}b_{1,\ell}\\ \vdots \\ b_{n,\ell}\end{pmatrix}^\top =$$

$$\begin{pmatrix}(1-b_{1,\ell})\mathbf{x}^1_{\ell+1,1} + b_{1,\ell}\mathbf{x}^1_{\ell+1,2} & \cdots & (1-b_{n,\ell})\mathbf{x}^1_{\ell+1,1} + b_{n,\ell}\mathbf{x}^1_{\ell+1,2}\\ \vdots & \ddots & \vdots \\ (1-b_{1,\ell})\mathbf{x}^n_{\ell+1,1} + b_{1,\ell}\mathbf{x}^n_{\ell+1,2} & \cdots & (1-b_{n,\ell})\mathbf{x}^n_{\ell+1,1} + b_{n,\ell}\mathbf{x}^n_{\ell+1,2}\end{pmatrix}.$$

If we view the previous matrix as one of size $n \times n$ where each entry is a vector from $\mathbb{Z}_q^{2^{\ell-1}}$, then the diagonal forms the right side of equation (7.7). We rewrite the left side of equation (7.7) as

$$\begin{pmatrix}\mathbf{x}^1_{\ell}\\ \vdots \\ \mathbf{x}^n_{\ell}\end{pmatrix}\begin{pmatrix}1\\ \vdots \\ 1\end{pmatrix}^\top = \begin{pmatrix}\mathbf{x}^1_{\ell} & \cdots & \mathbf{x}^1_{\ell}\\ \vdots & & \vdots \\ \mathbf{x}^n_{\ell} & \cdots & \mathbf{x}^n_{\ell}\end{pmatrix}.$$

and, again, the diagonal forms the left side of equation (7.7).

Now we prove that equation (7.7) holds by replacing variables with MP commitments and showing that

$$[\mathbf{c}_\ell]_1\left(\sum_{j=1}^n [\mathbf{h}_j]_2\right)^\top - [\mathbf{c}_{\ell,1}]_1\left([\mathbf{d}_\ell]_2 - \sum_{j=1}^n [\mathbf{h}_j]_2\right)^\top - [\mathbf{c}_{\ell,2}]_1[\mathbf{d}]_2^\top = [\boldsymbol{\Theta}]_1[\mathbf{I}]_2 + [\mathbf{I}]_1[\boldsymbol{\Pi}]_2,$$

where

$$\begin{aligned}
[\mathbf{c}_\ell]_1 &:= \mathsf{MP.Com}_{ck_\ell}\left(\begin{pmatrix}\mathbf{x}^1_{\ell}\\ \vdots \\ \mathbf{x}^n_{\ell}\end{pmatrix}; r_\ell\right) & [\mathbf{d}_\ell]_1 &:= \mathsf{MP.Com}_{ck}\left(\begin{pmatrix}b_{1,\ell}\\ \vdots \\ b_{n,\ell}\end{pmatrix}; t_\ell\right)\\
[\mathbf{c}_{\ell,1}]_1 &:= \mathsf{MP.Com}_{ck_\ell}\left(\begin{pmatrix}\mathbf{x}^1_{\ell+1,1}\\ \vdots \\ \mathbf{x}^n_{\ell+1,1}\end{pmatrix}; r_{\ell,1}\right) & [\mathbf{c}_{\ell,2}]_1 &:= \mathsf{MP.Com}_{ck_\ell}\left(\begin{pmatrix}\mathbf{x}^1_{\ell+1,2}\\ \vdots \\ \mathbf{x}^n_{\ell+1,2}\end{pmatrix}\right)\\
ck_\ell &:= [\begin{pmatrix}\mathbf{G}^1_\ell & \cdots & \mathbf{G}^n_\ell & \mathbf{g}_{\ell,n2^{\ell-1}+1}\end{pmatrix}]_1 & \mathbf{G}^i_\ell &:= \begin{pmatrix}\mathbf{g}_{\ell,(i-1)2^{\ell-1}+1} & \cdots & \mathbf{g}_{\ell,i2^{\ell-1}}\end{pmatrix}\\
ck &:= [\mathbf{H}]_2 & \mathbf{H} &:= \begin{pmatrix}\mathbf{h}_1 & \cdots & \mathbf{h}_n & \mathbf{h}_{n+1}\end{pmatrix}.
\end{aligned}$$

We need to show that $\boldsymbol{\Theta} + \boldsymbol{\Pi}$ is in the appropriate space, which is the one without components "in the diagonal" or with components in $\mathbf{g}_{\ell,n2^{\ell-1}+1}\mathbf{h}_j$ or $\mathbf{g}_i\mathbf{h}_{n+1}$ for any $i \in [n2^{\ell-1}], j \in [n+1]$. However, since we are working with matrices whose entries are vectors in $\mathbb{Z}_q^{2^{\ell-1}}$, we in fact need to show that

$$\boldsymbol{\Theta} + \boldsymbol{\Pi} \in \mathbf{Span}(\{\mathbf{g}_{\ell,i}\mathbf{h}_j^\top : j \in [n+1], i \notin [(j-1)2^{\ell-1}+1, j2^{\ell-1}] \setminus [n2^{\ell-1}+1]\}),$$

since the indices i and j where $i \in [(j-1)2^{\ell-1}+1, j2^{\ell-1}]$ are those which range over the elements in the diagonal of a matrix whose entries are elements from $\mathbb{Z}_q^{2^{\ell-1}}$.

It is only left to prove the "aggregated version" of equation (7.6) from the non-aggregated case, and to prove equation (7.8). Equation (7.6) is proven in the same way as in the non-aggregated case, but enlarging the matrix as consequence of the enlargement of commitment keys. Additionally, we prove equation (7.8) with a proof that

$$[\boldsymbol{\zeta}_1]_1, \ldots, [\boldsymbol{\zeta}_n]_1 \text{ and } [\mathbf{c}_1]_1 \text{ open to the same values,}$$

using the proof system from Section 3.4.

The Scheme

$\mathsf{K}_1(gk, ck_{\mathsf{GS}})$**:** Parse ck_{GS} as $[\mathbf{u}_1|\mathbf{u_2}]_1$. For each $\ell \in [m]$ let $\mathbf{G}_\ell := \mathbf{G}_\ell^1|\cdots|\mathbf{G}_\ell^n|\mathbf{g}_{\ell,n2^{\ell-1}+1} \leftarrow \mathcal{L}_1^{n2^{\ell-1}+1,0}$, where

$$\mathbf{G}_\ell^i = (\mathbf{G}_{\ell,1}^i|\mathbf{G}_{\ell,2}^i) =$$
$$(\mathbf{g}_{\ell,(i-1)2^{\ell-1}+1}\cdots\mathbf{g}_{\ell,(i-1)2^{\ell-1}+2^{\ell-2}}|\mathbf{g}_{\ell,(i-1)2^{\ell-1}+2^{\ell-2}+1}\cdots\mathbf{g}_{\ell,i2^{\ell-1}}) \in \mathbb{Z}_q^{2\times 2^{\ell-1}},$$

$i \in [n]$, and define $ck_\ell := [\mathbf{G}_\ell]_1$. Let $\mathbf{H} = \begin{pmatrix}\mathbf{h}_1 & \cdots & \mathbf{h}_n & \mathbf{h}_{n+1}\end{pmatrix} \leftarrow \mathcal{L}_1^{n,0}$ and define $ck := [\mathbf{H}]_2$.

For each $\ell \in [m]$, $i \in [n2^{\ell-1}+1]$, $j \in [n+1]$, such that $i \notin [(j-1)2^{\ell-1}+1, j2^{\ell-1}]$ define matrices

$$\mathbf{M}_{i,j}^\ell := ([\mathbf{C}_{i,j}^\ell]_1, [\mathbf{D}_{i,j}^\ell]_2) := ([\mathbf{g}_{\ell,i}\mathbf{h}_j^\top + \mathbf{T}]_1, [-\mathbf{T}]_2),$$

For $\ell \in [m]$, pick $\mathbf{T} \leftarrow \mathbb{Z}_q^{2\times 2}$ and let

$$\mathcal{M}_\ell := \{\mathbf{M}_{i,j}^\ell : j \in [n+1], i \notin [(j-1)2^{\ell-1}+1, j2^{\ell-1}] \setminus [n2^{\ell-1}+1]\}$$

and let

$$\mathcal{C}_\ell := \{\mathbf{C}_{i,j}^\ell : j \in [n+1], i \notin [(j-1)2^{\ell-1}+1, j2^{\ell-1}] \setminus [n2^{\ell-1}+1]\}.$$

Let Π_{sum} be the proof system for sum in subspace (Section 3.3), Π_{lin} the proof system for membership in linear subspaces from Section 2.7, Π_{bits} the proof system for proving that many commitments open to bit-strings from section 4.2.3, and Π_{com} be an instance of the proof system for equal commitment opening (Section 3.4).

For each $\ell \in [m]$, let $\mathsf{crs}_{\mathsf{sum},\ell} \leftarrow \Pi_{\mathsf{sum}}.\mathsf{K}_1(gk, \mathcal{M}_\ell)$.[4], let $\mathsf{crs}_{\mathsf{lin},\ell} \leftarrow \Pi_{\mathsf{lin}}.\mathsf{K}_1(gk; [\mathbf{G}_{\ell,\mathsf{split}}]_1, n2^{\ell-1}+3)$, let $\mathsf{crs}_{\mathsf{bits}} \leftarrow \Pi_{\mathsf{bits}}.\mathsf{K}_1(gk, [\mathbf{H}]_2, m)$, and let $\mathsf{crs}_{\mathsf{com}} \leftarrow \Pi_{\mathsf{com}}.\mathsf{K}_1(gk, ck_1, CK_{\mathsf{GS}}, m)$, where

$$\mathbf{G}_{\ell,\mathsf{split}} :=$$
$$\begin{pmatrix} \mathbf{G}_{\ell+1,1}^1 & \mathbf{G}_{\ell+1,2}^1 & \cdots & \mathbf{G}_{\ell+1,1}^n & \mathbf{G}_{\ell+1,2}^n & \mathbf{g}_{\ell+1,n2^\ell+1} & \mathbf{0} & \mathbf{0} \\ \mathbf{G}_{\ell,1}^1 & \mathbf{0} & \cdots & \mathbf{G}_{\ell,n}^n & \mathbf{0} & \mathbf{0} & \mathbf{g}_{\ell,n2^{\ell-1}+1} & \mathbf{0} \\ \mathbf{0} & \mathbf{G}_{\ell,1}^1 & \cdots & \mathbf{0} & \mathbf{G}_{\ell,n}^n & \mathbf{0} & \mathbf{0} & \mathbf{g}_{\ell,n2^{\ell-1}+1} \end{pmatrix},$$

$$CK_{\mathsf{GS}} := \begin{pmatrix} [\mathbf{u}_1]_1 & & [\mathbf{0}]_1 & [\mathbf{u}_2]_1 & & [\mathbf{0}]_1 \\ & \ddots & & & \ddots & \\ [\mathbf{0}]_1 & & [\mathbf{u}_1]_1 & [\mathbf{0}]_1 & & [\mathbf{u}_2]_1 \end{pmatrix} \in \mathbb{G}_1^{2n\times 2n}.$$

The common reference string is given by:

$$\mathsf{crs} \ := \ (gk, [\mathbf{G}]_1, [\mathbf{H}]_2, \{\mathcal{M}_\ell, \mathsf{crs}_{\mathsf{sum},\ell}, \mathsf{crs}_{\mathsf{lin},\ell} : \ell \in [m]\}, \mathsf{crs}_{\mathsf{bits}}, \mathsf{crs}_{\mathsf{com}})\,.$$

[4] We identify matrices in $\mathbb{G}_1^{2\times 2}$ (respectively in $\mathbb{G}_2^{2\times 2}$) with vectors in $\mathbb{G}_1^4$ (resp. in $\mathbb{G}_2^4$).

$\mathsf{P}(\mathsf{crs}, ([\boldsymbol{\zeta}_1]_1, \ldots, [\boldsymbol{\zeta}_n]_1, S), \langle (x_1, \ldots, x_n), (w_1, \ldots, w_n) \rangle)$**:** The prover compute commitments

$$\begin{aligned}
&[\mathbf{c}_\ell]_1 := \mathsf{MP.Com}_{ck_\ell}(\mathbf{x}_\ell^{1\top}, \ldots, \mathbf{x}_\ell^{n\top}; r_\ell), \text{ for } \ell \in [m],\\
&[\mathbf{c}_{\ell,1}]_1 := \mathsf{MP.Com}_{ck_\ell}(\mathbf{x}_{\ell+1,1}^{1}{}^\top, \ldots, \mathbf{x}_{\ell+1,1}^{n}{}^\top; r_{\ell,1}),\\
&[\mathbf{c}_{\ell,2}]_1 := \mathsf{MP.Com}_{ck_\ell}(\mathbf{x}_{\ell+1,2}^{1}{}^\top, \ldots, \mathbf{x}_{\ell+1,2}^{n}{}^\top; r_{\ell,2}), \text{ for } \ell \in [m-1]\\
&[\mathbf{d}_\ell]_2 := \mathsf{MP.Com}_{ck}(\mathbf{b}_\ell; t_\ell), \text{ for } \ell \in [m]
\end{aligned}$$

where $r_\ell, r_{\ell,1}, r_{\ell,2}, t_j \leftarrow \mathbb{Z}_q$ and the variables $\mathbf{x}_\ell^i, \mathbf{x}_{\ell,j}^i, \mathbf{b}_\ell$ are the ones defined in equation (7.7). The prover computes a proof π_{bits} that $[\mathbf{d}_1]_2, \ldots, [\mathbf{d}_m]_2$ open to bit-strings. Then, for $\ell \in [m]$, the prover pick matrices $\mathbf{R}_\ell \leftarrow \mathbb{Z}_q^{2\times 2}$, computes

$$\begin{aligned}
&([\boldsymbol{\Theta}_\ell]_1, [\boldsymbol{\Pi}_\ell]_2) :=\\
&\quad \sum_{i=1}^{n} \sum_{j \neq i} \sum_{k=1}^{2^{\ell-1}} (x_{\ell,k}^i - x_{\ell+1,k}^i(1 - b_{j,\ell}) - x_{\ell+1,2^{\ell-1}+k}^i b_{j,\ell}) \mathbf{M}^\ell_{(i-1)2^{\ell-1}+k,j}\\
&\quad + \sum_{i=1}^{n} \sum_{k=1}^{2^{\ell-1}} t_\ell (x_{\ell+1,k}^i - x_{\ell+1,2^{\ell-1}+k}^i) \mathbf{M}^\ell_{(i-1)2^{\ell-1}+k,n+1}\\
&\quad + \sum_{j=1}^{n} (r_\ell - r_{\ell,1}(1 - b_{j,\ell}) - r_{\ell,2} b_{j,\ell}) \mathbf{M}^\ell_{n2^{\ell-1}+1,j}\\
&\quad + (r_{\ell,1} - r_{\ell,2}) t_\ell \mathbf{M}^\ell_{n2^{\ell-1}+1,n+1} + ([\mathbf{R}_\ell]_1, [-\mathbf{R}_\ell]_2),
\end{aligned}$$

where $r_{1,1} = r_{1,2} = 0$, and computes proofs $\pi_{\mathsf{lin},\ell}, \pi_{\mathsf{sum},\ell}$ that, respectively,

$$\begin{pmatrix} \mathbf{c}_{\ell+1} \\ \mathbf{c}_{\ell,1} \\ \mathbf{c}_{\ell,2} \end{pmatrix} \in \mathbf{Span}(\mathbf{G}_{\ell,\mathsf{split}}) \text{ (if } \ell < m), \qquad \boldsymbol{\Theta}_\ell + \boldsymbol{\Pi}_\ell \in \mathbf{Span}(\mathcal{C}_\ell).$$

Finally, it computes a proof π_{com} that $([\boldsymbol{\zeta}_1]_1, \ldots, [\boldsymbol{\zeta}_n]_1)$ and $[\mathbf{c}_1]_1$ open to the same value.

The proof is $\pi := (\{([\mathbf{c}_\ell]_1, [\mathbf{c}_{\ell,1}]_1, [\mathbf{c}_{\ell,2}]_1, [\mathbf{d}_\ell]_2, [\boldsymbol{\Theta}_\ell]_1, [\boldsymbol{\Pi}_\ell]_2, \pi_{\mathsf{lin},\ell}, \pi_{\mathsf{sum},\ell}) : \ell \in [m]\}, \pi_{\mathsf{bits}}, \pi_{\mathsf{com}})$.

$\mathsf{V}(\mathsf{crs}, ([\boldsymbol{\zeta}_1]_1, \ldots, [\boldsymbol{\zeta}_n]_1, S), \pi)$**:** Let $[\mathbf{c}_{m,1}]_1 := \mathsf{MP.Com}_{ck_m}(s_1, \ldots, s_{t/2}; 0), [\mathbf{c}_{m,2}] := \mathsf{MP.Com}_{ck_m}(s_{t/2+1}, \ldots, s_t; 0)$. The verifier checks the validity of $\pi_{\mathsf{bits}}, \pi_{\mathsf{com}}$ and, for each $\ell \in [m]$, checks the validity of $\pi_{\mathsf{lin},\ell}, \pi_{\mathsf{sum},\ell}$ and of equations

$$\begin{aligned}
&[\mathbf{c}_\ell]_1 \left(\sum_{j=1}^{n} [\mathbf{h}_j]_2 \right)^\top - [\mathbf{c}_{\ell,1}]_1 \left(\sum_{j=1}^{n} [\mathbf{h}_j]_2 - [\mathbf{d}_\ell]_2 \right)^\top - [\mathbf{c}_{\ell,2}]_1 [\mathbf{d}_\ell]_2^\top =\\
&[\boldsymbol{\Theta}_\ell]_1 [\mathbf{I}]_2 + [\mathbf{I}]_1 [\boldsymbol{\Pi}_\ell]_2. \qquad (7.10)
\end{aligned}$$

If any of these checks fails, it rejects the proof.

$\mathsf{S}_1(gk, ck_{\mathsf{GS}})$**:** The simulator receives as input a description of an asymmetric bilinear group gk and a GS commitment key ck_{GS}. It generates and outputs the CRS in the same way as K_1, but additionally outputs the simulation trapdoor $\tau := (\mathbf{H}, \tau_{\mathsf{com}}, \tau_{\mathsf{bits}}, \{\tau_{\mathsf{sum},\ell}, \tau_{\mathsf{lin},\ell} : \ell \in [m]\})$, where $\tau_{\mathsf{sum}}, \tau_{\mathsf{bits}}, \tau_{\mathsf{sum},\ell}, \tau_{\mathsf{lin},\ell}$ are, respectively, $\Pi_{\mathsf{sum}}, \Pi_{\mathsf{com}}, \Pi_{\mathsf{sum}}, \Pi_{\mathsf{lin}}$ simulation trapdoors.

$\mathsf{S}_2(\mathsf{crs}, ([\boldsymbol{\zeta}_1]_1, \ldots, [\boldsymbol{\zeta}_n]_1, S), \tau)$**:** Define $\mathbf{x}_\ell^i := \mathbf{0}$ and $\mathbf{b}_\ell := \mathbf{0}$ for all $\ell \in [m], i \in [n]$, and computes $[\mathbf{c}_\ell]_1, [\mathbf{c}_{\ell,1}]_1, [\mathbf{c}_{\ell,2}]_1, [\mathbf{d}_\ell]_2$ and $[\boldsymbol{\Theta}_\ell]_1, [\boldsymbol{\Pi}_\ell]_2$, as an honest prover would do (that is, with all variables set to 0). Finally, simulate proofs $\pi_{\mathsf{com}}, \pi_{\mathsf{bits}}, \pi_{\mathsf{sum},\ell}, \pi_{\mathsf{lin},\ell}$ using the respective trapdoors.

We prove the following Theorem.

Theorem 7.2 *The proof system described above is a QA-NIZK proof system for the language $\mathcal{L}^n_{ck_{\mathsf{GS}},\mathsf{set}}$ with perfect completeness, computational soundness, and perfect zero-knowledge.*

Completeness

Completeness follows from completeness of $\Pi_{\mathsf{sum}}, \Pi_{\mathsf{lin}}, \Pi_{\mathsf{bits}}, \Pi_{\mathsf{com}}$, and from the fact that equation (7.10) is satisfied for each $\ell \in [m]$:

$$\begin{aligned}
&\mathbf{c}_\ell \left(\sum_{j=1}^n \mathbf{h}_j\right)^\top - \mathbf{c}_{\ell,1}\left(\sum_{j=1}^n \mathbf{h}_j - \mathbf{d}_\ell\right)^\top - \mathbf{c}_{\ell,2}\mathbf{d}_\ell^\top && = \\
&\sum_{i=1}^n\sum_{j=1}^n \mathbf{G}_\ell^i \mathbf{x}_\ell^i \mathbf{h}_j^\top + \sum_{j=1}^n r_\ell \mathbf{g}_{\ell,n2^{\ell-1}+1}\mathbf{h}_j^\top - \sum_{i=1}^n\sum_{j=1}^n \mathbf{G}_\ell^i \mathbf{x}_{\ell+1,1}^i (1-b_{j,\ell})\mathbf{h}_j^\top \\
&+ \sum_{i=1}^n \mathbf{G}_\ell^i \mathbf{x}_{\ell+1,1}^i t_\ell \mathbf{h}_{n+1}^\top - \sum_{j=1}^n r_{\ell,1}(1-b_{j,\ell})\mathbf{g}_{\ell,n2^{\ell-1}+1}\mathbf{h}_j^\top + r_{\ell,1}t_\ell \mathbf{g}_{\ell,n2^{\ell-1}+1}\mathbf{h}_{n+1}^\top \\
&- \sum_{i=1}^n\sum_{j=1}^n \mathbf{G}_\ell^i \mathbf{x}_{\ell+1,2}^i b_{j,\ell}\mathbf{h}_j^\top - \sum_{i=1}^n \mathbf{G}_\ell^i \mathbf{x}_{\ell+1,2}^i t_\ell \mathbf{h}_{n+1}^\top - \sum_{j=1}^n r_{\ell,2} b_{j,\ell}\mathbf{g}_{\ell,n2^{\ell-1}+1}\mathbf{h}_j^\top \\
&- r_{\ell,2}t_\ell \mathbf{g}_{\ell,n2^{\ell-1}+1}\mathbf{h}_{n+1}^\top && = \\
&\sum_{i=1}^n\sum_{j\neq i} \mathbf{G}_\ell^i(\mathbf{x}_\ell^i - \mathbf{x}_{\ell+1,1}^i(1-b_{j,\ell}) - \mathbf{x}_{\ell+1,2}^i b_{j,\ell})\mathbf{h}_j^\top + \\
&\sum_{i=1}^n \mathbf{G}_\ell^i(\mathbf{x}_{\ell+1,1}^i - \mathbf{x}_{\ell+1,2}^i)t_\ell \mathbf{h}_{n+1}^\top + \sum_{j=1}^n (r_\ell - r_{\ell,1}(1-b_{j,\ell}) - r_{\ell,2}b_{j,\ell})\mathbf{g}_{\ell,n2^{\ell-1}+1}\mathbf{h}_j^\top \\
&+ (r_{\ell,1} - r_{\ell,2})t_\ell \mathbf{g}_{\ell,n2^{\ell-1}+1}\mathbf{h}_{n+1}^\top && = \\
&\sum_{i=1}^n\sum_{j\neq i}\sum_{k=1}^{2^{\ell-1}} (x_{\ell,k}^i - x_{\ell+1,k}^i(1-b_{j,\ell}) - x_{\ell+1,2^{\ell-1}+k}^i b_{j,\ell}))\mathbf{g}_{\ell,(i-1)2^{\ell-1}+k}\mathbf{h}_j^\top \\
&+ \sum_{i=1}^n\sum_{k=1}^{2^{\ell-1}} t_\ell(x_{\ell+1,k}^i - x_{\ell+1,2^{\ell-1}+k}^i \mathbf{g}_{\ell,(i-1)2^{\ell-1}+k}\mathbf{h}_{n+1}^\top \\
&\sum_{j=1}^n (r_\ell - r_{\ell,1}(1-b_{j,\ell}) - r_{\ell,2}b_{j,\ell})\mathbf{g}_{\ell,n2^{\ell-1}+1}\mathbf{h}_j^\top + (r_{\ell,1}-r_{\ell,2})t_\ell \mathbf{g}_{\ell,n2^{\ell-1}+1}\mathbf{h}_{n+1}^\top && = \\
&\boldsymbol{\Theta}\mathbf{I} + \mathbf{I}\boldsymbol{\Pi}.
\end{aligned}$$

Soundness

The following theorem guarantees soundness.

Theorem 7.3 *Let $\mathsf{Adv}_{\Pi_{\mathsf{set}}}(\mathsf{A})$ be the advantage of an adversary A against the soundness of the proof system described above. There exist PPT adversaries $\mathsf{D}_1, \mathsf{D}_2, \mathsf{B}_{\mathsf{bits}}, \mathsf{B}_{\mathsf{com}}, \mathsf{B}_{\mathsf{sum}}, \mathsf{B}_{\mathsf{lin}}$*

such that

$$\begin{aligned}\mathsf{Adv}_{\Pi_{\mathsf{set}}}(\mathsf{A}) \leq n\,(&\mathsf{Adv}_{\mathcal{L}_1,\mathbb{G}_1}(\mathsf{D}_1) + t/2\,(4/q + \mathsf{Adv}_{\Pi_{\mathsf{bits}}}(\mathsf{B}_{\mathsf{bits}}) + \mathsf{Adv}_{\mathcal{L}_1,\mathbb{G}_2}(\mathsf{B}_2)\\ &+\ \mathsf{Adv}_{\Pi_{\mathsf{com}}}(\mathsf{B}_{\mathsf{com}}) + m\mathsf{Adv}_{\Pi_{\mathsf{sum}}}(\mathsf{B}_{\mathsf{sum}}) + m\mathsf{Adv}_{\Pi_{\mathsf{lin}}}(\mathsf{B}_{\mathsf{lin}}))).\end{aligned}$$

Recall that, given $b_1, \ldots, b_m \in \{0,1\}$, we defined $\alpha := \sum_{i=1}^{m} b_i 2^{i-1} + 1$. Recall also that, given a path $(b_m, \ldots, b_\ell)$ in the binary tree whose leaves are labeled from left to right by $s_1, \ldots, s_t$, we defined $\mathsf{left} := \sum_{i=\ell}^{m} b_i 2^{i-1} + 1$, $\mathsf{right} := \mathsf{left} + 2^{\ell-1} - 1$, and we defined $\alpha_\ell := \alpha - \mathsf{left} + 1$ the position of s_α relative to the leaves under $s_{\mathsf{left}}, \ldots, s_{\mathsf{right}}$.

The proof follows from the indistinguishability of the following games:

Real: This is the real soundness game. The output is 1 if the adversary submits some $([\boldsymbol{\zeta}_1]_1, \ldots, [\boldsymbol{\zeta}_n]_1, S) \notin \mathcal{L}^n_{ck_{\mathsf{GS}},\mathsf{set}}$ and the corresponding proof which is accepted by the verifier.

Game_0: This identical to Real, except that K_1 does not receive ck_{GS} as a input but it samples ck_{GS} itself together with its discrete logarithms.

Game_1: This game is identical to Game_0 except that now it chooses random $j^* \in [n]$ and it aborts if $x_{j^*} \notin S$.

Game_2: This game is identical to Game_1 except that now $\mathbf{H} \leftarrow \mathcal{L}_1^{n,j^*}$.

Game_3: This game is identical to Game_2 except that now it defines $b_m := b_{j^*,m}$ and chooses a random (sub-)path $(b_{m-1}, \cdots, b_1) \leftarrow \{0,1\}^{m-1}$ (which ignores the first edge) in the tree whose leaves are $s_1, \ldots, s_t$. This game aborts if $(b_{j^*,1}, \ldots, b_{j^*,m}) \notin \{0,1\}^m$ or $(b_1, \ldots, b_{m-1}) \neq (b_{j^*,1}, \ldots, b_{j^*,m-1})$, where $b_{j^*,1}, \ldots, b_{j^*,m}$ are the openings of $[\mathbf{d}_2]_2, \ldots, [\mathbf{d}_m]_2$ at coordinate j^*, respectively.

Game_4: This game is identical to Game_3 except that now $\mathbf{G}_\ell \leftarrow \mathcal{L}_1^{n2^{\ell-1},\Delta+\alpha_\ell}$, for $\ell \in [m]$ and $\Delta := (j^* - 1)2^{\ell-1}$.

It is obvious that the first two games are indistinguishable. The rest of the argument goes as follows.

Lemma 7.4 $\Pr[\mathsf{Game}_1(\mathsf{A}) = 1] \geq \dfrac{1}{n} \Pr[\mathsf{Game}_0(\mathsf{A}) = 1]$.

Proof The probability that $\mathsf{Game}_1(\mathsf{A}) = 1$ is the probability that a) $\mathsf{Game}_0(\mathsf{A}) = 1$ and b) $x_{j^*} \notin S$. The view of adversary A is independent of j^*, while, if $\mathsf{Game}_0(\mathsf{A}) = 1$, then there is at least one index $j \in [n]$ such that such that $x_j \notin S$. Thus, the probability that the event described in b) occurs conditioned on $\mathsf{Game}_0(\mathsf{A}) = 1$, is greater than or equal to $1/n$ and the lemma follows. □

Lemma 7.5 *There exists a* $\mathcal{L}_1$-$\mathsf{MDDH}_{\mathbb{G}_2}$ *adversary* D_2 *such that* $|\Pr[\mathsf{Game}_1(\mathsf{A}) = 1] - \Pr[\mathsf{Game}_2(\mathsf{A}) = 1]| \leq \mathsf{Adv}_{\mathcal{L}_1,\mathsf{Gen}_a}(\mathsf{D}_2)$.

Proof We construct an adversary D_2 that receives a challenge $([\mathbf{a}]_2, [\mathbf{u}]_2)$ of the $\mathcal{L}_1$-$\mathsf{MDDH}_{\mathbb{G}_2}$ assumption. From this challenge, D_2 just defines the matrix $[\mathbf{H}]_2 \in \mathbb{G}_2^{2\times(n+1)}$ as the matrix whose last column is $[\mathbf{a}]_2$, the ith column is $[\mathbf{u}]_2$, and the rest of the columns are random vectors in the image of $[\mathbf{a}]_2$. Obviously, when $[\mathbf{u}]_2$ is sampled from the image of $[\mathbf{a}]_2$, $\mathbf{H}$ follows the distribution $\mathcal{L}_1^{m,0}$, while if $[\mathbf{u}]_2$ is a uniform element of $\mathbb{G}_2^2$, $\mathbf{H}$ follows the distribution $\mathcal{L}_1^{n,j^*}$.

Adversary D_2 samples $\mathbf{G}^\ell \leftarrow \mathcal{L}_1^{n2^{\ell-1},0}$. Given that D_2 does not know the discrete logarithms of $[\mathbf{H}]_2$, it cannot compute the pairs $(\mathbf{C}^\ell_{i,j}, \mathbf{D}^\ell_{i,j})$ exactly as in Game_0. Nevertheless, for each $\ell \in [m], i \in [n2^{\ell-1}+1], j \in [n+1]$ such that $i \notin [(j-1)2^{\ell-1}+1, j2^{\ell-1}]$, it can compute identically distributed pairs by picking $\mathbf{T} \leftarrow \mathbb{Z}_q^{2\times 2}$ and defining

$$([\mathbf{C}^\ell_{i,j}]_1, [\mathbf{D}^\ell_{i,j}]_2) := ([\mathbf{T}]_1, \mathbf{g}_{\ell,i}[\mathbf{h}_j]_2^\top - [\mathbf{T}]_2).$$

The rest of the elements of the CRS are honestly computed. When $\mathbf{H} \leftarrow \mathcal{L}_1^{n,0}$, D_2 perfectly simulates Game_0, and when $\mathbf{H} \leftarrow \mathcal{L}_1^{n,j^*}$, D_2 perfectly simulates Game_1, which concludes the proof. □

Lemma 7.6 *There exists an adversary* $\mathsf{B}_{\mathsf{bits}}$ *against* Π_{bits} *such that* $\Pr[\mathsf{Game}_2(\mathsf{A})=1] \geq \frac{2}{t}(\Pr[\mathsf{Game}_3(\mathsf{A})=1] + \mathbf{Adv}_{\Pi_{\mathsf{bits}}}(\mathsf{B}_{\mathsf{bits}}))$.

Proof The probability that $\mathsf{Game}_3(\mathsf{A}) = 1$ is the probability that a) $\mathsf{Game}_2(\mathsf{A}) = 1$ and b) $(b_{j^*,1}, \ldots, b_{j^*,m}) \notin \{0,1\}^m$ or $(b_1, \ldots, b_{m-1}) \neq (b_{j^*,1}, \ldots, b_{j^*,m-1})$. If $(b_{j^*,1}, \ldots, b_{j^*,m}) \notin \{0,1\}^m$ we can build an adversary $\mathsf{B}_{\mathsf{bits}}$ against Π_{bits} and thus, the probability that $(b_{j^*,1}, \ldots, b_{j^*,m}) \in \{0,1\}^m$ is less than $\mathbf{Adv}_{\Pi_{\mathsf{bits}}}(\mathsf{B}_1)$. The view of adversary A is independent of $(b_1, \ldots, b_{m-1})$, while, if $\mathsf{Game}_2(\mathsf{A}) = 1$ and $(b_{j^*,1}, \ldots, b_{j^*,m}) \in \{0,1\}^m$, then $(b_{j^*,1} \cdots b_{j^*,m-1}) \in \{0,1\}^{m-1}$. Thus, the probability that the event described in b) occurs conditioned on $\mathsf{Game}_2(\mathsf{A}) = 1$ and $(b_{j^*,1}, \ldots, b_{j^*,m}) \in \{0,1\}^m$, is greater than or equal to $2/t$ and the lemma follows. □

Lemma 7.7 *There exists a* $\mathcal{L}_1$-$\mathsf{MDDH}_{\mathbb{G}_1}$ *adversary* D_1 *such that* $|\Pr[\mathsf{Game}_3(\mathsf{A})=1] - \Pr[\mathsf{Game}_4(\mathsf{A})=1]| \leq \mathsf{Adv}_{\mathcal{L}_1,\mathbb{G}_1}(\mathsf{D}_1)$.

Proof We construct an adversary D_1 that receives a challenge $([\mathbf{a}]_1, [\mathbf{u}]_1)$ of the $\mathcal{L}_1$-$\mathsf{MDDH}_{\mathbb{G}_1}$ assumption. From this challenge, D_1 defines for each $\ell \in [m]$ the matrix $[\mathbf{G}_\ell]_1$ as the matrix whose $\Delta + \alpha_\ell$ th column is $[\mathbf{u}]_1$, and the rest of the columns are random vectors in the image of $[\mathbf{a}]_1$. Obviously, when $[\mathbf{u}]_1$ is sampled from the image of $[\mathbf{a}]_1$, $[\mathbf{G}_\ell]_1$ follows the distribution $\mathcal{L}_1^{n2^{\ell-1},0}$, while if $[\mathbf{u}]_1$ is a uniform element of $\mathbb{G}_1^2$, $[\mathbf{G}_\ell]_1$ follows the distribution $\mathcal{L}_1^{n2^{\ell-1},\Delta+\alpha_\ell}$.

The rest of the elements of the CRS are honestly computed. When $[\mathbf{u}]_1$ is sampled from the image of $[\mathbf{a}]_1$, D_1 perfectly simulates Game_3, and when $[\mathbf{u}]_1$ is uniform, D_1 perfectly simulates Game_4, which concludes the proof. □

Lemma 7.8 *There exist adversaries* $\mathsf{B}_{\mathsf{com}}$*, against the strong soundness of* Π_{com}*,* $\mathsf{B}_{\mathsf{sum}}$*, against the soundness of* Π_{sum}*, and an adversary* $\mathsf{B}_{\mathsf{lin}}$ *against the soundness of* Π_{lin}*, such that* $\Pr[\mathsf{Game}_4(\mathsf{A})=1] \leq 4/q + \mathbf{Adv}_{\Pi_{\mathsf{com}}}(\mathsf{B}_{\mathsf{com}}) + m\mathbf{Adv}_{\Pi_{\mathsf{sum}}}(\mathsf{B}_{\mathsf{sum}}) + m\mathbf{Adv}_{\Pi_{\mathsf{lin}}}(\mathsf{B}_{\mathsf{lin}})$.

Proof With probability $1-4/q$, $\{\mathbf{g}_{\ell,\Delta+\alpha_\ell}, \mathbf{g}_{\ell,n2^{\ell-1}+1}\}$, $\ell \in [m]$, and $\{\mathbf{h}_{j^*}, \mathbf{h}_{m+1}\}$ are bases of $\mathbb{Z}_q^2$, and, for each $\ell \in [m], \mu \in \{1,2\}$, we can define $\tilde{s}_\ell, \tilde{s}_{\ell,\mu}, \tilde{r}_\ell, \tilde{r}_{\ell,\mu}, b_{j^*,\ell}, \tilde{t}_\ell$ as the unique coefficients in $\mathbb{Z}_q$ such that $\mathbf{c}_\ell = \tilde{s}_\ell \mathbf{g}_{\ell,\Delta+\alpha_\ell} + \tilde{r}_\ell \mathbf{g}_{\ell,n2^{\ell-1}+1}, \mathbf{c}_{\ell,\mu} = \tilde{s}_{\ell,\mu}\mathbf{g}_{\ell,\Delta+\alpha_\ell} + \tilde{r}_{\ell,\mu}\mathbf{g}_{\ell,n2^{\ell-1}+1}$, and $\mathbf{d}_\ell = b_{j^*,\ell}\mathbf{h}_{j^*} + \tilde{t}_\ell \mathbf{h}_{n+1}$.

Recall that if $\mathsf{Game}_4(\mathsf{A}) = 1$ then $x_{j^*} \notin S$. The adversary can win in Game_4 if one of the following events happen:

E_1**:** the adversary breaks soundness of Π_{com} and $x_{j^*} \neq \tilde{s}_1$,

E_2**:** the adversary breaks one of the m instances of Π_{sum} and $\boldsymbol{\Theta}_\ell + \boldsymbol{\Pi}_\ell \notin \mathbf{Span}(\mathcal{C}_\ell)$,

E_3**:** the adversary breaks one of the m instances of Π_{lin} and $(\mathbf{c}_{\ell+1}, \mathbf{c}_{\ell,1}, \mathbf{c}_{\ell,2}) \notin \mathbf{Span}(\mathbf{G}_{\ell,\mathsf{split}})$,

E_4**:** neither of E_1,E_2, or E_3 happens, but $x_{j^*} \notin S$ anyway.

By the law of total probabilities, $\Pr[\mathsf{Game}_4(\mathsf{A}) = 1] \leq 4/q + \Pr[E_1] + \Pr[E_2] + \Pr[E_3] + \Pr[E_4]$, and is not hard to see that there exist adversaries $\mathsf{B}_{\mathsf{com}}, \mathsf{B}_{\mathsf{sum}}, \mathsf{B}_{\mathsf{lin}}$ such that $\Pr[E_1] = \mathbf{Adv}_{\Pi_{\mathsf{com}}}(\mathsf{B}_{\mathsf{com}}), \Pr[E_2] = m\mathbf{Adv}_{\Pi_{\mathsf{sum}}}(\mathsf{B}_{\mathsf{sum}})$, and $\Pr[E_3] = m\mathbf{Adv}_{\Pi_{\mathsf{lin}}}(\mathsf{B}_{\mathsf{lin}})$. Below we will show that $\Pr[E_4] = 0$ (using the same argument used in the non-aggregated case).

We prove by induction on ℓ that $\tilde{s}_\ell = s_\alpha$. If this is the case, the fact that $\neg E_1$ implies that $x_{j^*} = \tilde{s}_1 = s_\alpha \in S$, which finish the proof.

But first note that given a vector $\mathbf{k} \in \mathbb{Z}_q^2$, such that $\mathbf{h}_j^\top \mathbf{k} = 1$ if $j = j^*$ and 0 if not (which exists since $\{\mathbf{h}_{j^*}, \mathbf{h}_{n+1}\}$ is a basis of $\mathbb{Z}_q^2$), if we multiply equation (7.10) on the right by $\mathbf{k}$ we get

$$[\mathbf{c}_\ell]_T - (1 - b_{j^*,\ell})[\mathbf{c}_{\ell,1}]_T - b_{j^*,\ell}[\mathbf{c}_{\ell,2}]_T = [(\mathbf{\Theta}_\ell + \mathbf{\Pi}_\ell)\mathbf{k}]_T.$$

The fact that $\mathbf{\Theta}_\ell + \mathbf{\Pi}_\ell \in \mathbf{Span}(\mathcal{C}_\ell)$, $\mathbf{g}_{\ell,i} \in \mathbf{Span}(\mathbf{g}_{\ell,n2^{\ell-1}+1})$ if $i \neq \Delta + \alpha_\ell$, and $\Delta + \alpha_\ell \in [\Delta + 1, \Delta + 2^{\ell-1}]$, implies that

$$(\mathbf{\Theta}_\ell + \mathbf{\Pi}_\ell)\mathbf{k} = \sum_{i \in [n2^{\ell-1}+1] \setminus [\Delta+1, \Delta+2^{\ell-1}]} \beta_i \mathbf{g}_{\ell,i} = \beta \mathbf{g}_{\ell,n2^{\ell-1}+1}$$

for some $\beta_i, \beta \in \mathbb{Z}_q$, $i \in [n2^{\ell-1} + 1] \setminus [\Delta + 1, \Delta + 2^{\ell-1}]$.

Therefore, given that we are in the case $b_\ell = b_{j^*,\ell}$, equation (7.10) implies that

$$[\mathbf{c}_\ell]_T = (1 - b_\ell)[\mathbf{c}_{\ell,1}]_T + b_\ell[\mathbf{c}_{\ell,2}]_T + \beta \mathbf{g}_{\ell,n2^{\ell-1}+1}.$$

In the base case ($\ell = m$), the fact that $\mathbf{g}_{m,i} \in \mathbf{Span}(\mathbf{g}_{m,n2^{m-1}+1})$, if $i \neq \Delta + \alpha_m$, implies that

$$\begin{aligned}
\mathbf{c}_m &= (1 - b_m) \sum_{i=1}^{2^{m-1}} s_i \mathbf{g}_{m,\Delta+i} + b_m \sum_{i=1}^{2^{m-1}} s_{i+2^{m-1}} \mathbf{g}_{m,\Delta+i} \\
&= (1 - b_m) s_{\alpha_m} \mathbf{g}_{m,\Delta+\alpha_m} + b_m s_{\alpha_m+2^{m-1}} \mathbf{g}_{m,\Delta+\alpha_m} + \tilde{r}_1 \mathbf{g}_{m,n2^{m-1}+1} \\
&= (1 - b_m) s_{\alpha-\mathsf{left}+1} \mathbf{g}_{m,\Delta+\alpha_m} + b_m s_{\alpha-\mathsf{left}+1+2^{m-1}} \mathbf{g}_{m,\Delta+\alpha_m} + \tilde{r}_1 \mathbf{g}_{m,n2^{m-1}+1} \\
&= \begin{cases} s_{\alpha-1+1} \mathbf{g}_{m,\Delta+\alpha_m} + \tilde{r}_1 \mathbf{g}_{m,n2^{m-1}+1} & \text{if } b_m = 0 \ (\mathsf{left} = 1) \\ s_{\alpha-(2^{m-1}+1)+1+2^{m-1}} \mathbf{g}_{m,\Delta+\alpha_m} + \tilde{r}_1 \mathbf{g}_{m,n2^{m-1}+1} & \text{if } b_m = 1 \ (\mathsf{left} = 2^{m-1} + 1) \end{cases}
\end{aligned}$$

for some $\tilde{r}_1 \in \mathbb{Z}_q$. In both cases $\mathbf{c}_1 = s_\alpha \mathbf{g}_{m,\Delta+\alpha_m} + \tilde{r}_1 \mathbf{g}_{m,n2^{m-1}}$.

In the inductive case we assume that $\mathbf{c}_{\ell+1} = s_\alpha \mathbf{g}_{\ell+1,2\Delta+\alpha_{\ell+1}} + \tilde{r}_{\ell+1} \mathbf{g}_{\ell+1,n2^\ell+1}$ and we want to show that $\mathbf{c}_\ell = s_\alpha \mathbf{g}_{\ell,\Delta+\alpha_\ell} + \tilde{r}_\ell \mathbf{g}_{\ell,n2^{\ell-1}+1}$.[5] Since $\mathbf{g}_{\ell+1,\alpha_{\ell+1}}$ is linearly independent from the rest of vectors in $ck_{\ell+1}$, any solution to

$$\begin{pmatrix} \mathbf{c}_{\ell+1} \\ \mathbf{c}_{\ell,1} \\ \mathbf{c}_{\ell,2} \end{pmatrix} = \mathbf{G}_{\ell,\mathsf{split}} \mathbf{w} \tag{7.11}$$

is equal to s_α at position $2\Delta + \alpha_{\ell+1} = 2\Delta + \alpha_\ell + b_\ell 2^{\ell-1}$ as depicted below.

$$\begin{pmatrix} \mathbf{c}_{\ell+1} \\ \mathbf{c}_{\ell,1} \\ \mathbf{c}_{\ell,2} \end{pmatrix} = \begin{pmatrix} \cdots & \mathbf{g}_{\ell+1,2\Delta+\alpha_\ell} & \cdots & \mathbf{g}_{\ell+1,2\Delta+\alpha_\ell+2^{\ell-1}} & \cdots \\ \cdots & \mathbf{g}_{\ell,\Delta+\alpha_\ell} & \cdots & \mathbf{0} & \cdots \\ \cdots & \mathbf{0} & \cdots & \mathbf{g}_{\ell,\Delta+\alpha_\ell} & \cdots \end{pmatrix} \begin{pmatrix} \vdots \\ s_\alpha \\ \vdots \end{pmatrix}$$

[5] Note that $\mathbf{G}_{\ell+1} \leftarrow \mathcal{L}_1^{n2^\ell,(j^*-1)2^\ell+\alpha_{\ell+1}}$ and thus, the $(j^* - 1)2^\ell + \alpha_{\ell+1} = 2\Delta + \alpha_{\ell+1}$ th column of $\mathbf{G}_{\ell+1}$ is l.i. from the rest.

If $b_\ell = 0$, by Lemma 7.1, $\alpha_{\ell+1} = \alpha_\ell$. Therefore, any solution to equation (7.11) is equal to s_α at position $2\Delta + \alpha_\ell$ and thus $\mathbf{c}_{\ell,1} = s_\alpha \mathbf{g}_{\ell,\Delta+\alpha_\ell} + \tilde{r}_{\ell,1}\mathbf{g}_{\ell,n2^{\ell-1}+1}$. Equation 7.10 implies that

$$\begin{aligned}\mathbf{c}_\ell =&(1-b_\ell)(s_\alpha \mathbf{g}_{\ell,\Delta+\alpha_\ell} + \tilde{r}_{\ell,1}\mathbf{g}_{\ell,n2^{\ell-1}+1}) + b_\ell \mathbf{c}_{\ell,2} + y_\ell \mathbf{g}_{\ell,n2^{\ell-1}+1}\\ =&s_\alpha \mathbf{g}_{\ell,\Delta+\alpha_\ell} + (\tilde{r}_{\ell,1} + y_\ell)\mathbf{g}_{\ell,n2^{\ell-1}+1}.\end{aligned} \qquad \square$$

If $b_\ell = 1$, then $\alpha_{\ell+1} = \alpha_\ell + 2^{\ell-1}$ and similarly, $\mathbf{c}_\ell = s_\alpha \mathbf{g}_{\ell,\Delta+\alpha_\ell} + (\tilde{r}_{\ell,2} + y_\ell)\mathbf{g}_{\ell,n2^{\ell-1}+1}$.

Perfect Zero-Knowledge

Note that the vectors $[\mathbf{c}_\ell], [\mathbf{c}_{\ell,1}]_1, [\mathbf{c}_{\ell,2}]_1, [\mathbf{d}_\ell]_2$ and matrices $[\mathbf{\Theta}_\ell]_1, [\mathbf{\Pi}_\ell]_2$, $1 \leq \ell \leq m$, output by the prover and the simulator are, respectively, uniform vectors and uniform matrices conditioned on satisfying equation 7.10. This follows from the fact that $ck, ck_1, \ldots, ck_\ell$ are all perfectly hiding commitment keys and that $[\mathbf{\Theta}_\ell]_1, [\mathbf{\Pi}_\ell]_1$ are the unique solutions of equation (7.10) modulo the random choice of $\mathbf{R}_\ell$. Finally, the rest of the proof follows from zero-knowledge of $\Pi_{\mathsf{com}}, \Pi_{\mathsf{bits}}, \Pi_{\mathsf{sum}}$, and Π_{lin}.

7.2.1 The case $S \subset \mathbb{G}_1$

We briefly justify that the case $S \subset \mathbb{G}_1$ follows directly from the case $S \subset \mathbb{Z}_q$ when S is a fixed witness samplable set. That is, there is a fixed set S for each CRS, and there is an efficient algorithm that samples $s_1, \ldots, s_t \in \mathbb{Z}_q$ such that $S = \{[s_1]_1, \ldots, [s_t]_1\}$.

The reason why is not clear how to compute proofs in this setting is that it requires to compute values of the type $[\mathbf{s}_i \gamma]_1$, where $[\gamma]_\mu$, $\mu \in \{1,2\}$, is a group element included in the CRS. The solution is straightforward: use $s_1, \ldots, s_t$ to compute these values and add them to the CRS (with the consequent CRS growth). Therefore, the new CRS contains also, for each $\alpha \in [n], \ell \in [m], i \in [n2^{\ell-1}], j \in [n]$, such that $i \neq (j-1)2^{\ell-1} + \alpha_\ell$:

$$s_\alpha[\mathbf{g}_{\ell,(i-1)2^{\ell-1}+\alpha_\ell}]_1 \text{ and } s_\alpha([\mathbf{C}^\ell_{(i-1)2^{\ell-1}+\alpha_\ell,j}]_1, [\mathbf{D}^\ell_{(j-1)2^{\ell-1},j}]_2).$$

Chapter 8

Conclusions

In this thesis we constructed many new and more efficient non-interactive zero-knowledge proofs. We showed that any set of quadratic equations of the type $b(b-1)=0$ and any set of linear equations with variables in $\mathbb{Z}_q$ have a proof whose size is independent of the number of equations. In the case of equations where variables are group elements, we showed that any set of linear equations has a proof whose size is independent of the number of equations, with the drawback that the CRS must be fixed to the specific set of equations.

Then we moved to the case of set-membership proofs, which can be equivalently seen as higher degree equations – a proof of membership in the set of roots of a polynomial p is a proof that $p(x)=0$ in the case where the variables are $\mathbb{Z}_q$ elements – and has the advantage that can also be applied to the case where the variables are group elements (since it is not clear how to define higher degree equations where variables are group elements). First, we showed that for any fixed set S, the statement $x_1, \ldots, x_n \in S$ can be proven with a proof whose size is linear in the size of the set and but independent of the number of proofs. Finally, we considered the cases of non-fixed subsets of $\mathbb{Z}_q$ and (again) the case of fixed subset of $\mathbb{G}_s$. For both cases we obtained even more efficient proofs. Specifically, we constructed proofs of size logarithmic in the size of the set and independent of the number of proofs.

With these results we constructed more efficient proofs of equal commitment opening, threshold Groth-Sahai proofs, ring signatures, proofs of correctness of a shuffle, and range proofs.

At the heart of most of our results was a new variant of Pedersen commitments and Groth-Sahai commitments, which we call extended multi-Pedersen commitments (MP commitments). MP commitments are length-reducing –they require less than n group elements to commit to a vector in $\mathbb{Z}_q^n$– which imply that they can not be perfectly binding. However, they can be perfectly binding at one coordinate (encoded in the commitment key) and behave as Groth-Sahai commitments at that coordinate (in fact, when $n=1$ MP commitments become Groth-Sahai commitments).

The major drawback of our results is its limited generality: (essentially) they only allow more efficient proofs for integer equations modulo q. When variables and constants are group elements, the results are much more limited. Indeed, they only work in the case of “fixed equations” or “fixed sets”, and they do not apply at all for quadratic pairing product equations. The reason for this limitation is our dependency on MP commitments. Our extensions to group equations (or set-membership in $S \subset \mathbb{G}_s$) essentially precomputes MP commitments for a fixed set of witness samplable group elements, that is, it is possible to sample the discrete logarithms and thus to compute MP commitments when setting up the CRS. This is of course not enough for general equations where group elements may be adversarially chosen and thus, there is no hope to compute its discrete logarithms. In fact, it can be shown that there does not exist an analogous of MP commitments for group elements. Indeed, Abe et al. showed that is impossible to construct length-reducing group to group commitments [AHO12] – i.e. commitment schemes that take n group elements as arguments and return a commitment whose size is $o(n)$ group elements.[1]

This is in fact a practical limitation. Consider the case of ring signatures, where the central problem is to show that some secret verification key $vk \in R$, and R is the set of all verification keys in the ring. This is just a (non-aggregated) set-membership proof, for which we constructed logarithmic proofs whenever the set is fixed. However, using our set-membership proofs the result is unsatisfactory: there is a single ring R (or a constant number of rings) for which one can construct a logarithmic size ring signatures. This is not a ring signature.

On the other hand, (quadratic) integer equations are general enough to encode any NP problem (quadratic integer equations can be shown NP-complete). In fact, any circuit $C : \{0,1\}^m \to \{0,1\}$ can be encoded into a set of quadratic equations which is satisfiable iff C is satisfiable. One may thus hope that our techniques could help on improving NIZK proofs for Circuit-Sat under falsifiable assumptions. The shortest proofs remains those of Groth et al. [GOS06b].[2] Essentially, Groth et al.'s proof computes a perfectly binding commitment to a satisfying assignment, requiring $\Theta(m)$ group elements, and computes perfectly binding commitments to the outputs of each gate and NIZK proofs that the output of each gate is correctly computed. The correctness of the output of each gate is expressed as the satisfiability of an integer equation, so essentially Groth et al.'s proof is $\Theta(m) + \Theta(\#\text{equations})$, where $\Theta(\#\text{equations}) = \Theta(\#\text{gates}) = \Theta(|C|)$. With our techniques we get a proof of size $\Theta(m) + \Theta(|\pi|)$, where the $\Theta(m)$ term comes from commitments to variables and the $\Theta(|\pi|)$ term comes from the proof that those variables satisfy the equations. In this thesis we basically show that for many equations $|\pi| \in o(\#\text{equations})$, so this could be a good indication that we can beat Groth at al's proof.

We discuss a little more about the generality/non-generality of integer equations. Indeed, we have said that our techniques are limited because they only work for integer equations, but then we pointed out that integer equations are general enough (in fact NP-complete). Can we encode general pairing product equations as integer equations? The answer is affirmative: group operations, pairings, exponentiations, etc. can be written in terms of quadratic integer equations and thus, any pairing product equation can be written as a polynomial number of quadratic integer equations. Thus we may hope to encode pairing product equations into integer equations and use our results to improve proofs for pairing product equations. We can even use constant-size NIZK proofs for NP from Gennaro et al. [GGPR13] to construct constant-size proofs of the satisfiability of any set of pairing-product equation.

However, we think that in this way the question is not properly answered. In fact, pairing product equations and Groth-Sahai proofs are usually used in the context of *structure*

[1] Abe et al. constructed group to group length-reducing structure preserving commitments relaxing the binding property [AKOT15]. However, since their commitment scheme is not homomorphic, it is far from clear how to use them to construct NIZK proofs.

[2] In another work, Groth et al. showed how to use *fully homomorphic encryption* to obtain a more efficient proof [GGI$^+$15]. However, fully homomorphic encryption is still a developing primitive and finding alternative solutions is an interesting open problem.

preserving cryptography, which essentially means that everything is done through the operations provided by the bilinear groups (essentially in the generic group model). If we reduce pairing product equations from an NP-complete problem, we are transforming group operations and all the group structure to operations over $\mathbb{Z}_q$. Furthermore, even from a practical point of view, the reduction from an NP-complete problem involves an overhead (at least in the prover's complexity) of reducing the instance to the satisfiability of a circuit which may be prohibitive. Therefore, we believe that it is worth to search more efficient proofs for pairing product equations (or impossibility results) in the generic group model.

Finally we comment that there is also much room for optimization in our results. Maybe the worst part of our NIZK proofs that $b_1, \ldots b_n \in \{0,1\}$ and set-membership proofs is the quadratic sizes of the CRS. This usually implies that the prover's time complexity is also quadratic, since the CRS defines the set of generators of a vector space and the proof is a linear combination of of the generators. This in general requires to compute a quadratic number of exponentiations ($x[g]$) and additions ($[g]+[h]$).[3] We showed that for weight 1 this problem can be avoided, but in general it is an open question if one can do better than this.

Proof sizes are also a good candidate for optimization. Starting from our proofs for linear subspaces of $\mathbb{G}_1 \times \mathbb{G}_2$, it is interesting to know if there is, even in the generic group model, a shorter proof or a lower bound on the proof size. The same applies for quadratic equations and set-membership proofs.

[3] Except when the coefficients that define the witness are in $\{0,1\}$ (as in the proof that $b_1 \ldots b_n \in \{0,1\}$), where it only requires a linear number of exponentiations and a quadratic number of additions.

Bibliography

[AFG$^+$10] Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo. Structure-preserving signatures and commitments to group elements. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 209–236. Springer, Heidelberg, August 2010.

[AGOT14] Masayuki Abe, Jens Groth, Miyako Ohkubo, and Takeya Tango. Converting cryptographic schemes from symmetric to asymmetric bilinear groups. In Juan A. Garay and Rosario Gennaro, editors, *CRYPTO 2014, Part I*, volume 8616 of *LNCS*, pages 241–260. Springer, Heidelberg, August 2014.

[AHO12] Masayuki Abe, Kristiyan Haralambiev, and Miyako Ohkubo. Group to group commitments do not shrink. In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 301–317. Springer, Heidelberg, April 2012.

[AKOT15] Masayuki Abe, Markulf Kohlweiss, Miyako Ohkubo, and Mehdi Tibouchi. Fully structure-preserving signatures and shrinking commitments. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 35–65. Springer, Heidelberg, April 2015.

[BB04] Dan Boneh and Xavier Boyen. Short signatures without random oracles. In Christian Cachin and Jan Camenisch, editors, *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 56–73. Springer, Heidelberg, May 2004.

[BBG05] Dan Boneh, Xavier Boyen, and Eu-Jin Goh. Hierarchical identity based encryption with constant size ciphertext. In Ronald Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 440–456. Springer, Heidelberg, May 2005.

[BBS04] Dan Boneh, Xavier Boyen, and Hovav Shacham. Short group signatures. In Matthew Franklin, editor, *CRYPTO 2004*, volume 3152 of *LNCS*, pages 41–55. Springer, Heidelberg, August 2004.

[BDR15] Priyanka Bose, Dipanjan Das, and Chandrasekaran Pandu Rangan. Constant size ring signature without random oracle. In Ernest Foo and Douglas Stebila, editors, *ACISP 15*, volume 9144 of *LNCS*, pages 230–247. Springer, Heidelberg, June / July 2015.

[BF01] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the Weil pairing. In Joe Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 213–229. Springer, Heidelberg, August 2001.

[BFKW09] Dan Boneh, David Freeman, Jonathan Katz, and Brent Waters. Signing a linear subspace: Signature schemes for network coding. In Stanislaw Jarecki and Gene Tsudik, editors, *PKC 2009*, volume 5443 of *LNCS*, pages 68–87. Springer, Heidelberg, March 2009.

[BFM88] Manuel Blum, Paul Feldman, and Silvio Micali. Non-interactive zero-knowledge and its applications (extended abstract). In *20th ACM STOC*, pages 103–112. ACM Press, May 1988.

[BFPV11] Olivier Blazy, Georg Fuchsbauer, David Pointcheval, and Damien Vergnaud. Signatures on randomizable ciphertexts. In Dario Catalano, Nelly Fazio, Rosario Gennaro, and Antonio Nicolosi, editors, *PKC 2011*, volume 6571 of *LNCS*, pages 403–422. Springer, Heidelberg, March 2011.

[BG13] Stephanie Bayer and Jens Groth. Zero-knowledge argument for polynomial evaluation with application to blacklists. In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 646–663. Springer, Heidelberg, May 2013.

[BKM06] Adam Bender, Jonathan Katz, and Ruggero Morselli. Ring signatures: Stronger definitions, and constructions without random oracles. In Shai Halevi and Tal Rabin, editors, *TCC 2006*, volume 3876 of *LNCS*, pages 60–79. Springer, Heidelberg, March 2006.

[BPV12] Olivier Blazy, David Pointcheval, and Damien Vergnaud. Compact round-optimal partially-blind signatures. In Ivan Visconti and Roberto De Prisco, editors, *SCN 12*, volume 7485 of *LNCS*, pages 95–112. Springer, Heidelberg, September 2012.

[BR93] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In V. Ashby, editor, *ACM CCS 93*, pages 62–73. ACM Press, November 1993.

[Cam13] Philippe Camacho. Fair exchange of short signatures without trusted third party. In Ed Dawson, editor, *CT-RSA 2013*, volume 7779 of *LNCS*, pages 34–49. Springer, Heidelberg, February / March 2013.

[CCs08] Jan Camenisch, Rafik Chaabouni, and abhi shelat. Efficient protocols for set membership and range proofs. In Josef Pieprzyk, editor, *ASIACRYPT 2008*, volume 5350 of *LNCS*, pages 234–252. Springer, Heidelberg, December 2008.

[CF13] Dario Catalano and Dario Fiore. Vector commitments and their applications. In Kaoru Kurosawa and Goichiro Hanaoka, editors, *PKC 2013*, volume 7778 of *LNCS*, pages 55–72. Springer, Heidelberg, February / March 2013.

[CGH98] Ran Canetti, Oded Goldreich, and Shai Halevi. The random oracle methodology, revisited (preliminary version). In *30th ACM STOC*, pages 209–218. ACM Press, May 1998.

[CGS07] Nishanth Chandran, Jens Groth, and Amit Sahai. Ring signatures of sublinear size without random oracles. In Lars Arge, Christian Cachin, Tomasz Jurdzinski, and Andrzej Tarlecki, editors, *ICALP 2007*, volume 4596 of *LNCS*, pages 423–434. Springer, Heidelberg, July 2007.

[Cha81] David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM*, 24(2):84–88, 1981.

[CHL05] Jan Camenisch, Susan Hohenberger, and Anna Lysyanskaya. Compact e-cash. In Ronald Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 302–321. Springer, Heidelberg, May 2005.

[CLZ12] Rafik Chaabouni, Helger Lipmaa, and Bingsheng Zhang. A non-interactive range proof with constant communication. In Angelos D. Keromytis, editor, *FC 2012*, volume 7397 of *LNCS*, pages 179–199. Springer, Heidelberg, February / March 2012.

[Cv91] David Chaum and Eugène van Heyst. Group signatures. In Donald W. Davies, editor, *EUROCRYPT'91*, volume 547 of *LNCS*, pages 257–265. Springer, Heidelberg, April 1991.

[DBS04] Ratna Dutta, Rana Barua, and Palash Sarkar. Pairing-based cryptographic protocols : A survey. Cryptology ePrint Archive, Report 2004/064, 2004. http://eprint.iacr.org/2004/064.

[DDN91] Danny Dolev, Cynthia Dwork, and Moni Naor. Non-malleable cryptography (extended abstract). In *23rd ACM STOC*, pages 542–552. ACM Press, May 1991.

[DFGK14] George Danezis, Cédric Fournet, Jens Groth, and Markulf Kohlweiss. Square span programs with applications to succinct NIZK arguments. In Palash Sarkar and Tetsu Iwata, editors, *ASIACRYPT 2014, Part I*, volume 8873 of *LNCS*, pages 532–550. Springer, Heidelberg, December 2014.

[DH76] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[EG14] Alex Escala and Jens Groth. Fine-tuning Groth-Sahai proofs. In Hugo Krawczyk, editor, *PKC 2014*, volume 8383 of *LNCS*, pages 630–649. Springer, Heidelberg, March 2014.

[EHK$^+$13] Alex Escala, Gottfried Herold, Eike Kiltz, Carla Ràfols, and Jorge Villar. An algebraic framework for Diffie-Hellman assumptions. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 129–147. Springer, Heidelberg, August 2013.

[EHM11] Alex Escala, Javier Herranz, and Paz Morillo. Revocable attribute-based signatures with adaptive security in the standard model. In Abderrahmane Nitaj and David Pointcheval, editors, *AFRICACRYPT 11*, volume 6737 of *LNCS*, pages 224–241. Springer, Heidelberg, July 2011.

[ElG85] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31:469–472, 1985.

[FL15] Prastudy Fauzi and Helger Lipmaa. Efficient culpably sound NIZK shuffle argument without random oracles. *IACR Cryptology ePrint Archive*, 2015:1112, 2015.

[FR94] Gerhard Frey and Hans-Georg Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Mathematics of computation*, 62(206):865–874, 1994.

[Fre10] David Mandell Freeman. Converting pairing-based cryptosystems from composite-order groups to prime-order groups. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 44–61. Springer, Heidelberg, May 2010.

[FS87] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In Andrew M. Odlyzko, editor, *CRYPTO'86*, volume 263 of *LNCS*, pages 186–194. Springer, Heidelberg, August 1987.

[GGI$^+$15] Craig Gentry, Jens Groth, Yuval Ishai, Chris Peikert, Amit Sahai, and Adam D. Smith. Using fully homomorphic hybrid encryption to minimize non-interative zero-knowledge proofs. *Journal of Cryptology*, 28(4):820–843, October 2015.

[GGPR13] Rosario Gennaro, Craig Gentry, Bryan Parno, and Mariana Raykova. Quadratic span programs and succinct NIZKs without PCPs. In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 626–645. Springer, Heidelberg, May 2013.

[GHR15a] Alonso González, Alejandro Hevia, and Carla Ràfols. QA-NIZK arguments in asymmetric groups: New tools and new constructions. In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Part I*, volume 9452 of *LNCS*, pages 605–629. Springer, Heidelberg, November / December 2015.

[GHR15b] Alonso González, Alejandro Hevia, and Carla Ràfols. QA-NIZK arguments in asymmetric groups: New tools and new constructions. Cryptology ePrint Archive, Report 2015/910, 2015. http://eprint.iacr.org/2015/910.

[GK15] Jens Groth and Markulf Kohlweiss. One-out-of-many proofs: Or how to leak a secret and spend a coin. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 253–280. Springer, Heidelberg, April 2015.

[GL07] Jens Groth and Steve Lu. A non-interactive shuffle with pairing based verifiability. In Kaoru Kurosawa, editor, *ASIACRYPT 2007*, volume 4833 of *LNCS*, pages 51–67. Springer, Heidelberg, December 2007.

[GM84] Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2):270–299, 1984.

[GMR89] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(1):186–208, 1989.

[GMW87] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or A completeness theorem for protocols with honest majority. In Alfred Aho, editor, *19th ACM STOC*, pages 218–229. ACM Press, May 1987.

[GO94] Oded Goldreich and Yair Oren. Definitions and properties of zero-knowledge proof systems. *Journal of Cryptology*, 7(1):1–32, 1994.

[GO05] Venkatesan Guruswami and Ryan O'Donnell. A history of the pcp theorem. http://courses.cs.washington.edu/courses/cse533/05au/pcp-history.pdf, 2005. Accessed: 2017-02-27.

[GOS06a] Jens Groth, Rafail Ostrovsky, and Amit Sahai. Non-interactive zaps and new techniques for NIZK. In Cynthia Dwork, editor, *CRYPTO 2006*, volume 4117 of *LNCS*, pages 97–111. Springer, Heidelberg, August 2006.

[GOS06b] Jens Groth, Rafail Ostrovsky, and Amit Sahai. Perfect non-interactive zero knowledge for NP. In Serge Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 339–358. Springer, Heidelberg, May / June 2006.

[GPS08] S. D. Galbraith, K. G. Paterson, and N. P. Smart. Pairings for cryptographers. *Discrete Applied Mathematics*, 156(16):3113–3121, 2008.

[GR16] Alonso González and Carla Ràfols. New techniques for non-interactive shuffle and range arguments. In Mark Manulis, Ahmad-Reza Sadeghi, and Steve Schneider, editors, *ACNS 16*, volume 9696 of *LNCS*, pages 427–444. Springer, Heidelberg, June 2016.

[Gro06] Jens Groth. Simulation-sound NIZK proofs for a practical language and constant size group signatures. In Xuejia Lai and Kefei Chen, editors, *ASIACRYPT 2006*, volume 4284 of *LNCS*, pages 444–459. Springer, Heidelberg, December 2006.

[Gro16] Jens Groth. On the size of pairing-based non-interactive arguments. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part II*, volume 9666 of *LNCS*, pages 305–326. Springer, Heidelberg, May 2016.

[GS08] Jens Groth and Amit Sahai. Efficient non-interactive proof systems for bilinear groups. In Nigel P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 415–432. Springer, Heidelberg, April 2008.

[GS12] Jens Groth and Amit Sahai. Efficient noninteractive proof systems for bilinear groups. *SIAM J. Comput*, 41(5):1193–1232, 2012.

[GSP16] Clémentine Gritti, Willy Susilo, and Thomas Plantard. Logarithmic size ring signatures without random oracles. *IET Information Security*, 10(1):1–7, 2016.

[GW11] Craig Gentry and Daniel Wichs. Separating succinct non-interactive arguments from all falsifiable assumptions. In Lance Fortnow and Salil P. Vadhan, editors, *43rd ACM STOC*, pages 99–108. ACM Press, June 2011.

[HW15] Pavel Hubacek and Daniel Wichs. On the communication complexity of secure function evaluation with long output. In Tim Roughgarden, editor, *ITCS 2015*, pages 163–172. ACM, January 2015.

[JCJ10] Ari Juels, Dario Catalano, and Markus Jakobsson. Coercion-resistant electronic elections. In David Chaum, Markus Jakobsson, Ronald L. Rivest, Peter Y. A. Ryan, Josh Benaloh, Miroslaw Kutylowski, and Ben Adida, editors, *Towards Trustworthy Elections, New Directions in Electronic Voting*, volume 6000 of *Lecture Notes in Computer Science*, pages 37–63. Springer, 2010.

[Jou00] Antoine Joux. A one round protocol for tripartite diffie-hellman. In *Algorithmic Number Theory, 4th International Symposium, ANTS-IV, Leiden, The Netherlands, July 2-7, 2000, Proceedings*, pages 385–394, 2000.

[Jou14] Antoine Joux. A new index calculus algorithm with complexity $L(1/4+o(1))$ in small characteristic. In Tanja Lange, Kristin Lauter, and Petr Lisonek, editors, *SAC 2013*, volume 8282 of *LNCS*, pages 355–379. Springer, Heidelberg, August 2014.

[JR13] Charanjit S. Jutla and Arnab Roy. Shorter quasi-adaptive NIZK proofs for linear subspaces. In Kazue Sako and Palash Sarkar, editors, *ASIACRYPT 2013, Part I*, volume 8269 of *LNCS*, pages 1–20. Springer, Heidelberg, December 2013.

[JR14] Charanjit S. Jutla and Arnab Roy. Switching lemma for bilinear tests and constant-size NIZK proofs for linear subspaces. In Juan A. Garay and Rosario Gennaro, editors, *CRYPTO 2014, Part II*, volume 8617 of *LNCS*, pages 295–312. Springer, Heidelberg, August 2014.

[JR17] Charanjit S. Jutla and Arnab Roy. Improved structure preserving signatures under standard bilinear assumptions. Cryptology ePrint Archive, Report 2017/025, 2017. http://eprint.iacr.org/2017/025.

[Kob87] Neal Koblitz. Elliptic curve cryptosystems, 1987.

[KPW15] Eike Kiltz, Jiaxin Pan, and Hoeteck Wee. Structure-preserving signatures from standard assumptions, revisited. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 275–295. Springer, Heidelberg, August 2015.

[KW15] Eike Kiltz and Hoeteck Wee. Quasi-adaptive NIZK for linear subspaces revisited. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 101–128. Springer, Heidelberg, April 2015.

[LLNW16] Benoît Libert, San Ling, Khoa Nguyen, and Huaxiong Wang. Zero-knowledge arguments for lattice-based accumulators: Logarithmic-size ring signatures and group signatures without trapdoors. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part II*, volume 9666 of *LNCS*, pages 1–31. Springer, Heidelberg, May 2016.

[LPJY13] Benoît Libert, Thomas Peters, Marc Joye, and Moti Yung. Linearly homomorphic structure-preserving signatures and their applications. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 289–307. Springer, Heidelberg, August 2013.

[LPJY14] Benoît Libert, Thomas Peters, Marc Joye, and Moti Yung. Non-malleability from malleability: Simulation-sound quasi-adaptive NIZK proofs and CCA2-secure encryption from homomorphic signatures. In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 514–532. Springer, Heidelberg, May 2014.

[LPJY15a] Benoît Libert, Thomas Peters, Marc Joye, and Moti Yung. Compactly hiding linear spans - tightly secure constant-size simulation-sound QA-NIZK proofs and applications. In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Part I*, volume 9452 of *LNCS*, pages 681–707. Springer, Heidelberg, November / December 2015.

[LPJY15b] Benoît Libert, Thomas Peters, Marc Joye, and Moti Yung. Compactly hiding linear spans: Tightly secure constant-size simulation-sound QA-NIZK proofs and applications. Cryptology ePrint Archive, Report 2015/242, 2015. http://eprint.iacr.org/2015/242.

[LZ12] Helger Lipmaa and Bingsheng Zhang. A more efficient computationally sound non-interactive zero-knowledge shuffle argument. In Ivan Visconti and Roberto De Prisco, editors, *SCN 12*, volume 7485 of *LNCS*, pages 477–502. Springer, Heidelberg, September 2012.

[Mil86] Victor S. Miller. Use of elliptic curves in cryptography. In Hugh C. Williams, editor, *CRYPTO'85*, volume 218 of *LNCS*, pages 417–426. Springer, Heidelberg, August 1986.

[MRV15] Paz Morillo, Carla Ràfols, and Jorge L. Villar. Matrix computational assumptions in multilinear groups. Cryptology ePrint Archive, Report 2015/353, 2015. http://eprint.iacr.org/2015/353.

[MVO91] Alfred Menezes, Scott A. Vanstone, and Tatsuaki Okamoto. Reducing elliptic curve logarithms to logarithms in a finite field. In *23rd ACM STOC*, pages 80–89. ACM Press, May 1991.

[Nao03] Moni Naor. On cryptographic assumptions and challenges (invited talk). In Dan Boneh, editor, *CRYPTO 2003*, volume 2729 of *LNCS*, pages 96–109. Springer, Heidelberg, August 2003.

[NY90] Moni Naor and Moti Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. In *22nd ACM STOC*, pages 427–437. ACM Press, May 1990.

[OPWW15] Tatsuaki Okamoto, Krzysztof Pietrzak, Brent Waters, and Daniel Wichs. New realizations of somewhere statistically binding hashing and positional accumulators. In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Part I*, volume 9452 of *LNCS*, pages 121–145. Springer, Heidelberg, November / December 2015.

[Ràf15] Carla Ràfols. Stretching groth-sahai: NIZK proofs of partial satisfiability. In Yevgeniy Dodis and Jesper Buus Nielsen, editors, *TCC 2015, Part II*, volume 9015 of *LNCS*, pages 247–276. Springer, Heidelberg, March 2015.

[RKP09] Alfredo Rial, Markulf Kohlweiss, and Bart Preneel. Universally composable adaptive priced oblivious transfer. In Hovav Shacham and Brent Waters, editors, *PAIRING 2009*, volume 5671 of *LNCS*, pages 231–247. Springer, Heidelberg, August 2009.

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signature and public-key cryptosystems. *Communications of the Association for Computing Machinery*, 21(2):120–126, 1978.

[RST01] Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to leak a secret. In Colin Boyd, editor, *ASIACRYPT 2001*, volume 2248 of *LNCS*, pages 552–565. Springer, Heidelberg, December 2001.

[Sha07] Hovav Shacham. A cramer-shoup encryption scheme from the linear assumption and from progressively weaker linear variants. Cryptology ePrint Archive, Report 2007/074, 2007. http://eprint.iacr.org/2007/074.

[Sho97] Victor Shoup. Lower bounds for discrete logarithms and related problems. In Walter Fumy, editor, *EUROCRYPT'97*, volume 1233 of *LNCS*, pages 256–266. Springer, Heidelberg, May 1997.

[Ver13] F Vercauteren. Final report on main computational assumptions in cryptography. *European Network of Excellence in Cryptography II*, 11, 2013.