Contents

Contents **ix**

1 Introduction **1**

1.1 Our Results 3

2 Preliminaries **5**

2.1 Notation 5

2.2 Public-Key Cryptography 6

2.2.1 The Discrete Logarithm and the Diffie-Hellman Assumptions 6

2.2.2 Public-Key Encryption 7

2.2.3 Commitment Schemes 7

2.2.4 Digital Signatures 8

2.3 Bilinear Groups 8

2.3.1 Definition 10

2.3.2 The Decisional k-Linear Diffie-Hellman Family of Assumptions . . . 10

2.4 Matrix Diffie-Hellman Assumptions 11

2.4.1 decisional Matrix Diffie-Hellman Assumptions 11

2.4.2 Computational Matrix Diffie-Hellman Assumptions 12

2.4.3 A new Computational Matrix Diffie-Hellman Assumption in Type III Groups 12

2.5 Non-Interactive Zero-Knowledge Proofs 14

2.5.1 Composable Non-Interactive Zero-Knowledge Proofs 15

2.5.2 Quasi-Adaptive Non-Interactive Zero-Knowledge Proofs 16

2.6 Groth-Sahai Proofs 17

2.6.1 Commit-and-Prove Schemes 18

2.6.2 Groth-Sahai Commitments 18

2.6.3 The Scheme 19

2.7 QA-NIZK Arguments of Membership in Subspaces of $\mathbb{G}_1$ or $\mathbb{G}_2$ 20

3 QA-NIZK Arguments of Membership in Subspaces of $\mathbb{G}_1 \times \mathbb{G}_2$ **21**

3.1 Introduction 21

3.2 Argument of Membership in Subspace Concatenation 22

3.3 Argument of Sum in Subspace 25

3.4 Argument of Equal Opening in Different Groups 26

3.5 Aggregation of Groth-Sahai Proofs 26

3.5.1 Aggregating Two-Sided Linear Equations in $\mathbb{Z}_q$ 27

3.5.2 QA Aggregation of Other Equation Types 27

3.6 Structure Preserving Linearly Homomorphic Signatures 29

3.6.1 One-Time LHSPS Signatures in Different Groups 31

4 QA-NIZK Arguments for Bit-Strings 34

4.1 The Perfectly Binding case 35

4.1.1 Intuition 36

4.1.2 Instantiations 38

4.1.3 The Scheme 39

4.1.4 Proof of Security 40

4.1.5 Extensions 43

4.1.6 Applications 44

4.2 The Computationally Binding Case 49

4.2.1 Extended Multi-Pedersen Commitments 49

4.2.2 The Scheme 51

4.2.3 Constant-Size Argument for $\mathcal{L}^n_{ck,\mathsf{bits}}$ 55

5 New Techniques for Non-Interactive Shuffle and Range Arguments 58

5.1 Related Work 58

5.2 Overview 59

5.2.1 Range Argument 60

5.2.2 Shuffle Argument 60

5.3 Aggregated NIZK Set Membership Arguments 61

5.3.1 Set Membership Proofs 61

5.3.2 Aggregated set membership proofs 63

5.3.3 QA-NIZK Argument of Membership in $\mathcal{L}^n_{[\mathbf{M}]_1,[\mathbf{N}]_1,\mathbf{\Lambda},\boldsymbol{\alpha}}$ 64

5.4 Proof of Correctness of a Shuffle 67

5.4.1 Our construction 67

5.5 Range Argument 70

5.5.1 Our Construction 70

6 Ring Signature of Size $\Theta(\sqrt[3]{n})$ without Random Oracles 72

6.1 High Level Description 72

6.2 Preliminaries 75

6.2.1 Groth-Sahai Proofs in the 2-Lin Instantiation 75

6.2.2 Flawed or Weaker Ring Signatures 75

6.2.3 Definition 75

6.2.4 Boneh-Boyen Signatures 77

6.3 Our Construction 77

7 Improved Aggregated Zero-Knowledge Set-Membership Proofs 82

7.1 Intuition 83

7.2 The Aggregated Case 87

7.2.1 The case $S \subset \mathbb{G}_1$ 96

8 Conclusions 97

Bibliography 100