Tabla de Contenido

1. Introducción **1**

1.1. Tipos de votación 1

1.2. Votación con ranking preferencial 2

1.3. Participa UChile 3

1.4. Objetivos 3

2. Herramientas criptográficas y protocolos **4**

2.1. Esquemas de encriptación 4

2.2. Mix Networks 5

2.3. Zero knowledge proof 6

3. Votación con ranking preferencial **7**

3.1. Single Transferable Vote 8

3.2. Implementaciones Single Transferable Vote 9

3.3. Shuffle-Sum 10

3.3.1. Explicación del algoritmo 10

3.3.2. Posible optimización 12

3.3.3. Ajustes de implementación 14

4. Contexto del desarrollo **15**

4.1. Herramientas previas 15

4.1.1. Psifos y Participa UChile 15

4.1.2. Trabajos relacionados 17
4.2. Análisis de costos 18

5. Implementación módulo de votación con ranking **22**
5.1. Implementación esquema con tabla de comparaciones 22
5.2. Subdivisión del módulo 22
5.2.1. Procedimiento seccionado 23
5.2.2. Estructura seccionada 25
5.3. Generalización esquema de encriptación 26
5.4. Simulación criptografía umbral 26
5.5. Simulación shuffle 27
5.6. Simulación Zero Knowledge Proof 28

6. Manejo de pesos **29**
6.1. Problema 29
6.2. Opciones 30
6.2.1. Precómputo 30
6.2.2. Representar los pesos como decimales de punto flotante 31
6.3. Solución final 34

7. Validación **35**
7.1. Caso base 35
7.2. Muchos votantes, muchos candidatos y con permutaciones variadas 35
7.3. Muchos candidatos para pocos votantes 36
7.4. Máxima cantidad de candidatos en competencia 36
7.5. Máxima cantidad de votantes 36

8. Conclusión **37**

Bibliografía **39**

Anexo A. **40**

Anexo B. **41**

Anexo C. **45**

Anexo D. **49**

Anexo E. **54**

Anexo F. **56**