



Universiteit
Leiden
The Netherlands

Compressed Σ -protocol theory

Attema, T.

Citation

Attema, T. (2023, June 1). *Compressed Σ -protocol theory*. Retrieved from <https://hdl.handle.net/1887/3619596>

Version: Publisher's Version

License: [Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden](#)

Downloaded from: <https://hdl.handle.net/1887/3619596>

Note: To cite this publication please use the final published version (if applicable).

Compressed Σ -Protocol Theory

Thomas Attema

This research has been supported by the Netherlands Organisation for Applied Scientific Research (TNO) and carried out at the Cryptology Group of Centrum Wiskunde & Informatica (CWI).



ISBN: 978-94-6469-236-5
Printed by: ProefschriftMaken || www.proefschriftmaken.nl
Cover design by: Univorm

Compressed Σ -Protocol Theory

Proefschrift

ter verkrijging van
de graad van doctor aan de Universiteit Leiden,
op gezag van rector magnificus prof.dr.ir. H. Bijl,
volgens besluit van het college voor promoties
te verdedigen op donderdag 1 juni 2023
klokke 13:45 uur

door

Thomas Attema
geboren te Amersfoort, Nederland
in 1990

Promotores:

Prof.dr. R. Cramer	(CWI Amsterdam & Leiden University)
Prof.dr. S.O. Fehr	(CWI Amsterdam & Leiden University)

Promotiecommissie:

Prof.dr. H.J. Hupkes	
Prof.dr. F.M. Spijksma	
Prof.dr. J. Groth	(DFINITY, Switzerland)
Prof.dr. A. Lysyanskaya	(Brown University, United States)
Prof.dr. J.B. Nielsen	(Aarhus University, Denmark)

Contents

1	Introduction	1
1.1	Background	3
1.1.1	Mathematical Proofs	3
1.1.2	Cryptography	4
1.1.3	Multilateral Cryptography	7
1.1.4	Probabilistic Proof Systems	8
1.1.5	Proofs and Arguments of Knowledge	9
1.1.6	Σ -Protocol Theory	10
1.1.7	Recent Efficiency Improvements in Proof Systems	11
1.2	Contributions	12
1.2.1	Compressed Σ -Protocols	13
1.2.2	Knowledge Extractor Analysis	16
1.2.3	Applications	20
1.3	Publications	21
2	Preliminaries	25
2.1	Basic Notation	27
2.2	Algorithms	28
2.3	Arithmetic Circuits	29
2.4	Probability Distributions	29
2.4.1	Geometric Distribution	31
2.4.2	Negative Hypergeometric Distribution	32
2.5	Commitment Schemes	33
2.6	Group-Based Cryptographic Assumptions	35
2.7	Lattices and Lattice Problems	36
2.8	Interactive (Zero-Knowledge) Proofs	39
2.8.1	Knowledge Soundness	40
2.8.2	Special-Soundness	43
2.8.3	Zero-Knowledge	44
2.9	Non-Interactive Proofs in the Random Oracle Model	46
2.9.1	Adaptive Knowledge Soundness	49
2.9.2	Fiat-Shamir Transformation	50
2.10	Secret-Sharing Schemes	51
2.10.1	Shamir Secret-Sharing	53
3	Compressible Σ-Protocols	57
3.1	Introduction	59
3.2	Proving Knowledge of Homomorphism Preimages	60
3.2.1	Basic Σ -Protocol	61

3.2.2	A Compression Mechanism	62
3.2.3	The Compressed Σ -Protocol	64
3.2.4	Amortizing the Communication Costs	68
3.2.5	Sublinear Communication in Constant Rounds	70
3.3	Proving Knowledge of <i>Short</i> Preimages	72
3.3.1	Basic Σ -Protocol	73
3.3.2	A Compression Mechanism	79
3.3.3	The Compressed Σ -Protocol for Short Preimages	82
3.3.4	Enlarging the Challenge Set	84
3.4	Compact Commitments and Linear Forms	87
3.4.1	Opening Linear Forms on Committed Vectors	88
3.4.2	Amortization - Opening Many Linear Forms	91
3.4.3	Opening Linear Forms with Unconditional Soundness	93
3.4.4	Compactification	94
4	Compressed Σ-Protocols: Higher Level Functionalities	105
4.1	Introduction	107
4.2	An Arithmetic Secret-Sharing Based Linearization Technique	108
4.2.1	Proving Correctness of Multiplication Triples	108
4.2.2	A Commit-and-Prove Variant	112
4.2.3	Correctness of Multiplication Triples in Small Fields	113
4.3	Proofs of Partial Knowledge	114
4.3.1	Knowledge of k -out-of- n Homomorphism Preimages	115
4.3.2	Pairing-Based Reduction of the Communication Costs	118
4.3.3	General Access Structures	119
5	Suitable Cryptographic Platforms	121
5.1	Introduction	123
5.2	Discrete Logarithm Assumption	123
5.3	Pairing-Based Platform	125
5.4	Knowledge of Exponent Assumption	128
5.5	Strong-RSA Assumption	132
5.6	A Lattice Assumption: Short Integer Solutions	136
6	Knowledge Soundness of Compressed Σ-Protocols	145
6.1	Introduction	147
6.2	The Knowledge Soundness Problem for Multi-Round Special-Sound Interactive Proofs	148
6.3	A Partial Solution: Strict Polynomial Time Extraction	150
6.3.1	Σ -Protocols	151
6.3.2	Multi-Round Interactive Proofs	156
6.4	A Complete Solution in Expected Polynomial Time	160
6.4.1	Σ -Protocols	161
6.4.2	Multi-Round Interactive Proofs	164
6.4.3	A Note on Witness Extended Emulation	167
6.5	Solving the Parallel Repetition Problem	167
6.5.1	A Generic but Suboptimal Solution	168

6.5.2	Parallel Repetition of k -out-of- n Special-Sound Σ -Protocols	172
6.5.3	Parallel Repetition of Multi-Round Interactive Proofs . . .	179
6.5.4	Threshold Parallel Repetition	184
6.6	Non-Interactivity: Knowledge Extraction under the Fiat-Shamir Transformation	187
6.6.1	Technical Overview	188
6.6.2	Related Work	190
6.6.3	An Abstract Sampling Game	191
6.6.4	The Fiat-Shamir Transformation of Σ -Protocols	196
6.6.5	A Refined Analysis of the Abstract Sampling Game . .	198
6.6.6	The Fiat-Shamir Transformation of Multi-Round Protocols	203
6.6.7	An Attack on the Fiat-Shamir Transformation of a Parallel Repetition	210
7	Applications of Compressed Σ-Protocols	215
7.1	Introduction	217
7.2	Circuit Zero-Knowledge Protocols	218
7.2.1	The Compressed Σ -Protocol for Arithmetic Circuits . .	218
7.2.2	An Extension to <i>Commit-and-Prove</i> Protocols	224
7.2.3	A Generalization to Bilinear Group Arithmetic Circuits	226
7.3	Threshold Signature Scheme	227
7.3.1	Definition and Security Model	228
7.3.2	The Threshold Signature Scheme	230
	Bibliography	235
	Summary	253
	Samenvatting	261
	Acknowledgments	269
	About the Author	275

