

A Study of Algebraic Methods in Asymmetric Cryptography – Algorithms, Constructions, and Attacks

Dissertation

zur

Erlangung der naturwissenschaftlichen Doktorwürde
(Dr. sc. nat.)

vorgelegt der

Mathematisch-naturwissenschaftlichen Fakultät

der

Universität Zürich

von

SIMRAN SUNIL TINANI

aus

Indien

Promotionskommission

Prof. Dr. Joachim Rosenthal (Vorsitz)

Prof. Dr. Andrew Kresch

Prof. Dr. Kenny Paterson

Zürich, 2023

Contents

1	Introduction	1
1.1	History	1
1.2	Mathematics and Cryptography	3
1.2.1	New one-way functions and post-quantum cryptography	3
1.3	Computational Complexity	4
1.4	Private Key Cryptography	5
1.5	Public Key Cryptography	6
1.5.1	Discrete log-based encryption	7
1.5.2	Algorithms for the discrete logarithm problem	9
1.5.3	Factoring-based encryption	10
1.5.4	Algorithms for Factoring	10
1.5.5	Digital Signatures	11
1.6	Hash Functions	14
1.6.1	SHA	14
1.6.2	Applications in cryptography	15
1.6.3	Security	15
1.7	Cryptographic protocols over the internet	16
1.8	Summary of Contributions in this Thesis	16
2	Discrete Logarithm Problem in Various Algebraic Platforms	21
2.1	Introduction	21
2.2	The discrete logarithm problem in a semigroup	23
2.2.1	Preliminaries	24
2.2.2	Existing Probabalistic Algorithms	26
2.2.3	Deterministic Solution of the DLP	33
2.3	DLP in an infinite polynomial semiring	41
2.4	Semigroup actions on a set	44
3	Public-Key Cryptography in Non-Abelian Groups	47
3.1	Introduction	47
3.2	Complexity of CSP in some polycyclic and matrix groups	50
3.2.1	Polycyclic groups	51
3.2.2	Matrix Groups	60

3.3	CSP in Central Products	67
3.4	An Overview of Braid-Based Cryptography	72
3.4.1	Platform Groups and Algorithmic Problems	73
3.4.2	Some Braid-Based Protocols	75
3.4.3	Methods for Attacks	76
4	Cryptanalysis of a System based on	
	Twisted Dihedral Group Algebras	79
4.1	Introduction	79
4.2	Structure of the Platform	81
4.2.1	A twisted dihedral group algebra	82
4.3	The key exchange protocol	84
4.3.1	Public parameters	84
4.3.2	Correctness	85
4.3.3	Security Assumption	85
4.4	Circulant Matrices	87
4.4.1	Probability of a circulant matrix being invertible	88
4.5	Cryptanalysis	89
4.5.1	Reduction to matrix equations	90
4.5.2	The algorithm for cryptanalysis	92
4.6	Examples	94
5	Methods for Collisions in some	
	Algebraic Hash Functions	97
5.1	Introduction	97
5.2	Generalized Zémor Hash functions	101
5.2.1	Euclidean Algorithm Attack for $\alpha = \beta = 1$	102
5.2.2	Extending messages for diagonal hashes over \mathbb{F}_p	103
5.2.3	Extending messages for triangular hashes over \mathbb{F}_{p^k}	105
5.3	Generalized Tillich-Zémor Hash Functions	112
5.3.1	Computing $f_n(x)$ for characteristic $p \neq 2$	112
5.3.2	Malicious paramaters	114