## Contents

1 Introduction

1.1 Results

1.1.1 Efficiency limitations of the $\Sigma_\psi$-protocol

1.1.2 Efficient proofs of knowledge for exponentiation homomorphisms in hidden order groups

1.2 Outline

2 Basic concepts

2.1 Some notation

2.2 Complexity theory

2.2.1 Algorithms and reducibility

2.2.2 Two-party protocols

2.3 Group theory

2.3.1 Notation and basic facts

2.3.2 Computational aspects

2.3.3 Concrete groups and homomorphisms used in cryptography

2.3.4 A note on the presentation

2.4 Zero-knowledge proofs

2.4.1 Definitions

2.4.2 Some fundamental results

3 Pseudo-preimages and related computational problems

3.1 Definition and basic facts

3.2 Pseudo-preimage problem

3.2.1 Solvable instances of the pseudo-preimage problem

3.2.2 Hardness of the pseudo-preimage problem

3.3 Pseudo-preimage generation problem

6
4 The $\Sigma_\psi$-protocol 61
  4.1 Protocol definitions and the zero-knowledge property 63
  4.2 Proof of knowledge property 67
    4.2.1 A note on pseudo-preimage extractors 72
  4.3 Knowledge error and efficiency of the $\Sigma_\psi$-protocol 73
    4.3.1 Efficiency analysis 74
    4.3.2 Efficiency limitations and the minimal standard knowledge error 76
  4.4 Interactive proofs 77
  4.5 The Damgaard-Fujisaki scheme 80

5 On the optimality of the standard knowledge extractor of the $\Sigma_\psi$-protocol 85
  5.1 Definition of lower bound on the knowledge error 87
  5.2 Lower bounds in the generic model 89
    5.2.1 Model 91
    5.2.2 Pseudo-random functions 95
    5.2.3 Results 96
  5.3 Lower bounds in the plain model 99
    5.3.1 Lower bounds for power homomorphisms 99
    5.3.2 Lower bounds for exponentiation homomorphisms 102
  5.4 Proof of Theorem 5.1 110
    5.4.1 Preliminaries 111
    5.4.2 Definition of cheating prover $P^*$ and $D_K(k)$ 114
    5.4.3 Non-triviality and uniformity 115
    5.4.4 Hardness 115
    5.4.5 Evaluation of bounds in the simulated world 120

6 Efficient proofs of knowledge for exponentiation homomorphisms 125
  6.1 Auxiliary information in the common input 127
  6.2 The $\Sigma_\psi$-protocol in the auxiliary setting 128
    6.2.1 Sketch of basic idea 128
    6.2.2 Formalization of basic idea 129
    6.2.3 Application to exponentiation homomorphisms in hidden order groups 132
  6.3 The $\Sigma_\psi^+$- and the $\Sigma_\psi^+\text{-WS}$-protocol 138
    6.3.1 Proofs of knowledge in the auxiliary string model 138
    6.3.2 The $\Sigma_\psi^+$-protocol 140
    6.3.3 The $\Sigma_\psi^+\text{-WS}$-protocol 149
  6.4 Comparison 154
## Contents

7 Concluding remarks .................. 156

Bibliography ......................... 158