CONTENTS

Introduction 5

1 Thesis Overview 5
- 1.1 Scope and Research Motivation . . . 6
- 1.2 Thesis Objectives . . . 6
- 1.3 Relation to Author's Publications and Contribution . . . 6

2 Cryptographic Background 7
- 2.1 Background and Preliminaries . . . 7
- 2.2 Conventional Digital Signature Schemes . . . 8
- 2.3 Privacy-Preserving Cryptographic Schemes . . . 8
- 2.4 Theoretical Evaluation of Digital Signature Schemes . . . 11
- 2.5 Post Quantum Public Key Cryptographic Schemes . . . 13

3 Assessment of Cryptographic Schemes on Constrained Devices 13
- 3.1 Conventional Cryptography on Constrained Devices . . . 13
- 3.2 Privacy-Preserving Cryptographic Schemes on Constrained Devices . . . 14
- 3.3 Post-Quantum Cryptography on Constrained Devices . . . 16

4 Novel Systems Based on Advanced Public Key Cryptographic Protocols for Constrained Devices 17
- 4.1 Secure and Efficient Two-factor Zero-knowledge Authentication System Based on Smart Cards . . . 17
- 4.2 Secure and Privacy-preserving Data Transfer System Based on Light-Weight Group Signatures with Time-Bound Membership . . . 21
- 4.3 Decentralized Privacy-Preserving Transactions Based on Lightweight Ring Signatures . . . 28

5 Conclusion 32

Bibliography 33

Bibliography 35