Contents

1 **Abstract and Organization** **4**

2 **Introduction and Preliminaries** **9**
- 2.1 Introduction . . . 9
- 2.2 Cryptography . . . 10
  - 2.2.1 Encryption . . . 12
  - 2.2.2 Diffie-Hellman Key Exchange . . . 14
  - 2.2.3 From Key Exchange to Encryption: the ElGamal Cryptosystem . 15
  - 2.2.4 Semantic Security . . . 17
  - 2.2.5 From Encryption to Key Exchange: Key Encapsulation Mechanism 20
  - 2.2.6 Digital Signature . . . 21
  - 2.2.7 Basic Security Notions for Signatures . . . 22
  - 2.2.8 Identification Schemes . . . 24
  - 2.2.9 From Identification to Signatures: The Schnorr Signature . . . 25
- 2.3 Post-Quantum Cryptography . . . 28
  - 2.3.1 Lattices . . . 30
  - 2.3.2 Hard Problems on Lattices . . . 31
  - 2.3.3 SIS, LWE and their Algebraically Structured Variants . . . 32
  - 2.3.4 NIST Standardization Process . . . 35

3 **Efficient KEMs Implementations on Embedded Devices** **38**
- 3.1 Preamble . . . 38
- 3.2 Introduction . . . 39
- 3.3 Polynomial Multiplication . . . 39
  - 3.3.1 NTT-based Multiplication . . . 40
  - 3.3.2 Fast Fourier Transform Algorithms . . . 40
- 3.4 Lattice-Based Key Exchange/Key Encapsulation . . . 45
  - 3.4.1 NewHope . . . 46
  - 3.4.2 Kyber . . . 50
- 3.5 Fast NTT for Fast Implementations of NewHope and Kyber on Cortex-M4 52
  - 3.5.1 Efficient Reduction Algorithms . . . 52
  - 3.5.2 Cortex-M4 . . . 54
  - 3.5.3 SIMD and Useful Instructions . . . 54
- 3.6 Original NewHope NTT . . . 56
  - 3.6.1 Optimized Assembly Code on Cortex-M4 . . . 57
- 3.7 Cortex-M4 Optimizations for {R,M}LWE Schemes (EPRINT 2020) . . . 62
  - 3.7.1 Polynomial Multiplication in Kyber . . . 63
  - 3.7.2 NewHope-Compact . . . 63

3.7.3 Speed Optimizations of Polynomial Multiplication 64
3.7.4 Optimization of NewHope and NewHope-Compact for Stack Usage 67
3.7.5 Tradeoffs Between Secret Key Size and Speed 68
3.7.6 Results and Comparison 69
3.7.7 Speed Comparison 69
3.7.8 Dominance of Hashing 70
3.7.9 Comparing Polynomial Multiplications 71
3.8 Conclusion 72
3.9 Thoughts and Future Works 73

4 Protecting Lattice-based Cryptography Against Physical Attacks 76
4.1 Preamble 76
4.2 Introduction 76
4.3 Power analysis attacks 77
4.3.1 Correlation Power Analysis 77
4.4 Concrete attack: Breaking Kalyna ! (SPACE 2016) 78
4.4.1 Encryption Algorithm 79
4.4.2 Key Scheduling 79
4.4.3 Side-Channel Attacks on Kalyna 80
4.4.4 Experiments 81
4.5 Masking 84
4.6 Lattice-Based Signatures 85
4.6.1 GLP 85
4.6.2 A Scheme from Bai and Galbraith 89
4.6.3 qTESLA 90
4.7 Masking qTESLA at any Order (CARDIS 2019) 93
4.7.1 Masking-Friendly Design 95
4.7.2 Existing Gadgets 96
4.7.3 New Gadgets 97
4.7.4 Masked Scheme 101
4.7.5 Proof of Masking 103
4.7.6 Practical Aspects and Implementation Details 107
4.8 Conclusion 109
4.9 Thoughts and Future Works 110

5 Efficient Design for Lattice-Based Cryptography 113
5.1 Preamble 113
5.2 Introduction 113
5.3 Signcryption 114
5.4 Security model for signcryption 116
5.5 Zheng’s Scheme 117
5.5.1 Schnorr Variant 118
5.6 Reconciliation Mechanism 119
5.7 SETLA: Signature and Encryption from Lattices (CANS 2018) 120
5.7.1 SETLA-KEX Signcryption 120
5.7.2 SETLA-KEM Signcryption 123
5.8 Security Arguments 125