

Contents

| | |
|---|------------|
| Abstract | v |
| Sommario | vii |
| 1 Introduction | 1 |
| 1.1 Basic Concepts | 2 |
| 1.1.1 Communications Model | 2 |
| 1.1.2 Security Goals | 2 |
| 1.2 Cryptography in Hardware | 3 |
| 1.2.1 High-Speed Encryption | 4 |
| 1.2.2 Portable Devices | 4 |
| 1.2.3 Implementation Security | 5 |
| 1.3 Contributions of this Thesis | 6 |
| 1.4 Thesis Outline | 9 |
| 2 Fundamentals | 11 |
| 2.1 Notation | 12 |
| 2.2 Symmetric-Key Cryptography | 12 |
| 2.2.1 Block Ciphers | 13 |
| 2.2.2 Stream Ciphers | 16 |
| 2.3 Cryptographic Hash Functions | 18 |
| 2.4 Authentication in Public-Key Cryptography | 20 |
| 2.5 Security of Cryptographic Functions | 21 |
| 2.6 Quantum Cryptography | 22 |
| 2.6.1 Quantum Key Distribution (QKD) | 23 |
| 2.6.2 The BB84 Protocol | 23 |
| 2.6.3 Authentication in Quantum Cryptography | 25 |

| | | |
|----------|--|-----------|
| 3 | Cryptographic Hash Functions | 27 |
| 3.1 | Iterated Hash Functions | 28 |
| 3.1.1 | The Merkle-Damgård Construction | 28 |
| 3.1.2 | Hardware Specifications | 30 |
| 3.1.3 | Design Strategies | 32 |
| 3.1.4 | Recent Hash Constructions | 36 |
| 3.1.5 | Block Cipher-based Constructions | 38 |
| 3.2 | The SHA-3 Competition | 39 |
| 3.3 | The Hash Function EnRUPT | 41 |
| 3.3.1 | Specification of EnRUPT | 41 |
| 3.3.2 | EnRUPT Architectures | 44 |
| 3.4 | The Hash Function BLAKE | 45 |
| 3.4.1 | Specification of BLAKE | 47 |
| 3.4.2 | High-Speed Architectures | 51 |
| 3.4.3 | Silicon Implementation of a Compact BLAKE- 32 Core | 59 |
| 3.5 | Development of a Hardware Evaluation Method for the SHA-3 Candidates | 68 |
| 3.5.1 | Evaluation Methodology | 69 |
| 3.5.2 | Implementation | 77 |
| 3.5.3 | Results | 81 |
| 3.5.4 | Final Remarks | 88 |
| 4 | High-Speed Authenticated Encryption | 91 |
| 4.1 | Background | 92 |
| 4.1.1 | Different Classes | 92 |
| 4.1.2 | Applications | 93 |
| 4.2 | The Advanced Encryption Standard | 94 |
| 4.2.1 | Algorithm Specifications | 95 |
| 4.2.2 | Hardware Architectures | 96 |
| 4.3 | The Galois/Counter Mode | 98 |
| 4.3.1 | Algorithm Specifications | 100 |
| 4.4 | FPGA Parallel-Pipelined AES-GCM Core for 100G Eth- ernet Applications | 103 |
| 4.4.1 | Hardware Design | 103 |
| 4.4.2 | Results and Comparison | 109 |
| 4.5 | 2G Fibre Channel Link Encryptor | 111 |
| 4.5.1 | AES-GCM Hardware Architecture | 112 |

| | | |
|----------|--|------------|
| 4.5.2 | FPGA Implementation | 113 |
| 4.5.3 | Frame Encryption | 115 |
| 4.5.4 | Results and Discussion | 118 |
| 5 | Lightweight Hashing | 121 |
| 5.1 | Lightweight Cryptography Overview | 122 |
| 5.2 | Cube Testers | 124 |
| 5.2.1 | Theoretical Background | 125 |
| 5.2.2 | Description of Grain-128 | 126 |
| 5.2.3 | Software Implementation | 128 |
| 5.2.4 | Hardware Implementation | 128 |
| 5.2.5 | Experimental Results | 134 |
| 5.2.6 | Conclusion | 135 |
| 5.3 | The QUARK Hash Function | 136 |
| 5.3.1 | Description of the QUARK hash family | 137 |
| 5.3.2 | Hardware implementation | 140 |
| 5.3.3 | Discussion | 142 |
| 6 | Summary and Conclusion | 147 |
| 6.1 | Summary | 147 |
| 6.2 | Conclusion | 150 |
| A | Hardware Architectures | 153 |
| | List of Acronyms | 157 |
| | List of Figures | 159 |
| | List of Tables | 161 |
| | Curriculum Vitae | 163 |