

1. Introduction1

2. Preliminaries7

2.1. The Patterson Algorithm for the Decoding of Goppa Codes7

2.2. The McEliece PKC8

2.3. The Niederreiter PKC8

3. Optimization for Resource-constrained Devices11

3.1. On-Line public Operation for Code-based Schemes11

3.1.1. The Storage Problem on Memory Constrained Devices12

3.1.2. Public Key Infrastructures12

3.1.3. Description of the On-line Public Operation13

3.1.4. Transmission Rates15

3.1.5. Example Implementation16

3.1.6. Non-interactive Version of the Protocol17

3.1.7. Simulation of higher Transmission Rates17

3.1.8. Experimental Results18

3.1.9. Column-wise vs. Row-wise Matrix-Vector Multiplication18

3.1.10. Code-based Signature Schemes20

3.2. McEliece Decryption without the Parity Check Matrix20

3.2.1. Optimized Algorithm for the Syndrome Computation without the Parity Check Matrix21

3.2.2. Implementation and Performance Results22

3.3. Efficient Root-Finding during the Decryption23

3.3.1. Remarks about the  $F_{2^m}$  Operations23

3.3.2. Variants of Root Finding24

3.3.2.1. Exhaustive Evaluation with and without Division24

3.3.2.2. Berlekamp Trace Algorithm25

3.3.2.3. Root Finding with linearised Polynomials26

3.3.2.4. New Hybrid Variants27

3.3.3. Performance of the Root-finding Variants28

3.4. Comparison of the McEliece and Niederreiter PKCs in Terms of Efficiency30

3.4.1. Public Key Size and Encryption Speed30

3.4.2. Private Key Size and Decryption Speed30

3.4.3. Message and Ciphertext Sizes31

<b>4. Side Channel Security</b>	<b>33</b>
4.1. Message-aimed Side Channel Attacks against the Decryption Operation	33
4.1.1. Timing Vulnerabilities in the Root-Finding based on the Degree of the Error Locator Polynomial	33
4.1.2. Timing Vulnerability of the Key Equation solving EEA and Countermeasures	35
4.1.2.1. Identification of the Vulnerability	36
4.1.2.2. Timing Countermeasure	38
4.1.2.3. Implementation and Verification of the Countermeasure	38
4.1.3. A related Simple Power Analysis Attack against the Key Equation Solving EEA	40
4.1.3.1. Measurement Setup	40
4.1.3.2. Attacks against the insecure Implementation	41
4.1.3.3. Countermeasure	41
4.1.4. Vulnerability in Root-Finding with exhaustive Evaluation and Division	42
4.2. Side Channel Attacks against the secret Support	44
4.2.1. Timing Attacks against the EEA	46
4.2.1.1. Properties of the Syndrome Inversion	46
4.2.1.2. Linear Equations from $w = 4$ Error Vectors	47
4.2.1.3. Cubic Equations from $w = 6$ Error Vectors	50
4.2.1.4. Enlargement of the Timing Differences by the Key Equation Solving EEA	51
4.2.1.5. The Zero Element of the Support from $w = 1$ Error Vectors	52
4.2.1.6. Combining the " $w = 1$ ", " $w = 4$ ", and " $w = 6$ " Vulnerabilities to a practical Attack	53
4.2.1.7. Experimental Results	57
4.2.1.8. Effect of Countermeasures against other Attacks	60
4.2.1.9. Possible Extensions of the Attack	61
4.2.1.10. The Problem of Countermeasures	62
4.2.2. Timing Attacks against Root-Finding Algorithms	62
4.2.2.1. Vulnerability of <i>eval-div-rf</i>	62
4.2.2.2. Vulnerability of <i>dcmp-rf</i>	64
4.3. Fault Attacks	66
4.3.1. Fault Attack Vulnerability revealing the Degree of the Error Locator Polynomial	66
4.3.2. Fault Attack Vulnerability revealing Information about the Number of Roots of the Error Locator Polynomial	66
4.4. Transferability of the Vulnerabilities and Countermeasures to the Niederreiter PKC	67

4.5.	Relation of the Side Channel Vulnerabilities to those of other Cryptosystems	67
4.5.1.	Message-aimed Side Channel Attacks against Cryptosystems with homomorphic Properties	67
4.5.1.1.	Manger's Attack against RSA-OAEP	68
4.5.1.2.	Homomorphic Properties of RSA and the McEliece Cryptosystem	70
4.5.1.3.	Comparison of Message-aimed Side Channel Attacks against RSA and McEliece	70
4.5.1.4.	Methodology for the Analysis of public Key Cryptosystems with homomorphic Properties	72
4.5.2.	Blinding Countermeasures for Code-based Cryptosystems	73
5.	Embedded Implementations of the McEliece PKC	75
5.1.	A Flexible Platform independent Implementation of the McEliece PKC	75
5.1.1.	Description of the Implementation	75
5.1.2.	Performance Results	75
5.2.	A Smart Card Implementation of the McEliece PKC	79
5.2.1.	Description of the Implementation	79
5.2.2.	Performance Results	81
6.	Open Problems	83
6.1.	Potential Cache-Timing Vulnerabilities in Code-Based Decryption Operations	83
6.2.	Countermeasures Against the Low-Weight Error Vector Attacks	83
6.3.	Side Channel Security of <i>BTA-rf</i>	84
6.4.	Side-Channel Secure Implementation of <i>dcmp-div-rf</i>	86
6.5.	The Problem of the Optimal Root-Finding Algorithm for Embedded Implementations with Hardware Support	88
7.	Conclusion	89
A.	Appendix	97
A.1.	Cubic Equations involving less than four Basis Elements are impossible	97