

Kurzfassung

Das Hauptziel dieser Arbeit ist, eine prägnante Einführung in das ursprüngliche McEliece-Verfahren von 1978 sowie in die Variante nach Niederreiter zu präsentieren. Das McEliece-Kryptosystem bietet nach heutigen Annahmen eine starke Sicherheit gegenüber bekannten Angriffen, insbesondere gegenüber Angriffen mit Quantencomputern. Zunächst werden die von Quantencomputern ausgehenden Risiken skizziert und das McEliece-Kryptosystem und seine Varianten innerhalb der Post-Quanten-Kryptografie eingeordnet. Zur Erklärung der Verfahren wird anschließend eine detaillierte Einführung in die verwendete Code-Klasse der Goppa Codes präsentiert. Im Anschluss daran werden Optimierungen und Schwächen sowohl des McEliece- als auch des Niederreiter-Systems aufgezeigt und jeweils ein Beispiel gegeben. Abschließend wird die aktuelle Classic McEliece-Variante des Systems vorgestellt.

Ergänzend zu diesem Buch steht im Github Repository 'GoppaCodes-and-McElieceKryptosystem' die Programmierung der Kryptosysteme als Jupyter Notebook zur Verfügung. Diese kann in cocalc ohne die Installation von Software ausprobiert werden.

Schlüsselwörter: Goppa Code, McEliece-Kryptosystem, asymmetrische Verschlüsselung, Fehlerkorrekturcodes, Post-Quanten-Kryptografie.

Abstract

The primary objective of this paper is to provide a concise introduction to the original McEliece scheme from 1978, as well as to the Niederreiter variant. The McEliece cryptosystem, under current assumptions, offers a high level of security against known attacks, particularly those involving quantum computers. Initially, the risks posed by quantum computers are outlined, and the McEliece cryptosystem and its variants are classified in the field of post-quantum cryptography. To explain the procedures, a detailed introduction to the class of codes used, known as Goppa codes, is presented.

Following that, optimizations and weaknesses of both the McEliece and Niederreiter systems are highlighted, with an example provided for each. Finally, the current Classic McEliece variant of the system is introduced.

In addition to this book, the Github repository 'GoppaCodes-and-McElieceKryptosystem' contains the programming of the crypto systems as a Jupyter notebook. This can be used in cocalc without the installation of software.

Keywords: Goppa code, McEliece cryptosystem, asymmetric encryption, error correction codes, post quantum cryptography.

Inhaltsverzeichnis

1. Einleitung	1
1.1. Motivation des McEliece-Kryptosystems	1
1.2. Struktur der Arbeit	2
1.3. Voraussetzungen	3
1.4. Notationen	3
2. Quantencomputer und moderne Kryptografie	7
2.1. Quantencomputer – Grundlagen und Algorithmen	7
2.2. Post-Quanten-Kryptografie	12
3. Goppa Codes	17
3.1. Einleitung	17
3.2. Definition und Parameter von Goppa Codes	18
3.2.1. Kontrollmatrix (und Generatormatrix)	19
3.2.2. Dimension und Minimalabstand	22
3.2.3. Minimalabstand quadratfreier binärer Goppa Codes	24
3.3. Decodierung	28
3.3.1. Decodierung allgemeiner Goppa Codes	28
3.3.2. Decodierung irreduzibler binärer Goppa Codes	35
4. Das McEliece-Kryptosystem und seine Varianten	40
4.1. Das McEliece-Kryptosystem	41
4.2. Das Niederreiter-Kryptosystem	46
4.3. Vergleich des McEliece- und Niederreiter-Kryptosystems	48
4.4. Beispiel	52
4.4.1. Beispiel zum McEliece-Kryptosystem	55
4.4.2. Beispiel zum Niederreiter-Kryptosystem	58

4.5. Sicherheitsanalyse	60
4.5.1. Grundlegende versionsunabhängige Angriffe	61
4.5.2. Versionsabhängiger Message Resend Angriff auf das McEliece-Kryptosystem	63
4.6. Das Classic McEliece-Kryptosystem	67
4.6.1. Besonderheiten des Systems	68
4.6.2. Wahl der Parameter	69
4.6.3. Vor- und Nachteile des Verfahrens	70
5. Zusammenfassung und Ausblick	73
A. Anhang: Übersicht über die Herleitungen	74
B. Anhang: Implementierung in SageMath	77
B.1. Implementierung des McEliece- und Niederreiter-Kryptosystems	77
B.2. Konvertierung der Kontrollmatrix hin zu einer binären Kon- trollmatrix	84
B.3. Implementierung der Decodierung nach Patterson	85
B.4. Demonstration zur CCA-2 Sicherheit	88
C. Anhang: Konvertierung des McEliece-Kryptosystems	89
Literaturverzeichnis	92

Abbildungsverzeichnis

1.1. Zusammenhang der Kapitel	6
2.1. Mengendiagramm der Komplexitätsklassen	10
2.2. Moscas Theorem	11
2.3. Übersicht über quantensichere Verfahren	13
4.1. Zusammenhang der Kryptosysteme	42
4.2. Optimierung der McEliece-Schulbuchversion	45
4.3. Optimierung der Niederreiter-Schulbuchversion	48
A.1. Übersicht über die Beweisstruktur zur Kontrollmatrix und Dimension von Goppa Codes	75
A.2. Übersicht über die Beweisstruktur zum Minimalabstand und der Decodierung von Goppa Codes	76

Tabellenverzeichnis

2.1. Quantencomputer und deren Gefahr für die Kryptografie . . .	8
2.2. Vergleich von Post-Quanten-Kryptografie (PQC) gegenüber Quantum Key Distribution (QKD)	16
3.1. Parameter von Goppa Codes	28
4.1. Vergleich McEliece- vs. Niederreiter-Kryptosystem	51
4.2. Elemente des Körpers \mathbb{F}_{2^4}	53
4.3. Mögliche Angriffe auf die Kryptosysteme ohne Konvertierung	67
4.4. Parameterspezifikation im Classic McEliece-Kryptosystem . .	69
4.5. Größen der In- und Outputs des Classic McEliece-Systems in Bytes	70
4.6. Annahme der asymptotischen Sicherheit des McEliece-Verfahrens und gitterbasierten Verfahren im Vergleich zu 2020	72
C.1. Bezeichnungen in den Konvertierungsalgorithmen	89

Liste der Algorithmen

3.1. Decodieralgorithmus für allgemeine Goppa Codes nach Sugiyama	34
3.2. Decodieralgorithmus für irreduzible binäre Goppa Codes nach Patterson	36
4.1. Schlüsselerzeugung im McEliece-Kryptosystem	42
4.2. Verschlüsselung im McEliece-Kryptosystem	43
4.3. Entschlüsselung im McEliece-Kryptosystem	43
4.4. Schlüsselerzeugung im Niederreiter-Kryptosystem	46
4.5. Verschlüsselung im Niederreiter-Kryptosystem	46
4.6. Entschlüsselung im Niederreiter-Kryptosystem	47
C.1. Fujisaki-Okamotos Konvertierung - Verschlüsselung	90
C.2. Fujisaki-Okamotos Konvertierung - Entschlüsselung	90

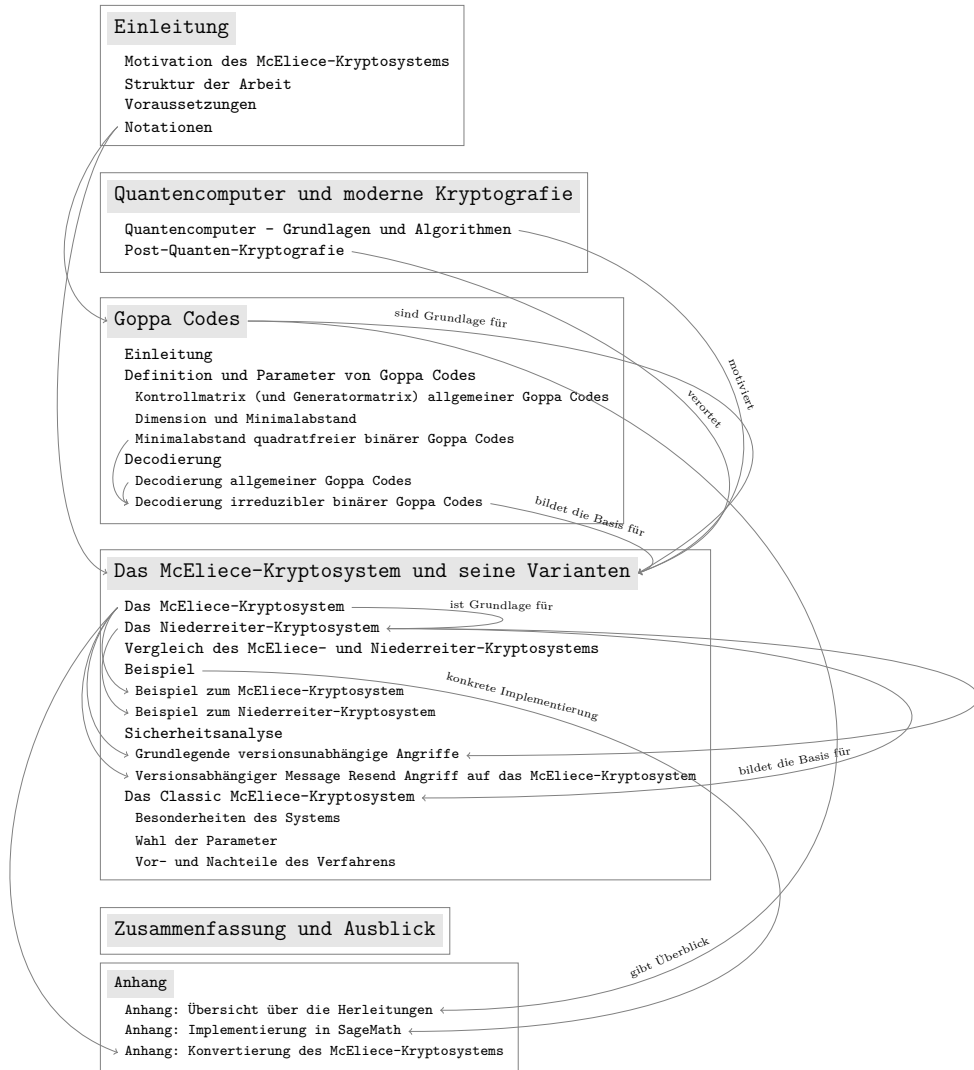


Abbildung 1.1.: Zusammenhang der Abschnitte und Kapitel

Aufeinanderfolgende Kapitel stehen immer in direktem Zusammenhang. Besondere Beziehungen sind durch die Pfeile hervorgehoben. Insbesondere der Zusammenhang der Kryptosysteme und die Einordnung, welcher Teil der Sicherheitsanalyse welches Kryptosystem betrifft, ist nochmal hervorgehoben.

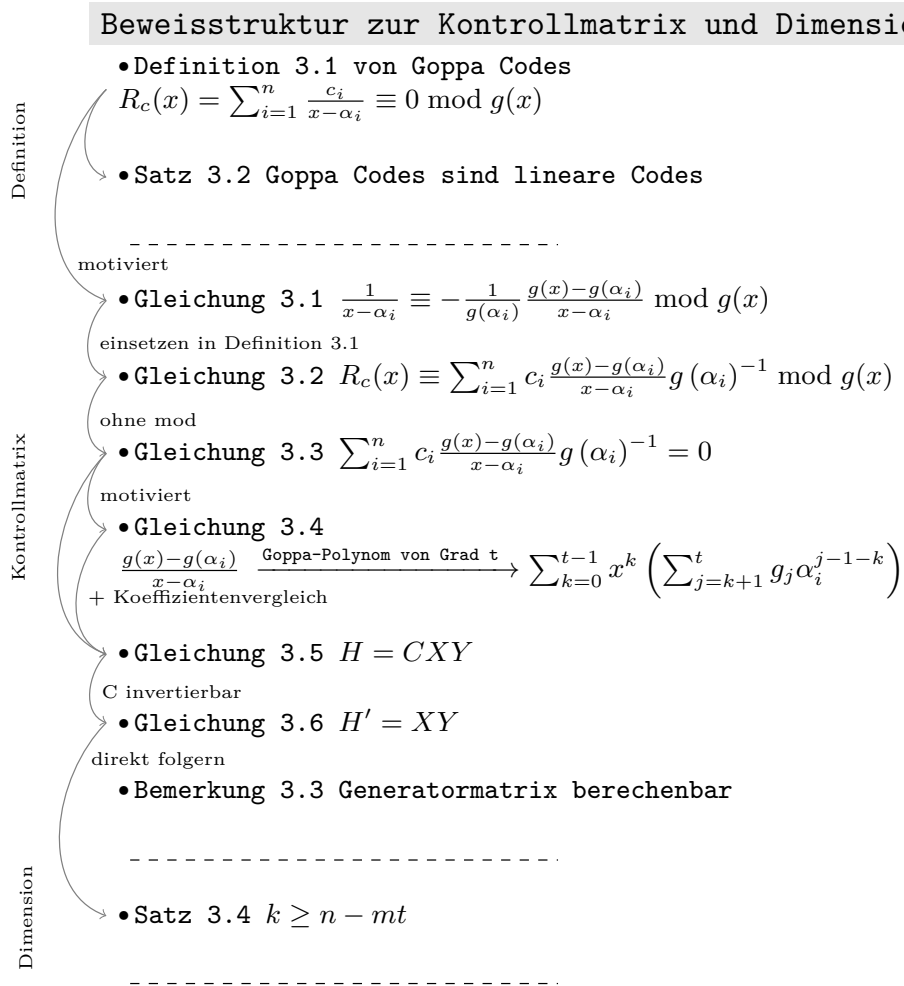


Abbildung A.1.: Übersicht über die Beweisstruktur zur Kontrollmatrix und Dimension von Goppa Codes

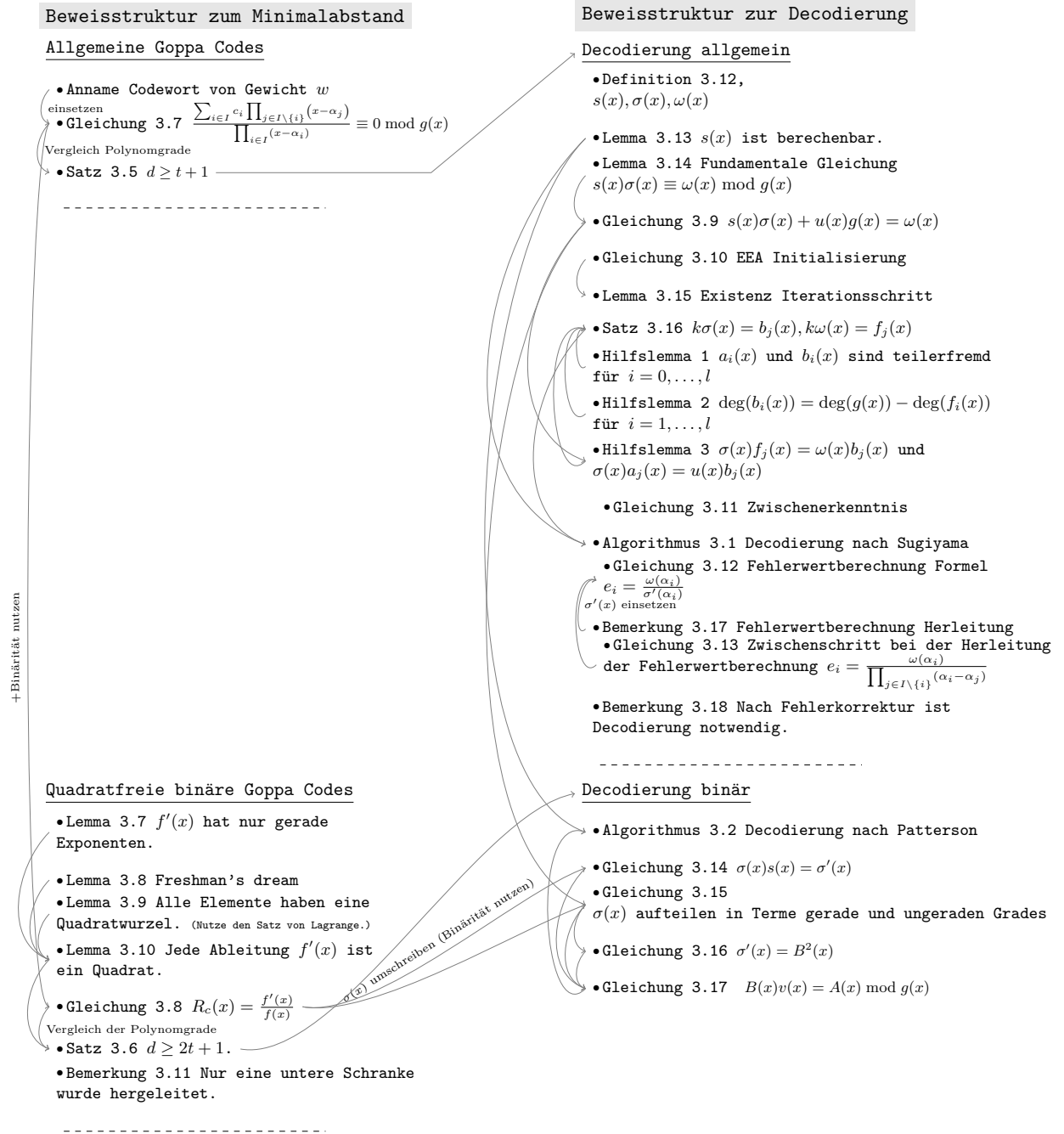


Abbildung A.2.: Übersicht über die Beweisstruktur zum Minimalabstand und der Decodierung von Goppa Codes