

Inhaltsverzeichnis

1	Einleitung	1
1.1	Motivation des McEliece-Kryptosystems	1
1.2	Struktur der Arbeit	2
1.3	Voraussetzungen	5
1.4	Notationen	5
2	Quantencomputer und moderne Kryptografie	7
2.1	Quantencomputer – Grundlagen und Algorithmen	7
2.2	Post-Quanten-Kryptografie	11
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	34
4	Das McEliece-Kryptosystem und seine Varianten	39
4.1	Das McEliece-Kryptosystem	41
4.2	Das Niederreiter-Kryptosystem	44
4.3	Vergleich des McEliece- und Niederreiter-Kryptosystems	47

4.4	Beispiel	50
4.4.1	Beispiel zum McEliece-Kryptosystem	53
4.4.2	Beispiel zum Niederreiter-Kryptosystem	55
4.5	Sicherheitsanalyse	58
4.5.1	Grundlegende versionsunabhängige Angriffe	58
4.5.2	Versionsabhängiger Message Resend Angriff auf das McEliece-Kryptosystem	60
4.6	Das Classic McEliece-Kryptosystem	64
4.6.1	Besonderheiten des Systems	65
4.6.2	Wahl der Parameter	65
4.6.3	Vor- und Nachteile des Verfahrens	67
5	Zusammenfassung und Ausblick	69
	Literaturverzeichnis	71