

Duale Hochschule Baden-Württemberg Mannheim

## **Studienarbeit**

# **Konstruktion eines kryptographischen Verfahrens basierend auf Reed-Solomon-Codes und Diskussion möglicher Angriffsmethoden**

**Studiengang Informatik**

**Studienrichtung Cyber Security**

Verfasser(in):	Roman Wetenkamp
Matrikelnummer:	5533869
Kurs:	TINF20CS1
Studiengangsleiter:	Prof. Dr. Konstantin Bayreuther
Wissenschaftliche(r) Betreuer(in):	Prof. Dr. Reinhold Hübl
Bearbeitungszeitraum:	18.10.2022 – 18.04.2023

# Ehrenwörtliche Erklärung

Ich versichere hiermit, dass ich die vorliegende Arbeit mit dem Titel "*Konstruktion eines kryptographischen Verfahrens basierend auf Reed-Solomon-Codes und Diskussion möglicher Angriffsmethoden*" selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Ich versichere zudem, dass die eingereichte elektronische Fassung mit der gedruckten Fassung übereinstimmt.

Ort, Datum

Roman Wetenkamp

# Inhaltsverzeichnis

Abbildungsverzeichnis	iii
Tabellenverzeichnis	iv
Quelltextverzeichnis	v
Algorithmenverzeichnis	vi
Abkürzungsverzeichnis	vii
Kurzfassung (Abstract)	viii
1 Einleitung	1
2 Beispiel-Kapitel: Gebrauchsanleitung $\text{\LaTeX}$	2
3 Beispiel-Kapitel: Noch ein Kapitel	3
4 Zusammenfassung	4
Anhang	

# Abbildungsverzeichnis

# Tabellenverzeichnis

# Quelltextverzeichnis

# Algorithmenverzeichnis

# Abkürzungsverzeichnis

RSC      Reed-Solomon-Codes



# Kurzfassung (Abstract)

# 1 Einleitung

„The lesson here is that it is insufficient to protect ourselves with laws;  
we need to protect ourselves with mathematics.“  
– BRUCE SCHNEIER

In einer Welt, in der so viele Daten wie nie zuvor übertragen werden, digitale Kriegsführung und *Nation-state-attacks* nicht mehr nur Gegenstand dystopischer Science-Fiction-Literatur, sondern Alltag sind, steigt die Relevanz und die Systemkritikalität kryptographischer Verfahren, die es ermöglichen, die Vertraulichkeit und Integrität schützenswerter Daten selbst unter der Annahme, dass Angreifenden nahezu unbegrenzte Ressourcen zur Verfügung stehen sicherzustellen.

Das Forschungsgebiet der *Post-Quanten-Kryptographie* hat die Entwicklung aussichtsreicher kryptographischer Systeme zum Gegenstand, die selbst mit den durch Quantentechnologie anzunehmenden Rechenleistungssteigerungen nicht gebrochen werden kann. Ein möglicher Kandidat dafür ist das *McEliece*-Kryptosystem, das auf linearen, fehlerkorrigierenden Codes basiert. Jene Schnittmenge der Codierungstheorie und Kryptographie ist Gegenstand dieser Arbeit: Basierend auf dem *McEliece*-Kryptosystem soll ein aufbauender Ansatz von HARALD NIEDERREITER betrachtet werden, das im Vergleich zum *McEliece*-Kryptosystem nicht auf *Goppa*-, sondern auf *Reed-Solomon*-Codes basiert.

Im Rahmen dieser Arbeit sollen zunächst die theoretischen Hintergründe der Codierungstheorie für kryptographische Zwecke dargelegt, bevor basierend darauf die Arbeiten von MCELIECE und NIEDERREITER analysiert und für die Entwicklung eines eigenen Kryptosystems genutzt werden. Auf jenes Verfahren werden abschließend Methoden der Kryptanalyse nach SIDELNIKOV und SHESTAKOV angewandt, um Aussagen über die Sicherheit des Verfahrens treffen zu können.

## 2 Codierungstheorie

### 3 Lineare fehlerkorrigierende Codes für kryptographische Zwecke

## 4 Zusammenfassung