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

Danksagung

Hier können Sie eine Danksagung schreiben.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Quelltextverzeichnis

Algorithmenverzeichnis

Abkürzungsverzeichnis

RSC	Reed-Solomon-Codes

Kurzfassung (Abstract)

1 Einleitung

Während in verschiedenen Forschungsgruppen der Welt intensiv an Quantencomputern gearbeitet wird, versucht die Kryptographie bereits, Kryptosysteme zu entwickeln, die sich selbst mit hochperformanten Quantencomputern nicht brechen lassen. In dieser Hinsicht erweisen sich Kryptosysteme, die auf linearen fehlerkorrigierenden Codes basieren, als aussichtsreiche Kandidaten, da das Problem, aus einer codierten Nachricht mit einer Matrix entsprechend zusätzlich hinzugefügten Fehlern die Originalnachricht zu entschlüsseln, als hinreichend schwierig gilt.

Ansätze, kryptographische Verfahren auf Codierungstheorie zu basieren, wurden unter anderem von McEliece und Niederreiter vorgeschlagen. Während das abstrakte Konzept der Ver- und Entschlüsslung diesen Verfahren gemein ist, liegen die wesentlichen Unterschiede der Verfahren überwiegend in den zugrundeliegenden Codes.

Gegenstand dieser Arbeit ist das von Harald Niederreiter vorgeschlagene Schema eines Kryptosystems basierend auf Reed-Solomon-Codes. Auf dieser Arbeit aufbauend, wird ein Kryptosystem entwickelt, implementiert und analysiert. Ein weiterer Teil dieser Arbeit widmet sich anschließend möglichen Angriffen auf das vorgeschlagene Kryptosystem, wobei auf die Arbeit von Shostakov & ... Bezug genommen wird.

2 Beispiel-Kapitel: Gebrauchsanleitung LaTeX

3 Beispiel-Kapitel: Noch ein Kapitel

4 Zusammenfassung