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

Quelltextverzeichnis

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 [1]

In einer Welt, in der so viele Daten wie nie zuvor übertragen werden, digitale Kriegsführung und *Nation-state-attacks* nicht mehr bloß Gegenstand dystopischer Science-Fiction-Literatur, sondern Alltag sind, steigt die Relevanz und die Kritikalität 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* [vgl. 2] hat die Entwicklung kryptographischer Systeme zum Gegenstand, die selbst mit den durch Quantentechnologie anzunehmenden Rechenleistungssteigerungen nicht gebrochen werden können. Ein aussichtsreicher 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, der im Vergleich zum McEliece-Kryptosystem nicht auf *Goppa*-, sondern auf *Reed-Solomon*-Codes basiert und dadurch zwar bessere Rechenzeiten erreicht, jedoch vermutlich auch an Sicherheit einbüßt.

Diese Arbeit stellt zunächst die theoretischen Hintergründe der Codierungstheorie für kryptographische Zwecke dar, 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 Kryptoanalyse unter Einbezug der Arbeit von Sidelnikov und Shestakov angewandt, um Aussagen über die Sicherheit des Verfahrens treffen zu können.

2 Codierungstheorie

Da im Rahmen dieser Arbeit ein kryptographisches Verfahren entwickelt wird, das auf Elementen der Codierungstheorie basiert, wird diese nun zunächst in Definitionen und Hintergründen motiviert.

2.1 Grundbegriffe

Sowohl in der Kryptographie, als auch in der Codierungstheorie fungieren **Nachrichten**, die über mit bestimmten Eigenschaften behaftete **Kanäle** übertragen werden, als die Subjekte der Anschauung.

Definition 1
*Eine **Nachricht** m sei definiert als eine endliche Folge von Zeichen $a_i \in \Sigma$, wobei Σ eine endliche Menge von Zeichen (genannt **Alphabet**) bezeichnet.*

$$m = (a_1, a_2, ..., a_{n-1}, a_n) \quad \forall i = 1, ..., n : a_i \in \Sigma$$

Ein typisches Alphabet sind die Zeichen der ASCII-Kodierung, mit denen nahezu alle Worte und Sätze der natürlichen englischen Sprache gebildet werden können [vgl. 3]. Dieses Alphabet besteht nun nicht aus Zeichen der natürlichen Sprache, sondern aus 7-Bit-langen Zahlenwerten, was die Anwendung von Codes oder kryptographischen Verfahren ermöglicht. Im Rahmen dieser Arbeit wird implizit angenommen, dass Zeichen stets in einem Zahlenformat repräsentiert werden.

Die Definition einer informationstheoretischen Nachricht impliziert eine Autorenschaft, folglich muss jeder Nachricht eine Partei (ein natürliche Person, ein System oder ein Dienst) zugeordnet werden können, die im Folgenden als **Sender**[1] der Nachricht bezeichnet wird. Wird diese Nachricht nun über einen Kanal an eine andere Partei übertragen, so nennen wir

[1] Da sich die Anwendung der modernen Kryptographie sehr überwiegend mit dem Austausch von verschlüsselten Nachrichten zwischen Systemen und nicht unmittelbar zwischen natürlichen Personen befasst, wird hier die männliche Form verwendet (Sender = Dienst/System).

diese den **Empfänger**. Entgegen der in der Kryptographie üblichen *Alice-Bob*-Notation wird diese Terminologie beibehalten, um an den codierungstheoretischen Hintergrund anzuknüpfen.

Ein **Kanal** bezeichne ein Medium zur Datenübertragung wie beispielsweise einen elektrischen Leiter, einen Lichtwellenleiter oder die Luft für eine drahtlose Verbindung.

Definition 2
*Ein **Kanal** sei definiert als ein Tupel $\langle e, d, g, s \rangle$, wobei e das Medium, d den Durchsatz, g die Übertragungsgüte und s den Vertraulichkeitsgrad des Kanals bezeichne.*

Des Weiteren sei die Übertragungsfunktion $f : K \times M \mapsto M$ definiert als:

$$f(k, m) \to m'$$

mit $m, m' \in M$ wobei M die Menge aller Nachrichten ist und $k \in K$ wobei K die Menge aller Kanäle ist.

Diese Definition impliziert, dass die Datenübertragung nicht zwingend fehlerfrei erfolgt und die Beziehung $m = m'$ daher nur im Idealfall gilt. Diese Feststellung liefert die Begründung für die Codierungstheorie.

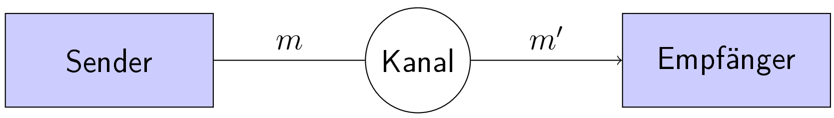

Abbildung 2.1: Gegenstand der Codierungstheorie (nach [4, S. 1])

2.2 Problemstellung und Zielsetzung

3 Lineare fehlerkorrigierende Codes für kryptographische Zwecke

4 Zusammenfassung

Literaturverzeichnis

[1] B. Schneier, *Applied Cryptography: Protocols, Algorithms and Source Code in C*, 20th anniversary edition. Indianapolis, IN: John Wiley und Sons, 2015, ISBN: 978-1-119-09672-6. Adresse: `https://www.schneier.com/books/applied-cryptography-2preface/` (besucht am 06. 11. 2022).

[2] D. J. Bernstein, J. Buchmann und E. Dahmen, Hrsg., *Post-Quantum Cryptography*. Heidelberg: Springer, 2009, ISBN: 978-3-540-88701-0.

[3] V. Cerf, „ASCII format for Network Interchange,“ RFC Editor, RFC 20, Okt. 1969, S. 1–56. DOI: `10.17487/RFC0020`.

[4] W. Willems, *Codierungstheorie und Kryptographie*. Basel: Birkhäuser, 2008. DOI: `10.1007/978-3-7643-8612-2`.