Implementierung des McEliece-Kryptosystems auf P4-programmierbaren Switches

Roman Wetenkamp[1]

Abstract: This is a brief overview of the paper, which should be 70 to 150 words long and include the most relevant points. This has to be a single paragraph.

Keywords: McEliece; Code-basierte Kryptography; Programmierbare Switches

1 Einführung

Seitdem die Aussicht auf einen Quantencomputer, der bisher in der Kryptographie verwendete Probleme wie jenes des *diskreten Logarithmus* oder der *Primfaktorzerlegung* für große Zahlen deutlich effizienter brechen kann als Computer mit herkömmlichen Prozessoren, immer realistischer wird, nimmt die Forschung zur *Post-Quanten-Kryptographie* stetig zu. Neben Verfahren, die auf Gittern oder multivariaten Polynomen basieren, gelten auch einige *code-basierte Verfahren* als quantensicher und sind somit beispielsweise Teil eines Standardisierungsprozesses des National Institute of Standards and Technology (NIST) in den USA [Al22]. Diese Kryptosysteme nutzen lineare, fehlerkorrigierende Codes wie *verallgemeinerte Reed-Solomon-Codes* oder *Goppa-Codes* und deren *Dekodierproblem* aus, das darin besteht, dass es hinreichend schwierig ist, von einem durch eine permutierte und verwürfelte Generatormatrix erzeugten Codewort auf die ursprünglich verwendete Generatormatrix zurückzuschließen [BMT78]. Eines der ersten und bekanntesten code-basierten Kryptosysteme ist jenes von McEliece [Mc78], dessen Implementierung die erste Hauptkomponente dieser Arbeit darstellt.
Die zweite Komponente ergibt sich durch *programmierbare Switches*. Während Verschlüsselungsoperationen von Netzwerkdatenpaketen typischerweise im Endgerät (beispielsweise einem Server oder einem Client) ausgeführt werden, ergibt sich mit programmierbaren Switches eine Möglichkeit, die Daten im Switch zu verschlüsseln.
Diese Arbeit widmet sich der Fragestellung, inwiefern das McEliece-Kryptosystem in programmierbaren Switches implementiert werden kann. Zunächst werden in Abschnitt **??** die Hintergründe beider Technologien erläutert, bevor in Abschnitt **??** die Umsetzung in der Domänen-spezifischen Sprache *P4* erfolgt. Die Ergebnisse werden abschließend anhand einer Switch-Emulation reflektiert und zusammengefasst.

[1] Duale Hochschule Baden-Württemberg Mannheim
s200376@student.dhbw-mannheim.de

Literatur

[Al22] Alagic, G.; Apon, D.; Cooper, D.; Dang, Q.; Dang, T.; Kelsey, J.; Lichtinger, J.; Liu, Y.-K.; Miller, C.; Moody, D.; Peralta, R.; Perlner, R.; Robinson, A.; Smith-Tone, D.: Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process, Bericht, National Institute of Standards und Technology, 2022.

[BMT78] Berlekamp, E.; McEliece, R.; van Tilborg, H.: On the inherent intractability of certain coding problems (Corresp.) IEEE Transactions on Information Theory 24/3, S. 384–386, 1978.

[Mc78] McEliece, R. J.: A Public-Key Cryptosystem Based On Algebraic Coding Theory. The Deep Space Network Progress Report 42-44/, NASA Code 310-10-67-11, 1978, URL: https://ntrs.nasa.gov/api/citations/19780016269/downloads/19780016269.pdf, Stand: 15. 02. 2023.