Das McEliece Kryptosystem basierend auf Codes in der Sum-Rank Metrik

Marina Schiroli

Master thesis in Mathematik

Die meisten aktuell genutzten Kryptosysteme basieren darauf, dass das Faktorisieren von grossen Zahlen oder das Berechnen des diskreten Logarithmus praktisch nicht durchführbar sind. Können Quantencomputer jedoch effizient genutzt werden, so sind die gängigen Verfahren nicht mehr sicher, da diese durch Shor's Algorithmen in polynomialer Zeit gebrochen werden können. Das National Institute of Standards and Technology lancierte 2016 einen Standardisierungsprozess für quantenresistente Public-Key-Kryptoalgorithmen. Unter den Kandidaten der dritten Runde befindet sich ein Kryptosystem, welches auf dem McEliece Kryptosystem basiert.

Dieses Kryptosystem basiert auf linearen Codes in der Hamming-Metrik. Der öffentliche Schlüssel des Kryptosystems ist die öffentliche Generatormatrix $G'=SGP$. Dabei ist S eine invertierbare Matrix, G eine Generatormatrix eines Codes C und P eine Permutationsmatrix.

In “Generic Decoding in the Sum-Rank Meric” von S. Puchinger, J. Renner und J. Rosenkilde wird der erste nicht triviale generische Decodierungsalogorithmus in der Sum-Rank Metrik vorgestellt. Die vorgeschlagene generische Entschlüsselung basiert darauf, dass zuerst ein Support des Fehlers gesucht und der Fehler anschliessend durch die Löschungsdecodierung berechnet wird. Die erwartete Laufzeit des vorgestellten Algorithmus ist exponentiell. Diese Erkenntnis eröffnet die Möglichkeit, Krypotsysteme in der Sum-Rank Metrik zu untersuchen.

Im letzten Teil der Arbeit wird auf diese Möglichkeit eingegangen. Es wird beschrieben, wie das klassische McEliece Kryptosystem verändert werden muss, wenn man neu mit Codes in der Sum-Rank Metrik arbeitet, statt wie üblicherweise in der Hamming Metrik. Dabei wird angenommen, dass eine effizient decodierbare Familie von Sum-Rank Metrik Codes existiert. Es stellt sich heraus, dass die Matrix S wiederum invertierbar sein muss. Bei der Wahl der Matrix P gibt es aufgrund der Sum-Rank Metrik einige Einschränkungen, welche in der Arbeit erläutert werden.

Um einzuschätzen, ob das Kryptosystem interessant für eine tatsächliche Anwendung ist, wird die Komplexität von generischen Decodierungsalgorithmen in den verschiedenen Metriken verglichen.

Prof. Dr. Elisa Gorla und Prof. Dr. Christian Mazza