SEMINAR ZU POST-QUANTEN-KRYPTOGRAFIE

DR. STEPHAN EHLEN

Im Seminar werden Grundlagen zu Gittern und Codes sowie darauf basierender Kryptografie eingeführt. Die Sicherheit der heute weit verbreiteten Public-Key-Kryptografie (z.B. RSA, ElGamal, Diffie-Hellman), ist durch die Entwicklung leistungsfähiger Quantencomputer fundamental bedroht. Weshalb das so ist, wird im Seminar besprochen werden, insbesondere wird auch der Algorithmus von Shor zur Faktorisierung von natürlichen Zahlen behandelt. Die Forschung beschäftigt sich schon seit geraumer Zeit mit der Entwicklung neuer Kryprografieverfahren, die auf Problemen beruhen für die keine effizienten Quantenalgorithmen (und auch keine effizienten klassischen Algorithmen) bekannt sind.

Insbesondere werden wir Algorithmen zum Auffinden von kurzen Vektoren in Gittern, das NTRU-Kryptosystem, Grundlagen zu Codes, das McEliece-Verfahren und je nach Teilnehmerzahl weitere Verfahren, die Kandidaten im NIST-Standardisierungsprozess zu Post-Quanten-Kryptografie sind, behandeln.

1. Vortragsthemen

Die Hauptreferenz für das Seminar ist das Buch von Hoffstein, Pipher und Silverman [HPS08] und alle Kapitelangaben in der Vortragsliste beziehen sich hierauf, falls nicht anders vermerkt. Zur Orientierung und Einordnung sei auch der BSI-Leitfaden "Kryptografie quantensicher gestalten" (siehe `https://bsi.bund.de/dok/997274`)sowie die Website der NIST zum Standardisierungsverfahren von Post-Quanten-Kryptografie (`https://www.nist.gov/pqcrypto`) empfohlen. Die Vorträge können auf Englisch oder Deutsch nach Wahl der Teilnehmenden erfolgen. Die vorläufige Aufteilung der Vorträge sieht wie folgt aus (die endgültige Aufteilung hängt von der Anzahl der Anmeldungen ab und Details können auch nach Interesse aller Teilnehmenden verändert werden):

(1) Einführung in die (Public-Key-)Kryptografie
   - Grundlagen: Kapitel 1.6-1.7
   - Diffie-Hellman und das diskrete Logarithmusproblem: Kapitel 2.2-2.10

(2) RSA
   - Zahlentheoretische Grundlagen: Kapitel 3.1
   - Das RSA-Kryptosystem: Kapitel 3.2
   - Primzahltests: Kapitel 3.4
   - Pollard $p-1$: Kapitel 3.5
   - Weitere Faktorisierungsmethoden und Siebalgorithmen: Kapitel 3.7

(3) Shors Algorithmus zur Primzahlfaktorisierung
   - Originalarbeit: [Sho97]

- Der klassiche Teil soll ausführlich dargestellt werden, der Quanten-Teil wird im folgenden Vortrag behandelt

(4) Einführung in Quantenalgorithmen / Shors Algorithmus II
- Originalarbeit: [Sho97]
- Literatur zu Quantenalgorithmen, z.B.: [NC10]

(5) Gitterbasierte Kryptografie (Einführung)
- Einführung: Kapitel 6.1
- Knapsack-Kryptosysteme (Merkle-Hellman): Kapitel 6.2
- Gitter: Kapitel 6.4

(6) Kurze Vektoren und Babais Algorithmus
- Kapitel 6.5
- Kapitel 6.6

(7) Gitterprobleme
- Ajtai-Dwork: Kapitel 6.7
- GGH: Kapitel 6.8
- "convolution polynomial rings": Kapitel 6.9

(8) NTRU
- Defintion: Kapitel 6.10
- NTRU als gitterbasiertes Kryptosystem: Kapitel 6.11

(9) Gitter-Reduktion
- LLL: Kapitel 6.12
- Anwendungen auf die Kryptoanalyse: Kapitel 6.13
- BKZ

(10) Digitale Signaturen
- RSA digitale Signaturen
- Gitterbasierte Signaturverfahren
- NTRU digitale Signaturen
- Referenz: Kapitel 7

(11) Learning with Errors
- Originalarbeit: [Reg05]

(12) Einführung in Codes
- [Ebe13], Kapitel 1.1-1.3

(13) Das McEliece-Kryptosystem
- Orignalarbeit von R. J. McEliece: [McE78]
- Classic McEliece: `https://classic.mceliece.org`

Bei einigen Themen werden Originalarbeiten als Referenz genannt. Selbstverständlich kann (und sollte) weitere Literatur zu Hilfe genommen werden, diese Liste liefert nur eine grobe Übersicht.

2. Organisatorisches

Die Vorträge sollten ca. 60 Minuten lang sein.

Literatur

[Ebe13] Wolfgang Ebeling. *Lattices and codes*. Advanced Lectures in Mathematics. Springer Spektrum, Wiesbaden, third edition, 2013. A course partially based on lectures by Friedrich Hirzebruch.

[HPS08] Jeffrey Hoffstein, Jill Pipher, and J.H. Silverman. *An Introduction to Mathematical Cryptography*. Springer Publishing Company, Incorporated, 1 edition, 2008.

[McE78] R. J. McEliece. A Public-Key Cryptosystem Based On Algebraic Coding Theory. *Deep Space Network Progress Report*, 44:114–116, January 1978.

[NC10] Michael Nielsen and Isaac Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.

[Reg05] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing*, STOC '05, page 84–93, New York, NY, USA, 2005. Association for Computing Machinery.

[Sho97] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, Oct 1997.