Blockseminar zum Thema Post-Quanten-Kryptografie

Universität des Saarlandes, 23.-26. März 2026

Dr. Andrea Thevis, Prof. Dr. Moritz Weber

Die Sicherheit der heute weit verbreiteten asymmetrischen Kryptografie (z.B. RSA, ElGamal, Diffie-Hellman) ist durch die Entwicklung leistungsfähiger Quantencomputer fundamental bedroht. Die Forschung beschäftigt sich schon seit längerer Zeit mit der Entwicklung von neuen kryptografischen Verfahren, die auf Problemen beruhen, für die keine effizienten Quantenalgorithmen (und auch keine effizienten klassischen Algorithmen) bekannt sind.

In zwei einführenden Vorträgen werde ich einige kryptografische Grundlagen vorstellen und die Notwendigkeit für neue kryptografische Verfahren erklären. Anschließend werden im Seminar Grundlagen zu multivariaten Systemen und Gittern sowie darauf basierende Kryptoverfahren behandelt. Je nach Teilnehmerzahl können auch Grundlagen zu Codes und das McEliece-Verfahren weitere Verfahren vorgestellt werden.

Die Seminarvorträge können auf deutsch oder englisch gehalten werden. Die Literatur ist englischsprachig. Informatikstudierende sind willkommen.

Voraussetzungen: Lineare Algebra 1 und 2 (oder äquivalente Vorlesungen), hilfreich sind Algebra und Elementare Zahlentheorie

Vortragsthemen

Die Hauptreferenzen für das Seminar sind das Buch von Ding, Petzoldt und Schmidt für multivariate Kryptografie [DPS20] sowie das Buch Hoffstein, Pipher und Silverman [HPS08] für gitterbasierte Kryptografie. Zum Einstieg in das Thema Post-Quanten-Kryptografie sind 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) gute Quellen.

Die vorläufige Aufteilung der Vorträge ist unten beschrieben. Die endgültige Aufteilung wird nach der Seminarvorbesprechung festgelegt. Sie hängt von der Anzahl der Anmeldungen ab und Details können auch nach Interesse aller Teilnehmenden verändert werden.

Grundlagen

1. Vortrag: Einführung ins Thema, Andrea Thevis

In diesem Vortrag führe ich in einige Grundlagen der Kryptografie ein. Ich erkläre grundlegende Konzepte wie Verschlüsselung, Signaturen, symmetrische und asymmetrische Kryptografie. Zusätzlich gehe ich auf Algorithmen ein, die in der klassischen Kryptografie verwendet werden, z.B. Diffie-Hellman-Schlüsselaustausch, RSA und Elliptische-Kurven-Kryptografie (ECC).

2. Vortrag: Einführung ins Thema, Andrea Thevis

Dieser Vortrag beschäftigt sich mit der Frage, warum Quantencomputer derzeit verwendete asymmetrische Kryptoalgorithmen bedrohen. Ich stelle einige mathematischer

Probleme vor, auf denen Post-Quanten-Kryptografie (PQC) beruhen. Zusätzlich möchte ich kurz auf die Themen Anwendung von PQC, politische Geschehnisse und den Stand der Migration eingehen.

Bei Interesse können nach Rücksprache ggf. einzelne Aspekte aus den beiden Einführungsvorträgen als Seminarthema vergeben werden. Hier sind Vorträge für MSc, BSc und LS I+II möglich.

Multivariate Kryptografie

3. Vortrag (MSc, BSc, LS I+II):

Grundlagen der multivariaten Kryptografie

Dieser Vortrag soll in die Grundlagen der multivariaten Kryptografie einführen. Zunächst sollen Grundlegende Definitionen und Konstruktionen für asymmetrische multivariate Kryptosysteme erklärt werden (s. [DPS20, Abschnitte 2.1 und 2.2]). Anschließend werden die mathematischen Probleme definiert, auf denen multivariate Kryptosysteme beruhen (s. [DPS20, Abschnitte 2.4]). Schließlich werden Vor- und Nachteile von multivariaten kryptosystemen erklärt (s. [DPS20, Abschnitte 2.5]).

4. Vortrag (MSc, BSc): Matsumoto-Imai-Kryptosystem Teil 1

In diesem Vortrag wird das Matsumoto-Imai Kryptosystem vorgestellt (s. [DPS20, Abschnitt 3.1]). Anschließend wird die Linearisierungsattacke erklärt (s. [DPS20, Abschnitt 3.2]).

5. Vortrag (MSc): Matsumoto-Imai-Kryptosystem Teil 2

In diesem Vortrag werden Verschlüsselungs- und Signaturalgorithmen vorgestellt, die auf dem Matsumoto-Imai-Kryptosystem beruhen. Zusätzlich werden Attacken gegen diese Verfahren vorgestellt (s. [DPS20, Abschnitt 3.3, 3.4]).

6. Vortrag (MSc): Hidden Field Equations (HFE)

In diesem Vortrag werden Kryptosysteme vorgestellt, die auf Hidden Field Equations beruhen (s. [DPS20, Abschnitt 4.1]). Anschließend wird die Sicherheit untersucht (s. [DPS20, Abschnitt 4.2]). Falls Zeit bleibt, kann auf Varianten von HFE eingegangen werden, die sich aus der Sicherheitsanalyse ergeben (s. [DPS20, Abschnitt 4.1]).

7. Vortrag (MSc, BSc nach Rücksprache möglich): Oil and Vinegar (OV)

In diesem Vortrag wird das OV-Kryptosystem vorgestellt und erklärt, warum das Kryptosystem in der „balanced“-Version unsicher ist (Kipnis-Shamir-Attacke). Anschließend wird darauf eingegangen, wie das Sicherheitsproblem mit dem Unbalanced-Oil-Vinegar-Kryptosystem (UOV) umgangen werden kann. (s. [DPS20, Abschnitte 5.1 und 5.2])

Mögliches Thema für Vortrag 8 (MSc, BSc nach Rücksprache möglich): Bei Interesse kann in einem weiteren Vortrag ein aktuelles multivariates Verfahren aus einem der NIST-Prozesse vorgestellt werden. Es würden sich z.B. die Verfahren Rainbow (ein gebrochenes Verfahren) oder MAYO anbieten.

Gitterbasierte Kryptografie

8. Vortrag (MSc, BSc, LS I+II): Einführung in Gitter

In diesem Vortrag werden grundlegende Definitionen und Eigenschaften von Gittern erläutert (s. [HPS08, Abschnitt 6.4]). Anschließend werden Eigenschaften von kurzen Vektoren in Gittern besprochen (s. [HPS08, Abschnitte 6.5]).

9. Vortrag (MSc, BSc, LS I+II): Babais Algorithmus und das GGH-Kryptosystem

In diesem Vortrag werden die Abschnitte 6.6, 6.7 und 6.8 von [HPS08] vorgestellt. Zunächst wird Babais Algorithmus erklärt. Anschließend wird auf Kryptosysteme eingegangen, die auf Gitterproblemen beruhen. Das GGH-Kryptosystem wird im Detail beschrieben. Falls Zeit bleibt, kann auf Nguyens Attacke gegen GGH eingegangen werden.

10. Vortrag (MSc, BSc nach Rücksprache möglich): das NTRU-Kryptosystem

Dieser Vortrag beschäftigt sich NTRU-Kryptosystem. Dazu wird zunächst das Konzept von „convolution polynomial rings“ eingeführt (s. [HPS08, Abschnitt 6.9]). Anschließend wird das Kryptosystem NTRU vorgestellt (s. [HPS08, Abschnitte 6.10 und 6.11]). Der Vortrag benötigt ein gutes Verständnis für Quotientenringe von Polynomringen.

11. Vortrag (MSc, BSc, LS I+II): Gitter-Reduktion

Ziel des Vortrags ist es, Algorithmen zur Gitter-Reduktion vorzustellen, insbes. den LLL-Algorithmus (s. [HPS08, Abschnitt 6.12]). Anschließend wird die Anwendung vom LLL-Algorithmus in der Kryptoanalyse besprochen (s. [HPS08, Abschnitt 6.13]).

12. Vortrag (MSc): gitterbasierte Signaturen

In diesem Vortrag werden gitterbasierte Signaturalgorithmen vorgestellt (s. [HPS08, Kapitel 7]).

Falls Interesse besteht kann ein Vortrag zum Konzept „Learning with errors“ oder zu einem aktuellen gitterbasierten Kryptosystem gehalten werden.

Codebasierte Kryptografie

Bei Interesse können in einem weiteren Themenblock Grundlagen zu Codes und das McEliece-Verfahren vorgestellt werden. Die Literatur wird dann bei Bedarf mit den Teilnehmenden direkt abgestimmt.

13. Vortrag (MSc, BSc, LS I+II): Einführung in Codes

14. Vortrag (MSc, BSc): Das McEliece-Kryptosystem

Referenzen:

[DPS20] J. Ding, A. Petzoldt, D. S. Schmidt, *Multivariate Public Key Cryptosystems.* Springer, 2 edition, 2020.

[HPS08] J. Hoffstein, J. Pipher, J.H. Silverman. *An Introduction to Mathematical Cryptography*. Springer, 1 edition, 2008.