Seminar Komplexität und Kryptologie

Prof. Dr. Johannes Köbler Frank Fuhlbrück

Sommersemester 2022

Mi 13:15–14:45, RUD 26, 1'307

In diesem Seminar werden aktuelle Forschungsthemen der Gebiete Komplexitätstheorie und Kryptografie vorgestellt und diskutiert. Hierbei gehen wir auch gern auf Teilnehmerwünsche ein. Vorkenntnisse aus dem Bereich Komplexitätstheorie und Graphalgorithmen sind hilfreich, aber nicht notwendig. Das Seminar eignet sich gut zur Vorbereitung auf Abschlussarbeiten.

In diesem Semester beginnen wir mit Themen aus der ***Komplexitätstheorie***, zum Ende hin folgen Themen aus der ***Kryptografie***.

Ideen für Referate

Folgende Themen halten wir für geeignet. Wer sich darüber hinaus für weitere Inhalte aus Komplexitätstheorie und Kryptografie interessiert kann gerne selbst ein Thema vorschlagen. Alle Konzepte, die über die jeweiligen Vorlesungen ***Einführung in die Komplexitätstheorie*** und ***Einführung in die Kryptologie*** hinaus gehen, müssen in Vortrag und Ausarbeitung eingeführt werden. Bei Vorträgen zu Signaturen kann auch auf die Master-VL ***Kryptologie*** verwiesen werden, bei Vorträgen zu parametrisierter Komplexität auch auf das Baumweitekapitel aus der Vorlesung ***Graphalgorithmen***. Bitte beachten, dass einige Studierende die jeweils andere VL nicht gehört haben. Es ist also keine schlechte Idee, ca. 1 Woche vor dem Vortrag auf nötige Kenntnisse hinzuweisen.

Komplexität

Parametrisierte Komplexität

1. **Einführung in parametrisierte Komplexität** 1 Vortrag

   Inhalt: In der Parametrisierten Komplexitätstheorie misst man den Aufwand (Zeit oder Platz) nicht nur anhand der Eingabelänge sondern zusätzlich mittels eines strukturellen Parameters. Für Graphen sind z.B. der Maximalgrad oder die Baumweite sinnvolle Parameter.

   Literatur: [DF13, Kapitel 2; Nie06, Kapitel 1 und 3]

2. **Cliquen- und Rangweite** ≥ 1 Vortrag

   Inhalt: Für die Baumweite ist mittlerweile die parametrisierte Komplexität weitreichend erforscht, für viele bekannte Probleme existieren sog. FPT-Algorithmen. Graphen mit beschränkter Baumweite sind allerdings immer dünn (nur $O(n)$ Kanten), sodass Parameter wie die Cliquenweite (äquivalent dazu die Rangweite) betrachtet werden. Interessant sind auch Parameter die ebenfalls dichte Graphen ermöglichen, aber restriktiver sind.

   Literatur: aktuell z.B. [CGR20], siehe https://arxiv.org/abs/2001.08122

3. **parametrisierte Platzkomplexität** ≥ 1 Vortrag

   Inhalt: Parametrisierte Zeitkomplexität (insbesondere FPT, W[1], W[P]) steht im Fokus. Aber auch parametrisierte Platzkomplexität wird erforscht. Grundsätzlich lässt sich zu jeder Klasse $\mathcal{C}$ eine parametrisierte Klasse para-$\mathcal{C}$ definieren.

   Literatur: [EST12], für para-Klassen auch [FG06]

Metakomplexität Metakomplexität betrachtet die Komplexität von Problemen, bei denen eine Funktion/Sprache o.ä. gegeben ist und gefragt wird, ob ein Schaltkreis/Maschine etc. mit bestimmten Einschränkungen existiert.

4. **Minimum Circuit Size Problem (MCSP)** ≥ 1 Vortrag

   Inhalt: Das Minimum Circuit Size Problem geht von einer als Wahrheitstabelle gegeben booleschen Funktion und einer Binärzahl aus. Die Frage ist, ob ein Schaltkreis existiert, dessen Größe durch die gegebene Zahl begrenzt ist.

   Dieses Problem ist ein bekannter Kandidat für Probleme zwischen P und NP.

   Literatur: [KC00]

5. **zeitbeschränkte Kolmogorov-Komplexität (MKTP)** ≥ 1 Vortrag

   Inhalt: Kolmogorov-Komplexität eines Wortes gibt (bezogen auf eine fixierte universelle Turingmaschine) die Länge der kürzesten Eingabe an, bei der dieses Wort als Ausgabe generiert wird. Man kann dieses Maß auf verschiedene Weise mit Zeitschranken kombinieren.

   Literatur: [ABK+06]

6. **Verhältnis zu Graphisomorphie und dem diskreten Logarithmusproblem** ≥ 2 Vorträge

   Inhalt: Beide Probleme sind ebenfalls Kandidaten für Probleme, die weder in P noch NP-schwer sind. Hier ist die komplexitätstheoretische Beziehung zwischen diesen und den Metaproblemen oben von Interesse.

   Literatur: [ABK+06; AGV+18; Rud17]

Graphisomorphie

7. **Isomorphie eingeschränkt durch Listen** ≥ 1 Vortrag

   Inhalt: 1981 betrachtete Anna Lubiw Varianten des Graphisomorphieproblems, die NP-schwer sind, darunter ein Problem, bei dem eine Liste $l(v) \in V(H)$ möglicher Bilder für jeden Knoten $v \in V(G)$ vorgegeben ist, sodass jeder Isomorphismus $\phi\colon V(G) \to V(H)$ die Bedingung $\phi(v) \in l(v)$ einhalten muss.

   Das Thema beschäftigt sich mit dem alten Resultat und neuen Resultaten für eingeschränkte Graphklassen. Bei 2 Vorträgen ist Zusammenarbeit angebracht, Aufteilung muss abgesprochen werden.

   Literatur: [Lub81; KKZ21]

Kryptografie

AES und andere klassische symmetrische Verfahren

8. **Schwächen des AES-Key-Schedule** 1 Vortrag

   Inhalt: Der AES-Key-Schedule leitet die Rundenschlüssel aus dem externen AES-Schlüssel ab. Dabei hängt die Sicherheit von AES davon ab, dass die Rundenschlüssel untereinander keine leicht erkennbaren Abhängigkeiten aufweisen, insbesondere keine linearen Zusammenhänge.

   Das hier zu betrachtende Paper stellt den Key-Schedule anders dar, woraus sich Zusammenhänge ableiteten lassen, die in der üblichen Darstellung nicht erkennbar sind.

   Literatur: [LP21]

9. **Cache-basierte Seitenkanalattacken auf die AES-S-Box** ≥ 1 Vortrag

   Inhalt: Die AES S-Box basiert auf Invertierung im endlichen Körper $\mathbb{F}_{2^8}$. Da dies eine recht teure Operation ist (die auch unterschiedlich viel Zeit je nach Eingabe braucht) wird die S-Box üblicherweise als Lookup-Tabelle realisiert.

   In diesem Thema sollen Methoden betrachtet werden, wie sich bei Kenntnis der Zugriffsmuster auf diese Lookup-Tabelle der Schlüssel berechnen lässt (mit ggf. adaptiv gewählten Klartexten).

   Im angegebenen Artikel wird bereits eine relativ robuste Implementierung angegriffen. Das Thema kann in zwei Vorträge geteilt werden, wo auch zunächst ältere Implementierungen und deren Schwächen betrachtet werden.

   Literatur: [RVM+20]

10. **Yoyo-Attacken auf SPNs** ≥ 1 Vorträge

    Inhalt: In der Einführung in die Kryptologie werden bereits die lineare und differentielle Kryptoanalyse als Angriffe auf Substitutions-Permutations-Netzwerke betrachtet. Yoyo-Attacken unterscheiden sich dadurch, dass Klartext-Kryptotextpaare mit bestimmten Eigenschaften in mehreren Durchläufen in beide Richtungen erzeugt werden.

    Das Thema kann so geteilt werden, dass erst die allgemeine Funktionsweise erläutert wird und in einem zweiten Teil Attacken auf rundenreduzierte Varianten von AES betrachtet werden.

    Literatur: [RBH17]

RSA

11. **RSA-Schlüsselgenerierung durch mehrere Parteien** ≥ 1 Vortrag

    Inhalt: Ziel ist, einen RSA-Modul $n = pq$ so mit mehreren Parteien zu generieren, dass ein gewisser Anteil an Parteien nötig ist, um den Modul zu faktorisieren.

    Es gibt zu diesem Thema bereits mehrere Resultate. Es kann sowohl der aktuelle Artikel als auch stattdessen ältere (einfachere) Verfahren vorgestellt werden.

    Literatur: [CDK+22]

Elektronisches (Bar)geld

12. **E-Cash** ≥ 1 Vortrag

    Inhalt: Elektronisches Bargeld beschreibt eine Form von digitalem Geld, das offline, also ohne Kontakt zu einer Zentralbank oder eines verteilten Systems (Blockchain/distributed Ledger) weitergegeben werden kann. Dabei darf eine Zentralbank grundsätzlich existieren.

    Basierend auf dem angegebenen Artikel kann hier der aktuelle Stand kurz wiedergegeben und eines der Systeme (nicht notwendig das aus dem Artikel) im Detail besprochen werden.

    Das Thema kann in einen Übersichts- und Detailvortrag geteilt werden, zudem ist eine Übersicht zu Blockchain-Währungen als Kontrast möglich.

    Literatur: [BFQ21]

Postquantenkryptografie

13. **Was bedeutet »Postquantenkryptografie«** ≤ 1 Vortrag

    Inhalt: Kurze Einführung in den Begriff, grobe Skizze von Shors Algorithmus und dessen Leistungsfähigkeit und Voraussetzungen (z.B. Anzahl Qubits). Eine allgemeine Einführung in Quanteninformation erfolgt nicht.

    Literatur: nach Bedarf

14. **McEliece-Kryptosystem** ≥ 2 Vorträge

    Inhalt: Das McEliece-Kryptosystem ist ein Code-basiertes System. Da die Grundlagen dazu bisher nicht in VL des Lehrstuhls abgedeckt sind, beinhaltet das Thema eine Einführung in Codes und speziell binäre Goppa-Codes, das klassische Verfahren von McEliece sowie Neuerungen im aktuellen 3.-Runde-Kandidaten für den NIST- Wettbewerb Postquantenkryptografie.

    Literatur: [McE78], https://classic.mceliece.org/nist.html

15. **Das NTRU-Kryptosystem** ≥ 1 Vortrag

    Inhalt: Das NTRU-Kryptosystem ist gitterbasiert. Ob eine formalere Behandlung von Gittern im Allgemeinen nötig ist, hängt vom Interesse ab, für die Sicherheit (z.B. [SS11]) ist das zwingend erforderlich, für die Korrektheit nicht. Auch hier soll kurz auf Unterschiede zwischen dem klassischen Algorithmus und dem NIST-Kandidaten eingegangen werden.

    Literatur: [HPS98; SS11], https://ntru.org/index.shtml

    Die anderen beiden gitterbasierten NIST-Kandidaten (CRYSTALS-KYBER, SABER) können bei Interesse auch besprochen werden.

Ablauf

- Die Auswahl des Themas erfolgt via Moodle. Dort wird es eine Umfrage zu Themenwünschen geben. Bestimmte Einführungsthemen sind allerdings nur sinnvoll, wenn auch jemand ein fortgeschrittenes Thema wählt.
- Im Lauf des Semesters halten Sie **Referate**
  - Die Referate haben das Ziel, dass Sie (a) sich ein Thema erarbeiten, (b) Ihr Thema den anderen vermitteln, (c) von den Referaten der anderen lernen und (d) Vortragspraxis sammeln.
  - Einerseits sollen die Referate ***anschaulich*** sein: Sie führen die anderen in Ihr Thema ein. Bitte setzen Sie dabei nicht mehr voraus, als sie schon wissen. Mit Beispielen und Bildern können Sie Ihren Zuhörern das Verstehen erleichtern. Eine gute Richtschnur für gute Erklärungen ist die Frage »Was hat mir selbst geholfen, das zu verstehen?«
  - Andererseits sollen die Referate auch ***präzise*** sein: Klare Definitionen und die Details von Konstruktionen und Algorithmen gehören auch dazu.
  - Für Ihr Referat stehen Ihnen ca. 90 Minuten zur Verfügung, bei sehr vielen Interessenten wird ein Thema ggf. auf 2 Personen aufgeteilt und der Vortrag dauert nur 45 Minuten. Bitte planen Sie Zeit für Rückfragen ein!
  - Nach jedem Referat gibt es eine Feedbackrunde.
- **Vorbereitung** des eigenen Referats:
  - Sie arbeiten sich in das Thema ein, indem Sie die angegebene (und ggf. weitere) Literatur lesen. Literatur, die es nicht in der Bibliothek oder im Netz gibt, kann bei uns kopiert werden.
  - Vor der Vorbereitung des Vortrags lesen Sie am besten [TWM, Abschnitt 5] – das lohnt sich auch dann, wenn Sie nicht LaTeX verwenden (es geht um die Gestaltung von Folien an sich).
  - Eine Woche vor dem Referat klären Sie mit uns restliche Fragen (z.B. per Zoom). Schicken Sie uns dazu vorab Ihre Folien.
- Es ist ein zentrales Element eines Seminars, auch von den Referaten der anderen zu lernen. Deshalb sollten Sie möglichst immer **anwesend sein**.
- Nach dem Referat fertigen Sie noch eine schriftliche **Ausarbeitung** zum eigenen Thema an.
  - Die Ausarbeitungen haben das Ziel, (a) das im Seminar gesammelte Wissen zusammenzufassen, (b) Interessierten einen Einstieg in das Thema zu ermöglichen und (c) Ihnen die Gelegenheit zu geben, wissenschaftliches Schreiben zu üben (Vorbereitung auf Abschlussarbeiten).
  - Der Umfang der Ausarbeitung soll dem Umfang des Referats entsprechen. Erfahrungsgemäß ergibt das 10–20 Seiten.
  - Hinweise zum wissenschaftlichen Schreiben finden Sie unter [Böt06] und [Mit07].
  - Der **Abgabeschluss** für Ausarbeitungen ist der erste Tag der Vorlesungszeit im folgenden Semester, vsl. der 17.10.2022. Wenn Sie die Bestätigung Ihres abgeschlossenen Seminars schnell brauchen, sollten Sie nicht erst zum neuen Semester abgeben, da die Beurteilung dann entsprechend länger dauert.

Literatur

[ABK+06] Eric Allender, Harry Buhrman, Michal Koucký, Dieter Van Melkebeek und Detlef Ronneburger. »Power from random strings«. In: ***SIAM Journal on Computing*** 35.6 (2006), S. 1467–1493.

[AGV+18] Eric Allender, Joshua A Grochow, Dieter Van Melkebeek, Cristopher Moore und Andrew Morgan. »Minimum circuit size, graph isomorphism, and related problems«. In: ***SIAM Journal on Computing*** 47.4 (2018), S. 1339–1372.

[BFQ21] Balthazar Bauer, Georg Fuchsbauer und Chen Qian. »Transferable e-cash: a cleaner model and the first practical instantiation«. In: ***IACR International Conference on Public-Key Cryptography***. Springer. 2021, S. 559–590.

[Böt06] Martin Böttcher. ***Einführung in das wissenschaftliche Arbeiten***. Universität Leipzig. 2006. URL: http://bis.informatik.uni-leipzig.de/de/Lehre/0506/SS/SemASKE/files?get=einfuehrung_in_das_wiss_arbeiten.pdf (besucht am 9. Okt. 2014).

[CDK+22] Megan Chen, Jack Doerner, Yashvanth Kondi, Eysa Lee, Schuyler Rosefield, Abhi Shelat und Ran Cohen. »Multiparty generation of an RSA modulus«. In: ***Journal of Cryptology*** 35.2 (2022), S. 1–84.

[CGR20] Gennaro Cordasco, Luisa Gargano und Adele A Rescigno. »Iterated Type Partitions«. In: ***International Workshop on Combinatorial Algorithms***. Springer. 2020, S. 195–210.

[DF13] Rodney G. Downey and Michael R. Fellows. ***Fundamentals of parameterized complexity***. London: Springer, 2013. ISBN: 978-1-4471-5558-4.

[EST12] Michael Elberfeld, Christoph Stockhusen und Till Tantau. »On the space complexity of parameterized problems«. In: ***International Symposium on Parameterized and Exact Computation***. Springer. 2012, S. 206–217.

[FG06] Jörg Flum and Martin Grohe. ***Parameterized complexity theory***. Texts in Theoretical Computer Science. An EATCS Series. Springer, 2006. ISBN: 3-540-29952-1.

[HPS98] Jeffrey Hoffstein, Jill Pipher und Joseph H Silverman. »NTRU: A ring-based public key cryptosystem«. In: ***International algorithmic number theory symposium***. Springer. 1998, S. 267–288.

[KC00] Valentine Kabanets und Jin-Yi Cai. »Circuit minimization problem«. In: ***Proceedings of the thirty-second annual ACM symposium on Theory of computing***. 2000, S. 73–79.

[KKZ21] Pavel Klavík, Dušan Knop und Peter Zeman. »Graph isomorphism restricted by lists«. In: ***Theoretical Computer Science*** 860 (2021), S. 51–71.

[LP21] Gaëtan Leurent und Clara Pernot. »New representations of the AES key schedule«. In: ***Annual International Conference on the Theory and Applications of Cryptographic Techniques***. Springer. 2021, S. 54–84.

[Lub81] Anna Lubiw. »Some NP-complete problems similar to graph isomorphism«. In: ***SIAM Journal on Computing*** 10.1 (1981), S. 11–21.

[McE78] Robert J McEliece. »A public-key cryptosystem based on algebraic«. In: ***Coding Thv*** 4244 (1978), S. 114–116.

[Mit07] Roland Mittermair. ***Hinweise für korrektes Zitieren***. Institut für Informatik-Systeme, Universität Klagenfurt. 2007. URL: http://www.uni-klu.ac.at/tewi/downloads/Zitierhinweise.pdf (besucht am 9. Okt. 2014).

[Nie06] Rolf Niedermeier. ***Invitation to fixed-parameter algorithms***. Oxford University Press, 2006. ISBN: 0-19-856607-7.

[RBH17] Sondre Rønjom, Navid Ghaedi Bardeh und Tor Helleseth. »Yoyo tricks with AES«. In: ***International Conference on the Theory and Application of Cryptology and Information Security***. Springer. 2017, S. 217–243.

[Rud17] Michael Rudow. »Discrete logarithm and minimum circuit size«. In: ***Information Processing Letters*** 128 (2017), S. 1–4.

[RVM+20] Bholanath Roy, M Venkatesh, Bernard L Menezes u. a. »"S-Box" Implementation of AES Is Not Side Channel Resistant«. In: ***Journal of Hardware and Systems Security*** 4.2 (2020), S. 86–97.

[SS11] Damien Stehlé und Ron Steinfeld. »Making NTRU as secure as worst-case problems over ideal lattices«. In: ***Annual international conference on the theory and applications of cryptographic techniques***. Springer. 2011, S. 27–47.

[TWM] Till Tantau, Joseph Wright, and Vedran Miletić. ***The* beamer *class***. URL: http://mirror.ctan.org/macros/latex/contrib/beamer/doc/beameruserguide.pdf.