Karlsruhe Institute of Technology

Gitter und Gitterbasierte Kryptographie

Seminar im Wintersemester 2015/16

Die Vorträge mit Schwerpunkt Mathematik sind mit „(M)“ markiert, die mit Schwerpunkt Informatik mit „(I)“. Wenn es verstärktes Interesse an einzelnen, umfangreicheren Vorträgen gibt, können diese auch aufgeteilt werden.

Teil 1: Grundlagen und einfache Kryptoprimitive

Vortrag 1: Grundlagen zu Gittern (M). Es werden Gitter eingeführt und charakterisiert, und die Grundmasche eines Gitters eingeführt. Des weiteren wird der Minkowski'sche Gitterpunktsatz gezeigt und auf dessen Anwendung in der gitterbasierten Kryptographie eingegangen. Außerdem soll hier das zu einem Gitter duale Gitter definiert werden.
Literatur: [Neu92, Kap. 1, §4], [MG02, Kap. 1, Abschn. 1], (evtl. [Sch13, Abschn. 2.1, 2.3]).
2015-10-26

Vortrag 2: Grundlagen Kryptographie (I). Es wird zunächst auf die Komplexität von Such- und Entscheidungsproblemen eingegangen und dabei die Komplexitätsklassen P und NP motiviert. Es soll anschaulich werden, auf welcher Art von Annahmen kryptographische Primitive und Reduktionen basieren. Familien von Einweg- und kollisionsresistenten Hashfunktionen, sowie asymmetrische Verschlüsselungssysteme werden definiert und veranschaulicht. Des weiteren wird geklärt, welchen Einfluss die Existenz von skalierbaren Quantencomputern auf die aktuell existierenden kryptographischen Systeme hätte.
Literatur: [KL07; Gol01], [HR14; Hof13]. **2015-11-02**

Vortrag 3: Schwierigkeit von Gitter-Problemen (M/I). Hier sollen die Problemstellungen SVP („Shortest Vector Problem“), SIVP („Shortest Independent Vectors Problem“), GapSVP und BDD („Bounded Distance Decoding“) eingeführt und motiviert werden. Bei SVP_γ zum Approximationsfaktor γ handelt es sich beispielsweise um das Problem, gegeben eine Basis $\boldsymbol{B}$ eines n-dimensionalen Gitters $\mathcal{L}$, einen von Null verschiedenen Vektor $\boldsymbol{v} \in \mathcal{L}$ zu finden, dessen Norm höchstens um einen Faktor von der Länge des kürzesten Gittervektors abweicht. Hier wird auch auf die Rundungsmethode von Babai und dessen Güte eingegangen. Um die Probleme genauer zu verstehen, kann der Vortrag durch eine Reduktion zwischen den Gitterproblemen oder durch ein NP-Schwierigkeitsresultat für bestimmte Approximationsfaktoren angereichert werden.
Literatur: [MG02, Ch. 3, 4]. **2015-11-09**

Vortrag 4: Gitterreduktionen: Der LLL-Algorithmus (M/I). Um einen (von Null verschiedenen) Gitterpunkt mit kleiner Norm, bzw. eine kurze Gitterbasis zu finden, ist man (bisher) für hohe Dimensionen auf einen Approximationsalgorithmus angewiesen. Um die Schwierigkeit des Problems nachzuvollziehen, beschäftigen wir uns in diesem Vortrag mit dem bekanntesten Algorithmus zur Reduktion von Gitterbasen, den LLL-Algoritmus, benannt nach den Erfindern H. Lenstra, A. Lenstra und Lovász. Dessen Laufzeit hängt polynomiell von der Gitterdimension ab und findet eine Basis, deren Länge von der minimal möglichen Länge um einen Faktor abweicht, der nur schwach subexponentiell ($2^{\Theta(n \log\log n/\log n)}$) in der Dimension ist. Der Algorithmus hat vielfältige Anwendungen, die weit über das Feld der Kryptographie hinausgehen.
Literatur: [Sch13, Kap. 3, 4], [NV10]. **2015-11-16**

Vortrag 5: Das GGH-Kryptosystem (I). Das Verschlüsselungsverfahren von Goldreich, Goldwasser und Halevi (GGH) ist der Vorläufer für beweisbar sichere Kryptosysteme, die auf Gitter-Falltüren basieren. Dies sind Systeme, die ausnutzen, dass bestimmte Gitterprobleme leicht sind, wenn man eine „kurze“ Basis kennt (der geheime Schlüssel), aber schwer mit einer „schlechten“ Gitterbasis (der öffentliche Schlüssel). Das GGH-Verfahren soll in seiner Grundidee vorgestellt werden. Ein Angriff von Nguyen [Ngu99] zeigt, dass jedes Chiffrat Informationen über den Klartext preisgibt und das für niedrige Dimensionen der Klartext sogar vollständig zurückgewonnen werden kann.
Literatur: [GGH97; Ngu99]. **2015-11-23**

Vortrag 6: Das SIS- und das LWE-Problem (I). Einer der Hauptvorteile von gitterbasierter Kryptographie ist, dass man kryptographische Primitive konstruieren kann, die auf der „worst-case“-Schwierigkeit von bestimmten Gitterproblemen beruhen. Hat man wie üblich nur die Annahme, dass ein bestimmtes Problem „durchschnittlich“ schwierig ist, muss man darauf achten, dass das Ziehen, z.B. eines öffentlichen Schlüssels nicht durch die geforderte Existenz eines geheimen Schlüssels, eher „leichte“ Probleminstanzen ausgibt. Im Vortrag soll das SIS („Short Integer Solution“) und LWE („Learning with Errors“)-Problem eingeführt und eine Reduktion der „average-case“-Problemstellung SIS auf SIVP im „worst-case“ gezeigt werden. Da sich aus SIS sehr direkt eine kollisionsresistente Hashfunktion konstruieren lässt, soll dies hier als anschauliches Beispiel dienen.
Literatur: [MR04], [Pei15, Abschn. 4.1]. **2015-11-30**

Vortrag 7: Auf SIS und LWE basierende Kryptosysteme (I). In diesem Vortrag geht es um fortgeschrittenere Konstruktionen z.B. von digitalen Signaturen, die auf sogenannten Gitter-Falltüren beruhen. Diese erlauben uns, wie im GGH-Schema von Vortrag 5, mit einem zusätzlichen Geheimnis (eine kurzen Gitterbasis) gewisse Probleme effizient zu lösen, was ohne dieses Geheimnis nicht möglich wäre. Hier werden wir uns auch mit diskreten Gaußverteilungen über Gittern beschäftigen, die uns erlauben, passende schwierige Instanzen zu erstellen.
Literatur: [GPV08], [Pei15, Abschn. 5.4]. **2015-12-07**

Teil 2: Idealgitter und effizientere Kryptoprimitive

Vortrag 8: Grundlagen algebraischer Zahlkörper (M). Hier werden die im Folgenden notwendigen Grundlagen algebraischer Zahlkörper erläutert. Es wird die Ganzheit algebraischer Zahlen und Ringerweiterungen eingeführt, und an Beispielen erläutert. Im Zentrum steht der Ring der ganzen Zahlen eines algebraischen Zahlkörpers und dessen Eigenschaft ein Dedekindring zu sein. Des weiteren werden ganze und gebrochene Ideale thematisiert.
Literatur: [Neu92, Kap. 1, §1–3]. **2015-12-14**

Vortrag 9: Minkowski-Theorie, Einbettungen (M). Ein algebraischer Zahlkörper lässt sich kanonisch in den sogenannten Minkowski-Raum $K_{\mathbb{R}}$ ($\cong \mathbb{R}^n$, für Körpergrad n) einbetten. Wenn wir über diese kanonische Abbildung ein nichttriviales Ideal des Ganzheitsrings einbetten, so bildet dies ein Gitter von Dimension n in $K_{\mathbb{R}}$. Da „Ideal-"Gitter dieser Art dank ihrer zusätzlichen Struktur für uns wichtig sind, werden wir dessen Eigenschaften genauer unter die Lupe nehmen.
Literatur: [Neu92, Kap. 1, §5]. **2015-12-21**

Vortrag 10: Kreisteilungskörper (M). In diesem Vortrag sollen die wichtigsten Eigenschaften über Kreisteilungskörper besprochen werden. Der $n$te Kreisteilungskörper ist gegeben als $\mathbb{Q}(\zeta_n) \cong \mathbb{Q}[X]/(\Phi_n(X))$, wobei ζ_n eine primitive $n$te Einheitswurzel, bzw. $\Phi_n(X)$ das $n$te Kreisteilungspolynom ist. Hauptinhalt des Vortrags ist die Bestimmung der ganzen Zahlen von $\mathbb{Q}(\zeta_n)$. Darüber hinaus könnte noch ein Zerlegungsgesetz von allgemeinen Kreisteilungskörpern in ein Tensorprodukt von Kreisteilungskörpern von Primpotenz-Ordnung eine Rolle spielen.
Literatur: [Neu92, Kap. 1, §§8, 10], [LPR13]. **2016-01-11**

Vortrag 11: Das Ring-SIS/LWE-Problem, mit Reduktion (I). Hier sollen die auf Idealgittern basierenden Varianten von SIS und LWE vorgestellt und mit den ursprünglichen Problemen in Beziehung gesetzt werden. An Hand eines konkreten Beispiels, z.B. dem digitalen Signaturverfahren aus Vortrag 7, soll die verbesserte Effizienz von Idealgittern aufgezeigt werden. Falls noch Zeit ist, könnte hier auch eine „average-case"-zu-„worst-case"-Reduktion, analog zu der aus Vortrag 6, über Idealgittern vorgestellt werden.
Literatur: [LPR13; Pei15]. **2016-01-18**

Vortrag 12: Der Dirichletsche Einheitensatz (M). Hier soll es um den Dirichletschen Einheitensatz gehen, einer wichtigen Folgerung aus der Minkowski-Theorie.
Literatur: [Neu92, Kap. 1, §7]. **2016-01-25**

Vortrag 13: Ein Angriff auf spezielle Idealgitter (M). Kürzlich wurde ein Angriff auf bestimmte Kryptosysteme veröffentlicht, die auf Idealgittern über speziellen Kreisteilungskörpern basieren, der hier vorgestellt werden könnte.
Literatur: [Cra+15; Oku+15]. **2016-02-08**

Vortrag 14: Kryptographische Primitive mit (Ring-)LWE (I). In diesem Vortrag geht es um fortgeschrittenere, auf (Ring-)LWE basierende Primitive. Hier gibt es ein bisschen Spielraum in der Ausgestaltung, so können z.B. aktiv-sichere oder vollhomomorphe Verschlüsselungsverfahren, identitätsbasierte Verschlüsselungsverfahren, oder multilineare Abbildungen vorgestellt werden. Ergänzung: Es wurde das aktiv-sichere Verschlüsselungssystem von [Pei09] vorgestellt.
Literatur: [Pei15; Pei09]. **2016-02-01**

Literatur

[Cra+15] Ronald Cramer, Léo Ducas, Chris Peikert und Oded Regev. „Recovering Short Generators of Principal Ideals in Cyclotomic Rings“. In: *IACR Cryptology ePrint Archive* (2015). URL: http://eprint.iacr.org/2015/313.

[GGH97] Oded Goldreich, Shafi Goldwasser und Shai Halevi. „Public-Key Cryptosystems from Lattice Reduction Problems“. In: *Advances in Cryptology – CRYPTO '97, Proceedings*. Hrsg. von Burton S. Kaliski Jr. Bd. 1294. Lecture Notes in Computer Science. Springer, 1997, S. 112–131. DOI: 10.1007/BFb0052231.

[Gol01] Oded Goldreich. *The Foundations of Cryptography – Volume 1, Basic Techniques*. Cambridge University Press, 2001.

[GPV08] Craig Gentry, Chris Peikert und Vinod Vaikuntanathan. „Trapdoors for hard lattices and new cryptographic constructions“. In: *Proceedings of the 40th Annual ACM Symposium on Theory of Computing*. Hrsg. von Cynthia Dwork. ACM, 2008, S. 197–206. DOI: 10.1145/1374376.1374407.

[Hof13] Dennis Hofheinz. *Komplexitätstheorie mit Anwendungen in der Kryptographie. Vorlesungsskript*. 2013. URL: https://crypto.iti.kit.edu/fileadmin/User/Hofheinz/Teaching/cct.pdf.

[HR14] Dennis Hofheinz und Andy Rupp. *Beweisbar sichere Kryptographie. Vorlesungsskript*. 2014. URL: https://crypto.iti.kit.edu/fileadmin/User/Rupp/bsk.pdf.

[KL07] Jonathan Katz und Yehuda Lindell. *Introduction to Modern Cryptography*. Chapman und Hall/CRC Press, 2007.

[LPR13] Vadim Lyubashevsky, Chris Peikert und Oded Regev. „A Toolkit for Ring-LWE Cryptography“. In: *Advances in Cryptology – EUROCRYPT 2013, Proceedings*. Hrsg. von Thomas Johansson und Phong Q. Nguyen. Bd. 7881. Lecture Notes in Computer Science. Springer, 2013, S. 35–54. DOI: 10.1007/978-3-642-38348-9_3.

[MG02] Daniele Micciancio und Shafi Goldwasser. *Complexity of Lattice Problems: a cryptographic perspective*. Bd. 671. The Kluwer International Series in Engineering and Computer Science. Boston, Massachusetts: Kluwer Academic Publishers, 2002.

[MR04] Daniele Micciancio und Oded Regev. „Worst-Case to Average-Case Reductions Based on Gaussian Measures“. In: *45th Symposium on Foundations of Computer Science (FOCS 2004), Proceedings*. IEEE Computer Society, 2004, S. 372–381. DOI: 10.1109/FOCS.2004.72.

[Neu92] Jürgen Neukirch. *Algebraische Zahlentheorie*. Springer Berlin Heidelberg, 1992.

[Ngu99] Phong Q. Nguyen. „Cryptanalysis of the Goldreich-Goldwasser-Halevi Cryptosystem from Crypto '97". In: *Advances in Cryptology – CRYPTO '99, Proceedings*. Hrsg. von Michael J. Wiener. Bd. 1666. Lecture Notes in Computer Science. Springer, 1999, S. 288–304. DOI: 10.1007/3-540-48405-1_18.

[NV10] Phong Q. Nguyen und Brigitte Vallée, Hrsg. *The LLL Algorithm – Survey and Applications*. Information Security and Cryptography. Springer, 2010. DOI: 10.1007/978-3-642-02295-1.

[Oku+15] Shinya Okumura, Shingo Sugiyama, Masaya Yasuda und Tsuyoshi Takagi. „Security Analysis of Cryptosystems Using Short Generators over Ideal Lattices". In: *IACR Cryptology ePrint Archive* (2015). URL: http://eprint.iacr.org/2015/1004.

[Pei09] Chris Peikert. „Public-key cryptosystems from the worst-case shortest vector problem: extended abstract". In: *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009*. Hrsg. von Michael Mitzenmacher. ACM, 2009, S. 333–342. DOI: 10.1145/1536414.1536461.

[Pei15] Chris Peikert. „A Decade of Lattice Cryptography". In: *IACR Cryptology ePrint Archive* (2015). URL: http://eprint.iacr.org/2015/939.

[Sch13] Claus P. Schnorr. *Gitter und Kryptographie. Vorlesungsskript*. 2013. URL: http://www.math.uni-frankfurt.de/~dmst/teaching/SS2014/Vorlesung/vorlesung.html.