Seminar on Lattice-based Cryptography

Organizers: Thomas Aulbach, Samed Düzlü, Prof. Dr. Juliane Krämer, Oscar Lapointe, Dr. Michael Meyer, Dr. Patrick Struck

FIDS - Chair of Data Security and Cryptography

Version 1.1

Abstract

In this seminar, we give an introduction to lattice-based cryptography, which is one of the most promising foundations for future cryptographic schemes.

In [Sho94], Shor showed how quantum computers can be used to efficiently compute the prime factorization of large numbers; a problem which to date seems inaccessible to classical computers. Hence, current cryptographic algorithms may be subject to attacks by quantum computers. This opens the question, whether it is possible to define cryptographic protocols that resist attacks by quantum computers. This branch of research is called *post-quantum cryptography.*

There are few foundational primitives on which post-quantum cryptography is based; hash functions, isogenies of supersingular elliptic curves, multivariate polynomial functions of degree 2, linear codes, and lattices. In this seminar, we focus on *lattice-based cryptography.*

First, we introduce the background from cryptography and quantum computing, and develop the mathematical foundations of the theory of lattices. We introduce the computational problems on which the protocols are grounded. Afterwards, we analyze lattice-based key encapsulation mechanism and signature schemes with concrete examples of the currently most popular lattice-based protocols. The security of cryptographic protocols can be attacked via physical tools. We will discuss such attacks in the case of lattice-based cryptography.

Examination. The speakers are required to prepare a detailed report of their talk, which is due two weeks after the last talk. An initial draft is supposed to be prepared and discussed with the advisor a week before the talk.

Distribution of the topics. Please contact Samed Düzlü ~~until the 30th of August with at least 3 topics you would be interested to present~~ in case you would like to present one of the remaining topics.

Prerequisites. All talks require a basic understanding of (linear) algebra. Further prerequisites are listed for the talks below.

Literature. We give hints to literature that may be helpful for preparing the talks. Contact us, if you do not have access to relevant sources. You may use other sources.

Master thesis. If the seminar topics arouse your interest and you would like to write your master thesis in lattice-based cryptography (or in another area of post-quantum cryptography), we are happy to develop an interesting topic for you.

Remark. Feel free to attend the talks if you are interested, even if you do not participate actively by giving a talk.

1 Public-Key Cryptography

Advisor. Patrick Struck
Date. 18 October 2022

This talk gives a basic introduction in public-key cryptography, which is the cryptographic foundation of the constructions of the later talks.

Content. Recall the definition of public-key encryption (PKE), key encapsulation mechanism (KEM), key exchange, and digital signatures. Define the relevant security notions for these cryptographic primitives. Describe the Rabin encryption scheme and present the reduction from prime factorization to breaking the Rabin encryption.

Literature.

[KL20] Katz and Lindell. *Introduction to modern cryptography.*

[Bin+] Bindel et al. “Hybrid key encapsulation mechanisms and authenticated key exchange”.

[Rot] Rothe. *Rabin’s Public-Key Cryptosystem.*

2 Quantum Computing and Shor’s Algorithm

Advisor. Patrick Struck
Date. 8 November 2022

Quantum computers and the application of Shor’s algorithms is the main motivation for post-quantum cryptography. This talk gives a basic introduction to the theory of quantum computing and discusses Shor’s algorithm to motivate the later talks. Moreover, reductions in post-quantum cryptography sometimes make use of quantum computation, which we will see in a later talk.

Content. Present the basics of quantum computers. Specifically, discuss the notions superposition, entanglement, and measurement. Present either the quantum period finding algorithm by Shor, or the classical reduction from factoring to period finding. Present the basic idea of the other result.

Literature.

[Sho94] Shor. “Algorithms for quantum computation: discrete logarithms and factoring”.

[Aar] Aaronson. *Introduction to Quantum Information Science Lecture Notes.*

[NC] Nielsen and Chuang. *Quantum computation and quantum information.*

[Wal] Wallach. *Quantum computing and entanglement for mathematicians.*

3 Introduction to Lattice Theory

Advisor. Oscar Lapointe
Date. 15 November 2022

The objects of lattice-based cryptography are discrete subgroups of a finite-dimensional Euclidean vector space, in other words, lattices. This talk sets up the foundations: the basic definitions, main examples, and first properties. The focus lies the theory necessary to develop the computational problems required in the cryptographic applications.

Content. Define lattices as discrete subgroups of (finite-dimensional) Euclidean spaces, and sketch characterizations, in particular, that a lattice admits a basis representation. Our focus lies on full rank lattices. Introduce the determinant of a lattice and the fundamental parallelogram, and show their relationship. Discuss examples, such as unimodular lattices, q-ary lattices, and dual lattices. Define (successive) minima of a lattice. Recall the Gram-Schmidt process and describe the connection to determinants and minima of a lattice. Prove the first Minkowski Theorem and state and sketch the second Minkowski Theorem. State the *shortest vector problem* (SVP) and describe the relation to Minkowski's Theorem.

Literature.

[MG02] Micciancio and Goldwasser. *Complexity of lattice problems.*

[Lan21] Lange. *Video Lectures on Lattice-based Cryptography.* – for brief introduction.

Prerequisites. A background on analysis and algebra is helpful.

4 NP-completeness of SVP

Advisor. Samed Düzlü
Date. 22 November 2022
Speaker. L. K.

SVP is one of the basic problems used in lattice-based cryptography. Another important problem is the *closest vector problem* (CVP). Solving CVP and SVP exactly is a highly difficult problem, more precisely, these problems are NP-complete. These complexity theoretic results will be discussed in this talk. In the next talk, algorithms for approximative solutions for SVP will be presented, when the approximation factor is large enough.

Content. Define the search and decision versions of CVP and SVP. Follow [MG02, Chapter 3] and discuss the equivalence of the search and decision versions of CVP, its NP-completeness and the relationship between CVP and SVP.

Literature.

[MG02] Micciancio and Goldwasser. *Complexity of lattice problems.*

Prerequisites. Some background in complexity theory will be helpful.

5 Lattice Reduction Techniques and Concrete Hardness of SVP and CVP

Advisor. Juliane Krämer
Date. 29 November 2022
Speaker. D. K.

In lattice-based cryptography, the security of the protocols is based on the hardness of (approximate) SVP or CVP. Therefore, it is an important task to understand the concrete difficulty of these problems depending on approximation factors. We will discuss one of the main algorithms, the LLL algorithm. There are extensions of the LLL algorithm, the BKZ algorithm and BKW algorithm. These algorithms output a *good* basis for a given lattice, which can be used to compute short/close vectors. The two approaches for the latter step are via enumeration and sieving, which are discussed in this talk.

Content. Recall SVP and CVP. Present the block reduction of a lattice to achieve a good basis, specifically, discuss the LLL algorithm. Explain the basic ideas of enumeration and sieving algorithms for solving SVP and CVP. List different variants of enumeration and sieving algorithms and state the quality of their result and their complexity. Present the pruning technique to make enumeration faster in practice.

Literature.

[Mic12] Micciancio. *Lattice Algorithms and Applications - The LLL Algorithm.*

[HPS11] Hanrot, Pujol, and Stehlé. "Algorithms for the Shortest and Closest Lattice Vector Problems".

[Vou11] Voulgaris. *Algorithms for the closest and shortest vector problems on general lattices.*

[GNR10] Gama, Nguyen, and Regev. "Lattice Enumeration Using Extreme Pruning".

[LMV] Laarhoven, Mosca, and Van De Pol. "Finding shortest lattice vectors faster using quantum search". – especially Table 1

6 Discrete Gaussians and Smoothing Parameter

Advisor. Michael Meyer
Date. 6 December 2022

In lattice-based schemes, we often need to sample random error vectors. This is usually done via sampling from a discrete Gaussian distribution. Smoothing parameters are a tool for such sampling methods in order to prove a close-to-uniform distribution of the output.

Content. Introduce Gaussians and discrete Gaussians as in [MR07], and sketch a sampling method for discrete Gaussians from [Pre15]. Follow [MR07] and introduce smoothing parameters. Explain and motivate the results from Section 4 of [MR07], in order to set the scene for the worst-case to average-case reduction in Talk 8.

Literature.

[Pre15] Prest. "Gaussian sampling in lattice-based cryptography".

[MR07] Micciancio and Regev. "Worst-case to average-case reductions based on Gaussian measures".

Prerequisites. Basic knowledge in probability theory.

7 The Short Integer Solution Problem and Learning With Errors Problem

Advisor. Samed Düzlü
Date. 13 December 2022
Speaker. M. W.

So far, we have seen SVP and CVP as computational problems on lattices. However, cryptographic protocols make use of mainly two different computational problems, the *Short Integer Solution* (SIS) problem, and the *Learning With Errors* (LWE) problem. These are computationally equivalent problems, with one reduction being quantum (i.e., makes use of quantum computers). These problems and the reductions will be covered in this talk.

Content. Give the definitions of the SIS and LWE problems, For LWE, describe the search and decision problems and state their equivalence. Show that there are reductions from SIS to LWE and vice versa. The reduction of SIS to LWE is easy. For the quantum reduction of LWE to SIS, see [Ste+09, Theorem 4.1].

Literature.

[Reg05] Regev. “On lattices, learning with errors, random linear codes, and cryptography”.

[Ste+09] Stehlé et al. *Efficient Public Key Encryption Based on Ideal Lattices.*

Prerequisites. A basic understanding of quantum computing might be helpful.

8 Worst-Case to Average-Case Reductions

Advisor. Samed Düzlü
Date. 20 December 2022

The computational lattice problems SVP and CVP as discussed in Talk 5 and the cryptographic problems SIS and LWE from Talk 7 are related via a worst-case to average-case reduction. This reduction is the most important result supporting the security of LWE and hence, the security of lattice-based protocols based on the LWE problem.

Content. Begin with explaining the concepts of worst-case and average-case. Follow [MR07, Section 5] and show the worst-case to average-case reduction of SIS to SVP. Note that GapSVP in [MR07] is the approximate version of SVP. Give definitions of the intermediate problems and sketch the reductions from SIS to the intermediate problems and SVP.

Literature.

[MR07] Micciancio and Regev. “Worst-case to average-case reductions based on Gaussian measures”.

Prerequisites. Background on complexity theory may be helpful.

9 Structured Lattices

Advisor. Oscar Lapointe
Date. 10 January 2023
Speaker. G. T.

In designing cryptographic protocols, one is confronted with the problem of balancing between security and efficiency. General lattices as introduced before, require large memory and high computational efforts. This is remedied by the introduction of additional structure on the lattices, specifically, algebraic structure from ideals in number fields. While we focus on the algebraic perspective in this talk, the details on the computational advantages are discussed in Talk 10.

Content. Introduce the number fields, embeddings to real and complex fields and the associated Euclidean space, which we call Minkowski space. Define the ring of integers and (fractional) ideals; and show that (fractional) ideals define lattices in the Minkowski space. Show that under a suitably chosen modulus q, the ring of integers modulo q decomposes into a product of copies of $\mathbb{Z}/q$. This is called *Number Theoretic Transform* (NTT). In particular, motivate the chosen number field and modulus. Describe ring versions of the lattice problems discussed in previous talks. Show bounds for ideal lattices like [Ste12, Slide 12, Properties 1, 2]. Briefly introduce module lattices and discuss their motivation. Conclude with the cryptanalysis of lattice problems on structured lattices.

Literature.

[Ste12] Stehlé. *Cryptography from Ideal Lattices.*

[LM06] Lyubashevsky and Micciancio. “Generalized Compact Knapsacks Are Collision Resistant”.

[LPR13] Lyubashevsky, Peikert, and Regev. “A Toolkit for Ring-LWE Cryptography”.

[LPR10] Lyubashevsky, Peikert, and Regev. “On Ideal Lattices and Learning with Errors over Rings”.

[LS15] Langlois and Stehlé. “Worst-case to average-case reductions for module lattices”.

Prerequisites. Some knowledge in algebra and algebraic number theory may be useful.

10 Optimizations

Advisor. Thomas Aulbach
Date. 17 January 2023

The structured lattices introduced in the previous talk allow more efficient algorithms. In particular, one can use a *Fast Fourier Transform* (FFT) and the NTT. We will discuss the implementation level details of these optimization steps in this talk.

Content. Recall the FFT and NTT, and describe their advantage in terms of the number of operations and compare these to direct approach via polynomial multiplication and matrix multiplication in the unstructured case. Discuss the trade-off between size and efficiency. We discussed the discrete Gaussian distribution as error-distribution for LWE. Describe the binomial distribution and state the variants of LWE problems in terms of binomial distributions. Finally, discuss the choice of symmetric primitives and hash functions in lattice-based protocols.

Literature.

[BB13] Bansarkhani and Buchmann. “Improvement and Efficient Implementation of a Lattice-Based Signature Scheme”.

[Sco17] Scott. “A Note on the Implementation of the Number Theoretic Transform”.

[How+19] Howe et al. “Optimised Lattice-Based Key Encapsulation in Hardware”.

11 Dilithium and Kyber

Advisor. Thomas Aulbach
Date. 24 January 2023

Kyber (PKE/KEM) and Dilithium (Signature) are both chosen to be standardized, as a result of the 3rd round of NIST’s PQC standardization process. They are both based on structured lattices and considered to have a good balance between key sizes and performance.

Content. Start with a note on the NIST PQC standardization process. Introduce the Kyber KEM with the key generation, encapsulation and decapsulation algorithms. Show that the basic version of Kyber is CPA-secure and describe the FO-transform which makes Kyber to a CCA-secure KEM. Introduce the Dilithium signature scheme with the key generation, signing and verification algorithms. Discuss parameter choices, the design rationale, performance and key-sizes for both, Kyber and Dilithium.

Literature.

[NIST17] National Institute of Standards and Technology. *Post-Quantum Cryptography Standardization Process.*

[HHK17] Hofheinz, Hövelmanns, and Kiltz. “A Modular Analysis of the Fujisaki-Okamoto Transformation”. – FO-Transform.

[BG14] Bai and Galbraith. “An Improved Compression Technique for Signatures Based on Learning with Errors”.

[GLP12] Güneysu, Lyubashevsky, and Pöppelmann. “Practical Lattice-Based Cryptography: A Signature Scheme for Embedded Systems”.

[Bos+18] Bos et al. “CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM”.

12 NTRU and FALCON

Advisor. Michael Meyer
Date. 31 January 2023

NTRU (PKE/KEM) and FALCON (Signature) are competitors of Dilithium and Kyber. While FALCON will be standardized alongside Dilithium, NTRU is kept as a backup option, and will be standardized by NIST in the case that patent issues connected to Kyber cannot be resolved. They are both based on structured lattices and considered to have a good balance between key sizes and performance.

Content. Introduce the NTRU problem and sketch its relation to other lattice problems. Describe the NTRU KEM with its key generation, encapsulation and decapsulation algorithms. Similarly, describe the FALCON signature scheme with its key generation, signing and verification algorithms. Show the security reduction of one of the protocols to the NTRU problem. Discuss the parameter choices, design rationales, and performances and compare the key-sizes with the protocols of the previous talk.

Literature.

[Che+19] Chen et al. *NTRU – Submission to the 3rd round of the NIST post-quantum project.*

[HPS98] Hoffstein, Pipher, and Silverman. “NTRU: A Ring-Based Public Key Cryptosystem”.

[Pre+20] Prest et al. *FALCON – Submission to the 3rd round of the NIST post-quantum project.*

13 Physical Attacks on Lattice-based Protocols

Advisor. Juliane Krämer
Date. 7 February 2023

In addition to mathematical cryptanalysis, in practical applications cryptographic schemes are threatened by so-called physical attacks, i.e., side-channel and fault attacks. For lattice-based cryptography, it is especially difficult to protect Gaussian sampling against timing attacks, which is a very practical kind of side-channel attacks.

Content. Start with providing a short introduction to side-channel and fault attacks (independent of lattice-based cryptography). Then explain how learning Gaussian samples helps an attacker to break a scheme. Go on and present different apporaches for Gaussian sampling (CDT, Rejection, Knuth-Yao), together with attacks against them and helpful countermeasures.

Literature.

[Krä15] Krämer. “Why cryptography should not rely on physical attack complexity”. – specifically, Chapter 2.3 and 2.4.

[DN12] Ducas and Nguyen. “Faster Gaussian Lattice Sampling Using Lazy Floating-Point Arithmetic”.

[Pei10] Peikert. “An Efficient and Parallel Gaussian Sampler for Lattices”.

[Kar+19] Karmakar et al. “Pushing the speed limit of constant-time discrete Gaussian sampling. A case study on the Falcon signature scheme”.

References

[Aar] Scott Aaronson. *Introduction to Quantum Information Science Lecture Notes.* URL: https://www.scottaaronson.com/qclec.pdf (cit. on p. 2).

[BB13] Rachid El Bansarkhani and Johannes Buchmann. "Improvement and Efficient Implementation of a Lattice-Based Signature Scheme". In: *Selected Areas in Cryptography - SAC 2013 - 20th International Conference, Burnaby, BC, Canada, August 14-16, 2013, Revised Selected Papers.* Ed. by Tanja Lange, Kristin E. Lauter, and Petr Lisonek. Vol. 8282. Lecture Notes in Computer Science. Springer, 2013, pp. 48–67. DOI: 10.1007/978-3-662-43414-7_3. URL: https://doi.org/10.1007/978-3-662-43414-7%5C_3 (cit. on p. 6).

[BG14] Shi Bai and Steven D. Galbraith. "An Improved Compression Technique for Signatures Based on Learning with Errors". In: *Topics in Cryptology - CT-RSA 2014 - The Cryptographer's Track at the RSA Conference 2014, San Francisco, CA, USA, February 25-28, 2014. Proceedings.* Ed. by Josh Benaloh. Vol. 8366. Lecture Notes in Computer Science. Springer, 2014, pp. 28–47. DOI: 10.1007/978-3-319-04852-9_2. URL: https://doi.org/10.1007/978-3-319-04852-9%5C_2 (cit. on p. 6).

[Bin+] Nina Bindel, Jacqueline Brendel, Marc Fischlin, Brian Goncalves, and Douglas Stebila. "Hybrid key encapsulation mechanisms and authenticated key exchange". In: *International Conference on Post-Quantum Cryptography.* URL: https://eprint.iacr.org/2018/903.pdf (cit. on p. 2).

[Bos+18] Joppe W. Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. "CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM". In: *2018 IEEE European Symposium on Security and Privacy, EuroS&P 2018, London, United Kingdom, April 24-26, 2018.* IEEE, 2018, pp. 353–367. DOI: 10.1109/EuroSP.2018.00032. URL: https://doi.org/10.1109/EuroSP.2018.00032 (cit. on p. 7).

[Che+19] Cong Chen, Oussama Danba, Jeffrey Hoffstein, Andreas Hülsing, Joost Rijneveld, John M. Schanck, Peter Schwabe, William Whyte, Zhenfei Zhang, Tsunekazu Saito, Takashi Yamakawa, and Keita Xagawa. *NTRU – Submission to the 3rd round of the NIST post-quantum project.* https://ntru.org/f/ntru-20190330.pdf. 2019 (cit. on p. 7).

[DN12] Léo Ducas and Phong Q. Nguyen. "Faster Gaussian Lattice Sampling Using Lazy Floating-Point Arithmetic". In: *Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings.* Ed. by Xiaoyun Wang and Kazue Sako. Vol. 7658. Lecture Notes in Computer Science. Springer, 2012, pp. 415–432. DOI: 10.1007/978-3-642-34961-4_26. URL: https://doi.org/10.1007/978-3-642-34961-4%5C_26 (cit. on p. 7).

[GLP12] Tim Güneysu, Vadim Lyubashevsky, and Thomas Pöppelmann. "Practical Lattice-Based Cryptography: A Signature Scheme for Embedded Systems". In: *Cryptographic Hardware and Embedded Systems - CHES 2012 - 14th International Workshop, Leuven, Belgium, September 9-12, 2012. Proceedings.* Ed. by Emmanuel Prouff and Patrick Schaumont. Vol. 7428. Lecture Notes in Computer Science. Springer, 2012, pp. 530–547. DOI: 10.1007/978-3-642-33027-8_31. URL: https://doi.org/10.1007/978-3-642-33027-8%5C_31 (cit. on p. 7).

[GNR10] Nicolas Gama, Phong Q. Nguyen, and Oded Regev. "Lattice Enumeration Using Extreme Pruning". In: *Advances in Cryptology – EUROCRYPT 2010.* Ed. by Henri Gilbert. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 257–278 (cit. on p. 4).

[HHK17] Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz. "A Modular Analysis of the Fujisaki-Okamoto Transformation". In: *Theory of Cryptography - 15th International Conference, TCC 2017, Baltimore, MD, USA, November 12-15, 2017, Proceedings, Part I.* Ed. by Yael Kalai and Leonid Reyzin. Vol. 10677. Lecture Notes in Computer Science. Springer, 2017, pp. 341–371. DOI: 10.1007/978-3-319-70500-2_12. URL: https://doi.org/10.1007/978-3-319-70500-2%5C_12 (cit. on p. 6).

[How+19] James Howe, Marco Martinoli, Elisabeth Oswald, and Francesco Regazzoni. "Optimised Lattice-Based Key Encapsulation in Hardware". In: 2019 (cit. on p. 6).

[HPS11] Guillaume Hanrot, Xavier Pujol, and Damien Stehlé. "Algorithms for the Shortest and Closest Lattice Vector Problems". In: *Coding and Cryptology.* Ed. by Yeow Meng Chee, Zhenbo Guo, San Ling, Fengjing Shao, Yuansheng Tang, Huaxiong Wang, and Chaoping Xing. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 159–190 (cit. on p. 4).

[HPS98] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. "NTRU: A Ring-Based Public Key Cryptosystem". In: *ANTS 1998.* Ed. by Joe Buhler. Vol. 1423. Lecture Notes in Computer Science. `https://www.ntru.org/f/hps98.pdf`. Springer, 1998, pp. 267–288 (cit. on p. 7).

[Kar+19] Angshuman Karmakar, Sujoy Sinha Roy, Frederik Vercauteren, and Ingrid Verbauwhede. "Pushing the speed limit of constant-time discrete Gaussian sampling. A case study on the Falcon signature scheme". In: *Proceedings of the 56th Annual Design Automation Conference 2019, DAC 2019, Las Vegas, NV, USA, June 02-06, 2019.* ACM, 2019, p. 88. DOI: `10.1145/3316781.3317887`. URL: `https://doi.org/10.1145/3316781.3317887` (cit. on p. 7).

[KL20] Jonathan Katz and Yehuda Lindell. *Introduction to modern cryptography.* CRC press, 2020. URL: `http://staff.ustc.edu.cn/~mfy/moderncrypto/reading%20materials/Introduction_to_Modern_Cryptography.pdf` (cit. on p. 2).

[Krä15] Juliane I. Krämer. "Why cryptography should not rely on physical attack complexity". Doctoral Thesis. Berlin: Technische Universität Berlin, Fakultät IV - Elektrotechnik und Informatik, 2015. DOI: `10.14279/depositonce-4523`. URL: `http://dx.doi.org/10.14279/depositonce-4523` (cit. on p. 7).

[Lan21] Tanja Lange. *Video Lectures on Lattice-based Cryptography.* 2021. URL: `https://hyperelliptic.org/tanja/teaching/pqcrypto21/#lattice` (cit. on p. 3).

[LM06] Vadim Lyubashevsky and Daniele Micciancio. "Generalized Compact Knapsacks Are Collision Resistant". In: *Automata, Languages and Programming, 33rd International Colloquium, ICALP 2006, Venice, Italy, July 10-14, 2006, Proceedings, Part II.* Vol. 4052. Lecture Notes in Computer Science. Springer, 2006, pp. 144–155. DOI: `10.1007/11787006\_13`. URL: `https://doi.org/10.1007/11787006%5C_13` (cit. on p. 5).

[LMV] Thijs Laarhoven, Michele Mosca, and Joop Van De Pol. "Finding shortest lattice vectors faster using quantum search". In: *Designs, Codes and Cryptography* (). URL: `https://eprint.iacr.org/2014/907` (cit. on p. 4).

[LPR10] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. "On Ideal Lattices and Learning with Errors over Rings". In: *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Monaco / French Riviera, May 30 - June 3, 2010. Proceedings.* Ed. by Henri Gilbert. Vol. 6110. Lecture Notes in Computer Science. Springer, 2010, pp. 1–23. DOI: `10.1007/978-3-642-13190-5\_1`. URL: `https://doi.org/10.1007/978-3-642-13190-5%5C_1` (cit. on p. 6).

[LPR13] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. "A Toolkit for Ring-LWE Cryptography". In: *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings.* Ed. by Thomas Johansson and Phong Q. Nguyen. Vol. 7881. Lecture Notes in Computer Science. Springer, 2013, pp. 35–54. DOI: `10.1007/978-3-642-38348-9\_3`. URL: `https://doi.org/10.1007/978-3-642-38348-9%5C_3` (cit. on p. 5).

[LS15] Adeline Langlois and Damien Stehlé. "Worst-case to average-case reductions for module lattices". In: *Des. Codes Cryptogr.* 75.3 (2015), pp. 565–599. ISSN: 0925-1022. DOI: `10.1007/s10623-014-9938-4`. URL: `https://doi.org/10.1007/s10623-014-9938-4` (cit. on p. 6).

[MG02] Daniele Micciancio and Shafi Goldwasser. *Complexity of lattice problems.* Vol. 671. The Kluwer International Series in Engineering and Computer Science. A cryptographic perspective. Kluwer Academic Publishers, Boston, MA, 2002, pp. x+220. ISBN: 0-7923-

7688-9. DOI: 10.1007/978-1-4615-0897-7. URL: https://doi.org/10.1007/978-1-4615-0897-7 (cit. on p. 3).

[Mic12] Daniele Micciancio. *Lattice Algorithms and Applications - The LLL Algorithm.* 2012. URL: https://cseweb.ucsd.edu/classes/wi12/cse206A-a/lec3.pdf (cit. on p. 4).

[MR07] Daniele Micciancio and Oded Regev. "Worst-case to average-case reductions based on Gaussian measures". In: *SIAM J. Comput.* 37.1 (2007), pp. 267–302. ISSN: 0097-5397. DOI: 10.1137/S0097539705447360. URL: https://doi.org/10.1137/S0097539705447360 (cit. on pp. 4, 5).

[NC] Michael A Nielsen and Isaac Chuang. *Quantum computation and quantum information.* URL: http://mmrc.amss.cas.cn/tlb/201702/W020170224608149940643.pdf (cit. on p. 2).

[NIST17] National Institute of Standards and Technology. *Post-Quantum Cryptography Standardization Process.* 2017. URL: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions (cit. on p. 6).

[Pei10] Chris Peikert. "An Efficient and Parallel Gaussian Sampler for Lattices". In: *Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings.* Ed. by Tal Rabin. Vol. 6223. Lecture Notes in Computer Science. Springer, 2010, pp. 80–97. DOI: 10.1007/978-3-642-14623-7_5. URL: https://doi.org/10.1007/978-3-642-14623-7%5C_5 (cit. on p. 7).

[Pre+20] Thomas Prest, Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. *FALCON – Submission to the 3rd round of the NIST post-quantum project.* https://falcon-sign.info/falcon.pdf. 2020 (cit. on p. 7).

[Pre15] Thomas Prest. "Gaussian sampling in lattice-based cryptography". PhD thesis. Ecole normale supérieure-ENS PARIS, 2015. URL: https://www.di.ens.fr/~prest/Publications/ThomasPrestThesis.pdf (cit. on p. 4).

[Reg05] Oded Regev. "On lattices, learning with errors, random linear codes, and cryptography". In: *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005.* Ed. by Harold N. Gabow and Ronald Fagin. ACM, 2005, pp. 84–93. DOI: 10.1145/1060590.1060603. URL: https://doi.org/10.1145/1060590.1060603 (cit. on p. 5).

[Rot] J. Rothe. *Rabin's Public-Key Cryptosystem.* URL: https://ccc.cs.uni-duesseldorf.de/~rothe/CRYPTOCOMPLEXITY2/folien-4-rabin.pdf (cit. on p. 2).

[Sco17] Michael Scott. "A Note on the Implementation of the Number Theoretic Transform". In: *Cryptography and Coding - 16th IMA International Conference, IMACC 2017, Oxford, UK, December 12-14, 2017, Proceedings.* Ed. by Máire O'Neill. Vol. 10655. Lecture Notes in Computer Science. Springer, 2017, pp. 247–258. DOI: 10.1007/978-3-319-71045-7_13. URL: https://doi.org/10.1007/978-3-319-71045-7%5C_13 (cit. on p. 6).

[Sho94] Peter W Shor. "Algorithms for quantum computation: discrete logarithms and factoring". In: *Proceedings 35th annual symposium on foundations of computer science.* Ieee. 1994, pp. 124–134. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=365700 (cit. on pp. 1, 2).

[Ste+09] Damien Stehlé, Ron Steinfeld, Keisuke Tanaka, and Keita Xagawa. *Efficient Public Key Encryption Based on Ideal Lattices.* Cryptology ePrint Archive, Paper 2009/285. https://eprint.iacr.org/2009/285. 2009. URL: https://eprint.iacr.org/2009/285 (cit. on pp. 4, 5).

[Ste12] Damien Stehlé. *Cryptography from Ideal Lattices.* 2012. URL: https://simons.berkeley.edu/talks/damien-stehle-2015-07-07 (cit. on p. 5).

[Vou11] Panagiotis Voulgaris. *Algorithms for the closest and shortest vector problems on general lattices.* 2011 (cit. on p. 4).

[Wal] N. R. Wallach. *Quantum computing and entanglement for mathematicians.* URL: https://mathweb.ucsd.edu/~nwallach/venice.pdf (cit. on p. 2).