Seminar Announcement

In the upcoming winter term 2022/23 we will offer again a seminar on

Advanced Topics in Post-Quantum Cryptography

The seminar builds on the lecture *Post-Quantum Secure Cryptography* [PQC21] which is usually offered in the summer term. However, interested students from Mathematics as well as Computer Sciences with a solid background knowledge in algebra (or related fields), e.g. as taught in the lecture *Mathematical Foundations of (Post-Quantum) Cryptography*, are also invited to join.

*On the Field of Post-Quantum Cryptography.* We heavily rely on cryptography in our everyday life, for example, when we do online shopping and online banking, pay with credit or debit card, open doors with electronic keys, or when we use social networks, instant messengers, online games, WiFi, mobile networks, or electronic currencies.

In all of these applications the most widely used cryptosystems, like RSA encryption and elliptic curve cryptography, are built on the hardness of certain algebraic problems, like the factorization of integers. While these problems withstood all attacks by classical computers so far, it is also known that a suitable quantum computer could easily solve the underlying mathematical problems in polynomial time and therewith break the corresponding cryptosystems. For example, the famous quantum algorithm by Shor can break the factorization problem efficiently.

Recent progress in the development of quantum computers led researchers and governmental organizations, e.g. the National Institute of Standards and Technology (NIST), to start the search for new cryptosystems usable on classical computers that can withstand attacks by quantum computers - so-called post-quantum cryptosystems. Although there are currently no sufficiently powerful quantum computers, it is still highly necessary to find and establish these post-quantum cryptographic standards in due time. This is particularly important for information which has to be kept secret for 5 or 10 years or even longer and which should not become public the moment someone constructs a powerful quantum computer.

*Starting Point for the Seminar.* In the lecture *Post-Quantum Secure Cryptography* [PQC21] we discussed Quantum Computing in general as well as Shor’s
algorithm [Sho97] to break the factorization problem; we introduced algebraic lattices; we then reduced the security of the Learning with Errors Problem [Reg05] to hard lattice problems like the Shortest Independent Vector Problem (SIVP) and constructed Regev’s cryptosystem. At the end of the lecture we reviewed general results from Galois Theory and elementary Algebraic Number Theory [NS13] and formulated the corresponding hard ideal lattice problems.

Our seminar starts with an introduction to algebraic number theory (which will be more detailed than in the lecture but still rather brief and focused on our applications). Furthermore, we will prove results on the discrete multivariate Gaussian distribution omitted in the lecture (with tools from harmonic analysis [HR70], [Ban93]). The previous results are then applied to construct a quantum reduction from ideal lattice problems to the Ring Learning with Errors Problem (R-LWE) [LPR10]. We will furthermore discuss classical alternatives [Pei09]. As an application of R-LWE we prove the security of the BGV cryptosystem [BGV12]. At the end of the seminar we will generalize the setup to module problems, in particular the Module Shortest Integer Solution Problem (M-SIS) and prove its security. Possible applications included commitment schemes [Bau+18].

**Topics in Detail**

The following topics are not completely fixed. In particular, we are open to suggestions by students as long as they treat a related topic. The topics will be assigned to the participating students in the first week of term - you may tell your preference, but note that given the dependencies between the different topics some topics will only become available if there are enough participants.

1. **Algebraic Number Fields, Integrality.** The first talk repeats the definitions of an algebraic number field and integrality as in [NS13], § 2. This includes integral closure, minimal polynomial, trace and norm. Using the canonical embedding of a separable field extension (known from algebra, e.g. [Bos20] or also [PQC21]) a proof of [NS13], Proposition 2.6. is given. Depending on the time the talk can also prove [NS13], Proposition 2.8, i.e. that the trace gives a non-degenerated bilinear form. Finally the talk introduces the concept of an integral basis and proves [NS13], Proposition 2.6.

2. **Ideals.** The talk presents the content of [NS13], § 3. In particular, one shows that $\mathcal{O}_K$ is a Dedekind domain and hence each ideal has a unique prime factorization. The Chinese Remainder Theorem (in its general form as in [PQC21]) can be assumed. Finally fractional ideals and the ideal class group are defined.

3. **Lattices.** The talk shortly reviews the definition of an algebraic lattice given in [PQC21]. A proof of [NS13], Proposition 4.2. should only be sketched, since it is already given in [PQC21]. The proof uses the *fundamental theorem on finitely generated abelian groups* - this theorem or preferable the more general *structure theorem for finitely generated modules over a principal ideal domain* should be stated (not proven) - see a suitable book on algebra, e.g. [Goo98]. Furthermore [NS13],
Lemma 4.3. and Minkowski’s Lattice Point Theorem should be presented.

4. Cyclotomic Number Fields. The content of this talk is covered by [NS13]. One proves Proposition 10.2 in [NS13], i.e. gives a basis of the integer ring of the cyclotomic number field. Furthermore, the decomposition in Proposition 10.3 of [NS13] should be presented. Apart from the actual proofs it will be important to connect the abstract versions of the statements presented in [NS13] with the special cases presented in [PQC21], in particular the case of a power two extension should be considered.

5. Poisson Formula on Lattices. The talk presents the Poisson formula as in 3.29 of [PQC21] on an arbitrary lattice. To get a more intuitive idea of the proof, consult [Ebe13] - this proof is however, restricted to the special lattice \( \mathbb{Z}^n \). A more general version is available in (31.46) of [HR70] or [Bou07], II.7. In order to use this version one first has to recall the Haar measure on our discrete lattices and then to present the proof on locally compact spaces. This topic assumes some background knowledge on \( L^p \) spaces.

6. Discrete Gaussian Distribution. This talk provides proofs for some of the optional parts of [PQC21]. In particular, prove [PQC21], Estimates of Gaussians on Lattices respectively [Ban93] using the Poisson formula from the previous talk. Furthermore, prove Lemma 3.20 in [PQC21] and after that state Lemma 3.21 on the concentration of the discrete multivariate Gaussian. You do not have to repeat the proof of Lemma 3.21 from the lecture.

7. Transference Theorems. The content of the talk is [Ban93], Section 2, i.e. a presentation of the transference theorems 2.1, 2.2 and 2.3 and their proofs. If possible, the notation should be adapted to the notation used in [PQC21] (and the previous talks).

8. R-LWE. Restate the R-LWE problem and the SIVP problem and recall the proof structure of Chapter 3 from [PQC21]. The talk then identifies the necessary changes needed to transfer the proofs from [PQC21], Chapter 3 from the LWE setup to the R-LWE setup, i.e. the BDD to R-LWE - see [LPR10]. The main part of the talk will be to prove this missing step in the ideal lattice setup. You do not need to repeat proofs from Chapter 3 in [PQC21]. As an additional source you can also use [LPR13].

9. Classical versus Quantum Reduction. The talk should explain the proof of Theorem 3.1. of [Pei09]. While the focus of the presentation should be on this proof, it should also shortly explain why the proof cannot be transferred to the ideal lattice setup. Finally, show a short comparison of the parameter sizes required for the classical reduction and for the quantum reduction by [Reg05] used in [PQC21].

10. Norm Estimate. Recall the canonical embedding from [PQC21] (respectively any algebra book) as well as the trivial coefficient embedding. [SPDZ12], C.2 and C.3 summarizes well-known norm estimates between the pullbacks of the \( p \)-norms under the two embeddings (alternatively [LPR13]). The talk should prove these
norm estimates and additionally treat the special case of power two cyclotomic rings, in particular, one proves that in this special case there are tighter bounds.

11. Security of the BGV Encryption Scheme. First repeat the version of the [BGV12] encryption scheme contained in chapter 4 of [PQC21]. Explain the bootstrapping technique to extend the encryption scheme to a levelled (or even a fully) homomorphic encryption. Prove the IND-CPA security of the extended scheme along the lines of [BGV12] (respectively [BV11]). Furthermore, compute the corresponding security parameters as in [SPDZ12], D.

12. Security of M-SIS. The talk presents [LS14], Theorem 3.6 and its proof. In particular, the necessary prerequisites are introduced. One observes that the majority of the material introduced in sections 1 and 2 of [LS14] is a straightforward generalization from the ring case to the module case. Rather than repeating the proofs in the module case, the talk should explain the general idea of the generalization to modules (maybe with one or two examples) and then concentrate on the proof of [LS14], Theorem 3.6.

13. Lattice-Based Commitment Schemes. The final talk will apply the previous results on M-SIS and M-LWE. As an example of a lattice-based commitment scheme present [Bau+18] and show that (for certain parameters) the scheme is information-theoretically binding and (for other parameters) information theoretically hiding. You are free to either reduce the security to M-LWE and M-SIS (see, e.g. [Pin+17], Theorem 3.1) or to equivalent problems (as in [Bau+18]).

Registration. By e-mail to pascal.reisert@sec.uni-stuttgart.de or via Ilias (once the corresponding course is online).

References


1 The generalization from R-LWE to M-LWE is mostly standard and can be omitted.


Adeline Langlois and Damien Stehlé. “Worst-Case to Average-Case Reductions for Module Lattices”. In: Designs, Codes and Cryptography 75 (June 2014).


