Karlsruhe Institute of Technology

KARLSRUHE INSTITUTE OF TECHNOLOGY
Institute of Theoretical Informatics
Lehrstuhl Prof. Dr. J. Müller-Quade
Seminar "*Post-Quantum Cryptography*"

Preliminary Seminar Program

Post-Quantum Cryptography

Theory

The Fujisaki-Okamoto Transformation (Supervisor: Michael Klooß) The transformation from Fujisaki and Okamoto [10, 11] constructs CCA-secure encryption schemes from schemes that satisfy much weaker notions (e.g. not even IND-CPA). The transformation was further analyzed by Hofheinz, Hövelmanns, and Kiltz [14].

Most NIST candidates for post-quantum secure encryption schemes rely on (forms of) the Fujisaki–Okamoto transformation. It is was proven secure against *quantum* attackers in the *quantum random oracle model (QROM)* [19, 14], that is, a random oracle that can be queried in *superposition* [7].

The student is expected to

- motivate the necessity of the QROM and introduce it.
- motivate and introduce the results of Fujisaki–Okamoto in the quantum world, following the modular framework in [14].
- present and explain the security proof. (Classical security suffices. Showing quantum security, assuming necessary background is also possible.)

References

[10] Eiichiro Fujisaki and Tatsuaki Okamoto. "Secure Integration of Asymmetric and Symmetric Encryption Schemes". In: vol. 1666. Lecture Notes in Computer Science. Springer, 1999, pp. 537–554

[11] Eiichiro Fujisaki and Tatsuaki Okamoto. "Secure Integration of Asymmetric and Symmetric Encryption Schemes". In: *J. Cryptol.* 26.1 (2013), pp. 80–101

[7] Dan Boneh et al. "Random Oracles in a Quantum World". In: vol. 7073. Lecture Notes in Computer Science. Springer, 2011, pp. 41–69

[19] Ehsan Ebrahimi Targhi and Dominique Unruh. "Post-Quantum Security of the Fujisaki-Okamoto and OAEP Transforms". In: vol. 9986. Lecture Notes in Computer Science. 2016, pp. 192–216

[14] Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz. "A Modular Analysis of the Fujisaki-Okamoto Transformation". In: vol. 10677. Lecture Notes in Computer Science. Springer, 2017, pp. 341–371

Lattice-based Cryptography

Learning with Errors (LWE) (Supervisor: Astrid Ottenhues) The Learning with Errors (LWE) problem is conjectured to be very hard for reasonable choices of parameters. Firstly, it can be seen as an extension of a well-known problem in learning theory, namely the *learning parity with noise* problem. Secondly, LWE is closely related to decoding problems in coding theory. Both related families of problems are believed to be hard themselfs.

In 2005, Regev showed in [16] that LWE is in the average case as hard as it is in the worst case. Additionally, Regev gives a worst-case quantum reduction from the *shortest independent vectors problem (SIVP)*. Which means that, assuming there exits no quantum algorithm to solve the SIVP, the decision version of LWE is hard to solve.

The student is expected to

- motivate and describe the different versions of the LWE problem
- present and explain the hardness reduction
- link the theoretic results to actual proposed candidates based on different LWE variants

References

[16] Oded Regev. “On lattices, learning with errors, random linear codes, and cryptography”. In: *J. ACM* 56.6 (2009), 34:1–34:40

KYBER (Supervisor: Astrid Ottenhues) For the PQ-crypto standardization process there were especially many submissions based on lattices. CRYSTALS Kyber [1] is one of the of the finalist. Kyber is and IND-CCA2-secure key encapsulation meachanism, whose security is based on the hardness of solving the Module-LWE problem.

The student is expected to

- explain the general protocol idea of KYBER.
- illustrate the advantages and disadvantes of the scheme.
- point out the security level and the best known attacks

References

[1] `https://pq-crystals.org/kyber/index.shtml`

Post-Quantum Forward-Secure Onion Routing (Supervisor: Christoph Coijanovic) Today, *Onion Routing* (OR) is the most widespread form of anonymous communication. It allows senders to unlink themselves from the messages they send. Unlinkability is achieved by encrypting messages in multiple layers (akin to an onion) and sent through a series of proxy servers. Each server removes the outermost encryption layer to ensure that the adversary cannot match incoming messages at a server to outgoing ones.

There have been efforts to make TOR, the most popular onion routing protocol, post-quantum secure. Based on [12], the student shall present TOR’s weaknesses against a post-quantum adversary and how Ghosh et al. propose to solve them.

The student is expected to

- Give an introduction of OR

- Motivate the need for post-quantum secure OR and introduce possible attacks on classical OR
- Introduce Ghosh et al.'s proposed HybridOR protcol [12]
- Present and explain HybridOR's security proof (security against Type-I adversary suffices)

References

[12] S. Ghosh and Aniket Kate. "Post-Quantum Forward-Secure Onion Routing - (Future Anonymity in Today's Budget)". In: 2015

Number Theoretic Transformation (NTT) (Supervisor: Wasilij Beskorovajnov) Asymmetric cryptoraphy (pre- and post-quantum equally) is rather inefficient in comparison with symmetric cryptography. This is the exact reason why the KEM/DEM [13] paradigm is so popular. But even when the PKE is used as a KEM within a hybrid construction there is still plenty of room for optimization.

Similar to modular/scalar exponentiation/multiplication being a bottleneck for many pre-quantum schemes the polynomial multiplication is a bottleneck for many lattice-based schemes.

Looking into the specification of Kyber [1], a Module-LWE-based KEM, one may stumble upon a seemingly bloated syntax that hides the rather simple construction of a KEM. (Fortunately the authors give an abstract description inside the comments) For Kyber, the authors decided to incorporate a quintessential optimization, i.e. the Number Theoretic Transformation (NTT).

The NTT aims at optimizing the modular polynomial multiplication. Multiplying polynomials in their plain form requires $O(n^2)$ coefficient multiplications. The NTT allows for $O(n \cdot log(n))$ multiplications.

The student is expected to

- explain the mathematical fundamentals of NTT, which includes explaining primitive roots of unity, cyclotomic rings, the Chinese Remainder Theorem (CRT) and the (forward/reverse) Fast Fourier Transformation (FFT) over cyclotomic rings.
- explain what significance the chosen cyclotomic fields and moduli in some of the lattice-based NIST candidates, e.g., Kyber [1] or Dilithium [2], have for the NTT.
- discuss what advantages and disadvantages the NTT has.

References

[13] Javier Herranz, Dennis Hofheinz, and Eike Kiltz. "KEM/DEM: Necessary and sufficient conditions for secure hybrid encryption". In: *Manuscript in preparation* (2006)

[1] `https://pq-crystals.org/kyber/index.shtml`

[2] `https://pq-crystals.org/dilithium/`

Kronecker Substitution (Supervisor: Wasilij Beskorovajnov) Kronecker Substituion is an alternative way of tackling the bottleneck of polynomial multiplication in lattice-based contructions. While the Number Theoretic Transformation (NTT) reduces the problem to a component-wise (instead of a cross-product) multiplication of polynomials of lower order, the appraoch of the Kronecker Substituion is to reduce the problem of multiplying polynomials to the well-known and (hardware side) optimized task of multiplying large integers.

Albrecht, Hanser, Hoeller, Pöppelmann, Virdia and Wallner [4] were the first ones to augment one of the NIST canidates Kyber [1] with this technique and reported a remarkable speedup.

The student is expected to

- explain the isomorphism of a polynomial and its evaluation $f(2^l)$ (for a sufficiently large l)
- discuss the possible generalizations, such as the negated/reciprocal evaluation points technique.
- describe and discuss which parameters and techniques were used by [4] in order to augment the scheme Kyber and why.

References

[4] Martin R Albrecht et al. “Implementing RLWE-based schemes using an RSA co-processor”. In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2019), pp. 169–208

[1] `https://pq-crystals.org/kyber/index.shtml`

Isogeny-based Cryptography

Isogeny-based cryptography has seen a large amount of attention in recent years. While it was first introduced by Couveignes [9] as “Hard Homogeneous Spaces”, later rediscovered as public-key cryptography by Rostovtsev and Stolbunov [17], it has been rather impractical in terms of computational resources.

Recently, with the rise of post-quantum cryptography, there have been significant improvements to towards speed Castryck et al. [8]. Moreover, a different kind of isogeny based public key crypto was introduced and submitted to NIST competition by Jao [15].

SIKE (Supervisor: Roland Gröll) Supersingular Isogeny Key Encapsulation (SIKE) is a Key Encapsulation Mechanism (KEM) based on the Supersingular Isogeny Diffie-Hellman (SIDH) key excange construction. The security relies on the hardness of the supersingular isogeny walk problem. It is an alternate candidate candidate in the NIST post-quantum competition

In this topic the student is expected to

- present the SIKE key encapsulation scheme
- and review its security propiertes.

References

[15] `https://sike.org/`

Hash-based Cryptography

SPHINCS+ (Supervisor: Clemens Fruböse) The stateless, hash based signature scheme SPHINCS+ [5] is an alternate candidate in the final round of the NIST post-quantum competition. Its security is based on the hardness of finding pre-images to hash function images. It is constructed from different (state-full) hash-based components that allow it to produce a very small public key but rather large signatures.

In this topic the student is expected to

- present the SPHINCS+ signature scheme,
- and review its security properties.

References

- SPHINCS+ Papers

  [5] Daniel J. Bernstein et al. “The SPHINCS⁺ Signature Framework”. In: CCS ’19. London, United Kingdom: Association for Computing Machinery, 2019, pp. 2129–2146. ISBN: 9781450367479

Mersenne-number-based Cryptography

KEMs (Supervisor: Marcel Tiepelt) *This topic is reserved for Proseminar students!!!* Mersenne-number based schemes are one of the simplest cryptographic schemes, requiring only addition and multiplication over the Mersenne-primes as well as black-box access to an error correcting code and hash function. The NIST post-quantum competition featured two such cryptosystems ([18, 3]) which both dropped out after the first round. While the the underlying schemes remain unbroken, the presumable quantum hard problem is relatively new. Moreover both schemes are fairly inefficient.

The student is expected is to

- introduce the underlying hard problem,
- present the general key encapsulation mechanism,
- and the expected classical and quantum security,
- (optional) present the best known attack (see [6]).

References

[6] Marc Beunardeau et al. “On the Hardness of the Mersenne Low Hamming Ratio Assumption”. In: 2017

[18] Alan Szepieniec. *Supersingular Isogeny Key Encapsulation*. 2018

[3] Divesh Aggarwal et al. “A New Public-Key Cryptosystem via Mersenne Numbers”. In: vol. 10993. Lecture Notes in Computer Science. Springer, 2018, pp. 459–482