Student Assistant in Cryptography

Context

Key-encapsulation mechanisms (KEMs) are cryptographic primitives that allow two communicating parties (Alice and Bob) to exchange a shared key which is then used for further communication. The standard security notion for KEMs is Indistinguishability under Chosen Ciphertext Attacks (IND-CCA). A common way to construct IND-CCA secure KEMs is to construct public-key encryption schemes that are secure in a weaker sense and then apply generic transformations to turn them into IND-CCA secure KEMs. One such transform is the Fujisaki-Okamoto (FO) transform which comes in a few different variants [HHK17]. Looking at the NIST post-quantum cryptography standardization process [NIST], the submitted KEMs almost exclusively rely on the FO transform—in some cases it is applied directly, in some other additional tweaks are added.

The Task

The overall goal of this position is to do literature research on the FO variants used by the KEMs in the NIST PQC standardization process via the following steps:

1. get familiar with the FO transform and its different variants
2. analyze the different KEMs with respect to which variant of the FO transform they are using

Requirements

- Interest in cryptography
- Fluent English

Application

If you are interested, please send an email to Maximiliane Weishäupl (maximiliane.weishaeupl@ur.de).

References

[HHK17] – Hofheinz, Hövelmanns, Kiltz. A modular analysis of the Fujisaki-Okamoto transformation. TCC 2017. (https://ia.cr/2017/604)
[NIST] - https://csrc.nist.gov/Projects/post-quantum-cryptography