SABER: Mod-LWR based KEM (Round 2 Submission)
Changes between Round 2 and Round 1 Submission

Principal submitter

This submission is from the following team, listed in alphabetical order:

- Jan-Pieter D'Anvers, KU Leuven, imec-COSIC
- Angshuman Karmakar, KU Leuven, imec-COSIC
- Sujoy Sinha Roy, KU Leuven, imec-COSIC
- Frederik Vercauteren, KU Leuven, imec-COSIC

E-mail address: `saber@esat.kuleuven.be`

Website: `https://www.esat.kuleuven.be/cosic/pqcrypto/saber/`

Telephone: +32-16-37-6080

Postal address:
Prof. Dr. Ir. Frederik Vercauteren
COSIC - Electrical Engineering
Katholieke Universiteit Leuven
Kasteelpark Arenberg 10
B-3001 Heverlee
Belgium

Auxiliary submitters: There are no auxiliary submitters. The principal submitter is the team listed above.

Inventors/developers: The inventors/developers of this submission are the same as the principal submitter. Relevant prior work is credited below where appropriate.

Owner: Same as submitter.

Signature: $\times$. See also printed version of "Statement by Each Submitter".

Document based on `pqskeleton` version 20170923 by Daniel Bernstein.

A Changes with respect to Round 1 submission

This section is also included in the main specification document as Appendix A.

Very few changes were made between the round 1 version and the round 2 version of Saber. The only changes made are as follows:

- Transposing matrix $\boldsymbol{A}$: in `Saber.PKE.KeyGen` given in Algorithm **??**, the matrix $\boldsymbol{A}$ is now transposed in line 5. On the other hand, in `Saber.PKE.Enc` given in Algorithm **??** the matrix $\boldsymbol{A}$ is used without transpose in line 5. In the first round submission, this was the exact opposite: we used $\boldsymbol{A}$ in `KeyGen`, whereas $\boldsymbol{A}^T$ was used in `Enc`. The advantage of the new approach is that it allows to speed-up encryption.

- The parameter T: to simplify the description of the algorithms we introduced a parameter T which equals $2t$ in the first round submission. This has no impact on the actual implementation.

- Simplification of the specification: the round 2 version of Saber has a much simpler specification than the round 1 version by working entirely in the interval $[0, q[$ and never resorting to the centered interval $[-q/2, q/2]$. This has no impact on the actual implementation.

- The constant polynomial h has been removed and replaced by two new constant polynomials h_1 and h_2. This is needed to provably reduce the security of Saber to Mod-LWR and it slightly changes the implementation.