Research into side-channels and timing attacks on NIST PQC proposals

Alexander Nilsson, Lund University

May 22, 2020

I will present my work with our latest paper [1], recently accepted to Crypto 2020, which details a key recovery timing attack. Abstract as follows:

In the implementation of post-quantum primitives, it is well known that all computations that handle secret information need to be implemented to run in constant time.

Using the Fujisaki-Okamoto transformation or any of its different variants, a CPA-secure primitive can be converted into an IND-CCA secure KEM. In this paper we show that although the transformation does not handle secret information apart from calls to the CPA-secure primitive, it has to be implemented in constant time. Namely, if the ciphertext comparison step in the transformation is leaking side-channel information, we can launch a key-recovery attack.

Several proposed schemes in round 2 of the NIST post-quantum standardization project are susceptible to the proposed attack and we develop and show the details of the attack on one of them, being FrodoKEM. It is implemented on the reference implementation of FrodoKEM, which is claimed to be secure against all timing attacks. In the experiments, the attack code is able to extract the secret key for all security levels using about 2^{30} decapsulation calls.

References

[1] Qian Guo, Thomas Johansson and Alexander Nilsson *A key-recovery timing attack on post-quantum primitives using the Fujisaki-Okamoto transformation and its application on FrodoKEM.* Crypto 2020 (preprint)