Studies and security of cryptographic code-based implementations against side-channel attacks

Guillaume GOY *(speaker)*
XLIM, University of Limoges &
Univ. Grenoble Alpes, CEA, Leti,
MINATEC Campus, F-38054 Grenoble
Grenoble, France
guillaume.goy@cea.fr

Antoine Loiseau
Univ. Grenoble Alpes, CEA, Leti,
MINATEC Campus, F-38054 Grenoble
Grenoble, France
antoine.loiseau@cea.fr

Philippe Gaborit
XLIM, University of Limoges
Limoges, France
gaborit@unilim.fr

***Abstract*—During this first year of the thesis, we focused on Hamming Quasi-cyclic (HQC). We introduce an horizontal attack against the Reed-Solomon (RS) decoding algorithm of HQC assuming an Hamming weight leakage model. In practice, our attack against the reference implementation of HQC128 can succeed by running 2^{96} operations over a Galois field.**

***Index Terms*—HQC, Post-Quantum Cryptography, Error Correcting Codes, Side-Channel Analysis, Horizontal Attack.**

HQC [1] is a post-quantum resistant KEM based on error-correcting code. It is an alternate candidate in the third round of the NIST call for proposal [2] and might be standardized in a fourth round. The exchanged message is protected by a random public key dependent error with a significant weight, too big to be decoded by the public decoder. The knowledge of the secret key allows to reduce the weight of the error which falls below the error correction capability of the code. The exchanged message can be decoded by a public decoder with public parameters and a shared key is derived from it.

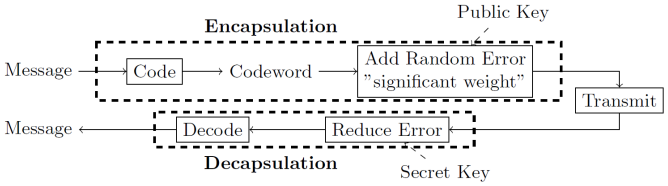

Fig. 1. HQC Framework

HQC uses a concatenated code with an internal duplicated Reed-Muller code, decode first, and an external Reed-Solomon (RS) code, decode after. An analysis of the HQC128 Decryption Failure Rate [1] shows that the RS codeword, between the two decoders, is error-free with a probability $1 - 2^{-10.96}$.

In our attack, we target this codeword during the syndrome computation of the RS decoding step, which is a matricidal multiplication. During this step, the codeword is no longer hidden by the secret key. If we are able to recover this codeword, we can deduce the exchanged message of the KEM using the public RS decoder. In practice, this codeword is 46 bytes long. The attack is developed thanks to two observations:
1. Each byte is involved in 30 Galois field multiplications which gives information redundancy. Given one measured trace of the decoding step, 30 informative sub-traces are available for each byte, allowing an horizontal correlation attack [3].
2. The knowledge of the decoder allows to cope with eventual attack errors. Indeed, if the number of erroneous recovered bytes is smaller than the error correction capability of the public RS decoder, the original message is recovered by applying it.

We go further by using a RS decoding algorithm called the Gurusami-Sudan (GS) decoder [4]. This kind of decoder provides a list of l closest codewords from the input and increases the error correcting capability. We combine this GS decoder with a listing strategy, assuming known the location of u error-free bytes in the codeword. We use the shortened RS code construction, by truncated the u coordinates and end up with a smaller RS codeword to decode. The number of errors to decode remains the same, but error correction capability increases when the $\frac{k}{n}$ rate of the RS code decreases. These strategies are not free, increasing the attack computation time as well as the final error correction capability and then the success rate of the attack.

One countermeasure, first presented by Clavier et al. [3] for RSA exponentiation, can be applied. It consists in randomizing the order of Galois multiplications within the syndrome decoding algorithm. This shuffle prevents from labeling sub-traces and succeeding the attack.

We compare practical results with the reference implementation of HQC [1] and an analysis of simulated traces in the Hamming weight leakage model. We show that an attack with a complexity of 2^{96} operations over the Galois field is enough to recover the KEM shared key. This attack challenges the claimed 128 bits of security of HQC.

References

[1] Aguilar-Melchor C., Aragon N., Bettaieb S., Bidoux L., Blazy O., Deneuville J.C., Gaborit P., Persichetti E., Zémor G.: Hamming quasi-cyclic (HQC) (2017) & reference implementation, https://pqc-hqc.org/implementation.html2
[2] NIST: Submission requirements and evaluation criteria for the post-quantum cryptography standardization process. (2016)
[3] Clavier C., Feix B., Gagnerot G., Roussellet M., Verneuil V.: Horizontal correlation analysis on exponentiation. In: International Conference on Information and Communications Security. pp. 46-61. Springer (2010)
[4] Justesen J., Hoholdt T.: A course in error-correcting codes, vol. 1. European Mathematical Society (2004)