Behind the mask: how a variable mask can reveal secret information (work in progress)

Agathe Cheriere[1,2]

Joint work with Benoit Gérard[2,4], Annelie Heuser[1,2], Pierre Loidreau[3,4], and Tania Richmond[4]

[1] CNRS, France
[2] IRISA, Rennes, France
{agathe.cheriere,benoit.gerard,annelie.heuser}@irisa.fr
[3] IRMAR
pierre.loidreau@univ-rennes1.fr
[4] DGA-MI, France
tania.richmond.nc@gmail.com

Abstract– The third round of the NIST standardisation process will soon be over and the selected schemes will become standard for the industry. This means that implementations based on selected schemes will be deployed into different kinds of devices used in our daily life. However, an implementation can be a significant weakness in the security of a scheme as first shown by Kocher [2]. Hence, NIST put forward the necessity of studying the implementations regarding side-channel attacks [3].

In this work, we focus on the schemes based on error-correcting codes, which reached the second round of the standardisation process. Those have at least one implementation that uses functions in constant-time to protect sensitive information. The constant-time is a common countermeasure to thwart remote timing attacks. One way to get a function that is executed in the same amount of time independently of the inputs is to replace conditional branching depending on the secret by using a variable call mask.

For instance, if an addition $a = a + b$ is only needed when a bit of secret is equal to one then the conditional branching can be replaced by the affectation of the variable *mask* depending on the secret bit. So the addition becomes $a = a + mask * b$. If *mask* is one then we have an addition with a non-zero element. Otherwise, it is an addition with a zero element.

But, depending on how the mask is created and used, an attacker may be able to recover sensitive information by other types of side-channel attacks. Indeed, when attackers have physical access to the device, they can use power consumption or electromagnetic emanation to get pieces of information. We have shown examples of attacks leading to a full key recovery by exploiting power measurements obtained during the processing of such masking technique [1].

Weaknesses related to power consumption are linked to the fact that not all operations have a similar energy cost. In the context of the aforementioned example, the weakness is that multiplying an element of 32 or 64 bits by one will induce a higher consumption than multiplying it by zero.Therefore as the mask is directly linked to the secret, the attacker obtained information on the secret.

The impact on security is not the same for each scheme, as the family of codes used and the structure of the cryptosystem are different. Thus, it is interesting to look at the specificity of schemes and their implementation. That is why we focus on both schemes' specificities and mask leakages for the second-round NIST candidates.

References

1. A. Cheriere, L. Mortajine, T. Richmond, and N. El Mrabet. Side-Channel Attack on ROLLO Post-Quantum Cryptographic Scheme. 2021. https://eprint.iacr.org/2021/477.pdf.
2. P. C. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In N. Koblitz, editor, *Advances in Cryptology – CRYPTO*, pages 104–113, Berlin, Heidelberg, 1996. Springer Berlin Heidelberg.
3. D. Moody, G. Alagic, D. C. Apon, D. A. Cooper, Q. H. Dang, J. M. Kelsey, Y.-K. Liu, C. A. Miller, R. C. Peralta, R. A. Perlner, A. Y. Robinson, D. C. Smith-Tone, and J. Alperin-Sheriff. Status report on the second round of the NIST post-quantum cryptography standardization process. Technical report, Jul 2020.