Internship of Master II

Cryptanalysis of Symmetric Primitives in the Post-Quantum World: ARX primitives

Mars-September 2018

with María Naya-Plasencia

1 Context of the Internship

The internship will take place at Inria-Paris, at the SECRET team[1] (Paris 12ème), in the context of the ERC project QUASYModo[2], that has started in september 2017. A PhD funding will be available for continuing the internship if pertinent.

2 Introduction

As years go by, the existence of quantum computers becomes more tangible and the scientific community is already anticipating the enormous consequences of the induced breakthrough in computational power. Cryptology is one of the affected disciplines. Indeed, the current state-of-the-art asymmetric cryptography would become insecure, and we are actively searching for alternatives. Symmetric cryptography, essential for enabling secure communications, seems much less affected at first sight: its biggest known threat is Grover's algorithm, which allows exhaustive key searches in the square root of the normal complexity. Thus, so far, it is believed that doubling key lengths suffices to maintain an equivalent security in the post-quantum world. The security of symmetric cryptography is completely based on cryptanalysis: we only gain confidence in the security of a symmetric primitive through extensive and continuous scrutiny. It is therefore not possible to determine whether a symmetric primitive might be secure or not in a post-quantum world without first understanding how a quantum adversary could attack it. Correctly evaluating the security of symmetric primitives in the post-quantum world cannot be done without a corresponding cryptanalysis toolbox, which neither exists nor has ever been studied. Next, doubling the key length is not a trivial task and needs to be carefully studied. The cryptographic community should propose effcient solutions secure in the post-quantum world with the help of the previously mentioned quantum symmetric cryptanalysis toolbox. This will help prevent the chaos that big quantum computers would generate: being ready in advance will definitely save a great amount of time and money, while protecting our current and future communications. Therefore, an important challenge to

[1] `https://www.rocq.inria.fr/secret/index.php`
[2] `https://www.inria.fr/en/centre/paris/news/erc-grant-for-maria-naya-plasencia`

solve is to redesign symmetric cryptography for the post-quantum world. We want to prepare ourselves for the post-quantum world. That is a fact, as shown by the efervescente about post-quantum asymmetric cryptography. Due to environmental constraints, it is very likely that common users will never take advantage of quantum capabilities, but a powerful adversary will. It is therefore vital that we dispose of primitives that are effcient on classical computers and secure against quantum adversaries. This means that we have definitely a lot of work to do with respect to symmetric cryptography. As symmetric cryptography completely lies in the variety and ever-changing landscape of symmetric cryptanalysis, we are convinced that it is not possible to determine for instance whether doubling the key length might make a concrete cipher secure or not in a post-quantum world, without first understanding how a quantum adversary could attack the primitive. Correctly evaluating the security of symmetric primitives in the post-quantum world cannot be done without a corresponding symmetric cryptanalysis toolbox, which neither exists nor has ever been studied. This internship will contribute to fill this gap. The aim of this toolbox is two-fold: 1) analyze existing cryptosystems/primitives, and 2) design new ones which will give us confidence in the post-quantum world.

3 Work Description

During the internship, an interesting first direction to follow will be to analyze the security of ARX constructions against quantum adversaries. The ARX construction is a largely used one in symmetric primitives: it uses three transformations that are XOR, modular additions and rotations. The two main symmetric recommendations for achieving post-quantum security now-a-days are AES-256 and Salsa20 with a key of 256 bits (as is pointed out for instance in `https://pqcrypto.eu.org/docs/initial-recommendations.pdf`). This might seem shocking due to the lack of detailed and dedicated security analysis of both these primitives in the post-quantum setting. The intern will try to determine and improve the understanding of the security of the primitive Salsa20 and better understand the effects of quantum computers on the security of ARX constructions. Some algorithms and tools that might be helpful for this are Grover's algorithm [2], Simon's algorithm [4] (see for instance the recent new applications on symmetric cryptography [3]) or the recently improved quantum collision search algorithm [1].

Contact

If you are interested, do not hesitate to contact María for any further information:
`maria.naya_plasencia@inria.fr`
INRIA Paris
2 Rue Simone IFF
75012 Paris - France

References

1. Chailloux, A., Naya-Plasencia, M., Schrottenloher, A.: An efficient quantum collision search algorithm and implications on symmetric cryptography. In: Asiacrypt 2017 (2017), to appear. http://eprint.iacr.org/2017/847
2. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: ACM Symposium on the Theory of Computing 1996. pp. 212–219. ACM (1996)
3. Kaplan, M., Leurent, G., Leverrier, A., Naya-Plasencia, M.: Breaking symmetric cryptosystems using quantum period finding. In: Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II. Lecture Notes in Computer Science, vol. 9815, pp. 207–237. Springer (2016)
4. Simon, D.R.: On the power of quantum cryptography. In: 35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 20-22 November 1994. pp. 116–123. IEEE Computer Society (1994), http://dx.doi.org/10.1109/SFCS.1994.365701