Internship of Master II

Advanced Post-Quantum Symmetric Cryptanalysis

Mars-Septembre 2019

with María Naya-Plasencia

1 Context of the internship

The internship will take place at Inria-Paris, at the SECRET team[1] (Paris 12‘eme), in the context of the ERC project QUASYModo[2], that 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 postquantum 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,

[1] https://www.rocq.inria.fr/secret/index.php

[2] https://project.inria.fr/quasymodo/

an important challenge to 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 postquantum 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: Find New Quantum Cryptanalysis

The community needs to design optimal cryptanalysis algorithms for evaluating the security of symmetric primitives when quantum computation is available. In the last few years, many results have appeared in this direction, like [BN18,CNS17,KLLN16b,LM17,KLLN16a].

During this stage we will consider the following possible approach: apply promising quantum algorithms to existing cryptanalysis families. We aim not only to use existing quantum algorithms as black boxes, but also to adapt them to our situations in order to optimise cryptanalysis algorithms, as we have started doing in [KLLNP15].

In particular we want to analyze the cryptanalysis based on the division property introduced in [Tod15] and better explained in [BC16]. The first aim will be to determine the complexity of a quantized division-property attack. Next, we will consider impossible differential attacks, as generalized in [BNPS14], and similarly provide a quantum version for this family, by using list-merging ideas as in the new quantum collision algorithms. We will also study the concrete applications on actual ciphers, and the complexity that would reach the theoretical attacks in this promising candidates, with the aim of determining the security margin of such primitives in the post-quantum world.

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

BC16. Christina Boura and Anne Canteaut. Another view of the division property. In *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I*, volume 9814 of *Lecture Notes in Computer Science*, pages 654–682. Springer, 2016.

BN18. Xavier Bonnetain and María Naya-Plasencia. Hidden shift quantum cryptanalysis and implications. page To appear, 2018.

BNPS14. C. Boura, M. Naya-Plasencia, and V. Suder. Scrutinizing and Improving Impossible Differential Attacks: Applications to CLEFIA, Camellia, LBlock and Simon. In *Asiacrypt 2014*, volume 8873 of *LNCS*, pages 179–199, 2014.

CNS17. André Chailloux, María Naya-Plasencia, and André Schrottenloher. An efficient quantum collision search algorithm and implications on symmetric cryptography. In *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part II*, volume 10625 of *Lecture Notes in Computer Science*, pages 211–240. Springer, 2017.

KLLN16a. Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. 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*, volume 9815 of *Lecture Notes in Computer Science*, pages 207–237. Springer, 2016.

KLLN16b. Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Quantum differential and linear cryptanalysis. *IACR Trans. Symmetric Cryptol.*, 2016(1):71–94, 2016.

KLLNP15. Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Simon's algorithm and applications on symmetric cryptography. http://naya.plasencia.free.fr/Maria/papers/simon.pdf, 2015.

LM17. Gregor Leander and Alexander May. Grover meets simon - quantumly attacking the fx-construction. In *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part II*, volume 10625 of *Lecture Notes in Computer Science*, pages 161–178. Springer, 2017.

Tod15. Yosuke Todo. Integral cryptanalysis on full MISTY1. In *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I*, volume 9215 of *Lecture Notes in Computer Science*, pages 413–432. Springer, 2015.