Internship of Master II

Key-Length Extensions for Post-Quantum Symmetric Primitives

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

[1] `https://www.rocq.inria.fr/secret/index.php`
[2] `https://project.inria.fr/quasymodo/`

and money, while protecting our current and future communications. Therefore, 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 secure ways for increasing the key-length

During the stage we plan to analyze pre-existing key schedules[3]; classify them in types; analyze the advantages and disadvantages with respect to adapting them to longer keys; and decide which ones might be a good starting point for achieving the desired goals. Next, concrete proposals for key schedules with longer keys must be studied in detail. We plan to define and analyse the best apparent options in different cases, as well as their portability: will they be easy to apply on any cipher? Which types of cipher can benefit from these extensions? Some more questions are still open, such as: Is it enough to consider longer keys, or do we also need larger internal states, for example in the cases where generic distinguishers on the internal state apply? Up to what point can we increase the key length for a given size of the internal state without compromising the security? How will this affect operation modes, and which security will they be able to provide in the post-quantum world? During this stage, we will try to solve them and find convincing answers.

Starting with Substitution-Permutation Networks (SPN) with elaborate key-schedules, like AES [DR02] and several AES-inspired ciphers, and followed by SPN ciphers with near-nonexistent key schedules (see the variants of LED with different key sizes), we will try to understand how far can a key be extended without reducing the security, as well as to correctly understand the relation

[3] Commonly, ciphers are composed of rounds, and the key-schedule is the algorithm that, from the master key, generates the subkeys to be processed during each round

between the size of the state and the maximum reachable security. For instance, if we wanted to provide an AES candidate with a 512-bit key, what would be the best option: to keep the same state and increase the key length and the number of rounds, or to consider bigger states, as was already proposed in the original Rijndael specification? In the case of LED-like ciphers [GPPR11], how can we increase key length without being limited by the state size? Which are the best distinguishers we can build in the post-quantum world with respect to the state size? These questions should be answered in order to be able to propose new candidates with bigger keys. The same procedure will be then performed with Feistel network ciphers, trying also to find generic answers and options.

Another important point to study in detail here is how these sizes will affect the different Time-Memory-Data trade-offs (as the ones from Hellman [Hel80]) 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

DR02. J. Daemen and V. Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Information Security and Cryptography. Springer, 2002.

GPPR11. J. Guo, T. Peyrin, A. Poschmann, and M. J.B. Robshaw. The LED Block Cipher. In *CHES 2011*, volume 6917 of *LNCS*, pages 326–341. Springer, 2011.

Hel80. M. Hellman. A cryptanalytic time-memory trade-off. *IEEE Transactions on Information Theory*, 26(4), 1980.