Thesis Subject for André Schrottenloher

Cryptanalysis of Symmetric Primitives in the Post-Quantum World

February 2018 - February 2021

with María Naya-Plasencia

1 Context of the Thesis

The PhD 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 is available to this effect.

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

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

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

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 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 PhD 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.

The direction of this PhD of adequately preparing symmetric cryptography for the post-quantum world can logically be decomposed in two main sequential objectives:

2.1 Elaborate a post-quantum symmetric cryptanalysis toolbox

In a nutshell, the first aim of the PhD will be to define and **design optimal cryptanalysis algorithms for evaluating the security of symmetric primitives when quantum computation is available**, making up for the current lack of investigation and results.

The main questions that could be investigated are: how to analyze the security of symmetric algorithms in the post-quantum world? How to optimally apply the known cryptanalysis techniques with the help of quantum algorithms such as [Gro96,Amb07,BHMT02,HH00,Sho97,Sim94]? Might there be new cryptanalysis techniques to study? Some other satellite questions that would be interesting to solve are: **when** can a primitive that is unbroken in the classical world become broken in the post-quantum one? When does a theoretical but impractical attack in the classical world become practical in the post-quantum world? **Two different approaches can be followed to answer these questions: Quantizing classical attacks, and designing quantum cryptanalysis afresh.**

To successfully complete the first approach substantial background work must be done first to survey all existing symmetric attacks, which are often too technical and specific to be seen in a general-optimized way, and to generalize them. Next, the generalized (and not generic!) cryptanalysis algorithms should be improved using quantum tools. Our recent results **[KLLNP15,KLLN16]** point out that some non-intuitive results may appear. It seems like an arduous

task that should be done carefully.
The second approach aims to apply promising quantum algorithms to new cryptanalytic applications. The aim is not only to use existing quantum algorithms as black boxes, but also to adapt them to our situations in order to optimise cryptanalysis algorithms. Simon's algorithm [Sim94] has proven to be an excellent candidate to start this task, breaking for instance popular constructions that are secure in the classical world, such as CBC-MAC. To sum up, the aim of this first objective is to help building a cryptanalysis toolbox for determining the post-quantum security of any symmetric primitive under consideration[3].

The first approach is to consider generalized cryptanalytic algorithms, rewrite them if needed, and provide optimized representations in order to reduce the complexity of the algorithm with quantum computing available. Some preliminary interesting results [KLLNP15,KLLN16] show, **for example, that slide attacks are drastically sped up: their complexity drops from exponential to linear, meaning that secure algorithms in the classical world might became insecure in the post-quantum one.** Also, considering basic differential and truncated differential attacks, it seems possible to find some cases where the basic attack works with a lower complexity than the truncated attack in the classical world, but the truncated attack works with a lower complexity in the post-quantum world. This shows that it does not suffice to simply quantize the best classical attacks one wants to find the best post-quantum attack. The second approach, to design quantum symmetric cryptanalysis afresh, will seek new applications of promising quantum algorithms, not just considering them as black boxes, but also adapting them to our situations. For instance, it could be of interest to study whether some particular ciphers or constructions might be vulnerable to new cryptanalysis techniques from the post-quantum world, for example using variants of [Sim94,HH00,Sho97], as in [KLLN16].

Studying quantum algorithms optimized with respect to our concrete scenarios is an interesting first direction to follow (as André Schrottenloher has already started doing during his internship in [CNPS17]).

2.2 Designing good post-quantum symmetric primitives

The first naive reaction from someone asked about symmetric cryptography in the post-quantum world might be to say that we should have all we need in AES-256 [DR02], an already existing standard that seems secure so far. But this is far from true: indeed, AES-256 does not meet most of the needs: 1) it is not suitable for lightweight applications; 2) it seems impossible to convince most users to start using it *right away* due to implementation/performance issues; 3) no alternative exists for more than 128-bit security; 4) it is good to have diversity; 5) as already pointed out, there is no way of determining its actual post-quantum security margin. No good alternative exists: Salsa-20 has been proposed as candidate in the H2020 project PQCrypto, but being much less

[3] even for broken primitives with known attacks better than generic ones

analyzed than AES and not yet standardized, it meets fewer general needs than AES-256. It is important to realize that adapting symmetric primitives to the post-quantum world by increasing the key length, which seems an easy measure in theory, is not that easy in practice. Therefore, the second possible aim of the PhD is three-fold: analyze the state-of-the-art symmetric cryptography with the toolbox obtained; find pseudo-generic and secure ways of extending the key length; and design, implement and standardize symmetric efficient cryptographic functions secure in the post-quantum world.

Indeed, a first task will be to evaluate the post-quantum security and security margin of the most used current symmetric designs with respect to these new attacks/tools. Once all of the optimized cryptanalysis algorithms have been found, applying them will be an arduous task, but we hope that it will be nearly automated after having obtained the toolbox. Studying and comparing the security and the security margins of state-of-the-art symmetric primitives with post-quantum adversaries would definitely be of interest, and would indicate how far we are from preparing symmetric crypto for the post-quantum world, and which gaps remain to be filled.

We will start by analyzing the security of the actual encryption standard, AES, against a quantum adversary.

Another direction is to find secure ways for increasing the key-length. First, the different existing key-schedules can be studied in order to classify them, analyze the advantages and disadvantages with respect to adapting them to longer keys, and decide which ones can be good starting points for achieving the desired goals. Concrete proposals for key schedules with longer keys may then be defined and the best apparent options should be analysed, as well as their portability: will they be easy to apply to any cipher? Which types of cipher can benefit from these extensions? 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 which point can we increase the key length for a given size of the internal state without compromising the security?

References

Amb07. A. Ambainis. Quantum walk algorithm for element distinctness. *SIAM J. Comput.*, 37(1):210–239, 2007.

BHMT02. G. Brassard, P. Høyer, M. Mosca, and A. Tapp. Quantum amplitude amplification and estimation. In *Quantum computation and information*, volume 305 of *Contemp. Math.*, pages 53–74. Amer. Math. Soc., RI, 2002.

CNPS17. André Chailloux, María Naya-Plasencia, and André Schrottenloher. An efficient quantum collision search algorithm and implications on symmetric cryptography. Asiacrypt 2017, to appear, 2017. `http://eprint.iacr.org/2017/847`.

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

Gro96. L. K. Grover. A fast quantum mechanical algorithm for database search. In *ACM Symposium on the Theory of Computing 1996*, pages 212–219. ACM, 1996.

HH00. L. Hales and S. Hallgren. An improved quantum fourier transform algorithm and applications. In *FOCS 2000*, pages 515–525. IEEE Computer Society, 2000.

KLLN16. 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.

KLLNP15. Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Quantum differential and linear cryptanalysis. In *quant-ph cs.CR*. arXiv, 2015.

Sho97. P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

Sim94. Daniel R. Simon. On the power of quantum cryptography. In *35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 20-22 November 1994*, pages 116–123. IEEE Computer Society, 1994.