New tools for quantum symmetric cryptanalysis

Context

Symmetric cryptography is one of the cornerstones of modern digital security, as it allows to protect the confidentiality, authenticity and integrity of communications as soon as participants share a common secret key. Symmetric cryptosystems answer to very high constraints on performance and security.

The development of quantum computing devices impacts severely the security guarantees of asymmetric cryptography, leading to an ongoing transition to *post-quantum*, i.e., quantum-secure, cryptosystems. Fortunately, mainstream symmetric primitives are considered robust against hypothetical quantum adversaries [1]. However, our confidence in the security of symmetric cryptosystems is upheld by a rigorous cryptanalysis effort. This effort needs to continue in the context of post-quantum security.

In recent years, *quantum symmetric cryptanalysis* has mostly focused on two aspects:

- The translation of classical symmetric cryptanalysis techniques into quantum attacks, by means of generic algorithmic frameworks [3]. These attacks usually fall in the scope of a *square root speedup*, i.e., halving of bit-security levels. However, they cannot be equated to their classical counterparts [6], as they usually exhibit different optimization strategies.

- The development of new algorithmic tools, leading to new attacks. Computational tasks exhibiting a large quantum advantage seem to be rare in symmetric cryptography, with no equivalent to Shor's algorithm [10]. Nevertheless, an "active" quantum attacker can break some classically-secure schemes [7], and in recent years, several cryptanalysis techniques have been shown to go further than a square root speedup. This was first shown with Simon's algorithm [4], and more recently using quantum convolution algorithms [9], which can be seen as a more general quantum enhancement of statistical cryptanalysis.

The development of more complex attack frameworks, whether classical or quantum, has made the use of *automatic tools* almost mandatory. Such tools allow to exhaust a set of possible attacks using dedicated or generic solvers and optimizers (MILP, SAT), simplifying the task of the cryptanalyst. However, writing an efficient tool requires to understand precisely the attack strategy that one studies, e.g. how to deduce the complexity of an attack algorithm from a minimal set of choices or patterns.

Objectives

The goal of this thesis is to improve the *tools* for quantum cryptanalysis of symmetric primitives, where *tools* is to be understood in two different ways.

Algorithmic Tools. At a fundamental level, quantum cryptanalysis relies on quantum algorithms for cryptographic problems. While quantum search and quantum period-finding [8] have been used for a long time, the quantum convolution algorithm [9] is a more recent development with the potential to adapt to a larger class of ciphers. Our goal will be to identify new applications of this algorithm to key-recovery attacks on block ciphers (which seems so far to be the area of interest), for example going from linear cryptanalysis (studied in [9]) to differential-linear cryptanalysis.

Automatic Tools. After gaining experience with both advanced quantum algorithms for cryptanalysis (i.e., the quantum convolution algorithm) and modeling techniques, we will study the automation of these new quantum attacks. Contrary to many attack algorithms, the complexity analysis of convolution algorithms is technical and likely needs to be simplified in order to fit into a MILP or SAT model. Our objective is to obtain a model still robust enough to easily obtain valid attacks.

Organization

This PhD position takes place within the QATS project (ANR JCJC, PI : André Schrottenloher), which studies automatic tools for quantum cryptanalysis.

Candidates for the PhD position should hold a Master or equivalent and have experience in cryptography. Basic knowledge of quantum computing is recommended.

The PhD student will be integrated in the team CAPSULE at the Inria Center at the University of Rennes. The PhD will be co-supervised by:

- Patrick Derbez, Inria starting faculty, (patrick.derbez@inria.fr)
- André Schrottenloher, researcher, Inria Rennes (andre.schrottenloher@inria.fr)

References

[1] ANSSI: Anssi views on the post-quantum cryptography transition (2022), https://www.ssi.gouv.fr/en/publication/anssi-views-on-the-post-quantum-cryptography-transition/

[2] Bao, Z., Guo, J., Li, S., Pham, P.: Automatic quantum multi-collision distinguishers and rebound attacks with triangulation algorithm. In: ACISP (2). Lecture Notes in Computer Science, vol. 14896, pp. 24–43. Springer (2024)

[3] Bonnetain, X., Naya-Plasencia, M., Schrottenloher, A.: Quantum security analysis of AES. IACR Trans. Symmetric Cryptol. **2019**(2), 55–93 (2019)

[4] Bonnetain, X., Schrottenloher, A., Sibleyras, F.: Beyond quadratic speedups in quantum attacks on symmetric schemes. In: EUROCRYPT (3). Lecture Notes in Computer Science, vol. 13277, pp. 315–344. Springer (2022)

[5] Dong, X., Guo, J., Li, S., Pham, P.: Triangulating rebound attack on aes-like hashing. In: CRYPTO (1). Lecture Notes in Computer Science, vol. 13507, pp. 94–124. Springer (2022)

[6] Kaplan, M., Leurent, G., Leverrier, A., Naya-Plasencia, M.: Quantum differential and linear cryptanalysis. IACR Trans. Symmetric Cryptol. **2016**(1), 71–94 (2016)

[7] Kuwakado, H., Morii, M.: Security on the quantum-type even-mansour cipher. In: ISITA. pp. 312–316. IEEE (2012)

[8] Leander, G., May, A.: Grover meets simon - quantumly attacking the fx-construction. In: ASIACRYPT (2). Lecture Notes in Computer Science, vol. 10625, pp. 161–178. Springer (2017)

[9] Schrottenloher, A.: Quantum linear key-recovery attacks using the QFT. In: CRYPTO (5). Lecture Notes in Computer Science, vol. 14085, pp. 258–291. Springer (2023)

[10] Shor, P.W.: Algorithms for quantum computation: Discrete logarithms and factoring. In: FOCS. pp. 124–134. IEEE Computer Society (1994)