Security of ASCON and Lightweight Symmetric Primitives against Quantum Attackers

Context

In 2018, the NIST[1] launched a competition to select a new family of *lightweight* symmetric authenticated encryption algorithms, therefore recognizing the importance that lightweight cryptography has taken in industrial applications and research.

In the context of symmetric cryptography, which secures communications when the participants already possess a shared secret key, performance is a crucial aspect. In recent years, the use of cryptography in constrained environments has risen (remote sensors, medical applications, *etc.*), prompting research and development of new algorithms specifically optimized for such aspects. After five years of competition, ASCON [6] was selected for standardization [11], and is now expected to become a major commercial standard. In parallel, many other lightweight designs have been proposed throughout the competition [5] and later on.

Meanwhile, the ongoing progress towards large-scale quantum computers has prompted cryptographers to design *post-quantum* cryptographic schemes, i.e., resistant to the enhanced computational power of such machines. The most urgent matter was to find replacements for discrete logarithm and factoring-based cryptography, both broken by Shor's algorithm [14]. This was the goal of another, independent standardization process from NIST [12] which is still ongoing. The first selected standards are progressively moving towards wide-spread adoption, as many governmental authorities recommend to transition [1].

Mainstream symmetric primitives are immune to Shor's algorithm and are widely believed to retain a good level of security against hypothetical quantum adversaries. However, security guarantees in symmetric cryptography come from dedicated cryptanalysis studies. While classical cryptanalysis is a well established field, *quantum* symmetric cryptanalysis does not have the same level of maturity. As an example, the ASCON family is a high-profile target with more than 20 published cryptanalysis papers [13, 2], but not a single one of them considered quantum attacks.

However, the past few years have shown that a lot can be said about the quantum security of symmetric ciphers. Notably, while it is typical to simply "halve" the security levels [7], this is not true for active adversary models [9] and even for passive adversaries in some examples [4]. These results were obtained by combining classical cryptanalytic properties [10] with more and more advanced quantum algorithms. In order to ensure its security on the long term, such a study needs to be made on ASCON.

Objectives

This PhD position takes place within the ASCON-CAT project, which studies the resistance of the ASCON cipher family against quantum attacks. ASCON-CAT aims at combining the expertise of its members in cryptography, quantum computing and physical implementations to assess the security levels of ASCON, and increase our understanding of the quantum security of symmetric cryptosystems as a whole.

Within this project, the goal of this PhD will be to analyze the impact of quantum cryptanalysis families on ASCON and develop dedicated attacks. The algorithms that we study will be formalized in the quantum circuit model, at the logical level. Different categories of attacks will be analyzed:

- Linear and differential attacks: while these do not lead to the most efficient classical attacks, there exists a large body of literature [10], including advanced attacks with dedicated quantum algorithms [8, 3].

- Algebraic attacks (including Meet-in-the-middle attacks on hashing or Duplex encryption modes): while these are the best classically, there is less available literature in the quantum setting.

[1] National Institute for Standards and Technology, a U.S. institution.

It is expected that some of the observations made on ASCON and / or cryptanalysis techniques will lead to results on other similar lightweight primitives.

Organization

Candidates for the PhD position should hold a Master or equivalent and have experience in cryptography. Basic knowledge of quantum computing is optional but 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, associate professor, University of Rennes / IRISA (patrick.derbez@irisa.fr)
- André Schrottenloher, researcher, Inria Rennes (andre.schrottenloher@inria.fr)
- Zoé Amblard, researcher, Thales SIX Gennevilliers (zoe.amblard@thalesgroup.com)

References

[1] ANSSI. *ANSSI Views on the Post-Quantum Cryptography transition.* 2022. URL: https://www.ssi.gouv.fr/en/publication/anssi-views-on-the-post-quantum-cryptography-transition/.

[2] Jules Baudrin, Anne Canteaut, and Léo Perrin. "Practical Cube Attack against Nonce-Misused Ascon". In: *IACR Trans. Symmetric Cryptol.* 2022.4 (2022), pp. 120–144. DOI: 10.46586/TOSC.V2022.I4.120-144. URL: https://doi.org/10.46586/tosc.v2022.i4.120-144.

[3] Xavier Bonnetain and André Schrottenloher. "Single-query Quantum Hidden Shift Attacks". In: *IACR Cryptol. ePrint Arch.* (2023), p. 1306. URL: https://eprint.iacr.org/2023/1306.

[4] Xavier Bonnetain, André Schrottenloher, and Ferdinand Sibleyras. "Beyond Quadratic Speedups in Quantum Attacks on Symmetric Schemes". In: *EUROCRYPT (3).* Vol. 13277. Lecture Notes in Computer Science. Springer, 2022, pp. 315–344.

[5] Joan Daemen et al. "Xoodyak, a lightweight cryptographic scheme". In: *IACR Trans. Symmetric Cryptol.* 2020.S1 (2020), pp. 60–87. DOI: 10.13154/TOSC.V2020.IS1.60-87. URL: https://doi.org/10.13154/tosc.v2020.iS1.60-87.

[6] Christoph Dobraunig et al. "Ascon v1.2: Lightweight Authenticated Encryption and Hashing". In: *J. Cryptol.* 34.3 (2021), p. 33.

[7] Lov K. Grover. "A Fast Quantum Mechanical Algorithm for Database Search". In: *STOC.* ACM, 1996, pp. 212–219.

[8] Akinori Hosoyamada. "Quantum Speed-Up for Multidimensional (Zero Correlation) Linear Distinguishers". In: *ASIACRYPT (3).* Vol. 14440. Lecture Notes in Computer Science. Springer, 2023, pp. 311–345.

[9] Marc Kaplan et al. "Breaking Symmetric Cryptosystems Using Quantum Period Finding". In: *CRYPTO (2).* Vol. 9815. Lecture Notes in Computer Science. Springer, 2016, pp. 207–237.

[10] Marc Kaplan et al. "Quantum Differential and Linear Cryptanalysis". In: *IACR Trans. Symmetric Cryptol.* 2016.1 (2016), pp. 71–94.

[11] NIST. *NIST Lightweight Cryptography - Finalists.* https://csrc.nist.gov/projects/lightweight-cryptography/finalists. 2023. URL: https://csrc.nist.gov/projects/lightweight-cryptography/finalists.

[12] NIST. *Post-quantum cryptography.* URL: https://csrc.nist.gov/projects/post-quantum-cryptography.

[13] Raghvendra Rohit et al. "Misuse-Free Key-Recovery and Distinguishing Attacks on 7-Round Ascon". In: *IACR Trans. Symmetric Cryptol.* 2021.1 (2021), pp. 130–155. DOI: 10.46586/TOSC.V2021.I1.130-155. URL: https://doi.org/10.46586/tosc.v2021.i1.130-155.

[14] Peter W. Shor. "Algorithms for Quantum Computation: Discrete Logarithms and Factoring". In: *FOCS.* IEEE Computer Society, 1994, pp. 124–134.