PhD proposal

Post-Quantum Cryptography for Aeronautics

Subject of the thesis

We would like to propose a thesis subject around the ongoing NIST post-quantum cryptography standardization, focusing on:

- the study of the various solutions proposed in the aeronautical context;
- the proposed alternatives or new solutions created for aerospace;
- the analysis of attacker models adapted to the constraints of aeronautics.

Description of the thesis

This thesis is related to the theme "Taking into account the threat of quantum algorithmics " in sub-theme 1 " Cryptography ".

The transition to resistant cryptographic systems to a quantum computer may be imposed shortly. NIST indeed has the power to impose this transition on any company working with the American government, and consequently to force in practice this transition on the world market. In France, the National Agency for Information System Security (ANSSI) also recommends the use of such mechanisms for applications requiring long-term security [LRANSSI].

The field of aeronautics, with life cycles that can extend over several decades, is preparing for this transition. An example, on the Toulouse site, are the R&T R-S3 / RE-0003-011 and R-S16 / RE-0003-011 proposed by CNES where it was asked to explicitly deal with the case of post-quantum cryptography for remote key injection in a satellite context. One of the future supervisors was the scientific expert carrying these two R&T.

NIST plans to standardize key exchange protocols (allowing two entities exchanging on an insecure channel to obtain a common secret) and signature protocols (allowing an entity to prove its identity). The competition has just gone into phase 2, and two of the future supervisors (Carlos Aguilar, ISAE, and Jean-Christophe Deneuville, ENAC) carry 4 of the 17 remaining proposals [NISTR2].

Some of these proposals have security based on problems deemed difficult in the theory of correcting codes. We would like to propose a thesis subject around:

- the study of the various solutions proposed in the aeronautical context;
- the proposed alternatives or new solutions created e s for aerospace;
- fine analysis of quantum attacker models adapted to the constraints of aeronautics.

[NISTR2] https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions

[LRANSSI] https://www.larecherche.fr/cryptographie/assurer-la-transition-vers-la-cryptographie-post-quantique-%C3%A0-laide-de-m%C3%A9canismes

Thesis program

The vast majority of work around the standardization of post-quantum cryptography targets the IT world with software implementations. Some works deal with hardware implementations, but not in the context of the usual constraints of aeronautics.

In addition, the attacker model generally chosen is that of an attacker having access to an ideal quantum computer (large number of qu-bits, no problems of consistency over time, etc.) and able to perform a large number of calculations even if these require considerable time (eg years). This model is interesting for candidates for the standardization of NIST because it makes it possible to propose standards which are usable even in the most adverse contexts. On the other hand, this approach requires the use of more complex mechanisms and larger keys than what is necessary in certain applications.

The objective of this thesis, as opposed to the works mentioned, is to study the question of the transition to a cryptography resistant to the quantum computer, in the context of aeronautics.

For this we will study which protocol would be optimal both in terms of signing and exchanging keys for various applications: satellites, planes, drones. A first question which is major in aeronautics, and especially for the satellite context, is the performance (time and size occupied) of an FPGA implementation (including an encoding of the keys in the FPGA so that they are inaccessible to the system operating). This constraint has absolutely not been taken into account for the moment and it is interesting to study what could be the best approach in such a context.

Thus, in a first step we will sort the candidates according to the estimated complexity for a hardware implementation including an encoding of the keys. We will carry out the first simple FPGA implementations for the most promising candidates and study the existing implementations.

Secondly, building on this first experience and our knowledge of the various candidates for standardization, we will focus on the choices that would have been made to optimize the algorithms in the IT context and which would have a negative impact in the FPGA context. For example, for the HQC candidate[1] that we proposed for standardization, the last phase of the key exchange corresponds to the decoding of a tensor code between a repetition code and a BCH code. This choice optimizes the size of the keys while allowing a formal analysis of the propagation of errors. Recent results (unpublished) from part of the HQC team show that it is possible to optimize even more the size of the keys if we use more elaborate codes (mixture of Reed-Solomon and Reed-Muller). This is probably a bad choice for an FPGA implementation because the gain in key size will certainly not compensate for the increase in the area used to process such codes. Conversely, a pure repetition code (with majority decoding) will significantly increase the keys but will simplify the decoding phase so much that it is very credible that the FPGA footprint is reduced. We emphasize HQC as this is one of the candidates we have proposed but equivalent questions arise for most candidates.

Third, we will review the more generic choices that have been made by the community or by NIST to achieve the highest possible security standards. For example we can cite the use of algorithms in constant time[2] or generic IND-CCA transformations. Let's focus on constant time, which ensures that local information leaks on the execution time of cryptographic algorithms will not give rise to attacks. This is particularly important when different applications, some of which are hostile, use the same memory cache. In a satellite in orbit, with a hard algorithm in an FPGA, one can question the credibility of such a context and therefore the use of constant time algorithms, often expensive, and it is interesting to study what would be the possible gains by renouncing to this approach.

Finally at the level of the attacker's modeling it is possible to replace the security analysis of the different protocols if we question some of the constraints that it is common to accept in the IT model. For example, at the signature level, the NIST requests that the candidates resist attackers who have access to 2^{64} signatures. In a satellite context we can consider that a much lower number if we force the signatory not to carry more than for example 2^{32} = 4 billion signatures, or even 2^{10} = 1024 signatures if for example the objective is to sign satellite firmware updates.

Another example is that of the transformations used by many candidates to resist an attacker in the QROM (quantum random oracle) model. Conventionally, we are satisfied with the ROM (classic random oracle) model which gives rise to less costly transformations, but it has been proven that a quantum attacker is strictly more powerful than the attacker considered in the ROM model, hence the use of the QROM model which takes into account this additional power of the quantum attacker. That said, there is no known effective quantum attack against a candidate for standardization that would use a proven transformation in the ROM model. It is therefore interesting to study the additional cost of QROM transformations and consider the alternatives.

References

1. AGUILAR MELCHOR C. , GABORIT P ,. "Cryptographic process and devices for the protection of private data", world patent, reference in France n ° 09/58598 of December 2, 2009
2. AGUILAR MELCHOR C. , BLAZY O., DENEUVILLE JC. , GABORIT P., ZEMOR G., “Efficient Encryption From Random Quasi-Cyclic Codes”, IEEE Trans. Information Theory 64 (5): 3927-3943 (2018)

These first two references correspond to the generic key exchange mechanism used by the vast majority of candidates for NIST standardization for a post-quantum key exchange (whether based on Euclidean networks or on codes). The publication of 2008 is a patent describing this mechanism and that of 2018 a formal proof of the security that this mechanism brings in the particular case of correcting codes.

3. Carlos Aguilar Melchor , Nicolas Aragon, Paulo Barreto, Slim Bettaieb, Loic Bidoux, Olivier Blazy, Jean-Christophe Deneuville , Phillipe Gaborit, Shay Gueron, Tim Guneysu, Rafael Misoczki, Edoardo Persichetti, Nicolas Sendrier, Jean-Pierre Tillich, Valentin Vasseur, Gilles Zemor ; BIKE: Bit Flipping Key Encapsulation ; NIST Candidate ; https://bikesuite.org/
4. Carlos Aguilar Melchor , Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jurjen Bos, Jean-Christophe Deneuville, Philippe Gaborit, Edoardo Persichetti, Gilles Zémor ; HQC (Hamming Quasi-Cyclic) ; NIST Candidate ; https://pqc-hqc.org/
5. Carlos Aguilar Melchor, Nicolas Aragon, Magali Bardet, Slim Bettaieb, Loic Bidoux, Olivier Blazy, Jean-Christophe Deneuville , Philippe Gaborit, Adrien Hauteville, Ayoub Otmani, Olivier Ruatta, Jean-Pierre Tillich, Gilles Zemor ; ROLLO (Rank-Ouroboros, LAKE and LOCKER ; NIST Candidate ; https://pqc-rollo.org/
6. Carlos Aguilar Melchor , Nicolas Aragon, Slim Bettaieb, Loic Bidoux, Olivier Blazy, Alain Couvreur, Jean-Christophe Deneuville , Phillippe Gaborit, Adrien Hauteville, Gilles Zemor ; RQC (Rank Quasi-Cyclic) ; NIST Candidate ; http://pqc-rqc.org/

These four references correspond to 4 of the 17 candidates still in course for post-quantum standardization (exchange of keys) for which the supervisors are part of the proposing team.

Finally, the thesis director was the scientific manager of the R&T R-S3 / RE-0003-011 and R-S16 / RE-0003-011 proposed by CNES where he was asked to deal explicitly with the case of post- quantum for remote key injection in a satellite context.

[1] https://pqc-hqc.org/

[2] For a description of the problem of constant time see https://www.bearssl.org/constanttime.html