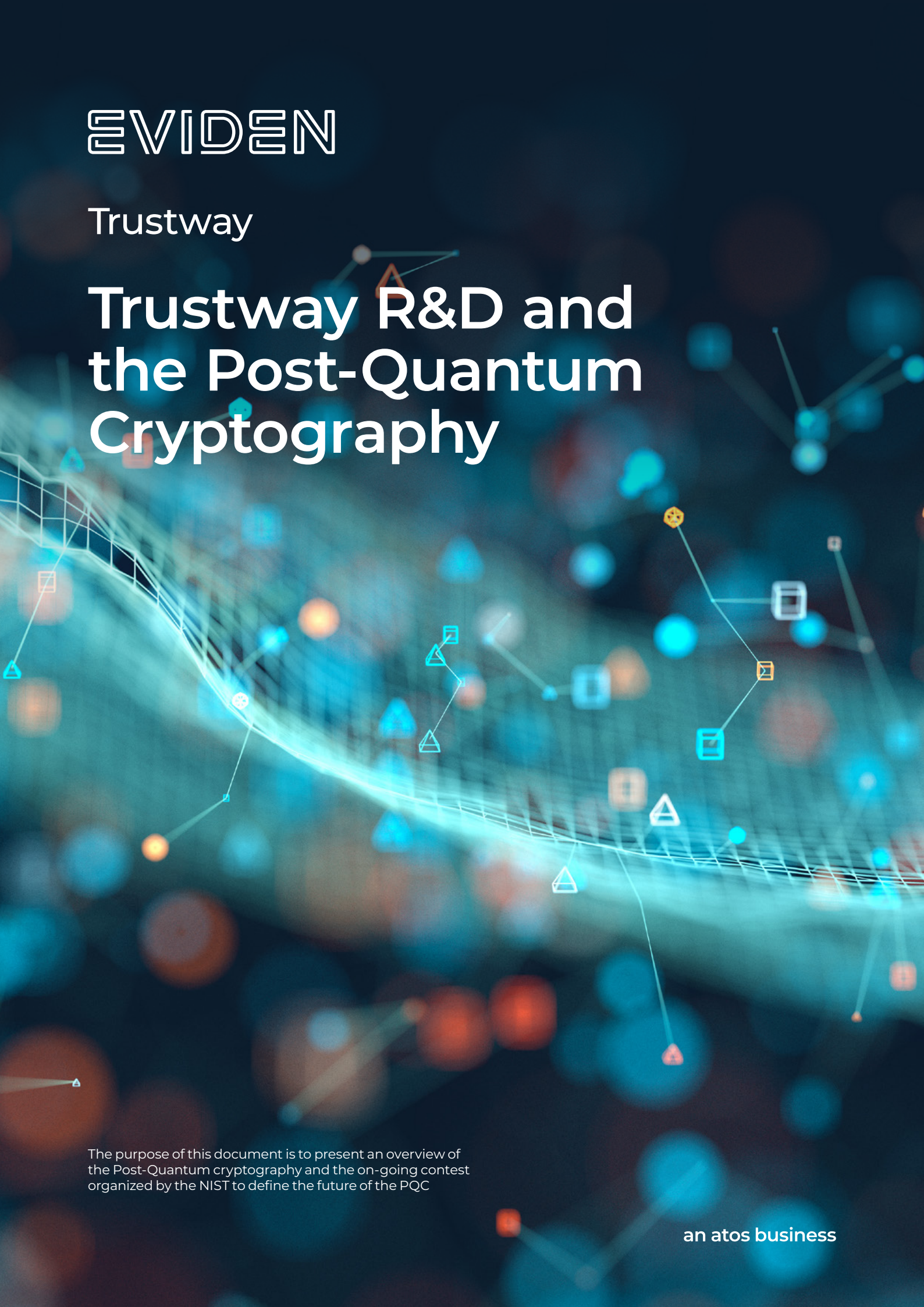
EVIDEN

Trustway

Trustway R&D and the Post-Quantum Cryptography



The purpose of this document is to present an overview of the Post-Quantum cryptography and the on-going contest organized by the NIST to define the future of the PQC

an atos business

About the author

Etienne Marcatel holds a bachelor's degree in Mathematics from the Université de La Rochelle and a Master degree in Cryptography from the Université de Rennes 1.

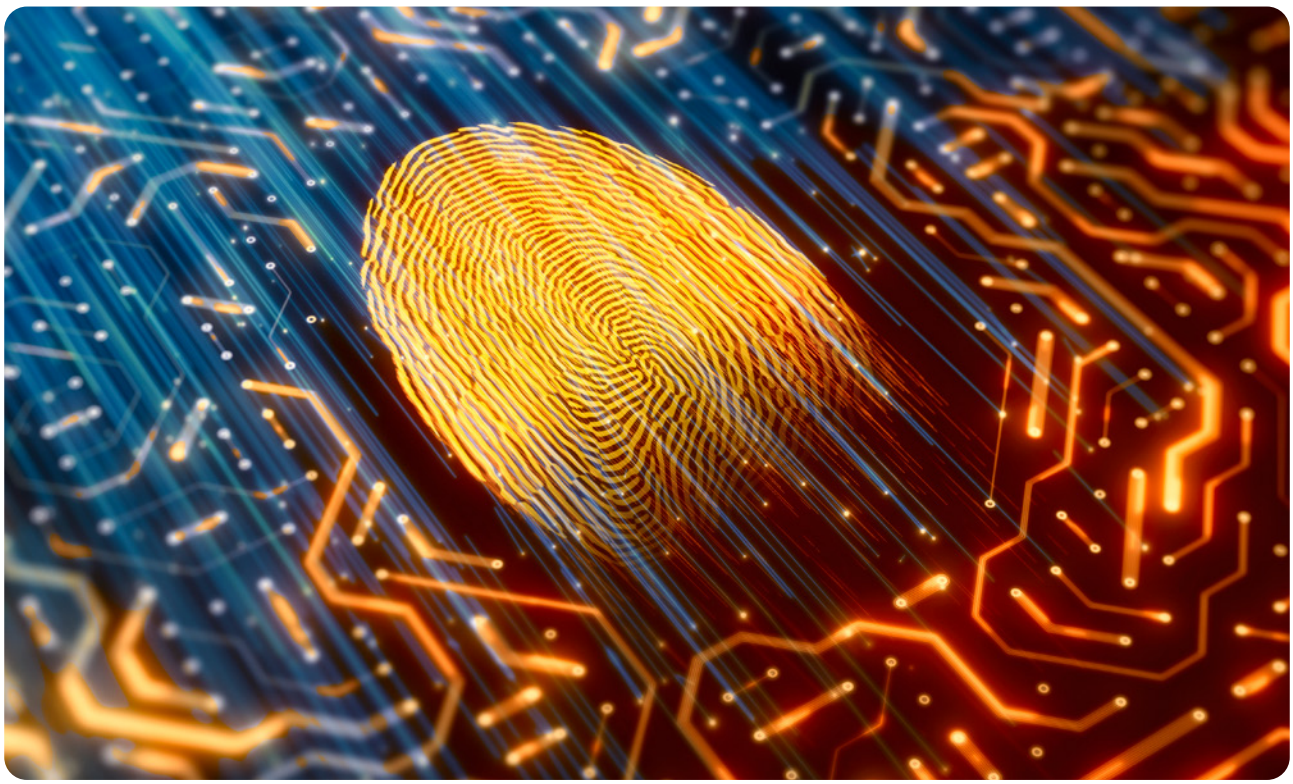
He is currently doing his PhD at the Université Grenoble Alpes.

Trustway Proteccio

Trustway Proteccio™ is a portfolio of Hardware Security Module (HSM) providing software solutions with a high performance and highly secure environment where they can carry out their most sensitive cryptographic operations.

The combination of its physical security equipment and a cryptographic core that is subject to the strictest security requirements brings one of the most certified cryptographic modules in the world to company information systems and cloud services.

With its simplified implementation designed for autonomous deployment, critical environments get an optimum solution for unconditional security of their sensitive data at the most competitive price.



2 | A cryptographic hybridization to ideally prepare for post-quantum migration.

Contents

1 Trustway

Cryptographic Products Business Unit

Cryptographic products, aa Eviden Security Division Business Unit geared to Secret Protection

As a European player in integrated security, Eviden has built up a unique body of expertise in information systems security, bringing together consulting and systems integration expertise and an in-depth understanding of corporate security technologies.

Eviden's experts capitalize on a recognized expertise gained during some of the biggest international security programs, involving millions of users. With Eviden, our customers can assess the risks they face, and implement and manage appropriate solutions to protect their business.

Cryptographic products Business Unit

The Cryptographic products Business Unit is focused on the development of advanced cryptographic products and their associated management infrastructures.

The Trustway Product Line delivers high-performance offer encompassing Crypto Devices (Hardware Security Modules), VPN (IP Encryptors, VPN Client) and globull™ secure mobile personal environment so as to deliver watertight security to nomadic individuals.

In Cryptographic products BU, from systems and software engineers to security consultants, from operational marketing to manufacturing specialists, each member of the team is an integral part of the everyday conduct of the business to the benefit of Trustway security-conscious clients.

Strong Culture

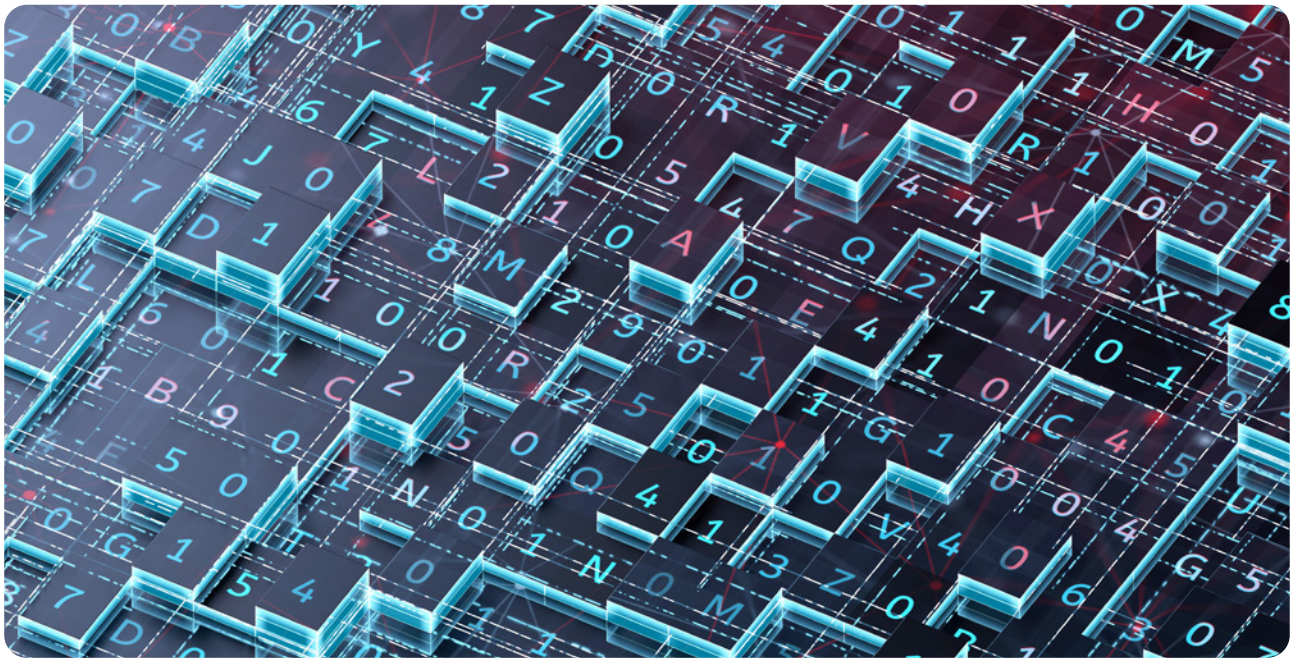
At Cryptographic products, we believe employees with varied backgrounds, experiences and perspectives strengthen our organization. Employees thrive in an environment that supports open communications with a true commitment to individual performance and growth. Our business operates within a culture that believes in constant respect for people and the highest ethical behavior by all.

Trustway

100% European

Trustway products and solutions are 100% designed and developed by Eviden in France. This means that customers and partners can benefit from 100% European technology and engineering control.

2 Post-Quantum Cryptography



In finance, transportation, health and many other areas, cybersecurity has become a crucial part of modern life. Many uses exist such as securing payments or guiding trains remotely, cybersecurity is of paramount importance and cryptography is the cornerstone.

There are two types of cryptography, symmetrical and asymmetrical with respective emblematic representatives: AES and RSA, which complement each other and are both essential to today's cybersecurity systems.

Nowadays, we also hear more and more about the quantum computer, a computer based on principles no longer derived from classical physics but quantum physics. These computers are not necessarily super calculators but have computational faculties that offer new possibilities. Among these possibilities is Shor's algorithm, released in the 1990s, which allows one to factor very large numbers, or to solve the discrete logarithm problem. This algorithm which seems innocuous to someone unaware can be devastating.

Currently 100% of the asymmetric cryptography used would be undermined by this algorithm, if one could use the Shor's algorithm, provided one had a sufficiently powerful quantum computer.

Shor's algorithm

The idea of the Shor's algorithm is first to reduce the factorization problem to a search problem of the order of an element in an abelian group. The reduction part can be done using a classical computer, then the search problem is solved using a quantum computer. The latter part heavily relies on the use of the Quantum Fourier Transform which is done efficiently on a Universal Quantum Computer.

To break RSA using Shor's algorithm, an attacker needs a quantum computer with twice the amount of logical Qbits than the modulus size. Nowadays, the recommended modulus size for RSA is 2048 bits, thus, one would require a 4096 logical Qbit Universal Quantum Computer to break it efficiently.

Why is this algorithm published 25 years ago considered only now?

The answer is simple, when it was published, most experts at the time thought that a quantum computer exceeding the capabilities of simulations was totally unfeasible for at least half a century, then it is called quantum supremacy. However, recent advances in the field have led to quantum supremacy and suggests that a large-scale computer could be built. This computer should be able to use Shor's algorithm. Even without reaching such a scale, our lack of knowledge about hybrid attacks using an intermediate quantum computer coupled with a conventional computer leaves a huge doubt. These possibilities threaten asymmetric cryptography, thus the entirety of cybersecurity.

But fortunately, this problem does not mark the end of cryptography, indeed since decades, other asymmetric cryptosystems resistant to Shor's algorithm and known attacks have emerged. The oldest is McEliece's cryptosystem, developed only a year after RSA, which is still secure today, with or without quantum computers. Other proposals from different theories have emerged since then. We call this asymmetric cryptography the Post-Quantum Cryptography or Quantum Safe Cryptography.

With the accelerating construction of the quantum computer, the NIST (American standardization institute) announced in 2016 a new standardization process dedicated solely to Post-Quantum Cryptography. The aim is to ensure the maintenance of secure cryptographic standards even in the quantum era, by releasing standards around 2022. This announcement gave a lot of visibility to the field, allowing the flowering of research projects and thus accelerating research on the subject. This process is relatively different from previous NIST competitions (AES and SHA-3) because this time, several cryptosystems will be standardized. The goal is to be able to change the standard if a theory becomes unusable.

This competition, combining Encryption/Key Exchange and Signatures, is mostly focused on four different approaches:

- Lattices (https://en.wikipedia.org/wiki/Lattice-based_cryptography),
- Error correcting codes (https://en.wikipedia.org/wiki/Error_correction_code),
- Multivariate polynomials (https://en.wikipedia.org/wiki/Multivariate_cryptography),
- The others, with more exotic proposals.

By the end of 2017, 69 candidates were competing in the first round, after a few weeks many were already discarded because they were vulnerable or totally broken. A year later, in early 2019, NIST announced a list of 26 candidates going to the second round. This list is composed of 17 encryptions/Key Exchange Mechanism (KEM) and 9 signatures. the 26 schemes are divided according to the approach on which they are based as follows:

- 12 lattices (3 signatures, 9 KEM), • 7 encryptions/KEM based on error correcting codes,
- 4 signatures based on multivariate polynomial,
- 1 KEM based on Isogenies of supersingular elliptic curves (https://en.wikipedia.org/wiki/Supersingular_elliptic_curve),
- 2 signatures using symmetrical cryptography.

The NIST conference at CRYPTO 19'

A few months after the start of the second round, NIST organized the second conference to monitor the progress of the competition.

This conference was an opportunity to bring together the international community working on the subject. It allowed to present the changes of the different candidates as well as the results of implementation on different platforms such as microcontrollers or FPGAs. This also gave the NIST the opportunity to interact with the various researchers from academic and industrial communities.

Major changes include merging of some proposals into single ones, such as:

- NTRUEncrypt and NTRU-HRSS-KEM became NTRU,
- LAKE, LOCKER and Ouroboros-R became ROLLO.

Some candidates were attacked, which reduced the security limits that were given. These candidates have therefore adapted their algorithms to increase security against these attacks, as illustrated by the qTesla algorithm.

Implementations have also evolved, some proposals are now implemented in constant-time or designed on microcontrollers. All proposals do not yet benefit from constant-time implementations. Other presentations announced some progress, such as physical implantations or integrations with TLS or SSH. It is important to note that unlike popular belief, most post-quantum cryptographic schemes fit rather well into TLS and SSH. They are usually a little larger than RSA with equal security, but much more effective.

First roundtable

The first roundtable brought together major industrials in the field such as AWS, Microsoft, or IBM. They provided their views on issues such as the set-up time of standards once they are announced. The most optimistic conclusion predicts a standardization within 2 years, the most pessimistic one estimates at least 5 to 6 years. It was also mentioned that the standardization of too many schemes could have a negative effect on the transition phase.

Second roundtable

The second roundtable was made up of members of the NIST team working on the subject, including Lily Chen, project manager on the standardization process. This session allowed NIST to answer regular questions to clarify the NIST's position and thus to increase transparency. The most controversial topic was whether a third round was needed, pushing back the release date of the standards. Time is a key variable in this process. On one hand, the NIST is compelled to quickly release standards due to the advances in quantum engineering. On the other hand, the lack of in-depth studies on the field could lead to the standardization of weaker-than-expected cryptosystems. The question of a third round had been raised from the start, but despite the fact that the second round has reached its half, the NIST have not yet decided on the matter.

Some members of the NIST considered that a new round was not necessary to make a choice as it would not bring any more evidence. Nevertheless, other members and most of the community believed that a third round is vital to further the analysis of security proofs, side-channel attacks and such. As a matter of fact, one of the major issues in this competition is the number of candidates. The 69-candidate list of the first round was only reduced to 26 in the second and the amount of work to evaluate each proposal in detail is huge. A presentation at CRYPTO 2019 illustrates the problem that could happen. The OCB2 encryption method was standardized more than 10 years ago despite insufficient studying of the security proof. Then an attack was carried out using a flaw in the said proof. This is the perfect example of a scheme that has been standardized without enough analysis. Therefore, the idea would be to reduce the list of candidates, for instance by half, in order to focus on a smaller number of candidates and seek to obtain more mature standards.

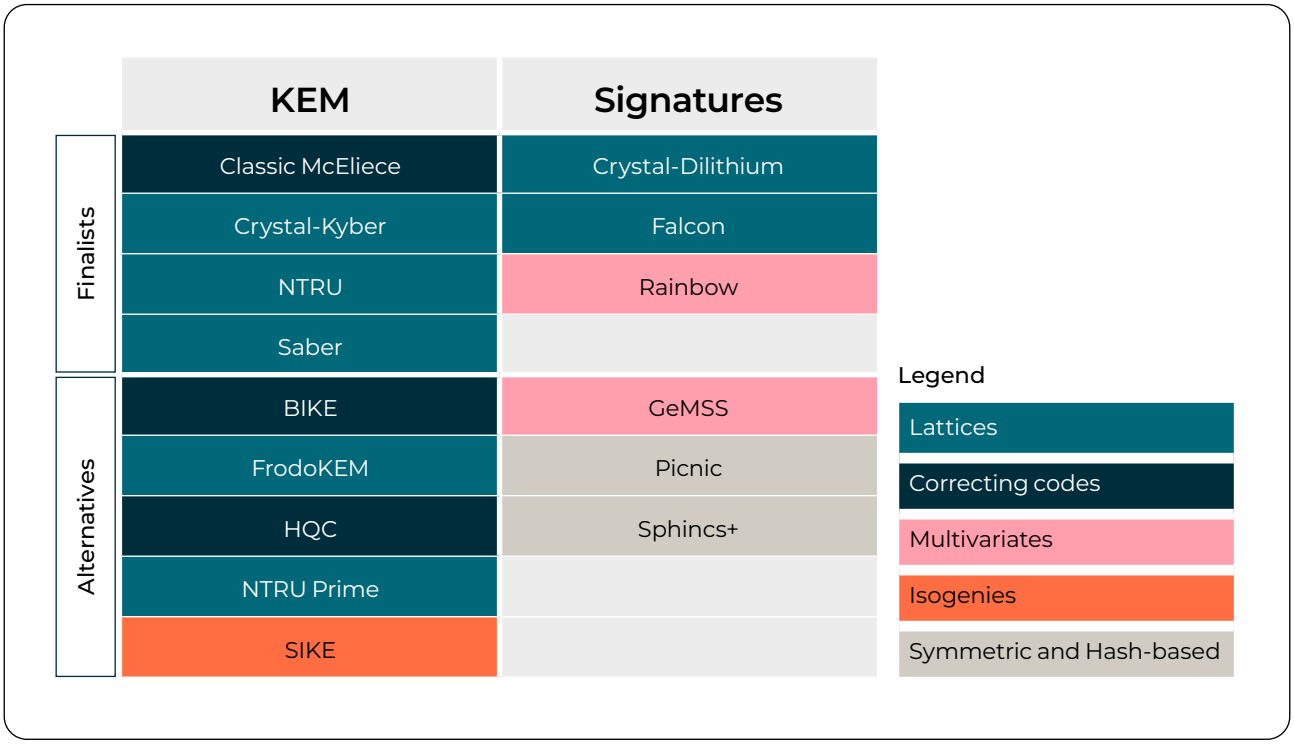
Third round of the NIST contest

Following the conference, NIST decided that a third round will occur.

On one hand this will allow the NIST to deepen the cryptanalyze and study of the side-channel aspect for the remaining candidate algorithms. On the other hand, this will provide the candidates with time to design additional proof of concept, especially in hardware, as most implementations yet are software. The NIST does not exclude to standardize unchosen schemes of the third round in a future process, or to pick some well-studied schemes right after the second-round while continuing the third round with a selection of others.

The third round started in august 2020. Among the 26 second round candidates, 15 are still consider for the third round. The remaining candidates are separated in two categories:

- The finalists, 4 KEM and 3 signatures, that are consider for a direct standardization after the third round. Among them, 4 are supposed to be standardize.
- The alternatives, 5 KEM and 3 signatures, that are consider for a later standardization or in case of new cryptanalytical results on some finalists.



There are various reasons that justifies the NIST's choices. They aim to standardize at least 2 KEM and 2 signatures based on different theories to have more flexibility in case of cryptanalytical breakthrough.

The lattice-based finalists all rely on cyclotomic number fields for efficiency reasons, NTRU and Falcon are based on NTRU lattices while the others are based on variants of LWE. On the other hand, NTRU Prime, which proposes a variant using NTRU lattices and another on a LWE variant, relies on structured lattices but on non-Galois number fields. Finally, FrodoKEM relies on unstructured lattices and is directly inspired by LWE. This range of choice allows to easily adapt the final choice depending on the advance of the cryptanalysis. If an attack reduce the security of NTRU-based schemes, LWE ones will preferred and the same applies for the other way around, if an attack reduce the security of cyclotomic number fields lattices schemes, NTRU Prime will be considered, finally, if an attack reduce the security of all structured lattice schemes, FrodoKEM will be considered.

For the case of code-based candidates, the NIST intends to standardize Classic McEliece because the original scheme endured forty years of cryptanalysis without being harmed. However, Classic McEliece has huge public keys (around 1 Mb), thus, it cannot be implemented in all circumstances. The NIST judged that the code-based schemes BIKE and HQC were not mature enough to be standardize at the end of the third round but since they offer much more practical sizes, the NIST decided to keep them as alternatives for a later standardization.

Rainbow and GeMSS were chose to add diversity to signature schemes. Rainbow has more structure than GeMSS, and as for structured lattices, the NIST decided to advance Rainbow as finalist and to keep GeMSS as alternative in case of cryptanalytical result using the additional structure used by Rainbow.

SIKE is the only scheme based on isogenies. It has competitive ciphertext and public key sizes but is also one order of magnitude slower than most of the other candidates. The NIST decided that SIKE could be a good candidate for a later standardization as it could benefit from a further study of its underlying problem and from more optimisation.

Picnic and Sphincs+ have strong security arguments for security since they only rely on the security of the underlying hash function for Sphincs+ and of the hash function and LowMC for Picnic where LowMC is a symmetric encryption scheme. Sphincs+ is similar to Classic McEliece since its original idea is well-known and studied but it suffers from high signature sizes and a slow signing algorithm. The NIST chose it as an alternative to keep the possibility to standardize a highly secured signature scheme even if it is not general purpose.

On the other hand, Picnic as much better performances and sizes compared to Sphincs+ but the NIST considered that it was not mature enough to be standardized at the end of the third round, but they kept the possibility of a later standardization. The LowMC symmetric encryption scheme could be replaced by the AES which would improve confidence in Picnic, but it would be at the cost of degraded signature sizes.

Virtual NIST Conference and future of the process

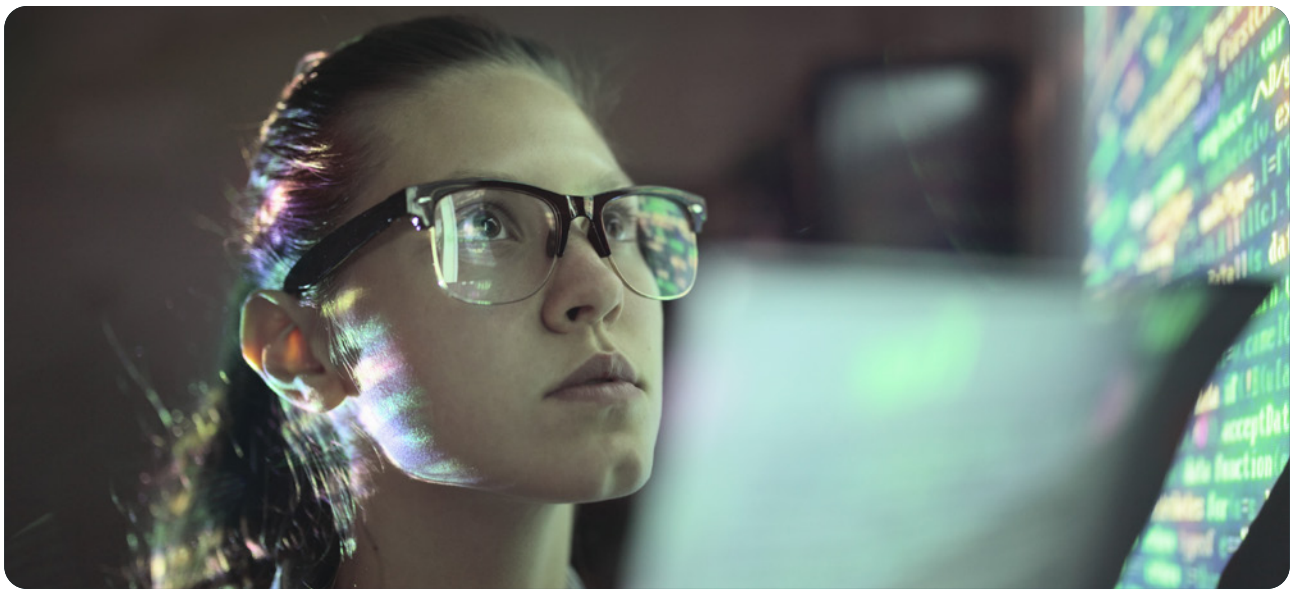
In June 2021, the NIST held a virtual conference to gather and exchange with the community. This event was the occasion to present the recent advances all around Post-Quantum Cryptography. There was presentations about the third round updates of the candidates given by the designers, progress on theoretical as well as practical cryptanalysis, some benchmark results for various candidates and platforms along with new implementations results, presentations of use cases where PQC will soon be deployed and the NIST agents concluded with a Q&A session.

There were very few changes to the candidates, particularly for the finalists which were predictable since only the more mature propositions were kept. But new implementation results were given, in particular, hardware implementation were present for almost all candidates. The main advance in theoretical cryptanalysis touched multivariate equations propositions, namely, Rainbow and GeMSS, the concrete security hasn't change that much, but we will discuss later the impact of this progress. The subject of practical cryptanalysis was much more present with a lot of presentation about SCA and/or masking of implementation, especially, the fact that all candidates are not equals in term protection, for example in lattice based signature, Falcon is much harder to mask than Dilithium because it partly relies on floating point arithmetic. The application session mainly focused the practical aspects of the candidates: data and code sizes, implementation speed in various conditions etc. This session allowed to have a different point of view on the candidates. For example, the key and signature sizes of Falcon are more appealing than any other DSA candidates because the actual number of packets sent is lower which leads to better performances as well as more reliability.

There were some interesting questions raised by the community. Known patent issue arise in several candidates especially the CNRS one, but no one rely know what patent could exists. Also, the NIST consider that the difficulty to mask Falcon was more a technical point than a real issue, despite that an attack on the implementation was performed recently, without known countermeasures.

The NIST confirmed that winners will be chosen at the end of 2021 with the end of the third round and that standards will be released by the end of 2023. Furthermore, the NIST planned to run a fourth round for some alternative candidates judged not mature enough for a quick standardization. Moreover, the standardization process of DSA will not be delayed. More precisely, the attack on multivariate-based schemes eroded the NIST's confidence on both Rainbow and GeMSS. Thus, the NIST seriously consider the standardization of Sphincs+ along with a structured lattice signature schemes for general purpose.

Since Sphincs+ is not efficient enough to be considered as a general-purpose signature, the NIST plans to start a new process to standardize general-purpose digital signature schemes not relying on structured lattices. Multivariate-based signature schemes might be reconsidered at that time. Code-based signature schemes were proposed at the first round but were all weaken or broken. This new process may allow new code-based signature with more mature design to emerge as potential alternatives. The fourth round might be mixed with this new call and lead to new standards for KEM and signatures several years after the end of the actual process.



3 Eviden and Post-Quantum Cryptography

Cybersecurity has always been a priority for Eviden, and post-quantum cryptography is now critical to prevent the possible digital disaster brought forth by the quantum computer. This is why Eviden has closely followed the NIST standardization process since its very beginning. Eviden is studying the various proposals of the competition in terms of security. In order to include future standards in the existing product range, Eviden will use its skills and resources to provide hardware implementations of several candidates.

The goal is, of course, to provide our customers with products that are always at the forefront of technology and security by protecting them from attacks using a quantum computer. The upstream study of future standards will enable Eviden to bring Quantum-Safe products to market as soon as the standardization process is completed.

This swift availability will allow our customers to evolve their infrastructures in order to be fully prepared for the quantum computing era.

Connect with us

eviden.com

ECT-230630-CS-BR-Trustway-Paper-Post-Quantum-Cryptography_Web