EVIDEN

Trustway

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

The purpose of this document is to present an overview of the hybrid post-quantum cryptography

an atos business

About the author

Louis Tajan holds a PhD degree in Applied Cryptography from University of Mannheim, Germany and a master's degree from Université de Paris VII. He is currently working for Trustway as an embedded cryptography development engineer.

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, an 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 a strong R&D capabilities to developed custom products and studies

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 Introduction

Cryptographic hybridization for post-quantum cryptography

Cryptographic hybridization, not to be mistaken with a hybrid cryptography mixing asymmetric and symmetric primitives as, for example TLS/SSL protocol, represents one of the main areas of evolution for products' security in a very short-term basis. Indeed, the certain arrival of quantum computer and the cryptographic revolution that will result from this, initiate a phase of thoughtful transition. This consists in the combination of robust quantum schemes with cryptosystems described as "classical" with a proven and reliable security.

If the goal of post-quantum cryptography is to support attacks from both classical and quantum computers, most current information systems suffer from a crying lack of cryptographic agility. Indeed, they are not designed and developed with the intent of being able to easily change the cryptographic algorithms on which the security relies. Migrating to a brand-new set of cryptographic primitives requires in-depth changes within the infrastructures and requires several years to deploy. According to the given type of post-quantum algorithm, it could result in a significant increase of the length of keys or signatures or a significant increase of the calculations to be performed. Therefore, it is of main interest to stress the need to anticipate and to prepare for the upcoming post-quantum revolution.

That being said, a main consideration to avoid any runaway reaction consists of the lack of maturity of these new post-quantum algorithms. Indeed, unlike their predecessors, these algorithms are relatively young and have not yet been studied and analyzed in depth over the years by the international scientific community. If not sufficiently tested, they are not considered secure in the current environment. For this reason, a reasoned way of use must guarantee an absence of regression regarding classical computers.

Two approaches are being considered.

One could easily propose to use solely classical symmetrical cryptosystems, already proven, and recognized as resistant to the post-quantum era such as AES or SHA3. But such a strategy would limit considerably the range of primitives offered by modern cryptography and disable any use of asymmetric cryptography and in particular any key exchange protocols such that IKE. Such a limitation would also result in a significant increase of the key length. For example, to obtain a similar level of security, AES encryption scheme requires a key size two times larger in a post-quantum configuration.

The second solution, of which it is the subject here, consists of using hybrid cryptosystems by combining a classical algorithm with a post-quantum algorithm. On the one hand, if an early breakthrough in quantum computer development should occur in the next few years and breaks the classical scheme, then the hybrid construction could still guarantee security through the postquantum scheme. On the other hand, if any failures were to be discovered in one type of postquantum scheme, the classical scheme would preserve the security of the hybrid construction.

Such an approach will thus enable to overcome the challenges previously stated and to optimally prepare the transition to the quantum computer paradigm.

3 A race to post-quantum cryptography

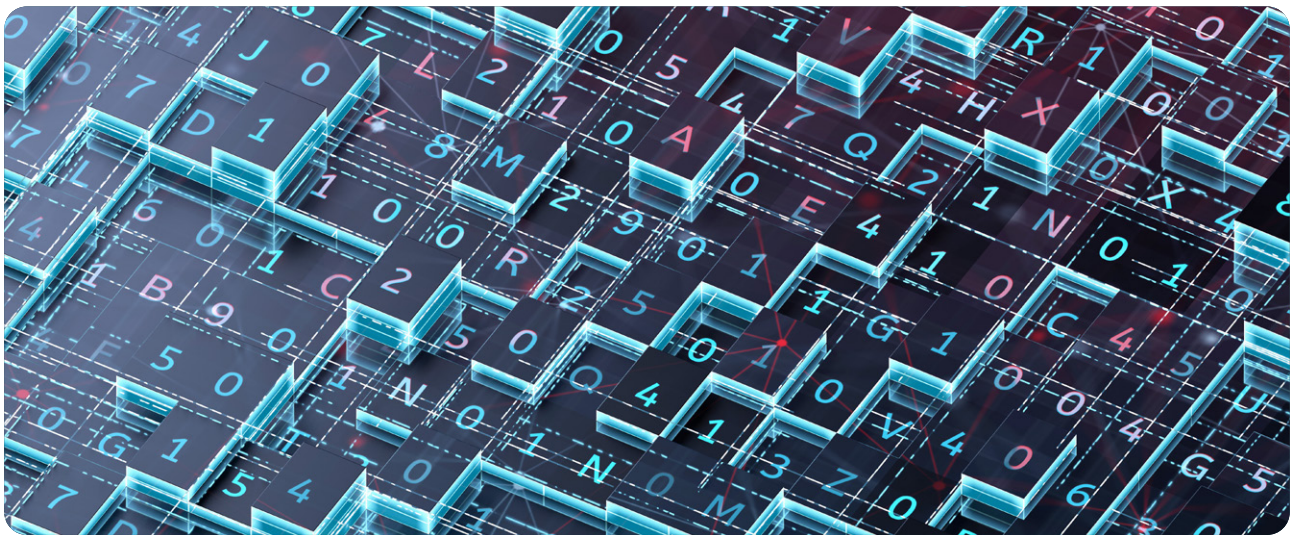
Post-quantum cryptography, also called “quantum safe”, corresponds to a family of cryptosystems considered resistant to quantum computers. More concretely, it is about resisting the Shor algorithm, which allows a quantum computer to break the classical asymmetric cryptosystems. To hedge against this attack imagined by Peter Shor in 1994, new asymmetric encryption and signature algorithms are being developed based on various mathematical principles such as Euclidean networks, corrective codes, or even multivariate cryptography.

In 2016, the NIST launched a program to standardize post-quantum algorithms. Still in the running today, this competition has selected so far 7 finalist algorithms and 8 alternative ones. This third round is expected to result in an upcoming announcement of which algorithms will be standardized.

Finalist algorithms		Alternate algorithms	
Public-key Encryption and KEM	Type		Type
Classic McEliece	Code-Based	**BIKE**	Code-Based
CRYSTALS-KYBER	Lattice-Based	**HQC**	Code-Based
NTRU	Lattice-Based	**FrodoKEM**	Lattice-Based
SABER	Lattice-Based	**NTRU Prime**	Lattice-Based
		SIKE	Supersingular Isogeny Based
Signatures	Type		Type
CRYSTALS-DILITHIUM	Lattice-Based	**GeMSS**	Multivariate Based
FALCON	Lattice-Based	**Picnic**	Hash-Based
Rainbow	Multivariate Based	**SPHINCS+**	Hash-Based

Once Shor’s algorithm is usable on quantum computers, all private (asymmetric) and secret (symmetric) keys will be at the mercy of an attacker, as well as all the data stored and protected by these keys. Their confidentiality and integrity can no longer be guaranteed. To do this, all the data will have to be re-encrypted using the new algorithms and backups meticulously deleted.

However, one could easily predict that an attacker may already be storing sensitive data protected with classic algorithms in anticipation of decrypting them as soon as they have the means to do so, a process known as “capture now, exploit later”. Another reason to initiate this cryptographic migration as soon as possible.



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

4 Post-quantum hybridization in industry and research

First, the **ANSSI** recommends hybridization of asymmetric algorithms by 2025 and a related white paper should be published very soon. This very principle of hybridization was already addressed by ANSSI back in 2018 and is also mentioned in "Guide de sélection d'algorithmes cryptographiques" as a full recommendation (R19):

Hybridization. It is recommended that a scheme based on these asymmetric primitives [post-quantum, Editor's note] should not be used independently at this stage, and when such a scheme is implemented, to combine it with a scheme based on proven asymmetric primitives or with a symmetric scheme implementing a pre-shared key

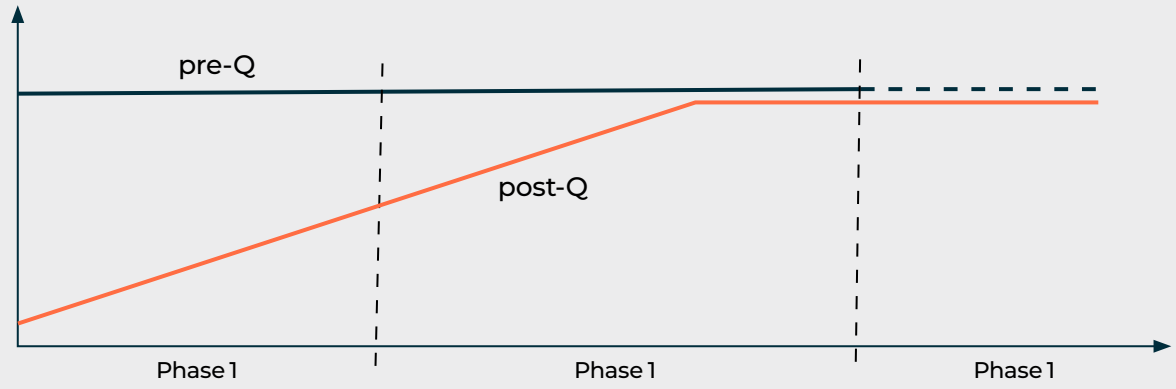


Figure 1 – ANSSI's projection [1]

In a communication document [1], the ANSSI exposes its short- and medium-term vision of this cryptographic transition and proposes 3 milestones corresponding to

- **Phase 1** - from now until 2025, an incentive to hybridization,
- **Phase 2** - from 2025 until 2030, a total and mandatory hybridization and finally
- **Phase 3** - from 2030 onwards, an obligation to use post-quantum cryptography in an autonomous way without hybridization.

Note that during phase 1 and possibly phase 2, the ANSSI gives some flexibility in the choice of the post-quantum cryptosystem and does not require that the chosen one is part of the standards selected by the NIST in the end.

The **NIST**, in parallel to their work of standardization, also insists on a certain cryptographic agility and highlights the importance of establishing an intermediate stage of hybridization towards the post-quantum transition [2].

The **CEA**, also convinced of such an approach, presents on its website that:

To ensure the transition between current and post-quantum cryptography, a hybrid cryptography should be developed, composed of two layers of encryption, one classical and the other post-quantum.

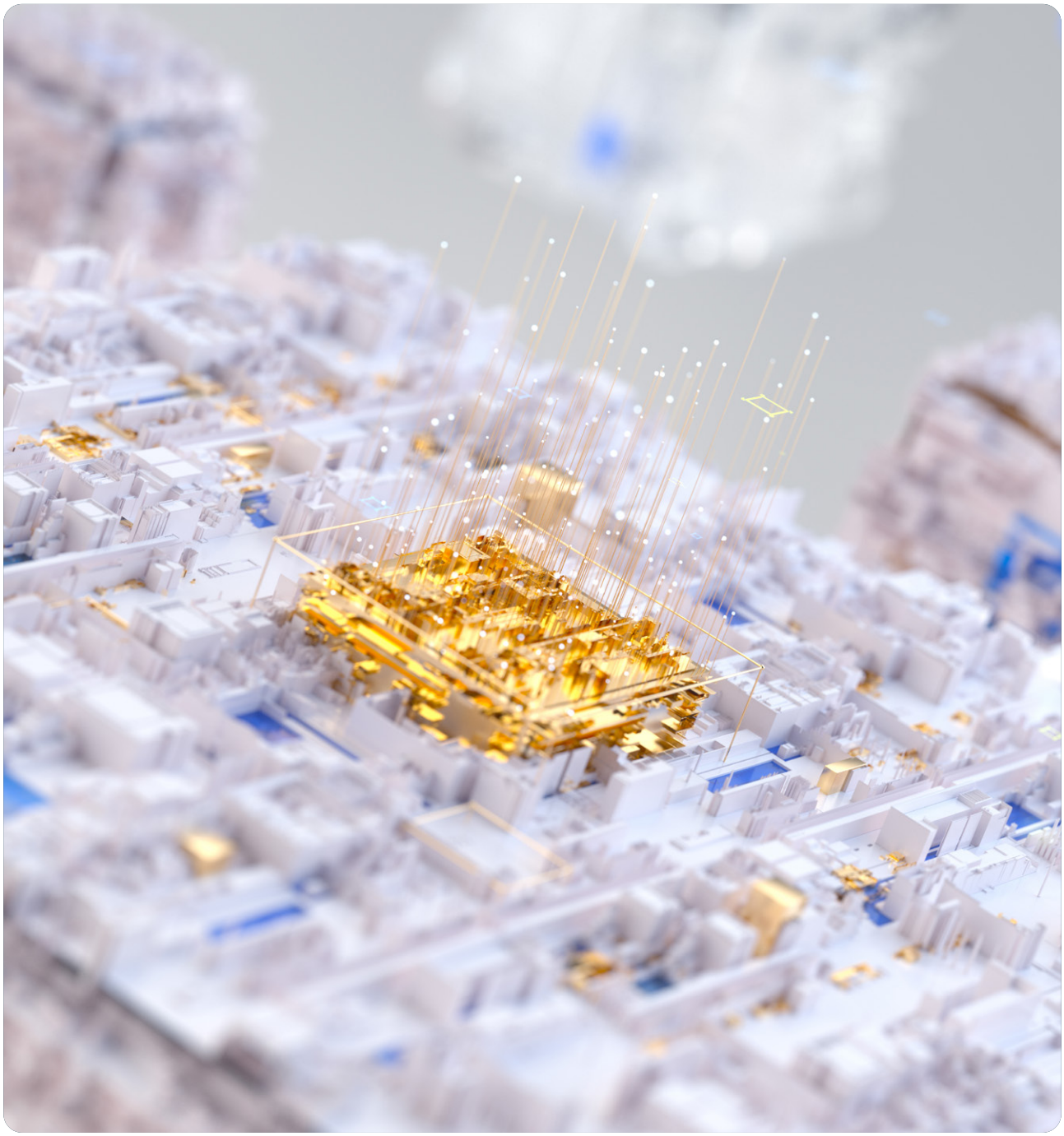
Implementations have even started to be developed. Researchers at Amazon Web Service (AWS) have implemented the hybrid key exchange protocol for TLS and SSH with their open-source solution s2n-tls. In [3] they also propose a hybrid authentication approach. Google has developed the CECPQ2 project [4] allowing its Chrome browser to integrate a hybrid combination for TLS protocol based on elliptic curves on the one hand and the NTRU-HRSS-KEM scheme (part of the NTRU finalist) on the other. We note that such an additional feature has recently been disabled by default on the latest versions of Chrome, due to the reports of several connection problems. Cloudflare has also proposed a TLS implementation of a key exchange protocol combining X25519 and SIDH [5].

In the scientific literature, Bindel et al [6] and Azarderakhsh et al [7] propose hybrid key exchange constructions by combining ECDH schemes with SIKE. On key certification, Kampanakis et al [8] present a construction of hybrid X.509 certificates as well as de Paul et al [9] where the authors propose to use several signature algorithms within the same certification chain. They use both classical algorithms based on elliptic curves and post-quantum algorithms such as SPHINCS+, XMSS or CRYSTALS-Dillithium and Falcon.

Finally, in a quite recent paper, Loïs Huguenin-Dumittan and Serge Vaudenay [10] refer to hybridization as we have presented but focus on the combination of post-quantum algorithms of different types together to anticipate any potential breakthrough enabling to discard one of them.

An Internet Draft [11], titled Multiple Key Exchanges in IKEv2, proposes to combine one classical key exchange with multiple post-quantum ones in IKEv2 protocol. With such an approach, the final shared key will depend on all of these keys, and we will obtain a construction that fits a hybrid combination as we previously presented.

At the initialization step, IKE_SA_INIT, the initiator and the responder negotiate and agree on which additional key exchanges should be used. Then, to complete the exchanges, the authors of [11] propose to use several intermediate steps denoted by IKE_INTERMEDIATE and introduced in [12]. Per each additional key exchange, one of these steps will be used. We also specify that this Internet Draft expires on 3 April 2022.



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

5 Key outlooks for Eviden

It goes without saying that all security products developed by Trustway will be affected by this transition. And so, regarding both an update of the signature schemes of our equipment and authentication protocols that fit perfectly an ingenious construction allowing hybridization, such as TLS or IKEv2. We note that there exists an implementation of BLISS [13], a post-quantum signature scheme, for strongSwan. RFC 8784 [14] allows the use of post-quantum keys with the IKEv2 protocol but in a symmetric way using preshared keys. As aforementioned, the internet draft [11] could be of interest to enhance IKEv2 to support hybridization.

In-depth analysis and rapid response will be key to placing Eviden at the leading edge of cryptographic innovation.

6 Références

[1] M. Rossi, «PQC TRANSITION ANSSI VIEWS, PQCRYPTO,» 2021. [En ligne]. Available: http://pqcrypto2021.kr/download/program/PQC_transition_in_France.pdf.

[2] NIST, «Getting Ready for Post-Quantum: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms,» [En ligne]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf.

[3] C. P. D. S. Eric Crockett, «Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH,» iacr ePrint, 2019.

[4] «The Chromium Projects,» [En ligne]. Available: https://www.chromium.org/cecpq2.

[5] H. d. Valence, «SIDH in Go for quantum-resistant TLS 1.3,» 2017. [En ligne]. Available: https://blog.cloudflare.com/sidh-go/.

[6] J. B. M. F. B. G. D. S. Nina Bindel, «Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange,» 10th International Workshop on Post-Quantum Cryptography (PQCrypto 2019), 2019.

[7] R. E. B. K. B. L. Reza Azarderakhsh, «Hardware Deployment of Hybrid PQC,» 2021.

[8] P. P. E. D. D. V. G. Panos Kampanakis, «The Viability of Post-Quantum X.509 Certificates,» 2018.

[9] Y. K. N. L. R. N. Sebastian Paul, «Mixed Certificate Chains for the Transition to PostQuantum Authentication in TLS 1.3,» ACM ASIA CCS '22, 2021.

[10] L. H.-D. a. S. Vaudenay, «FO-like Combiners and Hybrid Post-Quantum,» eprint, 2021.

[11] M. T. B. F. D. V. G. G.-M. V. S. C. Tjhai, «Multiple Key Exchanges in IKEv2,» Internet Engineering Task Force, 2021.

[12] V. Smyslov, «Intermediate Exchange in the IKEv2 Protocol,» Internet Engineering Task Force, 2021.

[13] A. D. T. L. a. V. L. Léo Ducas, «Bimodal Lattice Signature Scheme (BLISS),» [En ligne]. Available: https://wiki.strongswan.org/projects/strongswan/wiki/Bliss.

[14] P. K. D. M. V. S. S. Fluhrer, «RFC 8784 Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security,» [En ligne]. Available: https://www.rfc-editor.org/rfc/rfc8784.pdf

Connect with us

eviden.com

ECT-230626-CS-BR-Trustway-Paper-Hybridation-Cryptography_Web