Secure Implementation of Post-Quantum Cryptography

DOI: https://doi.org/10.54654/isj.v1i24.1079

Souhayl Ben El Haj Soulami, Yann Connan, Sylvain Guilley*, Sofiane Takarabt

Abstract— **Post-Quantum Cryptography (PQC) is now required by several institutions and vendors, especially for applications related to low-level security functions (secure boot, firmware management, secure channels establishment, etc.). Not only standardized PQC algorithms must match correctly their specification, but also they must be implemented in accordance with market requirements. Those mostly consist of Performance-Power-Area (PPA) and certification constraints. In turn, the PPA encompasses tradeoffs between speed and implementation size, but also optimal adequation with available resources (vectorization in software, parallelism in hardware, dedicated accelerators in embedded systems, etc.) The certification relates to secure implementation in the context of adversaries trying to gain information on the secrets, exploiting for instance some surreptitious information leakage (secret-dependent timing or power consumption). There is an interplay between PPA and certification aspects that we detail in this paper, for different classes of PQC algorithms. We also give some insights on the order in which PQC algorithms will be rolled-out, dictated by the requirements to implement in hardware some services which cannot be retrofitted later on in software, namely those that are in charge of firmware lifecycle management.**

Tóm tắt— **Mật mã hậu lượng tử (Post-Quantum Cryptography – PQC) hiện đang được yêu cầu bởi nhiều tổ chức và nhà cung cấp, đặc biệt đối với các ứng dụng liên quan đến các chức năng bảo mật cấp thấp (như khởi động an toàn, quản lý firmware, thiết lập kênh an toàn,...). Không chỉ các thuật toán PQC đã được chuẩn hóa phải phù hợp chính xác với đặc tả của chúng, mà việc triển khai chúng cũng phải tuân thủ các yêu cầu của thị trường. Những yêu cầu này chủ yếu bao gồm các ràng buộc về Hiệu năng - Năng lượng - Diện tích (Performance - Power - Area - PPA) và chứng nhận an toàn. Về phần PPA, điều này bao hàm sự đánh đổi giữa tốc độ và kích thước triển khai, đồng thời đòi hỏi sự tương thích tối ưu với các tài nguyên hiện có (như khả năng vector hóa trong phần mềm, song song hóa trong phần cứng, hay các bộ gia tốc chuyên dụng trong hệ thống nhúng,...). Chứng nhận liên quan đến việc triển khai một cách an toàn trong bối cảnh có các kẻ tấn công cố gắng thu thập thông tin về các bí mật, chẳng hạn thông qua các kênh rò rỉ thông tin ngầm (ví dụ như thời gian xử lý hoặc mức tiêu thụ điện phụ thuộc vào giá trị bí mật). Có một mối liên hệ qua lại giữa các khía cạnh PPA và chứng nhận, mà chúng tôi sẽ trình bày chi tiết trong bài báo này đối với các lớp thuật toán PQC khác nhau. Nhóm tác giả cũng đưa ra một số nhận định về thứ tự triển khai các thuật toán PQC, thứ tự này được xác định bởi yêu cầu triển khai phần cứng cho một số dịch vụ không thể bổ sung sau này bằng phần mềm, cụ thể là các dịch vụ chịu trách nhiệm về vòng đời firmware.**

Keywords*— *Post-Quantum Cryptography, algorithm, implementation, performances, countermeasures, provisioning, authorization, secure channel, authentication, attestation.

Từ khóa*— *Mật mã hậu lượng tử, thuật toán, triển khai, hiệu năng, biện pháp phòng chống, cấp phát, ủy quyền, kênh an toàn, xác thực, chứng thực.

I. Introduction

The recent advance in quantum physics is noticeable, and has applications in many aspects of our lifes (optics, like lasers, materials, characterization tools, such as spectroscopy and

This manuscript was received on January 16, 2025. It was reviewed on February 14, 2025, revised on May 19, 2025 and accepted on May 26, 2025.

* Corresponding author

high resolution electronic microscopy). One byproduct of this progress is the so-called quantum computer. It is a machine able to solve some problem exponentially faster than current classical computers. The exponential gain arises from the fact the data is not encoded as input values, but as input superimposition of values. Hence multiple computations can be carried out in parallel. This capability empowers quantum computer to solve otherwise complex problems in reasonable (linear, or at maximum, polynomial complexity), whereas classical computers would be glued into intractable exponential complexities.

In the field of information security, quantum computers are seen as a threat, because they jeopardize the basic security assumptions. It is remarkable to notice that quantum computers can be used to cryptanalyze classical cryptography. No longer RSA is secure for data encryption or signature, as is the case of any algorithm leveraging elliptic curves. The current question is not whether quantum computers have the capability to break classical cryptography, but when they will succeed. The Graal is the so-called quantum supremacy, meaning the practical way to computer faster than classical computers (present in full deployments as datacenters).

Without surprise, some regulatory cyber-agencies have captured the risk, and concur to start a transition as soon as possible. The motivation is backed by the "harvest now, decrypt later" surveillance strategy that relies on the acquisition and long-term storage of currently unreadable encrypted data awaiting for the quantum era. Thus, the trend is to engage into the migration of legacy classical codes into new PQC algorithms. In this paper, we concentrate on the (recently) standardized algorithms.

The algorithms that must evolve are mainly asymmetrical, i.e., involving a bikey (public key `pk` and private key `sk`). Indeed, symmetrical algorithms can be used as is, simply by pushing their key size to their maximum value. The classical asymmetrical algorithms that must transition are those based on:

- Integer factorization, namely algorithms leveraging RSA (Rivest, Shamir, Adleman [1]), such as digital signature (PSS, [2, 5]) and encryption (e.g., OAEP);
- Discrete logarithm, namely algorithms leveraging ECC (Elliptic Curve Cryptographic [3, 4]), such as digital signature (ECDSA [2, 6]) or Diffie-Hellman key exchange (ECDH).

But some others, such as the Massey-Omura [5], ECIES (IEEE P1363-2000 & 1363a-2004, ISO/IEC 18033-2), Paillier [6], pairing-based cryptography [7], attribute-based encryption, fully homomorphic encryption (FHE), or blockchain cryptosystems, might have their security be investigated as well.

Since the call for candidates for standardization by the NIST, many algorithms have been proposed, leveraging different PQC hard problems. Two classes to PQC hard problems have received the most attention, namely hash-based and lattice-based cryptography. In particular they are those listed on the USA list of Commercial National Security Algorithm (CSNA) Suite 2.0, well known as "CNSA 2.0". The necessity to act fast is materialized by coercive regulation. Indeed, the CNSA 2.0 roadmap is compelling, as executive orders [8] in the United States of America.

There are two kinds of cryptographic algorithms: those for which the two parties share the same key (symmetrical algorithms) and those for which each party has its own keypair asymmetrical algorithms. In this paper, we let alone the symmetrical algorithms. They are only threatened by the Grover algorithm, that marginally speeds up exhaustive key search. This is not an actual cryptanalysis per se, hence symmetrical is less destabilized. The only recommendation is to use the maximum key size for such algorithm.

On the other hand, asymmetrical algorithms are clear targets of cryptanalysis by a quantum computer. Indeed, it can collapse the complexity of solving all the current "computationally hard" problems, seen under the prism of a classical computer. For this reason, asymmetrical algorithms, namely today those based on integer factorization (RSA) and discrete logarithm (ECC) are badly endangered. Thenceforth, the PQC algorithms we will focus on are:

- Key Encapsulation Mechanisms (KEM), consisting of keypair generation, encapsulation and decapsulation;

- Digital Signatures Algorithms (DSA), consisting of keypair generation, signature generation and verification.

Obviously, the keypair generation algorithms are sensitive, since they establish the private keys. Then, for both KEM and DSA, there is one private-key operation (namely decapsulation and signature generation) and one public-key operation (namely encapsulation and signature verification).

Since the launch of international competition for PQC algorithms, several candidates have emerged. If we let apart:

- McEliece [9] cryptosystem, dated back from 1978, and
- Nth degree Truncated polynomial ring (NTRU) [10], dated back from 1998, and has been once standardized by IEEE [11],

which came too early (hence which are today perceived as inefficient), the dominant classes of algorithm today are *hashed-based* and *lattice-based* PQC algorithm.

The original question we address in this paper is: "*How to roll out PQC, in an industrial context?*"

The rest of this paper is structured as follows. Section II introduces what is currently at stake in the transition from classical to post-quantum cryptography. Section III details the tradeoffs for stateful hash-based PQC. Section IV discusses in depth the tradeoffs for modular lattice-based PQC. Section V concludes and opens some perspectives.

II. Implementation aspects

As precognized PQC algorithms have now been standardized, there is no more reason to wait before turning to post-quantum cryptographic realm. This transition shall nonetheless be managed carefully. Indeed, the markets and the regulators have defined security levels adapted to operational contexts, and thus PQC must be up to those requirements. Namely, algorithms shall be efficient (see Sec. I) and shall safeguard the secrecy of the private key (see Sec. II).

Part of this problem has already been covered for software implementation in general in [12]. Now, in this article, we delve into the details of selected algorithms for standardization.

A. PPA

1) Requirements in terms of PPA: Cryptographic operations cannot be the bottleneck in terms of operation completion duration. For instance, a secure boot should last at most a couple of milliseconds. As an other example, the timing of a signature verification should neither exceed a few milliseconds. These constraints are dictated primarily by usability, but also sometimes by a more compelling reason, such as safety. Assume a chip is found to be in an inconsistent state, then it shall be rebooted. As such reboot can occur in mission mode, it had better be executed promptly, to prevent the system from erring.

As a consequence hardware acceleration is mandated. Still, most PQC algorithms are in fact consisting in a composition of various primitives, most instantiations actually include some firmware to glue the different pieces together. It is thus paramount to make transfers as efficient as possible, so as to avoid data movements to become the speed limiting factor. Some collaboration between hardware and software developers is thus required. Use of direct memory access (DMA) specialized module can make it possible to discharge a central processing unit (CPU) while data is moved temporally in parallel. On platforms where single instruction multiple data (SIMD) is enabled, the ordering of instructions is important; for instance, one technique, known as software pipelining, allows to have several SIMD operations execute in parallel: some operation is launched, and known to require several clock cycles to complete. But in the meantime, without further waiting, some other independent operation is also launched. This allows for a maximal usage of the available hardware whilst not being limited by a sequential scheduling.

Moreover, there are some intrinsic constraints to the post-quantum cryptographic algorithms such as the infamous signature rejection in ML-DSA which computes signature candidates and rejects them if they do not meet the security requirements. On average, ML-DSA computes 4 signature candidates involving mostly operations that can be fully accelerated in hardware [13]. Another example is the rejection sampling for both ML-DSA and ML-KEM to generate the secret and error vectors.

TABLE I. OPTIMIZED RESOURCES NEEDED TO IMPLEMENT ML-KEM & ML-DSA IN AN FPGA TARGET

Algorithm	Platform	#LUT	#FF	#DSP	#BRAM	Freq. (MHz)
ML-KEM (Kyber) ML-KEM + ML-DSA (Dilithium + Kyber)	AMD/Xilinx Zynq Ultra-Scale+	2796 5678	660 748	15 50	5 (*) 5 (*)	80

(*): More BRAMs can be used to enhance the throughput

TABLE II. OPTIMIZED RESOURCES NEEDED TO IMPLEMENT ML-KEM & ML-DSA IN AN ASIC TARGET

Algorithm	Platform	Area	Gate Equivalent (kGE)	Freq. (MHz)
ML-KEM ML-KEM + ML-DSA	ASIC 28 nm	10k µm² 30k µm²	30 100	100
Masked SHA3/SHAKE → kept masked end-to-end	ASIC 28 nm	34 k µm²	104	100
DMA (to speed data transfer)	ASIC 28 nm	22k µm²	65	100

TABLE III. PERFORMANCE OF ML-KEM & ML-DSA IN µS, FOR A SYSTEM CLOCK FREQUENCY OF 100 MHZ

Security Level	Kyber-512 (ML-KEM-512)			Kyber-768 (ML-KEM-768)			Kyber-1024 (ML-KEM-1024)		
Function	Keypair	Encaps	Decaps	Keypair	Encaps	Decaps	Keypair	Encaps	Decaps
Simple	1358	1814	2178	2421	3030	3508	3891	4504	5128
Simple (°)	-	1104	1355	-	1503	1824	-	1869	2262
With DMA (*)	1055	1404	1845	1901	2369	2631	3095	3546	3891
With DMA (**)	-	857	1245	-	1173	1686	-	1455	2100

Security Level	DILITHIUM-II (ML-DSA-44)			DILITHIUM-III (ML-DSA-65)			DILITHIUM-V (ML-DSA-87)		
Function	Keypair	Verify	Sign	Keypair	Verify	Sign	Keypair	Verify	Sign
Simple	4878	5102	6993	8547	8403	10989	14492	14492	17857
Simple (°)	-	1872	3322	-	2409	4405	-	3300	6024
With DMA (*)	4219	4424	6060	7407	7246	9523	12500	12345	15384
With DMA (**)	-	1515	2849	-	1915	3773	-	2638	5154

(°) Without Key-expansion (`pk` and `sk` are already expanded and loaded into the hardware memory)
(*) Estimation with 32-bit word transfer / clock cycle

2) PPA values and optimization: Minimizing the implementation size is paramount in embedded systems, where the number of available resources is constrained. Indicative amount of resources required to implement two modular lattice algorithms (namely ML-KEM, ML-DSA) is given in Tab. I and II for FPGA and ASIC targets, respectively. Those figures are those obtained by Secure-IC in industry-level Securyzr [14] products, e.g., as validated against NIST CAVP [15]. Of course, some tradeoffs are possible. For example, in FPGA, the resources are shown as bare minimum, but more performance can be obtained at the expanse of adding more BRAMs. Also, in ASIC, the current maximal frequency is 277 MHz. A higher frequency can be reached by adding pipelining, at the expanse of more latency and a larger area (pipelining incurs more registers).

In terms of speed, performance is given in Tab. III. Such results, expressed in μs per operation, are delivered by either FPGA or ASIC implementation. The same hardware is used for the three different levels (1, 3, 5) defined by NIST. Optimized timing can be obtained by specializing the hardware to a given key size. Besides, the line in green highlights the best configuration:

- with key expansion (i.e., the key considers unpacked, and the time taken by this operation is not added up to the performance, as this structure is reused across subsequent operations under the same key);
- leveraging a DMA block to speed up the transfers between the modular lattice accelerator and the SHA3 / SHAKE operations, capable of moving one 32-bit word per clock cycle.

Notice that similar optimizations can be put forward for XMSS/LMS algorithms. Namely, the use of a DMA can drastically speed up the computations: indeed, when implemented on top of an existing hash primitive, more than 90% of the time is spent in data transfer. This burden can be alleviated by automating the data movements. One step further of optimization arises when avoiding at all the data transfers in the case of tree hashing, which involves iterative calls to hash functions. This innovative optimization is extensively described in [16].

B. Implementation Security

Let us recall that PQC algorithms remain sensitive, in that some operations (namely: keypair generation and decapsulation/signature) are manipulating the private key. Of course, private keys must be protected while at rest. This is typically ensured by secure elements [14]. Our concern is more related to the confidentiality of private keys while in computation. Therefore, implementations must be protected against attacks exploiting dynamic leakage occurring through side-channels. This task is not easy, as:

- identification of assets is not trivial: apart from the private key, the output of some algorithms (e.g., KEM) are also keys (namely, ephemeral session keys); besides, some values, such as the nonces, can lead to cryptanalysis if revealed;

- the protection is uneven: some parts of the algorithm are manipulating steady sensitive values, and thus signals can be denoised by constructively accumulating traces; other parts manipulate ephemeral values, which are thus less at risk because they require thus more evolved single-trace attacks; eventually, some parts (which can intersect the two previously mentioned parts) can process random values in addition to the sensitive value an attacker might be interested in. Such parts can be considered as intrinsically immune to attacks, hence require only little if not null protection. This strategy is termed levelling [17], and applies both to key generation and signature generation algorithms. For that purpose, variables are classified according to three sensitivity levels:
  - Level 0: no side-channel protection required.
  - Level 1: protection against SPA (single-trace attacks, such as intra-trace analysis or template / machine-learning attacks).
  - Level 2: protection against DPA (multi-trace attacks, such as Differential ElectroMagnetic Analysis, known as EMA [18]).

  Thus, protections are added accordingly to efficiently fulfill the minimum security requirements. For Level 1, one basic requirement is to ensure that the implementation is constant-time. Such implementation protects against both timing attacks and cache-timing attacks. Detecting and fixing those issues is fully described in [19]. In addition, against simple vertical side-channel attacks, operations shuffling is sufficient. It is especially efficient in software implementations. However, it is irrelevant on hardware implementations since operations are inherently conducted concurrently so it is not obvious to isolate operations.

  For Level 2, data masking [20, Chap. 9] required. It is efficacious in both software and hardware implementations, albeit costly. An example of masking of ML-KEM is given in [21].

A proper analysis shall thus be conducted, to avoid gaps. Actually, implementation efficacy (dictated by high PPA), shall not come at the expense of security.

III. Hash-based Standardized PQC

Hash-based PQC can be used for signature only. Indeed, hash functions being one-way, it is hard to imagine a use-case for a necessarily "symmetrical" key exchange (the agreed key is eventually the same for the interacting parties, Alice and Bob). There are two kinds of hash-based digital signatures:

- *stateful*: a limited number of signatures can be produced; it shall be known in advance, and is in often of the form 2^h for some integer h (when the algorithm consists in hashing in a tree of arity two);
- *stateless*: the limitation in the number of signatures is waived, at the expense of a more expensive computation time, though.

Representatives of those algorithms are, regarding stateful hash functions,

- eXtended Merkle Signature Scheme (XMSS, IETF RFC 8391, dated back from May 2018), and
- Leighton-Micali hash-based Signatures (LMS, IETF RFC 8554, dated back from April 2019).

The USA NIST has published recommended parameters for XMSS and LMS in FIPS 800-208. For instance `XMSS-SHA2_20_256` is XMSS with an binary tree of depth 2^h where $h = 20$, meaning that about one million ($1,048,576$ to be exact) messages can be signed.

Regarding stateless algorithms, one algorithm has been standardized, namely SPHINCS$^+$. It is now nicknamed SLH-DSA (standing for "State-Less Hash-based Digital Signature Algorithm"), and referred to as FIPS 205. The use-case of stateless algorithm is when the chip owner (meaning owner of its specification) cannot be definitive about the number of times the firmware can be changed. It occurs when:

- The chip owner will delegate the firmware management to its client (hence cannot be restrictive in amount of messages that can be signed);
- Either want to not infringe novel regulations that explicitly demand arbitrary number of updates, such as NIST SP 800-193 (Platform

Firmware Resiliency [22]), or European Cyber Resiliency Act (EUCRA [23]).

IV. Lattice-based Standardized PQC

The migration of classical key exchange algorithms (namely those based on Diffie-Hellman, such as DH, ECDH, or their ephemeral versions) seems to be less crucial, because those functions are known to be required for Internet applications. Migration of Internet applications is not urgent, as they consist in software: protocols such as IKE or handshake part of TLS. But when looking into details more carefully, there are uses of key exchanges that are intricated with the chip early capabilities. Those are the services which must occur in the first place, such as provisioning. This service is critical, as one does not want anybody to be able to write firmware into the chip. Hence authorization and secure channel establishment, including user authentication resisting to replay (need for fresh challenging) shall be put in place. Obviously, the supporting cryptographic algorithm for these services cannot be in software/firmware, since otherwise they would need to be provisioned first. Indeed, recall that a chip is fabricated without its firmware: when it comes out of the foundry, it is blank. Hence a chicken-and-egg issue, regarding the chip lifecycle management. The provisioning algorithms must pre-exist the provisioning, hence must be in hardware.

Chips specified and designed today might well be in the field only several years afterward. Indeed, chips must be fabricated, tested, placed in package, soldered on a printed circuit board (PCB), and integrated into the final appliance. All these operations take time, hence some anticipation is needed. Otherwise, the chips can be sadly designed as already no longer being suited for the regulation of the market. As a matter of fact, the CNSA 2.0 roadmap states that the cryptography in charge of firmware management shall be transitioned as early as now, and shall have finished its transition by 2030 (i.e., in 5 to 6 years from now).

In this respect, it is worthwhile considering already ML-KEM (“standing for Modular Lattice based Key Encapsulation Algorithm”), and referred to as FIPS 203. It is a direct standardization of the CRYSTALS-Kyber proposal to the NIST competition. This ML-KEM algorithm allows to provision in an untrusted environment (hence the need for the secure, *i.e.* encrypted channel). Notice that other algorithms for KEM are possible. Namely, in the context of the NIST competition:

- HQC: offers strong security assurances and mature decryption failure rate analysis. Its public key and signatures size is larger than that of BIKE, but still, despite this apparent handicap, it has been recently (March 11, 2025) selected for standardization by NIST [24].
- BIKE: features the most competitive performance of the NIST 4th round of competition. But its IND-CCA security is not vetted enough.
- Classic McEliece: NIST claims it is confident in its security. Admittedly, it has the smallest ciphertexts, but also, sadly, the largest public keys. Not enough feedback has been received with respect to use-cases regarding Classic McEliece.

Also, in the context of international standardization, e.g., ISO/IEC JTC1/SC 27/WG2, FrodoKEM (https://frodokem.org/) has been approved as a candidate for international standardization, alongside Kyber and Classic McEliece. Eventually, NTRU has already been standardized in the context of IEEE, as P1363.1 (algorithms NTRUEncrypt & NTRUSign [11]). Those have not been reaffirmed as standards recently though.

Besides, in order to also check that provisioning payload (firmware, keys, credentials, etc.) is licit, it shall be signed. Any of the PQC digital signatures mentioned in previous Sec. III are satisfactory. However, they come with limitations: XMSS/LMS restrict the number of signatures, and SLH-DSA is slow. For this reason, it makes sense to leverage a companion algorithm of ML-KEM, namely ML-DSA (“standing for Modular Lattice based Digital Signature Algorithm”), and referred to as FIPS 204. Notice that SLH-DSA and ML-DSA are respectively the standardized versions of SPHINCS$^+$ and CRYSTALS-Dilithium.

The NIST has already selected another lattice based signature, namely FALCON. However, this algorithm is not yet standardized officially, and is

more difficult to protect (in particular because it involves a floating point operation, admittedly hard to mask against side-channel attacks). Thus we do not comment more on it, despite its advantage over Dilithium / ML-DSA is its shorter signatures.

An advantage of leveraging ML-KEM and ML-DSA for firmware management is that those functions are then readily available for Internet applications, which are required to transition (according to CNSA 2.0 roadmap) slightly later, in 2033. Also, these bricks are already in place for alternative device-level security services, such as attestation. The attestation is the proof that the device is running genuine (untampered) firmware. This proof consists in a concatenation of firmware images hashes, signed with a device endorsement key. The attestation services are now considered for being described as optional services in NIST FIPS 140, and thus eligible to being transitioned as per the CNSA 2.0 roadmap.

V. Conclusions and Perspectives

We explain that the transition to PQC is actually already accelerated from the CNSA 2.0 roadmap. The reason is that some devices cannot migrate only secure boot of firmware (leveraging XMSS/LMS), but must ensure that the provisioning (first after fabrication, or subsequent updates) be PQC-ready as well. Therefore, we recommend that designers anticipate transition already to modular lattice PQC algorithms. Besides, NIST has opened in 2023 an additional digital signature competition [25]. The goal is to allow for more choices in digital signatures, namely:

1) diversification of the underlying hard problems (other than structured modular lattices);
2) short signatures and fast verifications;
3) modular lattice based signatures which are faster than CRYSTALS-Dilithium and/or FALCON, or with an increased security level.

Hence, it is prevalent to remain future-proof in the likely case more PQC digital signature algorithms arrive (from this competition). Also endogenous algorithms, stemming from different geographies, will certainly emerge.

Compliance to unknown algorithms may be ensured, for instance by having coprocessors ready, or by having some ROM update mechanism leveraging the OTP as a patching mechanism. Such posture is that of crypto-agility, several times acclaimed in the context of PQC migration [26].

Acknowledgements

This consolidating work has partly benefited from the funding by French Bank for Innovation (BPI), through the project X7PQC (project call "Cryptographie post quantique", held by the National Quantum Strategy "Develop the post-quantum cryptographical offering" and the National Cyber Strategy "Development of innovative and critical cyber technologies"). This project involves as partners Hensoldt France (lead), Secure-IC, XLIM, and Institut Polytechnique de Paris / Telecom-Paris. Project number: DOS0209793 -- DOS0209794.

The authors also wish to thank the European Commission for partial funding via Allegro (Agile uLtra Low EnerGy secuRe netwOrks) project, Grant Agreement No. 101092766.

References

[1] R. L. Rivest, A. Shamir, and L. M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[2] NIST, Federal Information Processing Standards Publication, "FIPS 186-5, Digital Signature Standard (DSS) (Supersedes FIPS 186-4)," February 3 2023.

[3] V. S. Miller, "Use of Elliptic Curves in Cryptography," in *Advances in Cryptology - CRYPTO '85, Santa Barbara, California, USA, August 18-22, 1985, Proceedings*, ser. Lecture Notes in Computer Science, H. C. Williams, Ed., vol. 218. Springer, 1985, pp. 417–426. [Online]. Available: https://doi.org/10.1007/3-540-39799-X_31

[4] N. Koblitz, "A Family of Jacobians Suitable for Discrete Log Cryptosystems," in *Advances in Cryptology - CRYPTO '88, 8th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1988, Proceedings*, ser. Lecture Notes in Computer Science, S. Goldwasser, Ed., vol. 403. Springer, 1988, pp. 94–99. [Online]. Available: https://doi.org/10.1007/0-387-34799-2_8

[5] J. L. Massey and J. K. Omura, "Method and apparatus for maintaining the privacy of digital messages conveyed by public transmission," January 28 1986, United States Patent: 4567600 ; https://patents.google.com/patent/US4567600A/.

[6] P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," in *EUROCRYPT*, ser. Lecture Notes in Computer Science, vol. 1592. Springer, May 2-6 1999, pp. 223–238, Prague, Czech Republic.

[7] N. E. Mrabet and M.Joye, Eds., Guide to Pairing-Based Cryptography. CRC Press, Taylor & Francis Group, December 2016, ISBN 9781498729505.

[8] USA, “Executive Order (EO) 14028 - “Improving the Nation’s Cybersecurity”,” May 12 2021.

[9] R. J. McEliece, “A Public-Key Cryptosystem Based On Algebraic Coding Theory,” *The Deep Space Network Progress Report, DSN PR 42-44*, pp. 114–116, January and February 1978, https://ipnpr.jpl.nasa.gov/progress_report2/42-44/44N.PDF.

[10] J. Hoffstein, J. Pipher, and J. H. Silverman, “NTRU: A Ring-Based Public Key Cryptosystem,” in *Algorithmic Number Theory, Third International Symposium, ANTS-III, Portland, Oregon, USA, June 21-25, 1998, Proceedings*, ser. Lecture Notes in Computer Science, J. Buhler, Ed., vol. 1423. Springer, 1998, pp. 267–288. [Online]. Available: https://doi.org/10.1007/BFb0054868

[11] IEEE P1363, “Standard Specifications For Public-Key Cryptography,” October 2000, http://grouper.ieee.org/groups/1363/.

[12] S. Guilley, Y. Souissi, F. Zhang, and B.-L. Yang, “Post-Quantum Cryptography — Having it implemented right,” *Journal of Cryptologic Research*, vol. 10, no. 03, pp. 650–666, 2023, DOI: 10.13868/j.cnki.jcr.000624.

[13] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé, “CRYSTALS-Dilithium: Algorithm Specifications and Supporting Documentation,” November 30 2017, https://pq-crystals.org/dilithium/data/dilithium-specification.pdf.

[14] Secure-IC S.A.S., “Securyzr™ Product Line,” 2025, https://www.secure-ic.com/products/securyzr/. Accessed May 9, 2025.

[15] K. Lorvellec, R.-R. Shrivastwa, and S. Guilley, “Secure-IC PQC Solutions,” October 30 2024, Version 1, https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=18755.

[16] Sylvain Guilley and Sofiane Takarabt (Secure-IC), “Architecture configured for providing a compression function from within a hash function,” May 1st 2025, Patent pending, US20250141690A1.

[17] M. Azouaoui, O. Bronchain, G. Cassiers, C. Hoffmann, Y. Kuzovkova, J. Renes, T. Schneider, M. Schönauer, F. Standaert, and C. van Vredendaal, “Protecting Dilithium against Leakage Revisited Sensitivity Analysis and Improved Implementations,” *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 2023, no. 4, pp. 58–79, 2023. [Online]. Available: https://doi.org/10.46586/tches.v2023.i4.58-79

[18] K. Gandolfi, C. Mourtel, and F. Olivier, “Electromagnetic Analysis: Concrete Results,” in *Proceedings of the Third International Workshop on Cryptographic Hardware and Embedded Systems*, ser. CHES ’01. London, UK, UK: Springer-Verlag, 2001, pp. 251–261. [Online]. Available: http://dl.acm.org/citation.cfm?id=648254.752700

[19] S. CarrÃ, A. Facon, S. Guilley, S. Takarabt, A. Schaub, and Y. Souissi, "Cache-timing attack detection and prevention - application to crypto libs and PQC" in Constructive Side-Channel Analysis and Secure Design - 10th International Workshop, COSADE 2019, Darmstadt, Germany, April 3-5, 2019, Proceedings, ser. Lecture Notes in Computer Science, I. Polian and M. Stottinger, Eds., vol. 11421. Springer, 2019, pp. 13–21. [Online]. Available: https://doi.org/10.1007/ 978-3-030-16350-1_2

[20] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. Springer, December 2006, ISBN 0-387-30857-1, http://www.dpabook.org/.

[21] M. Hamoudi, A. Bel Korchi, S. Guilley, S. Takarabt, K. Karray, and Y. Souissi, “Side-Channel Analysis of CRYSTALS-Kyber and A Novel Low-Cost Countermeasure,” in *Security and Privacy*, P. Stănică, S. Mesnager, and S. K. Debnath, Eds. Cham: Springer International Publishing, 2021, pp. 30–46.

[22] A. Regenscheid, “NIST Special Publication 800-193 – Platform Firmware Resiliency (PFR) Guidelines,” May 2018, DOI: 10.6028/NIST.SP.800-193.

[23] European Commission, “European Cyber Resiliency Act,” July 13 2023, https://data.consilium.europa.eu/doc/document/ST-11726-2023-INIT/en/pdf.

[24] NIST, “NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption,” March 11 2025, https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption.

[25] L. Chen, D. Moody, and Y.-K. Liu, “Post-Quantum Cryptography: Digital Signature Schemes,” 2024, https://csrc.nist.gov/projects/pqc-dig-sig/standardization/call-for-proposals.

[26] L. Chen, D. Cooper, D. Moody, W. Newhouse, and A. Regenscheid, “Crypto Agility,” February 28 2025, https://csrc.nist.gov/projects/crypto-agility.

ABOUT THE AUTHORS

Souhayl Ben El Haj Soulami
Workplace: Valeo BRAIN division, Secure-IC S.A.S., Cesson-Sévigné office, Paris
Email: souhayl.ben-el-haj-soulami@valeo.com
Education: He received his master's degree in computer science and applied mathematics from Grenoble-INP ENSIMAG in 2022.
Recent research direction: Currently pursuing a PhD on side-channel attacks on post-quantum cryptographic schemes.

Tên tác giả: **Souhayl Ben El Haj Soulami**
Cơ quan công tác: Bộ phận BRAIN của Valeo, Secure-IC S.A.S., văn phòng Cesson-Sévigné, Pháp.
Email: souhayl.ben-el-haj-soulami@valeo.com
Quá trình đào tạo: Nhận bằng Thạc sĩ về khoa học máy tính và toán ứng dụng tại trường Grenoble-INP ENSIMAG, Pháp vào năm 2022.
Hướng nghiên cứu hiện nay: Nghiên cứu sinh về tấn công kênh kề vào các chương trình mật mã hậu lượng tử.

Yann Connan
Workplace:Secure-IC S.A.S., Cesson-Sévigné office, Paris.
Email: yann.connan@secure-ic.com
Education: He received a first master's degree in mathematics and didactics in 2011, a second master's degree in cryptography in 2018, both from Rennes university and his PhD in code-based post-quantum cryptography in 2021 from Limoges university.
Recent research direction: Elaboration of a new side-channel attack on lattice-based cryptographic schemes and a countermeasure to it.

Tên tác giả: **Yann Connan**
Cơ quan công tác: Secure-IC S.A.S., văn phòng Cesson-Sévigné, Pháp.
Email: yann.connan@secure-ic.com
Quá trình đào tạo: Nhận bằng Thạc sĩ toán học và sư phạm vào năm 2011; Thạc sĩ mật mã vào năm 2018 tại Đại học Rennes; Tiến sĩ về mật mã hậu lượng tử vào năm 2021 tại Đại học Limoges.
Hướng nghiên cứu hiện nay: Xây dựng tấn công kênh kề vào các chương trình mật mã dựa trên mạng và biện pháp phòng chống.

Sylvain Guilley
Workplace:
Secure-IC S.A.S., Paris office. Email: sylvain.guilley@secure-ic.com
Education: He received his Master degrees in quantum physics in 2000 from Ecole Polytechnique, in quantum mechanics from ENS in 2002, his PhD in cryptography from Télécom Paris in 2007, and his Habilitation to Direct Researches (HDR) in 2012 in computer science from Paris Diderot University.
Recent research direction: Interplay between embedded cybersecurity technologies and normalization, certification and regulation.

Tên tác giả: **Sylvain Guilley**
Cơ quan công tác: Secure-IC S.A.S., văn phòng tại Pháp.
Email: sylvain.guilley@secure-ic.com
Quá trình đào tạo: Nhận bằng Thạc sĩ vật lý lượng tử vào năm 2000 từ Ecole Polytechnique và Cơ học lượng tử từ ENS vào năm 2002; Tiến sĩ về mật mã từ Télécom Paris vào năm 2007; bằng Habilitation to Direct Researches (HDR) về khoa học máy tính từ Đại học Paris Diderot vào năm 2012.
Hướng nghiên cứu hiện nay: Sự tương tác giữa các công nghệ an ninh mạng nhúng và chuẩn hóa, chứng thư số và quy chuẩn.

Sofiane Takarabt
Workplace: Secure-IC S.A.S., Paris office. Email: sofiane.takarabt@secure-ic.com
Education: He holds a Ph.D. in secure implementations and physical attacks from the French university Télécom Paris.
Recent research direction: Secure implementations and physical attacks.

Tên tác giả: **Sofiane Takarabt**
Cơ quan công tác: Secure-IC S.A.S., văn phòng tại Pháp.
Email: sofiane.takarabt@secure-ic.com
Quá trình đào tạo: Nhận bằng Tiến sĩ về triển khai an toàn và các cuộc tấn công vật lý từ Đại học Pháp Télécom Paris.
Hướng nghiên cứu hiện nay: Triển khai an toàn và các cuộc tấn công vật lý.