LINC
CNIL.

FILE

The keys to decipher cryptography

March 2025
linc.cnil.fr

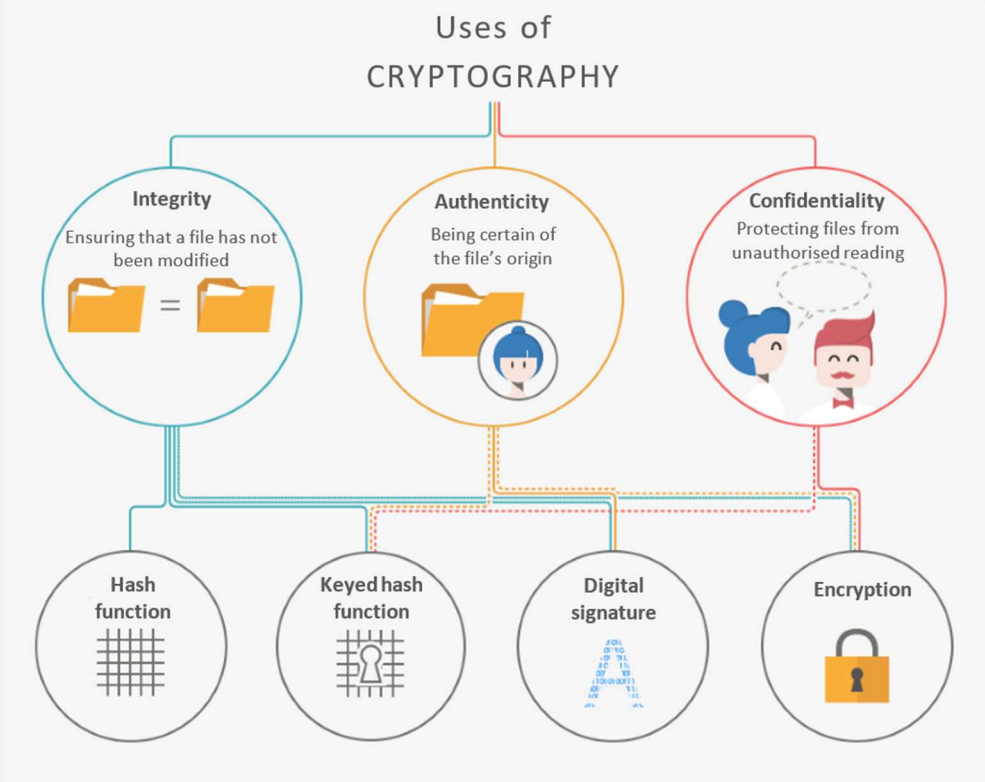
Monir Azraoui, Privacy Technology Expert

Cryptography has always been a cornerstone of communication and data security. What's new in cryptography? What are the main trends in cryptography for data and privacy protection? What developments should we anticipate? To help answer these questions, we spoke with several French cryptography experts. This article highlights the key points emerging from these discussions.

SUMMARY

Experts provide the keys to deciphering today's and tomorrow's cryptography

In our constantly evolving, hyperconnected world, the personal data we store, process, or share online is more vulnerable than ever to cyber threats. Cryptography provides tools to protect data and communications against these threats. Beyond the goal of confidentiality that encryption aims to achieve, cryptography also plays a key role in ensuring data integrity (i.e. the data has not been altered) and authenticity (verifying the origin) through hashing functions and digital signatures.



Source : https://www.cnil.fr/fr/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement[1]

These tools (encryption, hashing, and digital signature) are used on a daily basis today. However, with the emergence of new digital paradigms such as the Cloud, Artificial Intelligence, and Internet of Things, cryptography had to be modernised. These new technologies have introduced new challenges in terms of security and data protection, requiring more advanced cryptographic solutions. Not only do these advancements aim to

[1] https://www.cnil.fr/fr/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement

address increasingly sophisticated threats, but they also adapt to the specific needs of new digital applications.

We initiated work to explore these advanced cryptographic technologies through a series of interviews with French experts in the field:

- **Olivier Blazy, Professor and researcher at École Polytechnique**
  Olivier Blazy is a professor of cybersecurity at École Polytechnique in the Computer Science department. He has been a researcher in cryptography for 10 years, working on various topics including cryptography for privacy protection and post-quantum cryptography. At the national level, he co-chairs the CNRS Code and Cryptography working group within the Information Security and Computer Science-Mathematics Research Groups (GDR).

- **Sébastien Canard, Professor at Télécom Paris, formerly a research engineer at Orange**
  Sébastien Canard has been a professor at Télécom Paris since 2023, working with the Cybersecurity and Cryptography [C²] team. At the time of our interview, Sébastien was a research engineer since 2003 for the R&D department of the telecom operator Orange, where he was a member of the « applied cryptography » group. His research focuses, among other things, on the design of privacy-preserving cryptographic protocols.

- **Melek Önen, Professor at EURECOM**
  Melek Önen is a professor in the Digital Security Department at EURECOM (Sophia-Antipolis). Her research focuses on applied cryptography, information security, and privacy protection. She works on the design and development of cryptographic protocols for various technologies, including cloud computing and machine learning.

- **Pascal Paillier, Co-founder and Chief Technology Officer at Zama**
  Pascal Paillier is a researcher and entrepreneur in cryptography and currently serves as Chief Technology Officer at Zama. For over 25 years, his work has focused on designing and developing cryptographic techniques for sensitive industries. He is notably the designer of the homomorphic cryptographic system that bears his name. He also contributes to efforts to standardise encryption.

- **ANSSI, Technical Assistance Division (Anthony Journault) and Cryptography Lab (Henri Gilbert ; Jérôme Plût ; Mélissa Rossi ; Yannick Seurin)**
  The cryptography lab is ANSSI's center of expertise for cryptographic algorithms, mechanisms, and architectures. In these areas, the lab is involved in research, requirement analysis, and the design of solutions to meet those requirements, as well as product evaluation and the development and updating of technical standards.

ANSSI's Technical Assistance Division is designed to assist public administrations in securing their information systems, and in the case of the experts interviewed, in projects involving cryptographic mechanisms.

We present a summary of the interviews with these experts in a series of three articles.

The first and second articles explore the four advanced cryptographic technologies that experts consider crucial to the IT security landscape :

- post-quantum cryptography,
- cryptography enabling operations to be performed on encrypted data,
- zero-knowledge proofs, and
- group signatures.

Finally, the third article presents three contexts in which these technologies can be applied:

- personal data processing,
- artificial intelligence, and
- confidential cloud computing.

It also identifies the challenges that need to be addressed in order for advanced cryptographic technologies to be adopted and used on a larger scale.

Acknowledgments

These articles would not have been possible without the support of the experts listed above, who devoted their valuable time to their experiences with us.

These articles are the result of a collective effort, and the author would like to thank his colleagues Solenn Brunet et Amandine Jambert for their essential collaboration in this work.

Post-quantum cryptography

The discussions with cryptography experts provided insight into the transition to « post-quantum » cryptography, meaning cryptography that is robust against attacks from quantum computers, a field currently experiencing strong momentum both in academia and in industry. In this article, we present a synthesis of the ideas shared during these interviews, highlighting the challenges and opportunities ahead.

The threat of quantum computers to traditional cryptography

Introduction to quantum computing

Traditional computing relies on a binary system, in which the bit, taking a value of 0 or 1, is the smallest unit of information processed by a computer. In quantum computing, the fundamental unit is the qubit, which can take on a whole range of states between 0 and 1, and these states can be entangled across multiple qubits. These characteristics can, in some cases, enable faster computations than classical bits by processing multiple possible values in parallel. Ultimately, a quantum computer[2] could perform calculations that traditional computers would never be able to complete within a reasonable timeframe.

Extensive research on quantum computing has been conducted for several decades (notably by IBM, Google, and Microsoft), and the ecosystem is highly dynamic. In France, the President presented in January 2021 a €1.8 billion investment plan in quantum technologies over five years[3]. Various technologies for building quantum computers exist but currently they only allow very limited computations. However, progress is fast: several players, including IBM and startups such as the French companies Pasqal, Alice & Bob, and Quandela, are developing increasingly sophisticated quantum computer prototypes

However, the cybersecurity community is concerned about the potential impact of quantum computing on cryptography. Indeed, it has been known since 1994 that a quantum computer could break most of the cryptographic algorithms currently in use. What was until recently a purely theoretical threat has, over the past decade, become a more serious concern with the development of the first quantum computers. This applies mainly to asymmetric mechanisms,

[2] Here, « quantum computer » refers to a device capable of performing large-scale quantum computations, potentially on a limited number of specialised tasks, rather than as a quantum equivalent of a « classical » computer.

[3]https://www.elysee.fr/emmanuel-macron/2021/01/21/presentation-de-la-strategie-nationale-sur-les-technologies-quantiques

but also (to a lesser extent) to symmetric mechanisms, whether they consist of encryption, hashing, and digital signature techniques.

The looming threat of quantum computers

Thus, what is considered secure today could be compromised with the advent of quantum computers of sufficient capacity. It is difficult to predict if or when a quantum computer will ever reach the required power. This is likely a matter of decades. Nevertheless, this threat is already prompting cryptography researchers (including some of the experts interviewed) to anticipate the challenges posed by quantum computing. This anticipation is driven by two main reasons:

- The potentially very serious consequences of attacks (see below); and
- The fact that industry often takes time to react to new technologies, which requires preparations must be made as early as possible.

Specifically, the ANSSI has identified the particular threats[4] posed by quantum computers and quantum algorithms to the current security of data:

- Retroactive attacks, which consist in storing today data that is transmitted in encrypted form with the expectation of being able to easily decrypt it in the future (« store now, decrypt later »);
- Forgery attacks on digital signatures, which allow an attacker to impersonate the signer.

The best-known quantum attacks rely on specific algorithms that theoretically enable the resolution of computationally « hard » problems (for example, factorisation for RSA or the discrete logarithm for Diffie-Hellman key exchange) that traditional computers cannot solve within a reasonable timeframe :

- Shor's quantum algorithm, which threatens the most widely used public-key cryptography systems today. It efficiently solves the discrete logarithm problem (Diffie-Hellman, DSA) and the integer factorization problem (RSA) with a sufficiently large quantum computer (even though such a size is currently beyond the reach of existing technologies);
- Grover's quantum algorithm, which impacts the security of symmetric cryptographic systems and provides a so-called « quadratic » speedup (meaning a moderate improvement, but theoretically sufficient for sufficiently powerful adversaries) to solve the problem of finding the secret key.

In the case of quantum attacks on symmetric cryptosystems, the impact of a quantum computer is generally limited. Indeed, simply doubling the key size and slightly adjusting the

[4]https://cyber.gouv.fr/sites/default/files/document/EN_Position.pdf

hash function parameters will suffice to restore a level of security equivalent to that against a classical computer.

For public-key cryptosystems, the impact is far more serious. One of the main approaches consists in replacing current asymmetric mechanisms with new mechanisms robust against quantum attacks: so-called post-quantum cryptography.

Post-quantum cryptography

The goal of post-quantum cryptography is to develop cryptography that is robust against both quantum and classical computers, while remaining compatible with existing architectures and protocols (such as TLS, a secure communication protocol used on the web). In other words, post-quantum cryptography is not quantum.

In 2016, the National Institute of Standards and Technology (NIST) launched an international call for proposals for algorithms with the goal of standardising a new family of quantum-resistant cryptographic algorithms. The interviews took place a few days or weeks after NIST announced the first four selected algorithms[5] : one for key establishment (for encryption) and three for digital signatures (for authentication). Several of the selected algorithms include French researchers among their authors. The first draft standards based on these four algorithms were published in August 2023 for public consultation[6]. Other algorithms are still in the selection process[7]. Indeed, NIST's goal, and more generally that of the cryptographic community, is to provide the industry, in the near future, with several standards adapted to the constraints of each domain. This will ensure the availability of alternative solutions in the event that one standard is compromised.

The candidates for standardisation have generally followed the same approach: building cryptographic primitives based on computational problems that a quantum computer cannot solve efficiently. These problems are generally grouped into several families:

- Lattice-based cryptography[8] relies on the problem of finding the shortest vectors in a lattice of regularly spaced points within a multidimensional mathematical space. This approach has been widely studied in academia since 2005 and is also used for homomorphic encryption. Of the four algorithms selected by NIST, three are based on this approach.

[5] https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4

[6] https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers

[7] At the time of preparing this article, NIST announced the conclusion of the selection process for encryption algorithms and chose a second algorithm based on error-correcting codes. As for digital signatures, the selection process is still ongoing.
https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption

[8] https://en.wikipedia.org/wiki/Lattice-based_cryptography

- Code-based cryptography[9] relies on the problem of decoding a pseudo-random error-correcting code. This is also a well-established approach, studied since the 1970s. Among the algorithms still under consideration for standardisation, some are based on this mathematical problem.
- Hash-based cryptography[10] relies on the problem of inverting a hash function. This approach is very mature and considered highly secure by the interviewed experts, but it is only relevant for constructing digital signatures and is generally somewhat inefficient.
- Isogeny-based cryptography[11] relies on the problem of finding an isogeny between elliptic curves (simply put, an isogeny is a special function linking two elliptic curves while preserving their key properties). This approach is the most recent compared to the others (about ten years old) but promising. Among the candidate algorithms, the one based on this cryptography was broken. The interviewed experts believe that research on this approach is worth continuing due to its small key sizes, although it still suffers from a lack of maturity and the computational power required for encryption. It can be adapted to certain applications where data volume constraints are more critical.
- Multivariate polynomial-based cryptography[12] mainly relies on solving systems of multivariate polynomial equations. This approach dates back to the 1980s. While the basic scheme remains secure, many mechanisms based on this technique have been broken. Some multivariate mechanisms may nevertheless remain relevant, particularly for digital signatures.

Smooth migration to post-quantum cryptography

The ANSSI has commented on NIST's decision[13] regarding the first algorithms selected for the standardisation of post-quantum cryptographic algorithms. While satisfied from a scientific standpoint, the ANSSI does not advocate the immediate replacement of current asymmetric algorithms with post-quantum algorithms. Given that these algorithms are recent, the ANSSI recommends using them in a hybrid manner[14], that is, combining them with well-established pre-quantum algorithms (such as RSA encryption and elliptic curve cryptography) to ensure security at least equivalent to each of the two mechanisms used. This approach provides long-term protection against quantum computing while preventing any security regression. The agency recommends deploying post-quantum cryptography in three phases.

[9] https://fr.wikipedia.org/wiki/Code_correcteur
[10] https://en.wikipedia.org/wiki/Hash-based_cryptography
[11] https://en.wikipedia.org/wiki/Post-quantum_cryptography#:~:text=Isogeny%2Dbased%20cryptography
[12] https://fr.wikipedia.org/wiki/Cryptographie_multivari%C3%A9e
[13] https://cyber.gouv.fr/actualites/selection-par-le-nist-de-futurs-standards-en-cryptographie-post-quantique
[14] https://cyber.gouv.fr/en/publications/follow-position-paper-post-quantum-cryptography

- From now: hybridising post-quantum algorithms with classical cryptography for certain specific use cases (e.g., particularly sensitive data or products that cannot be updated before 2030);
- In a second phase (around 2025): possible implementation of post-quantum algorithms, still in hybrid mode, is strongly recommended whenever long-term security is required (the ANSSI may provide more detailed guidance on post-quantum cryptography and recommendations on how to implement hybrid schemes);
- By around 2030: use of post-quantum algorithms alone, without hybridisation, if they are recognised as secure.

Other European security agencies share the same position and adopt recommendations very similar to those of the ANSSI, particularly regarding hybridisation.

By exception to the general rule, signature mechanisms based on hash functions, which are well-known and have been studied for a long time, are considered secure today and can therefore be used without hybridisation. However, these algorithms are not very efficient (notably in terms of signature size), and their practical use is limited to specific use cases.

Conclusion of article #1

The potential threat posed by quantum computers to current cryptographic systems was clearly highlighted during the interviews. This sword of Damocles is driving significant efforts to develop robust solutions through post-quantum cryptography. The NIST's work to standardise post-quantum algorithms marks a crucial milestone in this evolution.

However, the need for a gradual transition to these systems, as recommended by the ANSSI, underscores the importance of adopting a careful and well-thought-out approach for deploying post-quantum cryptography. While some actors handling information requiring long-term protection must begin addressing this migration today, others can still wait a few years for the ANSSI to provide guidance, although it is possible to anticipate these changes, particularly by promoting « crypto-agility ».

Securing personal data largely relies on the use of robust cryptographic systems, whose deployment the CNIL has long recommended in numerous contexts. The potential emergence of powerful quantum computers within the next few decades not only requires designing technologies that will remain secure in this new context but also demands proactive anticipation, as it is no longer feasible to ensure the long-term security of personal data without taking this likely evolution into account.

Advanced privacy-preserving cryptographic techniques

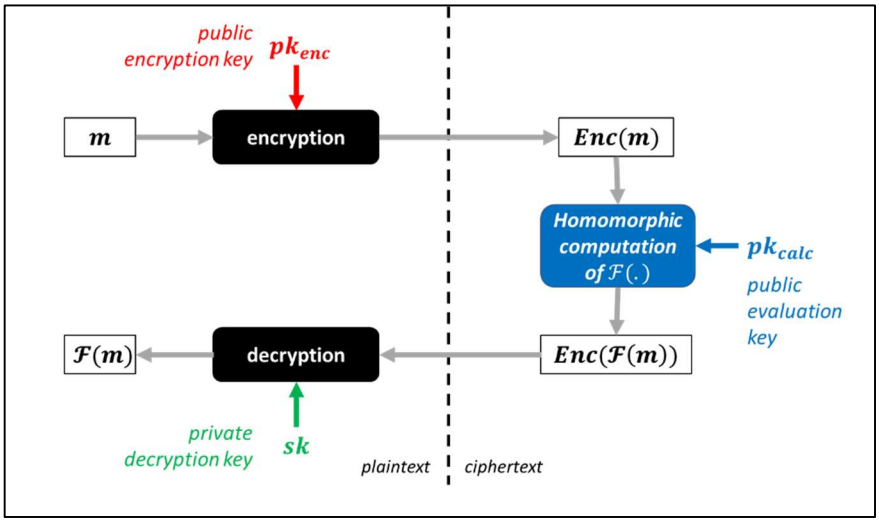
Interviews with cryptography experts explored privacy-enhancing technologies, commonly referred to as PETs. Although this field has historically been a subject of interest in academia for several decades, it is now attracting interest beyond the research sphere, bringing with it great promise. In this article, we present a summary of the ideas shared during these interviews with O. Blazy, S. Canard, M. Önen, P. Pailler, and experts from ANSSI.

Operations on encrypted data

Encryption is the main technique used to ensure data confidentiality. However, the need to process this data while preserving its confidentiality poses a major challenge. All the experts interviewed discussed the emerging opportunities and challenges associated with operations on encrypted data.

Fully homomorphic encryption (FHE)

Homomorphic encryption allows mathematical operations to be performed on encrypted data without knowing the underlying plaintext data. In practical terms, this means that calculations can be performed directly on the encrypted data, producing an encrypted result which, once decrypted, corresponds to the result of the calculation as if it had been performed on the plaintext data.



Descriptive diagram of homomorphic encryption

More specifically, there are several classes of homomorphic encryption, depending on the complexity of the operations that can be performed on the ciphertext:

- « Partially homomorphic » encryption only allows one type of operation to be performed: addition or multiplication. Although less general in use than somewhat homomorphic or fully homomorphic encryption (see below), it is of great interest due to its greater efficiency. Classic examples include private information retrieval (PIR), which is similar to an online search without revealing the search terms to the search engine, which can be performed with partially homomorphic encryption.
- Somewhat homomorphic encryption allows a small number of operations to be performed before the resulting ciphertext becomes impossible to decrypt.
- Fully homomorphic encryption (FHE) allows arbitrary operations to be performed on ciphertexts and therefore has the most applications in theory.

First imagined in the late 1970s, a first theoretical realisation of Fully Homomorphic Encryption (FHE) only appeared in 2009 thanks to the work of Craig Gentry[15][16]. The mechanism proposed by Gentry relied on lattices[17] but was not efficient in practice. Its use was limited by excessive complexity and significant performance costs compared to computations on plaintext data. Since then, fuelled by renewed industrial interest, FHE has made significant progress in terms of practicality, thanks to continuous advances in algorithms, hardware performance, and software optimization.

The opportunities for homomorphic encryption

One of the experts provided an overview of the solutions proposed by stakeholders in this ecosystem:

- At the hardware level: computations using FHE on encrypted data require far more operations than computations on unencrypted data. To enable faster processing, hardware acceleration may be necessary. Companies such as Intel, Optalysys, and Galois Inc. are developing processors specifically designed to perform the required resource-intensive mathematical operations.
- At the software level: the availability of software libraries, i.e., computer code providing specific functionalities for FHE and intended for developers, is a major asset for the democratisation of homomorphic encryption. Industry leaders such as IBM and Microsoft respectively offer the HELib and SEAL libraries. Other smaller companies are also active in this field (Duality Technologies, Inpher, Cosmian, etc.).
- At the compiler level: FHE compilers are software tools that simplify the programming of functions that can be executed in the encrypted domain. They enable to translate computer programs into FHE-compatible instructions, thereby facilitating the

[15] https://www.cs.cmu.edu/~odonnell/hits09/gentry-homomorphic-encryption.pdf
[16] Gentry, C. (2009, Mai). Fully homomorphic encryption using ideal lattices. In Proceedings of the forty-first annual ACM symposium on Theory of computing (pp. 169-178).
[17] https://en.wikipedia.org/wiki/Lattice-based_cryptography

adaptation of existing programs. Google and the French startup Zama both offer such compilers. The CEA also provides its own compiler, Cingulata from CEA-LIST, as an open-source project.

Most of the interviewed experts acknowledged that the FHE tools available today already enable to start using the technology, even for non-cryptography experts. In terms of efficiency, FHE is steadily progressing toward greater practicality, but it still requires significant technological investments before it can be broadly deployed in industry.

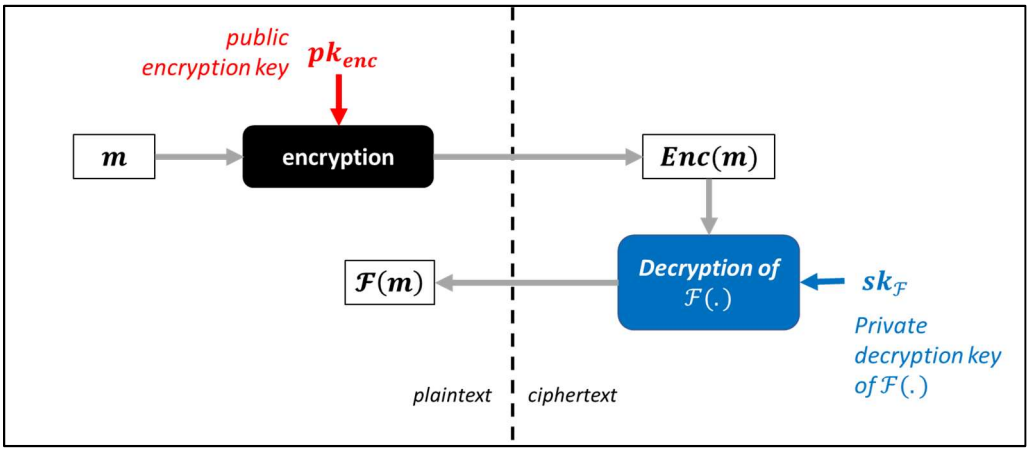
Other research perspectives around FHE were also discussed during the interviews:

- The first research avenue concerns scenarios involving multiple data sources that wish to perform computations on their pooled data. Standard FHE does not support this type of configuration, and in such cases, multi-party FHE or multi-key FHE should be prioritised.
- The second research avenue focuses on verifying the correctness and integrity of computations performed under FHE (« verifiable FHE »). This applies to the case of a cloud server executing computations delegated by a client, where the accuracy of the computation on encrypted data could be compromised. Verifiable FHE solutions would allow the client to verify the integrity of the computations carried out on the encrypted data, based on a proof generated by the cloud. The key challenge lies in ensuring that verifying the proof is more efficient than having the client perform the computation themselves.

Functional Encryption

Some experts mentioned functional encryption as a complementary tool for performing operations on encrypted data. It consists of encrypting data in such a way that it can be selectively decrypted, depending on the operations the user is authorised to perform. Functional encryption thus makes it possible to control access to data according to the specific functions each user is allowed to execute. For each function, a specific decryption key is generated.

In FHE, any computation is theoretically possible on the encrypted data, but the result remains encrypted and must be sent back to the holder of the decryption key in order to access it in cleartext. With functional encryption, however, the result of the computation is directly accessible in cleartext after the operation, but the data holder can only perform computations explicitly authorised by the data owner. Depending on the specific use cases, one or the other of these techniques may therefore prove more suitable.



Descriptive diagram of functional encryption

Today, functional encryption is still in its early stages. In terms of efficiency, research in this field has primarily focused on specific operations, such as the inner product, for which solutions have been developed to improve performance and practicality. However, when it comes to applying functional encryption to more general and complex functions, performance remains prohibitive for large-scale deployment.

It is therefore an active area of research, aimed at making functional encryption more efficient and practical.

Secure Multiparty Computation (MPC)

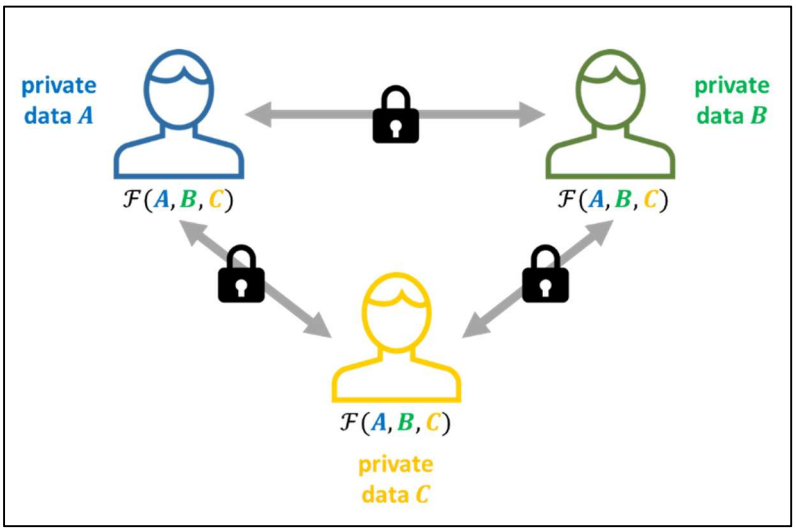
To perform computations on encrypted data, MPC was also discussed during interviews with experts. This branch of cryptography, which emerged in the 1980s, has been extensively explored since then. MPC has continuously evolved over the years, becoming increasingly practical and applicable to various use cases.

One of the first MPC protocols, the (*garbled circuits*[18]), was proposed by Andrew Yao[19] in 1982. In his study, Yao introduced the famous « millionaires' problem »: two millionaires want to determine which of them is richer, without revealing the exact value of their wealth to each other. A naïve but complex solution would involve a trusted third party: each millionaire would communicate the value of their wealth to this third party, who could then determine who is richer without revealing any other information. MPC techniques aim to replicate this scenario without relying on a trusted third party, while ensuring the same guarantees of confidentiality and correctness of the result.

In an MPC protocol, a set of parties, who do not trust each other, collaborate to jointly compute a function over their data without ever revealing anything about their initial inputs to the other participants, except what is implied by the final result of the function. This process

[18] https://en.wikipedia.org/wiki/Garbled_circuit
[19] https://crysp.uwaterloo.ca/courses/pet/W11/cache/www.cs.wisc.edu/areas/sec/yao1982-ocr.pdf

relies on advanced cryptographic techniques (secure secret sharing [20], oblivious transfer [21]; homomorphic encryption, etc.) and on communication among the participants.



Descriptive diagram of secure multiparty computation of a function $\mathcal{F}$

There are two main types of MPC protocols:

- Generic protocols, which allow the computation of an arbitrary function on the parties' data. They can be flexible and suitable for various applications, but may be complex and costly to implement;
- Specialised, or ad-hoc protocols, which are designed for specific functions chosen in advance. These protocols are optimised for these particular tasks and are often more efficient in terms of computation time and required resources. They have been studied enough to be usable today. This is particularly the case for protocols enabling the computation of private set intersections (see below), whose computation times have been significantly reduced compared to the early versions of these protocols.

Some of the experts mentioned tools for developing MPC-based solutions (namely SCALE-MAMBA and MP-SPDZ). These open-source tools can be used to compile a general function into a secure MPC protocol.

In recent years, advances in MPC have made it possible to consider implementing systems based on this paradigm. In addition, MPC-based applications are often more mature than applications based solely on homomorphic encryption. This is because homomorphic encryption remains more expensive than MPC, particularly for large-scale operations. For several years now, there have been concrete applications of MPC:

[20] https://fr.wikipedia.org/wiki/Secret_r%C3%A9parti
[21] https://fr.wikipedia.org/wiki/Transfert_inconscient

- In Denmark, in 2008, an auction of sugar beets[22] was secured using MPC;
- In Boston, since 2016, studies on gender pay inequality commissioned by the Boston Women's Workforce Council[23] have been conducted using MPC techniques.

Focus on PSI

Private Set Intersection (PSI) is a form of MPC that allows multiple parties to find common elements in their data sets without revealing the contents of their respective data sets. PSI only reveals the shared elements (the intersection) in the different data sets. Of all the existing MPC protocols, PSI is undoubtedly the one that has seen the most concrete applications (or use cases): Apple[24] and Google's[25] password monitoring tools, and Apple's project to detect child sexual abuse material[26] (CSAM).

Zero-knowledge proofs

Some of the experts interviewed identified zero-knowledge proofs (ZKPs) as cryptographic mechanisms that could be immediately deployed in various real-world use cases. Proofs of concept already exist, particularly in the context of privacy-friendly age verification[27]. ZKPs are also promoted by a number of experts for the implementation of future European digital identity wallets[28] planned under the European Union Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS 2 Regulation[29]).

These proofs, introduced in the 1980s, make it possible to prove that a condition (or assertion) is true without revealing the underlying information, thereby ensuring confidentiality. They can be useful in many scenarios: proving that a data subject is of legal age without revealing their identity, proving that they have a certain amount of money without revealing their bank account balance, etc.

[22] https://ercim-news.ercim.eu/en73/special/trading-sugar-beet-quotas-secure-multiparty-computation-in-practice
[23] https://thebwwc.org/mpc?rq=mpc
[24] https://support.apple.com/fr-fr/guide/security/sec78e79fc3b/web
[25] https://security.googleblog.com/2019/12/better-password-protections-in-chrome.html
[26] https://www.apple.com/child-safety/
[27] https://linc.cnil.fr/en/demonstration-privacy-preserving-age-verification-process
[28] https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/Security+and+Privacy
[29] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ%3AL_202401183

ZKPs still present significant challenges in terms of implementation. Their design requires expertise in advanced cryptography, and translating them into real-world applications requires a thorough understanding of the underlying concepts.

Furthermore, the practical implementation of ZKPs can sometimes require significant computing power. For applications such as age verification, where a server does not need to verify a large number of proofs simultaneously, this may not pose a major problem. However, for large-scale applications, such as the use of ZKPs in blockchain, response times can be crucial. Finding the best compromise between privacy and performance remains a major challenge: some protocols may sacrifice a little privacy for better performance, or vice versa.

Moreover, another challenge lies in the fact that some ZKP systems require a trusted setup phase to generate the initial parameters necessary for the execution of the proof protocol. This phase may involve trust assumptions that are too demanding in real-world scenarios.

However, ZKPs are still evolving and gaining maturity. Research in this field is focusing in particular on improving computational efficiency, reducing resource requirements, and standardisation for widespread adoption. These advances may even be accelerated by the explicit mention of ZKPs in recital 14 of the eIDAS 2 regulation.

In the near future, the experts anticipate a more widespread integration of ZKPs as these systems become more efficient. Moreover, ZKP solutions robust to quantum attacks exist and are currently subjects of ongoing research. Other research directions aim to combine ZKPs with, or construct them from, other cryptographic building blocks. For instance, « MPC-in-the-head », a paradigm for building a ZKP system from a multiparty computation (MPC) protocol, has been the subject of several scientific publications. Other ongoing work combines ZKPs with FHE to ensure confidentiality and verifiability of computations on encrypted data, as discussed earlier.

Group Signatures

This technology was introduced in the 1990s by Chaum et van Heyst[30]. It refers to a type of digital signature for a group of people. The group is associated with a single public key used to verify signatures. Each member of the group has their own private signing key, which allows them to generate signatures that can be verified using the group's public key. This type of signature enables a group member to prove their membership without revealing their individual identity (i.e., in practice, it is difficult to determine which group member generated the signature). Each group member can sign messages on behalf of the group, and, like any digital signature, anyone can verify the signature. It is also possible to give a trusted authority the ability to reveal the identity of the signer.

Group signatures are a well-established cryptographic mechanism. Certain forms of group signatures are already standardised by the ISO (International Organization for

[30] https://link.springer.com/chapter/10.1007/3-540-46416-6_22

Standardization) under the ISO/IEC 20008 standard. Group signatures are used in industry, particularly in TPM (Trusted Platform Module) cryptoprocessors, in the form of Direct Anonymous Attestations, a cryptographic primitive that allows remote authentication of the TPM while preserving the identity of the user of the platform containing the module. A similar approach is employed in Intel processors through EPID (Enhanced Privacy ID).

Nevertheless, one of the experts expressed regret that group signatures remain largely confined to research and development, despite the existence of efficient implementations and established standards. One practical application mentioned, which could work effectively in practice, is the use of group signatures to control access to a building entrance or to perform privacy-preserving age verification. In this regard, LINC has published a demonstrator[31] of an age verification mechanism based on group signatures.

Conclusion of article #2

At a time when privacy protection is a major concern, interviews with cryptography experts have provided several key insights.

The emergence of privacy-enhancing technologies (PETs) such as homomorphic encryption (FHE), zero-knowledge proofs (ZKP), and group signatures offers innovative solutions to address these concerns. Despite significant progress in these areas, challenges remain, particularly regarding performance and practicality. However, with growing industry interest and ongoing research efforts, the widespread adoption of these technologies appears increasingly realistic.

Although the GDPR does not explicitly mention these technologies, its Article 25 on « data protection by design and by default » underscores the importance they could have in fulfilling this obligation. The CNIL could promote and encourage their use in implementing the regulation to further strengthen the protection of personal data.

[31] https://linc.cnil.fr/demonstrateur-du-mecanisme-de-verification-de-lage-respectueux-de-la-vie-privee

Practical applications of advanced cryptography

The interviews gave us an overview of the foundations and promises of post-quantum cryptography (article #1) and advanced privacy-preserving cryptography techniques (article #2). The experts discussed practical use cases for these promising technologies while highlighting the challenges that need to be overcome for their widespread adoption.

While classical cryptography continues to play an essential role in everyday life, advanced cryptographic tools respond to new challenges posed by uses such as cloud computing and artificial intelligence, where data processing is often delegated to remote servers. When it comes to zero-knowledge proofs (ZKP), the approach is slightly different: the primary goal is to improve security guarantees by reducing the need to trust a third party, while minimizing the associated risks. It is also important to note that these new cryptographic tools are based on the fundamentals of traditional cryptography, such as encryption and hashing.

The practical applications of advanced cryptography

During the interviews, the experts all agreed that these technologies can play a key role in the processing and protection of data, particularly personal data.

Contributing to compliance with GDPR principles

Advanced cryptography technologies can contribute in part to compliance with certain data protection principles set out in Article 5 of the GDPR[32] :

The principle of confidentiality

Advanced cryptographic technologies naturally contribute to compliance with the principle of confidentiality. Techniques such as FHE (Fully Homomorphic Encryption), FE (Functional Encryption) and secure multiparty computation (MPC) enable operations to be performed on encrypted personal data without decrypting it, thereby preserving its confidentiality at every stage of processing. On the other hand, by allowing knowledge of information to be demonstrated without revealing it, zero-knowledge proofs (ZKP) can also contribute to the confidentiality of personal data.

[32] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

The principle of data minimisation

The ability of ZKPs to provide proof of the veracity of a statement without disclosing the underlying information contributes to compliance with the GDPR's principle of data minimisation. Thus, ZKPs could prove useful in authentication and access control systems, where proof of a user's identity is required without revealing unnecessary personal information (such as « age verification[33] »).

The principle of fairness and transparency

Advanced cryptographic techniques providing verifiability guarantees (verifiable storage, verifiable computation, verifiable encryption, etc.) could contribute to the principle of transparency by enabling data subjects to verify the data operations performed by a data controller.

The principle of purpose limitation

Functional encryption (FE) seems particularly well suited to contributing to the principle of purpose limitation. This technology allows access to data only for specific purposes using functional keys, thereby limiting the use of data to a defined objective. Similarly, ad-hoc MPC protocols, designed for a particular use, allow data operations for specific purposes.

The principle of accountability

Group signatures, for example, provide, by design, a mechanism that can contribute to the principle of accountability: in the event of abuse, the group administrator can identify the signers and hold them accountable for the transactions they signed with their private signature key.

Machine learning and artificial intelligence

Among the most dynamic applications of advanced cryptography, machine learning and artificial intelligence (AI) occupy an important place. This is particularly true in the context of deep neural networks.

MPC techniques are highly relevant in the field of machine learning, particularly in scenarios where models are trained collaboratively by multiple parties on data that must remain confidential. One of the challenges of MPC protocols is the requirement that stakeholders remain connected throughout the protocol.

[33] https://linc.cnil.fr/en/demonstration-privacy-preserving-age-verification-process

The training phase on encrypted data is a hot topic in research. This approach would make it possible to preserve the confidentiality of training data. However, its implementation is still complex today. On the other hand, the inference phase on encrypted data in FHE already allows AI models to make predictions while keeping the data encrypted.

Furthermore, one of the experts mentioned ongoing work on the digital watermarking of AI models and training data (see LINC's articles on digital watermarking in AI[34]) which attracts strong interest from many industries, particularly for the purpose of protecting the intellectual property of models. The goal of watermarking is to embed a unique, unalterable, undetectable, and hard-to-predict signal into the data or the model. This would allow the model owner to prove actual ownership and to demonstrate when their model is being used without authorisation.

Confidential computing in the cloud

In the context of cloud computing, the end customer is responsible for protecting the data they store and process in the cloud. Encryption is one of the measures they can use[35].

Advanced encryption techniques, particularly FHE, are proving to be a relevant measure in this context. By encrypting data with FHE before it leaves the customer and keeping it encrypted during transit, storage, and processing in the cloud, the data remains unreadable to both malicious third parties and the provider itself, while maintaining the functionality of the cloud service.

In addition, MPC offers advanced applications for secure storage and processing of personal data in cloud environments. MPC enables calculations to be performed on distributed datasets while preserving the confidentiality of information. For example, it can be used to perform calculations on personal data distributed across multiple cloud service providers, ensuring that data is never centralised in a single location (this is particularly true for secret sharing-based MPC protocols, where data is fragmented and processed collaboratively without revealing the entirety of the information to each party). This approach reduces the risk of compromise in the event of a breach at a single provider, as the data is fragmented and distributed securely. MPC is also useful for performing calculations on data from multiple customers while preserving the confidentiality of each customer's individual data (in cases of data pooling and collaborative computing). MPC allows these processes to be carried out in the cloud without disclosing specific customer data to the cloud provider or other customers.

[34] https://linc.cnil.fr/en/overview-and-out-perspective-artificial-content-detection-solutions-12
[35] https://www.cnil.fr/fr/les-pratiques-de-chiffrement-dans-linformatique-en-nuage-cloud-public

What are the barriers to adoption?

This is a legitimate question. These technologies offer innovative, even revolutionary potential in terms of how personal data could be processed while maintaining its security. However, their adoption is not yet widespread. The interviews enabled us to identify some answers to this paradox.

A constantly evolving field

The interviews highlighted that the field of advanced cryptography is constantly evolving, and that this evolution is rapid. Technologies that were considered mere theories a few years ago (FHE, post-quantum, etc.) are now among the most dynamic areas of research. This uncertainty about technologies can make decision-making difficult for companies, as they must constantly assess whether new advances are ready for adoption.

Furthermore, the technical complexity of these solutions can be an obstacle to their widespread adoption. However, frameworks such as Concrete-ML (for FHE), or initiatives aimed at simplifying implementation, such as the SCALE-MAMBA tool (for MPC), can help overcome this complexity and make these technologies more accessible.

Finally, performance trade-offs can hinder the adoption of these technologies. Advanced encryption techniques are inherently computationally intensive. They introduce significant overhead when processing encrypted data, which inevitably leads to longer processing times compared to operations performed on unencrypted data. This can be a limiting factor for companies that require high performance. However, depending on the use case, some organisations may be satisfied with slower technologies that do not require real-time processing. In such cases, they should be able to accommodate the intensive calculations (for example, by running a process overnight). Nevertheless, improving performance is an ongoing goal, with researchers and manufacturers working on new techniques (particularly hardware) and more efficient algorithms. It is therefore reasonable to expect that eventually performance will improve sufficiently to meet the needs of organisations.

Industrial adoption not widely encouraged

Despite the maturity of certain advanced cryptography technologies, their adoption has been slow. Industry inertia, resistance to change, and a lack of regulatory incentives are all factors that can hinder their widespread implementation.

One expert noted that the barrier to widespread adoption of advanced cryptographic technologies can be partly attributed to a lack of market demand. Why invest heavily in research and development for these technologies if customers are not explicitly asking for them? As long as the adoption of these technologies is not a requirement clearly stated by customers or imposed by strict regulations, many companies may prefer to invest their

resources elsewhere, where they perceive more immediate demand and therefore greater profit. Some form of external incentive may be necessary.

This same expert therefore envisages calls for tenders for specific projects that could include PET requirements in their specifications, thereby forcing manufacturers to meet these requirements in order to be eligible for these projects. Ultimately, he believes that normative or regulatory obligations could change the situation.

The complexity of the transition to post-quantum cryptography

This transition is complex and requires thorough planning by the stakeholders. It will not simply be a matter of replacing pre-quantum algorithms with new post-quantum algorithms. ANSSI therefore recommends implementing hybrid systems. However, managing these hybrid systems could be complex. It will be necessary to raise awareness among bodies and inform them about the measures needed to prepare for post-quantum.

Conclusion of the three articles

In conclusion, interviews with experts reveal that certain advanced cryptography tools are already practical and deployable, even if they have not yet been widely adopted by industry.

Furthermore, the interviews show that the field of advanced cryptography is currently experiencing a period of rapid growth, both in research and in industrial applications. The emerging opportunities are promising, offering relevant solutions for the protection of personal data and AI security.

In addition, the standards currently being developed by organisations such as NIST (for post-quantum), ISO (for FHE, MPC, ZKP, and group signatures), and the Homomorphic Encryption Standardization Consortium (for FHE) play a key role in adoption by industry.

However, the widespread adoption of these technologies is not without challenges, such as technological maturity that has yet to be achieved and the lack of incentives to use these technologies.

It is undeniable that the CNIL has an important role to play, within the framework of its missions, in promoting the adoption and encouraging the use of advanced cryptographic technologies.