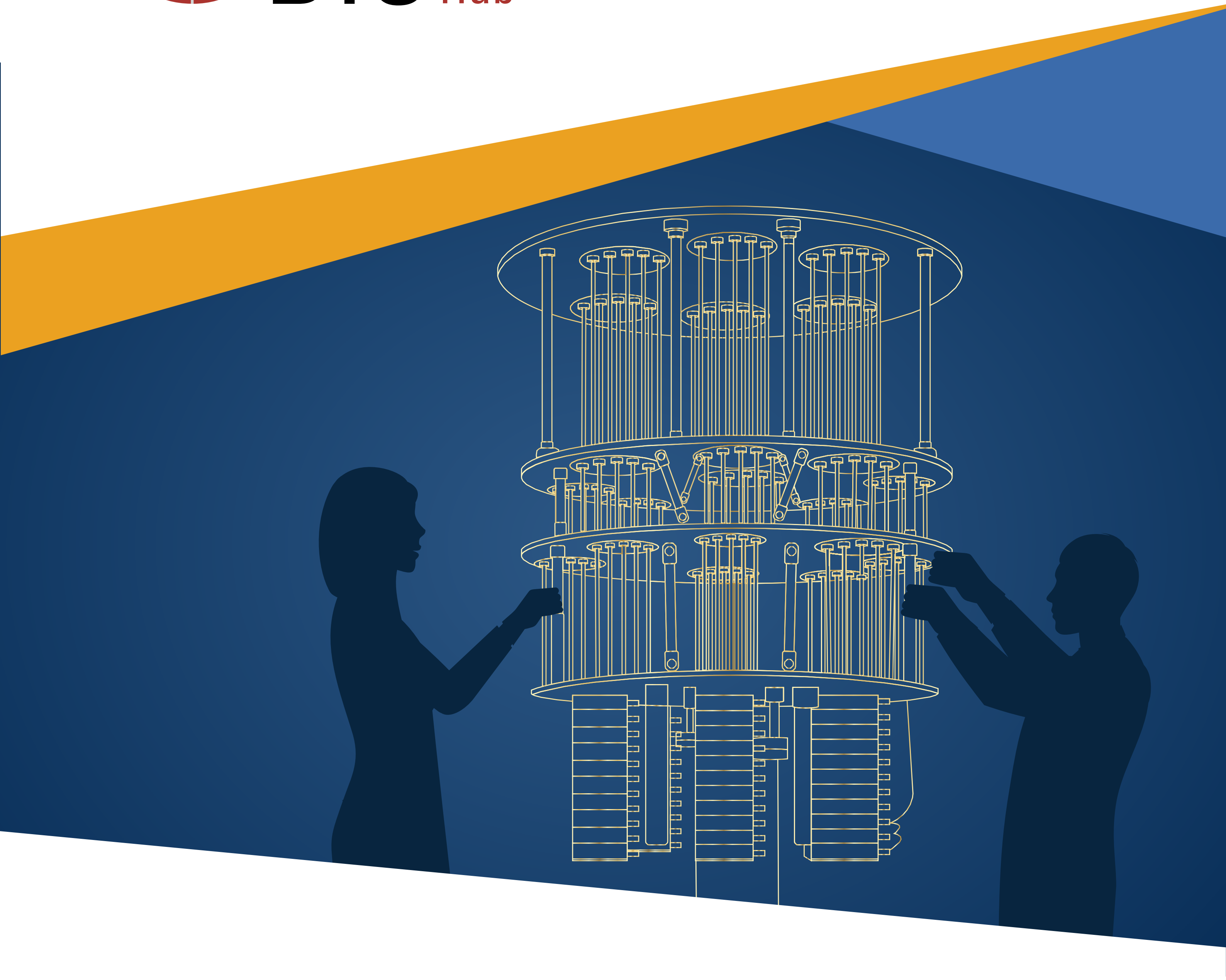
BIS Innovation Hub



Project Leap

Quantum-proofing the financial system

June 2023

BANQUE DE FRANCE
EUROSYSTÈME

DEUTSCHE
BUNDESBANK
EUROSYSTEM

Executive summary

Quantum computers represent a serious threat for the financial system. If they become practicable, they could be used to compromise the security of the current mainstream cryptographic protocols upon which the financial system relies to secure data and transactions. In the mid-1990s, researchers created quantum algorithms that – at least in theory and given a sufficiently powerful quantum computer – could break today’s widely used public key cryptographic schemes. This would instantly obsolete many current cryptographic techniques, threatening the foundations of our financial services infrastructure and severely impacting financial stability.

While functional quantum computers are not yet available, the security threat needs to be urgently addressed. Already, malicious actors can intercept and store confidential, classically encrypted data with the intention of decrypting it later when quantum machines become powerful enough to do so. This means that data stored or transmitted today are, in fact, exposed to “harvest now, decrypt later” attacks by a future quantum computer. The long-term sensitivity of financial data means that the potential future existence of a quantum computer effectively renders today’s systems insecure.

The aim of Project Leap is to help secure the financial system against this threat. It is already feasible to implement quantum-resistant cryptographic protocols. However, implementing them in financial systems raises a number of challenges. Specifically, the lack of flexibility in legacy systems means that a major transition effort will be necessary. Project Leap addresses some of the specific challenges of implementing quantum-resistant IT environments for the financial system, with a view to preparing for this transition and accelerating it.

This joint experiment by the BIS Innovation Hub Eurosystem Centre, the Bank of France and Deutsche Bundesbank aims at quantum-proofing the financial system, starting with central bank processes. Project Leap’s first phase explored the implementation of post-quantum cryptographic protocols to central bank use cases such as payments. A quantum-safe environment was created to secure infrastructures against the interception of data in transit. This solution could protect highly sensitive communications. With its two key objectives of quantum-proofing the financial system and raising awareness among the central banking community, the project aims to contribute valuable insights into the financial system‘s quantum journey.

One specific challenge addressed by Project Leap’s first phase is cryptographic agility, namely the ability to switch between cryptographic schemes and algorithms without affecting the applications. Since the new quantum-resistant cryptographic standards are still under discussion, cryptographic agility will be crucial in the transition to quantum-resistant encryption. Another important finding relates to the trade-off between security strength and performance. In the world of post-quantum cryptography, security may need to be configured according to application requirements. These, and other technical findings are summarised in Chapter 6.

The first phase of Project Leap successfully established a quantum-safe environment in a financial systems context. As this has been achieved in a test environment, more work will be needed to explore complex real-life environments. Hence, a second phase of Project Leap is planned in order to investigate more network architectures, test different types of hardware, and incorporate additional communications layers to build a complete chain of trust, as well as to include additional central bank processes.

Contents

1. Introduction

1. Introduction

Quantum computing has become a major field of research. Since the early 1990s, there has been a significant increase in publications on quantum computing (Scopus (2021)), with more than 48,000 publications in 2020 alone demonstrating the interest in this rapidly emerging technology. Leading tech companies as well as start-ups have been developing quantum computers with an increasing number of qubits. In the near future, quantum computers may be able to significantly surpass the capabilities of today's classical computers for certain kinds of task.

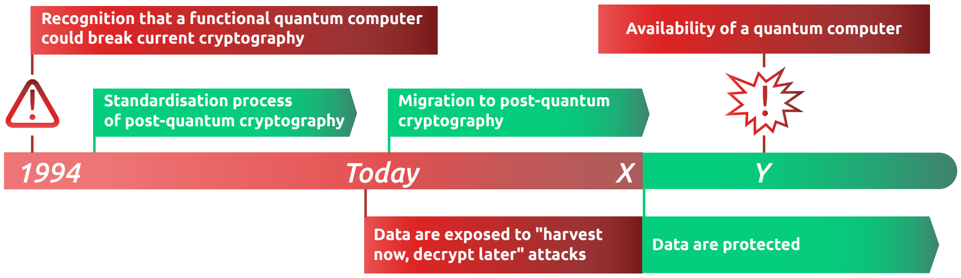
The potential power of quantum computers could be a boon for many industries. This includes the financial industry, where quantum computers could support the use of artificial intelligence in financial services or improve financial modelling. In the banking industry, for example, there is increasing interest in using quantum algorithms to speed up Monte Carlo simulations.

But, because today's financial system is heavily dependent on traditional cryptographic security protocols to secure data and communications, quantum computers could expose the financial system to new forms of cyber attacks. Indeed, a fully functional quantum computer would have a significant impact on the cryptographic algorithms currently in wide use. The Financial Stability Board stated in its report on Financial Sector Cybersecurity that cyber attacks are a damaging threat to the financial system. The cyber risk suffered by the financial sector has been mitigated by regulatory and supervisory work conducted by authorities around the world. Nevertheless, a hostile use of financial data would have a disrupting impact on important financial services, by threatening security and data confidentiality, with a damaging effect on financial stability (FSB (2017)). Also, in its most recent global risks report, the World Economic Forum listed the cyber threat of quantum computing as one of the major emerging global technological risks (WEF (2022)). This situation has called for collective action, including the development of new encryption standards capable of protecting financial services IT systems.

While functional quantum computers are not yet available, the security threat is immediate, and needs to be urgently addressed. Already, malicious actors can intercept and store confidential, classically encrypted data with the intention of decrypting it later when quantum computers become powerful enough to do so. This means that data stored or transmitted today are, in fact, exposed to "harvest now, decrypt later" attacks by a future quantum computer. The long-term sensitivity of financial data means that the potential existence of a quantum computer in the future effectively renders today's systems insecure.

This urgency is further illustrated in Graph 1, in which the line Y shows when a quantum computer that can break current cryptographic algorithms might become available. Correspondingly, X denotes the time when the transition to quantum-resistant cryptography is completed. Even if X is earlier than Y, so that the transition is completed "in time", this will safeguard only data that are stored or transmitted afterwards. All data that are stored or transmitted today are, effectively, exposed to the threat represented by a future quantum computer.

Graph 1


Recognition that a functional quantum computer could break current cryptography
Availability of a quantum computer
Standardisation process of post-quantum cryptography
Migration to post-quantum cryptography
1994
Today
X
Y
Data are exposed to "harvest now, decrypt later" attacks
Data are protected

It is paramount that central banks understand the urgency of the quantum cyber threat, and the complexity of migrating to quantum-resistant cryptography. It is also crucial to prepare to implement the new cryptographic protocols as soon as possible. Project Leap aims to contribute insights regarding this transition, thereby paving the way for a successful migration to quantum-resistant systems.

2. The quantum cyber threat to central bank IT systems

2.1 Why quantum computing represents a cyber threat

To understand the quantum cyber threat, it is crucial to grasp the functioning of a quantum computer. In traditional computer systems, information is converted into a series of binary digits, called bits. Each bit has only one possible value, either 0 or 1. With this two-dimensional classical system, computers can carry out a wide range of tasks and provide the foundation upon which the entire Web-based economy, including financial services, is built.

A quantum computer processes information by representing data using quantum particles, very differently to the way in which classical computers operate (see Annex A Box 1). The basic unit of information in a quantum computer is not a bit but a qubit – which stands for a quantum bit. Like a classical bit, a qubit can have a value of either 0 or 1. Unlike a classical bit, a qubit can also be in a superposition state in which its value is both 0 and 1 simultaneously. This superposition state gives quantum computers vastly more processing power than classical computers for certain kinds of tasks.

Considerable challenges remain to be solved when it comes to successfully building a quantum computer. One of the main challenges is "noise". During computation, all atomic and subatomic particles present in and around the quantum computer can potentially interfere with the qubits, creating imperfect states and so negating their computational advantage. Even though physical implementations of quantum computers operate at close to absolute zero temperatures in highly isolated environments in order to minimise interference, it is currently difficult to create sufficient numbers of perfect qubits, limiting what quantum devices can achieve.

Due to this noise problem, today's quantum computers are limited to between 50 and a few hundred qubits. This prompted John Preskill, a professor of theoretical physics at the California Institute of Technology, to dub the current state-of-the-art in quantum computing the Noisy Intermediate-Scale Quantum (NISQ) era (Preskill (2018)). Because quantum computers continue to evolve, though, the expectation is that these limitations will eventually be overcome.

Companies and organisations working in the field of quantum computing generally follow two different approaches in the quest to generate a higher number of qubits. Some have been trying to stabilise physical qubits and create perfect ones. Others apply error correction techniques to offset the lack of stability. This involves adding more qubits, called logical qubits. Even though NISQ devices are limited in terms of what they can do, noisy quantum computers can already carry out certain specific tasks successfully.[1]

It is still uncertain just when an operational quantum computer will be built that is powerful enough to break current cryptographic protocols. However, expert opinion is that this likely to take place in the next 10–15 years (Mosca (2021)). The rapid pace of advances in the industry make prediction difficult: a new breakthrough that completely changes the outlook could happen at any time. In December 2022, Chinese researchers claimed in a debated paper that it could be possible to break the widely used RSA-2048 (Rivest–Shamir–Adleman) cryptographic scheme with the current generation of quantum

[1] There have been many debates in the quantum computer community about if and when we will reach the moment of "quantum supremacy" – that is, the moment when quantum computers outperform classical ones. In 2019, Google announced that its 53-qubit "Sycamore" processor had performed a particularly complex calculation 158 million times faster than the world's most powerful classical computer, reducing the time required from 10,000 years to less than four minutes. Although it turned out that the task was artificially designed for the purpose of the experiment, this clearly showed that 50 qubits represent a significant threshold – the point at which a quantum machine can begin to perform specific tasks in less time than a classical computer. At the end of 2020, Chinese researchers at the University of Science and Technology of China in Hefei announced that their quantum computer is capable of solving a problem that the most powerful existing computers are not able to solve. In 2022 IBM researchers presented a quantum roadmap targeting 4,158 noisy qubits in 2025.

machines (Yan et al (2022)). In February 2023, a major actor in quantum computing reported a reduction in the error rate of qubits, generating less noisy quantum machines. These rapid performance improvements significantly increase the risk of a quantum attack.

Of equal or perhaps more concern is the current "harvest now, decrypt later" quantum cyber threat, in which malicious actors could intercept and store confidential, classically encrypted data today with the intention of decrypting them later when quantum computers become powerful enough to do so. Any data that require long-term cryptographic protection (ie all data that must be kept secure and private for more than 10 years) will require post-quantum protection as soon as possible, especially if these data are being stored off-site (eg in the cloud).

Such a cyber risk would have damaging consequences for the financial system. It is paramount to consider this risk and subsequent vulnerabilities that could affect the financial stability.

2.2 The potential threat to current cryptographic techniques

Cryptography is based on computational complexity. Today's cryptography reliably protects information in today's computer systems, assuring secure internet communications among other things. It is an essential tool that ensures the confidentiality, integrity and authentication of online communication. This means that the information should be accessible only to a pre-determined recipient, who can be sure that the information comes from the correct sender and that this information was not altered in transit.

There are two types of encryption systems currently in use: symmetric and asymmetric encryption (which is also known as public key cryptography). Creating a secure tunnel between two different IT systems is usually carried out in a multi-step process, using both symmetric and asymmetric encryption systems (see Graph 2). First, a secret key is exchanged in a process called key exchange mechanism (KEM), the secret key being encrypted with asymmetric encryption, and then this shared secret key is used to encrypt the message sent between the two parties, using symmetric encryption. One reason for this combined approach is the fact that asymmetric encryption is significantly slower than symmetric encryption.

Asymmetric cryptography relies on complex mathematical problems, such as prime factorisation. The idea is that, while it is trivial for classical computers to generate a number by multiplying two sufficiently large numbers together, factorising that number back into the original prime numbers is extremely challenging.

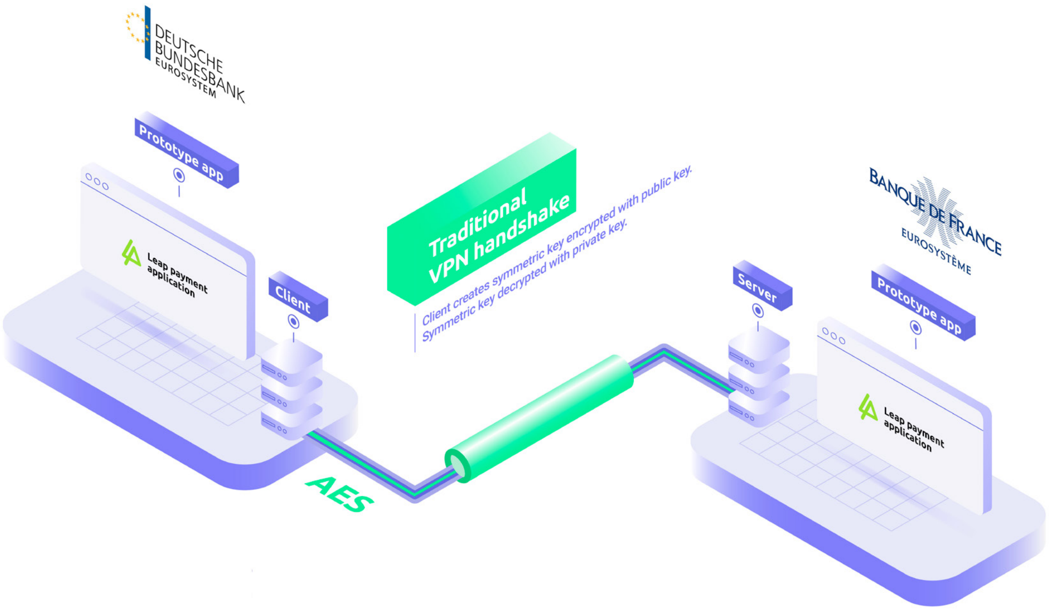
In 1994, the mathematician Peter Shor devised a quantum algorithm theoretically capable of calculating prime factors of large numbers. Cyber security experts immediately confirmed the threat that Shor's algorithm posed to asymmetric cryptography such as the encryption algorithm RSA, which relies for its security on the difficulty of efficiently factoring very large numbers. If run on a quantum computer with enough qubits, Shor's algorithm could render the prime factorisation challenge insignificant, reducing an operation that would take hundreds or thousands of years on today's classical computers to hours or even minutes on a sufficiently powerful quantum computer. A second quantum algorithm named Grover also represents a threat to such symmetric encryption algorithms as AES (Advanced Encryption Standard) or SHA, which is used in cryptoasset mining processes. Regarding AES, the solution consists in increasing the key length from 128-bit to 256-bit, making it secure against an attack based on Grover's algorithm.

In addition, it is important to understand that this cyber threat will have an impact not only on public key algorithms, but also on the ways the cryptographic keys are generated. To guard against this threat, all the cryptographic protocols using asymmetric encryption must be strengthened, including authentication. Digital signatures are a cryptographic mechanism that is used to verify data integrity and authentication. In a digital signature scheme, a signer has a secret signing key, and a signature verifier has a corresponding public key. When a signer signs a message using its secret key, the signature can be verified by using the corresponding public key. Digital signatures are widely used in payment systems.

As research in quantum computing is rapidly evolving, the pressing question is when will a quantum computer be capable of breaking current cryptographic schemes. To answer this question, it would be necessary to have a precise idea of how many perfectly stable qubits are needed to efficiently apply Shor's or Grover's algorithm, with the aim of mounting an attack against an asymmetric encryption scheme. As different estimates have been published regarding the number of qubits that are needed to break the RSA encryption algorithm, it is difficult to predict the exact date when it will become obsolete. To complicate matters, estimates of when a quantum machine will become operational often differ wildly depending on whether the person making the prediction comes from the research community or is involved in a company building (and trying to sell) quantum computers. What is beyond doubt is that no organisation, and certainly not central banks, will want to risk becoming a victim of a quantum computer cyber attack through inaction.

To respond to this cyber security threat, the scientific community has been working on new cryptographic protocols to create quantum-resistant environments. Project Leap explores these new cryptographic schemes.

Graph 2 Setting up a traditional VPN

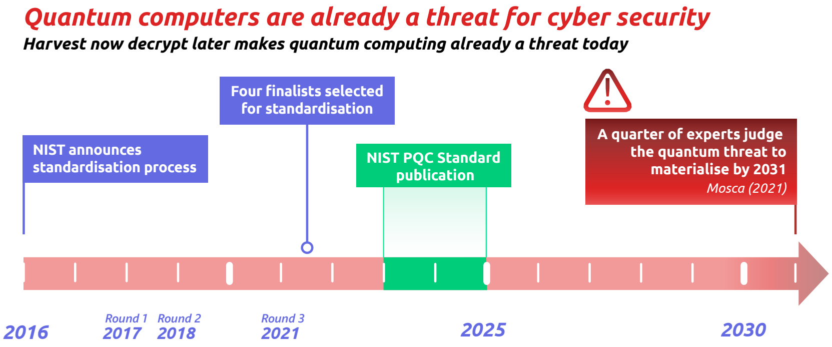

DEUTSCHE BUNDESBANK EUROSYSTEM
Prototype app
Leap payment application
Client
Traditional VPN handshake
Client creates symmetric key encrypted with public key.
Symmetric key decrypted with private key.
AES
Server
BANQUE DE FRANCE EUROSYSTÈME
Prototype app
Leap payment application

3. How to defend against the quantum threat

3.1 An international cooperation organised by NIST

Researchers and national standards authorities have been working on solutions to keep internet information safe. In 2016, the US National Institute of Standards and Technology (NIST) announced a public competition to select quantum-resistant public key cryptographic algorithms. More than 80 algorithms (23 signature schemes and 59 key encryption mechanism schemes) were developed through a collaborative process involving experts from all over the world. This was followed by a number of competitive rounds in which the scientific community tested the proposed algorithms. This process resulted in different algorithms being excluded from the competition by peers or by the work of experts of NIST.[1]

Graph 3


Quantum computers are already a threat for cyber security
Harvest now decrypt later makes quantum computing already a threat today
Four finalists selected for standardisation
NIST announces standardisation process
NIST PQC Standard publication
A quarter of experts judge the quantum threat to materialise by 2031
Mosca (2021)
2016
Round 1
2017
Round 2
2018
Round 3
2021
2025
2030

In July 2022, after three rounds of competition (Graph 3), the first set of four algorithms were selected for standardisation. This means that it is now feasible to implement and test these algorithms for real-world use cases.

In Project Leap, one of the major objectives was to implement the selected algorithms and understand the impacts when migrating to new cryptographic standards. During the project all the algorithms selected by NIST for standardisation were tested. Also implemented and tested was the FrodoKEM algorithm, which is considered by the French and German authorities for cyber security[2] to be as reliable as the other algorithms selected for standardisation by NIST (see Table 1).

Table 1 List of algorithms tested in project Leap

Algorithm	Type	Family*	Round
CRYSTALS-Kyber	Public key encryption	Lattice-based	Selected for standardisation
CRYSTALS-Dilithium	Digital Signature	Lattice-based	Selected for standardisation
FALCON	Digital Signature	Lattice-based	Selected for standardisation
SPHINCS+	Digital Signature	Hash-based	Selected for standardisation
FrodoKEM	Public key encryption	Lattice-based	Considered a good option by French and German authorities

** Annex B describes different families of algorithms.*

[1] In 2022, for example, two algorithms were tested, and their weaknesses exposed. A digital algorithm called Rainbow submitted to the NIST for message verification was broken, and a cryptographic algorithm known as Supersingular Isogeny Key Encapsulation (SIKE), was cracked in about an hour using one core of a 2013 Intel Xeon processor. These algorithms were thereupon excluded from the competition process.

[2] ANSSI and BSI (see glossary).

Cryptographic algorithms are often based on specific families of mathematical problems. Three of the four algorithms selected by NIST for standardisation are from the lattice-based family of problems, and one is from the hash-based family (see Annex B for a full list).

One important objective of the NIST process was to employ a diverse set of families of mathematical problems as the basis for the algorithms. This is because, while one algorithm could be considered reliable enough to secure IT systems today, it is uncertain if this would be the case over the long run as cyber threats evolve quickly. To encourage algorithms from a wider range of families, NIST launched a fourth round in 2022. This round includes public key encryption mechanisms based on such families as Isogeny and code-based algorithms. At the same time, NIST put out a call for new digital signature proposals, with the aim of encouraging diversity in mathematical problems that digital signature standards are based on. The long-term objective is to standardise different types of algorithms designed for different use cases.

The results for this standardisation process, upon which European authorities for cyber security are relying, will be final in 2024. In the meantime, national authorities have published their views on the implementation of post-quantum cryptography. The French authority for cyber security has pointed out that security should be the main priority, and an algorithm that is not in the NIST selection for standardisation but proves to offer a higher level of security than a NIST standard, should be accepted too (ANSSI (2022)).

3.2 Solutions can be implemented now

Preparing for the quantum era is a major concern of cyber security departments. Different approaches have been defined and are possible. This report aims to provide an understanding of some of these approaches without being exhaustive. The strategy utilised in Project Leap has been recommended by standard bodies and national cyber security authorities. Specifically, NIST recognises that a hybrid approach is important to maintain interoperability during the migration phase (NIST (2023)). It consists of implementing a hybrid mode with a combination of traditional and post-quantum algorithms. This two-layer implementation scheme offers a solution for pre-shared keys when using public key cryptography. To implement such solutions, a cost-benefit analysis was developed by testing a range of algorithms.

4. How to prepare and create quantum-safe environments

4.1 Post-quantum cryptography vs quantum cryptography

Two approaches are currently being explored by researchers to ensure that data sent though the web are secure against a potential quantum computer attack. These are known as post-quantum cryptography and quantum cryptography. Despite the similarity in their names, these are two fundamentally different approaches to the problem, and it is important to be able to distinguish between them.

Post-quantum cryptography involves the use of new families of mathematical problems (see Annex B) to serve as the basis for algorithms that can reinforce the security of cryptographic protocols currently in use. These can be deployed on existing IT infrastructure. As it is impossible to predict what new techniques might be devised that are capable of cracking these new algorithms, a certain amount of cyber risk will always exist with this approach. Nevertheless, protecting IT systems with post-quantum cryptography is considered highly reliable as we may assume that breaking this type of quantum-resistant cryptography, if possible, would still require a prohibitively heavy investment in terms of time and money.

Rather than relying on the complexity of mathematics, quantum cryptography relies on fundamental principles of quantum mechanics, such as the uncertainty principle, to create quantum-resistant systems. For example, to secure key distribution, particles can be used to assure the randomness of a key selected to encrypt the data. Known as quantum key distribution (QKD), this approach allows for the issuance of a one-time key exchange. While a very promising technology, quantum cryptography requires specialised hardware and does not tackle the authentication issue. This would require it to be combined with post-quantum cryptography in practice. Implementing it would mean major upgrades to the global IT infrastructure, significantly increasing the cost of the transition to secured environments.

National cyber security authorities therefore favour the deployment of post-quantum cryptography as soon as possible, since this would probably allow for the migration to be carried out before a quantum computer powerful enough to break current cryptographic protocols becomes operational. In today's web-based economy, it is also easier for institutions such as central banks to experiment with new types of classical cryptography than it is for them to work with quantum cryptography as they can more easily adapt browsers and servers to add support for a new protocol. This type of replacement was previously attempted when a widely deployed hash function, Message Digest algorithm 5 (MD5), was found to be vulnerable to attack. While alternative solutions were deployed rapidly, it took over a decade for the vulnerable hash function to be completely removed from use. However, adapting systems on an industry scale, as in the financial sector, will always be cumbersome, as the move can only become operational when almost every participant has made the transition.

Thus, national authorities such as ANSSI, BSI and NIST advocate starting on the transition to post-quantum cryptographic schemes in a hybrid mode as soon as possible. Project Leap assumes the coexistence of old and new protocols during a transition period.

4.2 Central banks need to prepare now

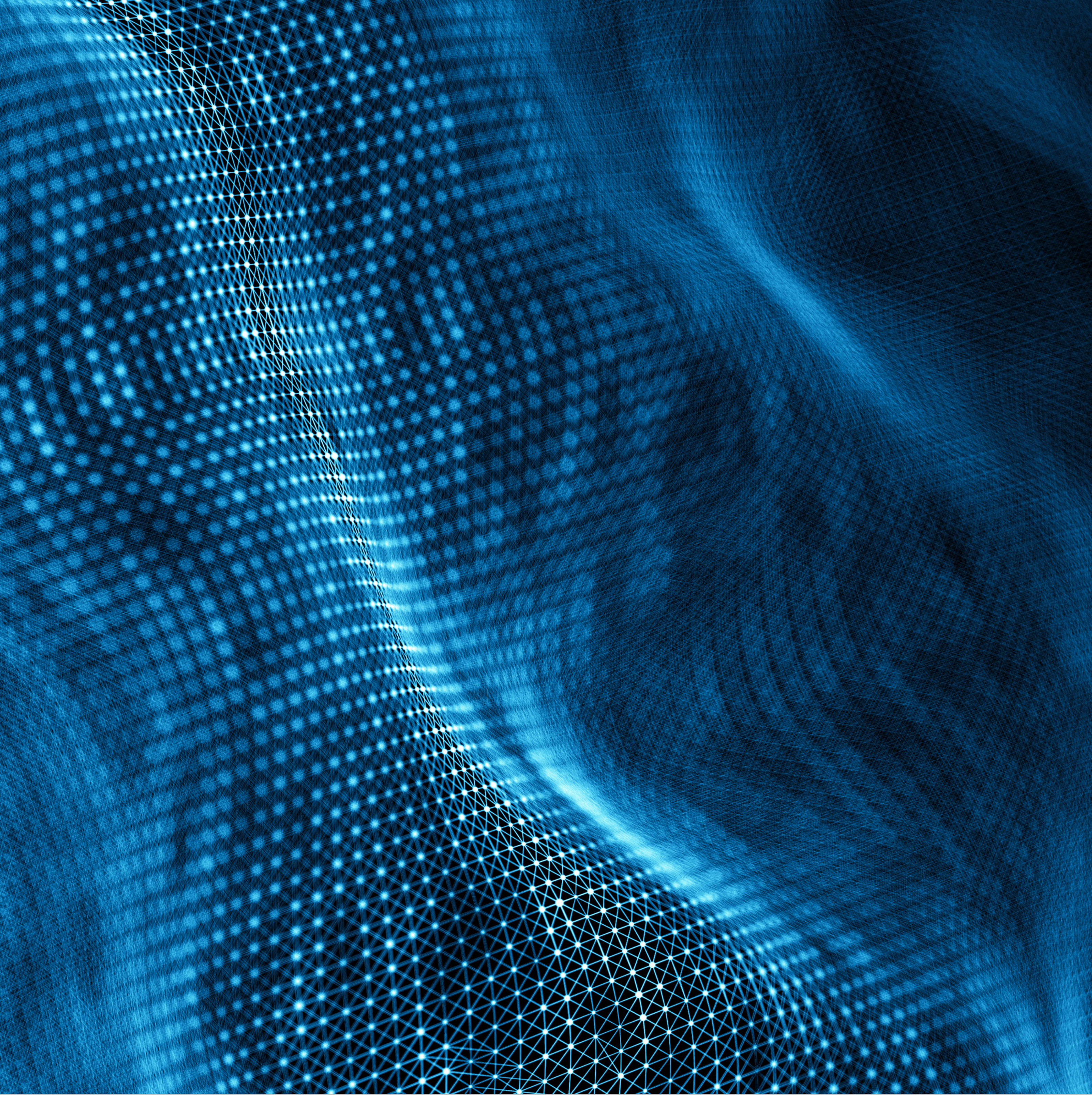
There is no doubt that quantum computing represents a major risk to financial stability. The financial industry has always been subject to conventional cyber attacks that could lead to solvency and liquidity shocks. Eisenbach et al (2021) show that a cyber attack on a mid-sized bank could have a large-scale impact. The interlinked structure of financial market infrastructures is also vulnerable to contagion effects that could affect the entire financial industry. A quantum computer attack could have a far more damaging and costly impact for the financial system than a conventional one. Given the long-term sensitivity of financial data and the complexity of today's IT systems, not to mention the potential cost of recovering from a major cyber intrusion, central banks need to address this threat well in advance.

The stakes are high, given that data protection mechanisms for internet communications, digital signatures, passwords, contracts and other documents would become instantly obsolete as soon as a sufficiently powerful quantum computer became operational. Among other things, this would destroy the integrity of today's digitally signed contracts, as the validity of the signer's identity could no longer be ensured.

The good news is that many organisations and governments are starting to respond. In November 2022, the White House issued a memorandum on planning for the implementation of post-quantum cryptography, outlining a concrete timeline to shift vulnerable systems into quantum-resistant encryption. Meanwhile, national authorities, such as ANSSI in France, have been issuing guidance to governments and businesses on migrating systems to quantum-safe cryptography.

Complacency in the face of this threat is dangerous, however, central banks need to act now, since replacing current encryption standards is likely to take decades, as NIST has warned (NIST (2021)). Experience has shown it could take decades to migrate after the new standards have been published. Transition planning should start with a quantum risk assessment to identify and inventory the systems that are vulnerable to quantum computer attacks. This should be followed by a strategic and long-term quantum roadmap, including a transition phase, as this will be key to protecting and strengthening critical central bank infrastructure.

In Project Leap, a quantum-safe environment was created to secure infrastructure against the interception of data in transit. This solution can protect highly sensitive communications that may possibly be intercepted now from being decrypted later. It is important to consider the impact that such a transition will have on central bank IT systems. It will be necessary not only to implement new algorithms but to change the entire set of cryptographic protocols. Until now, when setting up a VPN tunnel, the protocol was able to rely on the RSA scheme alone. But with quantum-safe protocols, it is the way that data are protected that will change. The migration to new cryptographic protocols needs to be defined well in advance to be sure that all the complexity implied by the new protocols will be resolved.

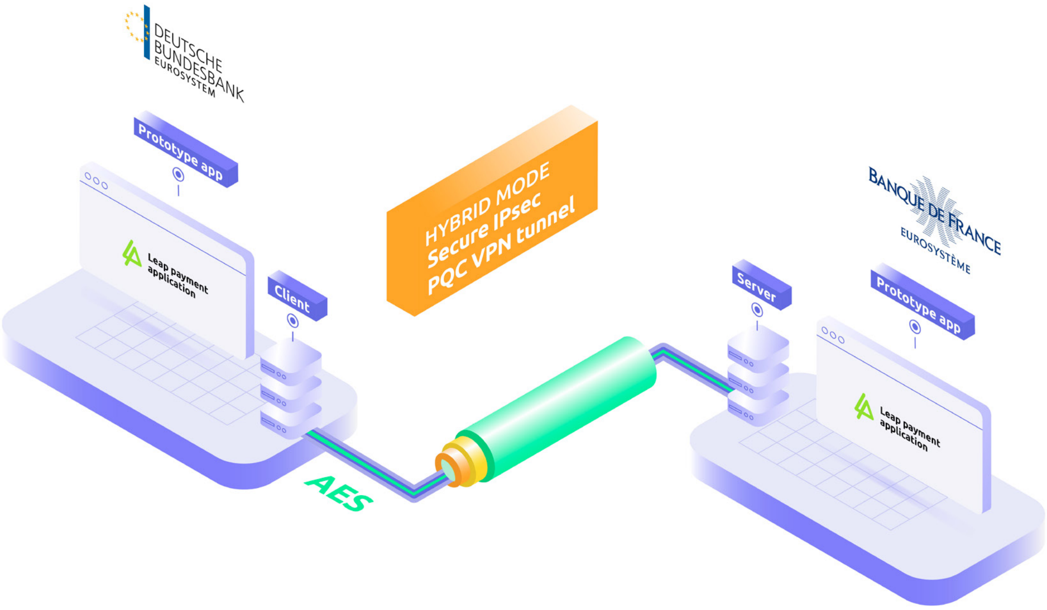


5. Project Leap

5.1 Objectives and scope

Project Leap sought to create a quantum-safe environment by implementing a traditional public key algorithm alongside a quantum-resistant algorithm in hybrid cyphering, ensuring the confidentiality of messages sent across two different IT systems, as well as integrity of data, authentication and anti-replay, ensuring that any data exchanged could not be resent. The connection was set up between a public cloud and an on-premises infrastructure. Payment messages were then transmitted between the Bank of France and Deutsche Bundesbank though a virtual private network (VPN) configured using a vendor-modified version of an open-source internet protocol security (IPsec) VPN solution, strongSwan.

Graph 4 Leap scheme – Secure VPN tunnel built with quantum hybrid cryptography

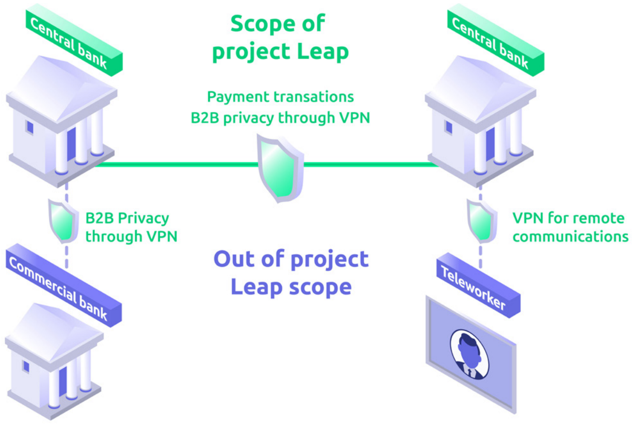


In central bank systems, VPNs are widely used to protect information and systems when connecting through a public network and transmitting data securely around the world. To create a secure tunnel between two locations, a VPN both encrypts data as they travel over the untrusted network and keeps the identity of the user secret, thus hiding the internet traffic. Project Leap focused on setting up a quantum-safe site-to-site VPN.

The test phase focused on testing cryptographic agility, performance, and security. The initial scope was to demonstrate that new cryptographic protocols could provide the required level of security for central bank systems in the quantum era. As the field of post-quantum cryptography is evolving rapidly, the project team also tested the ability for current cryptographic systems to adapt to new encryption schemes. A major aim was to demonstrate that post-quantum cryptography is compatible with the use of public networks.

In conjunction with a technology partner, the project focused on the integration of a library of post-quantum algorithms. Another objective was to inform the central banking community on how such projects can be set up. One important lesson involved staffing. For now, individuals with the requisite skills and expertise are still rare. There will be a massive need for the training of cyber security experts and cryptographers in quantum security-related skills to meet increasing demand. In the case of Project Leap, a team of cyber security experts was specially trained in the specific competencies needed for the tests.

Graph 5 Scope of project Leap



5.2 Solution designs

A quantum-safe environment was built to send an XML payment message under the ISO 20022 standard between two central banks via a hybrid quantum-resistant virtual private network (VPN) internet protocol security (IPsec) tunnel, using a library of post-quantum algorithms, and implementing a secure channel of communication with key exchange and authentication. As part of the testing, a front-end application named Leap payments was also developed with a high-level user interface.

In this project, virtual machines were set up in different locations and offering enough flexibility to allow technical integration when using a vendor software and different IT environments. On the German side, the cloud environment supported AVX2 (Advanced Vector Extensions) enabling the use of the most efficient implementation of post-quantum algorithms. On the French side, virtual machines were set up in a private cloud based on a legacy IT system.

In the project's first phase, different algorithms were tested (Kyber and FrodoKEM for key exchange; Crystals-Dilithium, Falcon and Sphincs+ for digital signatures), focusing on high levels of security (see Table 2). Algorithms were selected keeping in mind security requirements in a central bank environment and the evolution of the on-going standard process. Moreover, the solution used was configured by the vendor to generate x.509 post-quantum certificates.

Table 2 List of combinations of algorithms implemented

Test ID	KEM	PQC Security Strength categories	DS	PQC Security Strength categories
Legacy	RSA 2048	0*	RSA 2048	0*
Kyber3_dilithium5	Crystals-Kyber	3	Crystals-Dilithium	5
Kyber5_dilithium5	Crystals-Kyber	5	Crystals-Dilithium	5
Kyber5_falcon5	Crystals-Kyber	5	Falcon	5
Frodoa5_dilithium	FrodoKEM (AES)	5	Crystals-Dilithium	5
Frodos5_dilithium	FrodoKEM (Shake)	5	Crystals-Dilithium	5
Kyber5_sphincs1	Crystals-Kyber	5	Sphincs+	1
Kyber5_sphincs5	Crystals-Kyber	5	Sphincs+	5

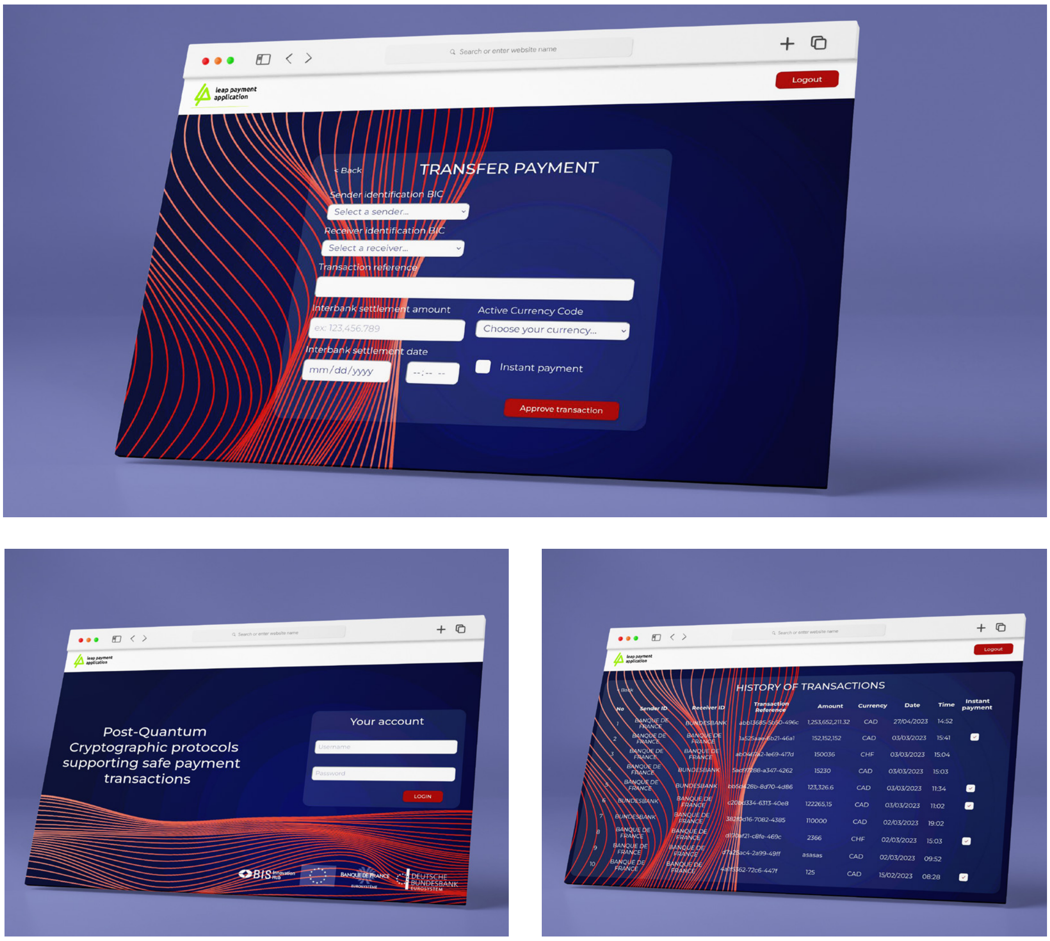
* Post-quantum security strengths categories do not apply to traditional cryptography as RSA security levels refer to a different scale. The scale of the security is detailed above in Table 4.

5.3 Implementation and testing

Once the multi-layer VPN tunnel was set up, the testing was executed following the different steps of the new protocol with hybridisation. The additional steps that it takes to build a quantum-resistant VPN in comparison with a classical one adds complexity to the protocol and poses a question of performance. In fact, when setting up a classical VPN, the first step is to exchange keys, and then certificates are transmitted to be verified. The client creates a symmetric key encrypted with the public key, and then the session is encrypted with symmetric key. Finally, the symmetric key is decrypted with the private key on the server side. This protocol widely used today is far more straightforward. The new hybrid VPN set-up includes additional steps as classical algorithms are used alongside post-quantum ones.

The first stage of the testing phase was to demonstrate that the solution was fully operational: this was demonstrated by running the full use case scenario demonstrating the opening of the tunnel and the capacity to send a payment message from sender to recipient (see graph 6).

Graph 6 Screenshots of Leap application



Search or enter website name
leap payment application
Logout
< Back
Approve transaction
LOGIN
BIS Innovation Hub
BANQUE DE FRANCE EUROSYSTÈME
DEUTSCHE BUNDESBANK EUROSYSTEM

TRANSFER PAYMENT

Sender identification BIC: Select a sender...

Receiver identification BIC: Select a receiver...

Transaction reference

Interbank settlement amount: ex: 123,456.789

Active Currency Code: Choose your currency...

Interbank settlement date: mm/dd/yyyy --:-- --

□ Instant payment

Post-Quantum Cryptographic protocols supporting safe payment transactions

Your account

Username

Password

HISTORY OF TRANSACTIONS

No	Sender ID	Receiver ID	Transaction Reference	Amount	Currency	Date	Time	Instant payment
1	BANQUE DE FRANCE	BUNDESBANK	abb13685-5b50-496c	1,253,652,211.32	CAD	27/04/2023	14:52	
2	BANQUE DE FRANCE	BANQUE DE FRANCE	1a525aae-6b21-46a1	152,152,152	CAD	03/03/2023	15:41	✓
3	BANQUE DE FRANCE	BANQUE DE FRANCE	ab0467a2-1e69-417d	150036	CHF	03/03/2023	15:04	
4	BANQUE DE FRANCE	BUNDESBANK	5ad97288-a347-4262	15230	CAD	03/03/2023	15:03	
5	BANQUE DE FRANCE	BUNDESBANK	bb5d428b-8d70-4d86	123,326.6	CAD	03/03/2023	11:34	✓
6	BUNDESBANK	BANQUE DE FRANCE	c20bd334-6313-40e8	122265,15	CAD	03/03/2023	11:02	✓
7	BUNDESBANK	BANQUE DE FRANCE	382f0d16-7082-4385	110000	CAD	02/03/2023	19:02	
8	BANQUE DE FRANCE	BANQUE DE FRANCE	d170af21-c8fe-469c	2366	CHF	02/03/2023	15:03	✓
9	BANQUE DE FRANCE	BANQUE DE FRANCE	d7a25ac4-2a99-49ff	asasas	CAD	02/03/2023	09:52	
10	BANQUE DE FRANCE	BANQUE DE FRANCE	4a1f5362-72c6-447f	125	CAD	15/02/2023	08:28	✓

A strategic test plan (Table 3) was drawn up to verify that setting up a secure tunnel with post-quantum cryptographic protocols in a hybrid mode would provide a fully functional solution in the context of two separate locations and different IT environments, as described above. The testing phase focused on three aspects of cyber security: cryptographic agility, performance and security. Some tests, like test 4, responded to two of these topics, giving insights on performance and security at the same time. The testing was automated via scripts, making the testing procedure repeatable.

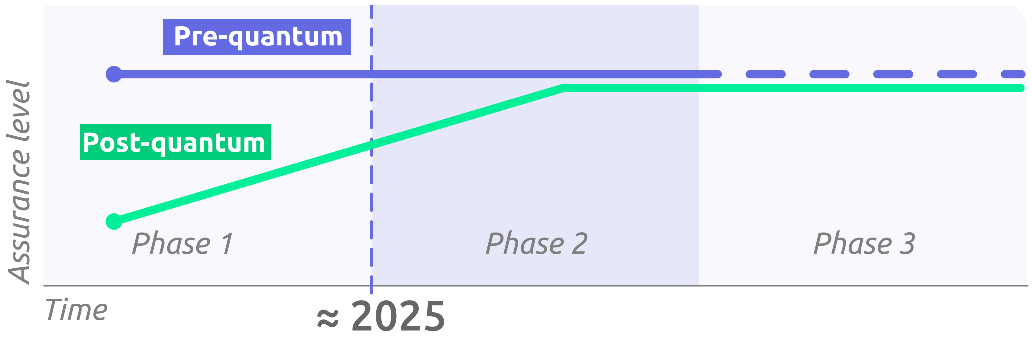
Table 3 List of tests performed

Test	Description
1	Ability to set up a VPN secure tunnel between two central banks with post-quantum protocols
2	Performance comparison of post-quantum cryptography vs traditional cryptography
3	Performance comparison of between different post-quantum algorithms
4	Testing a case of a disaster recovery by setting up a VPN from scratch
5	Testing the performance stability of a secure tunnel over a full working day
6	Investigating the trade-off between security and performance
7	Identifying the algorithm used in the certificate exchange
8	Testing a false certificate

Cryptographic agility

Cryptographic agility is dependent upon the way information security protocols and standards are designed. The most agile schemes are those that support multiple cryptographic primitives while also offering flexibility in the combination of the selected algorithms. Cryptographic agility is desirable for several reasons. It enables fast adaptation to new standards without requiring disruptive modifications to current IT systems, which is important given that quantum-resistant cryptographic standards are rapidly evolving. Agility is also desirable given that traditional cryptography will have to be completely replaced when compromised by quantum computing, as recommended by national cyber security authorities. Graph 7 shows a potential timeline, including a transition period where both traditional and post-quantum cryptography are used.

Graph 7 ANSSI timeline to be considered in the migration plan



In this context, different combinations of traditional and post-quantum cryptography were tested to ensure agility. Since algorithms were switched quite often to test the different configurations, Project Leap was able to clearly demonstrate that changing from one algorithm to another is easy, fast and reliable.

Performance

The project team designed its test plan to collect performance comparisons between different combinations of algorithms. Different tests allowed the team to compare latency by measuring performance times when implementing only classic cryptography, such as the RSA encryption algorithm, and then measuring the impact of adding an additional layer of post-quantum cryptography. The performance was tested between different algorithms and between different variants of a single algorithm, as well as at different levels of security. The test protocol configuration was defined in a way that made it possible to have a fair comparison of the results; specifically, some parameters were increased to limit the size of the packets and the size of the fragments in strongSwan. The tunnel's performance stability and the impact when building a VPN from scratch were also tested.

Security

Cryptographic algorithms provide different strengths of security, depending on the algorithm and the key size used. The security strength categories of a post-quantum algorithm are defined along a range from 1 to 5 (5 being the most secure). NIST (2016) defined these security categories, based on standards in symmetric cryptography, as any attack requiring the computational power equal or greater than those needed for breaking a determined symmetric key.

Table 4 Security categories defined by NIST

Security strength categories	Level of computing power to break the symmetric key	Symmetric key
1	Key search on a block cipher with a 128-bit key	AES 128
2	Collision search on a 256-bit hash function	SHA256/SHA3-256
3	Key search on a block cipher with a 192-bit key	AES192
4	Collision search on a 384-bit hash function	SHA384/SHA3-384
5	Key search on a block cipher with a 256-bit key	AES 256

When setting up the VPN tunnel, time measurement results were compared between the algorithms that were selected for standardisation by NIST, as well as FrodoKEM, and including the different levels of security between 1 and 5. Additional tests on the certificates were conducted to identify the certificate used and test a false certificate.

To thoroughly test cryptographic agility, performance, and security, eight families of tests were performed, and at least 100 tests were carried out per configuration (see more details about tests in Annex D). The testing phase demonstrated that implementing post-quantum cryptographic protocols is already feasible today. The section below dedicated to findings provides more insights into the different possible combinations of algorithms depending on the performance and security requirements of central bank processes.

6. Findings

6.1 Cryptographic agility

Today, a significant number of information systems suffer from a lack of cryptographic agility because these systems are not designed with their easy replacement in mind. Shifting to new protocols would require in-depth infrastructure modifications. Hence, post-quantum algorithms need to be tested in current hybrid systems that integrate adapted cryptographic solutions. In Project Leap, the open-source solution strongSwan was selected as it offers the required flexibility. Implementing post-quantum cryptography in a hybrid mode allows new algorithms to be implemented alongside traditional ones, with the flexibility required to drop any specific algorithm that is no longer recommended by national cyber security authorities.

National standardisation authorities such as NIST, and national cyber security authorities such as BSI or ANSSI recommend hybridisation (BSI (2023)), meaning that a post-quantum algorithm should be combined with a scheme based on traditional cryptography with cryptographic agility. In such a setup, the client and the server negotiate and agree at the outset on which additional key exchanges will be implemented. During Project Leap's first moves to build a VPN with quantum-safe cryptography it was demonstrated that both key agreement and digital signatures could be implemented in a hybrid mode.

A green-light approach was adopted to detect if the information came through a quantum-safe VPN. Once the quantum-safe connection is established, the colour of the Leap Payment Application logo is green, meaning that the VPN tunnel has been established and encrypted in a hybrid mode. This mirrors existing VPN applications in which the type of cryptography used is completely transparent. This is also analogous to the small lock symbol in browsers that indicates to users when there is a secure connection to a web server. The intention was the same in the Project Leap test, but only for the subnet. The screenshots showing the green light can be found in Annex C.

Regarding the agility of the cryptographic protocol used, it was noticed that the key exchange mechanism could easily accept any post-quantum algorithm. This was not the case with the digital signature, where the standard configuration is not pre-configured to detect the algorithm. Nevertheless, such a configuration is possible. The X.509 certificate is a standard format for public key management using a digital signature based on asymmetric cryptography[1]. It was selected for its cryptographic agility.

> **The final functional finding during the testing phase with regard to agility is that systems with a high degree of cryptographic agility will be better equipped to handle the coming transition. Central banks should examine their systems to identify where systems lacking such flexibility are used and plan their substitution. This will most likely be the case for certain types of hardware such as HSMs, firewalls and smart cards.**

[1] X.509 certificates involve CA certificates that generate other certificates or end user certificates. These certificates are standardised by IETF: RFC 5280.

6.2 Performance

Implementing post-quantum cryptography involves a potential performance cost due to the time needed for keys to be generated and signatures verified. These aspects were therefore tested in Project Leap as well.

The performance of cryptographic algorithms was tested with time measurement in the context of setting up a VPN. The tests were conducted with the transmission of a 1 Mb file. Additionally, a standard Pacs.008 payment message of about 1 Mb was transferred through the VPN between the Bank of France and Deutsche Bundesbank.

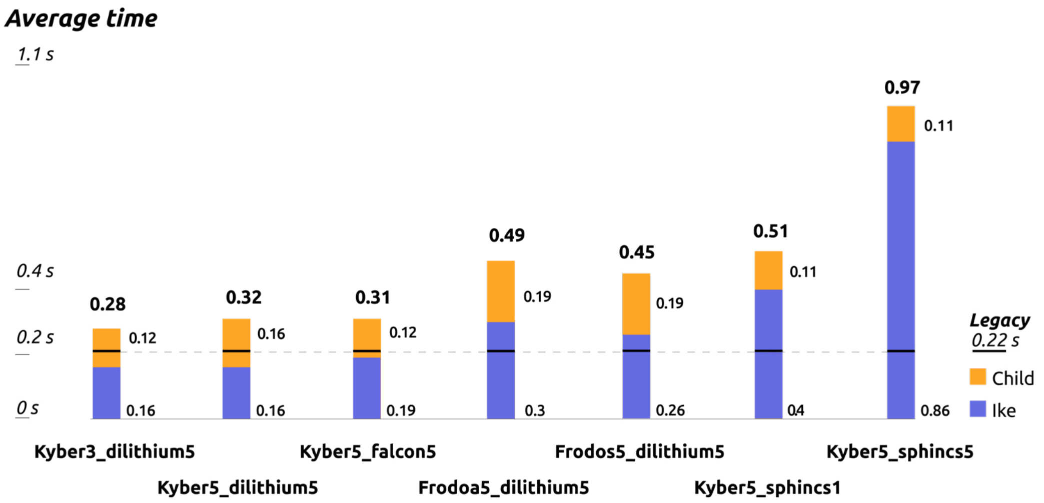
There was no impact at the performance level when sending data through the VPN tunnel, whatever the size of the data, as when the post-quantum VPN tunnel is set up, information is encrypted with traditional cryptography (AES-256). The timing metrics registered for the sent messages were identical to the length of time needed to set up the VPN with traditional cryptography. Performance was impacted initially when setting up the tunnel due to the additional layer of cryptography, but the performance of the data transfer was not affected. In real-world applications, the initial tunnel would be set up only once or twice during a business day.

During the test phase, algorithms were tested on different IT systems, including a legacy system as well as a cloud environment with a more recent configuration. Performance of the two versions of FrodoKEM (AES vs Shake) were slightly affected when carried out in a legacy system. As expected, testing showed that hardware acceleration such as AVX2 allowed for an increase in speed when setting up the tunnel, specifically for the FrodoKEM AES version, as compared with FrodoKEM Shake.

Having a diversified range of algorithms helps with the variety of use cases that exist in central bank IT systems. At this stage, all post-quantum algorithms tested are suitable for central bank processes and various security strength categories for post-quantum algorithms are considered strong. Nevertheless, differences in terms of performance need to be taken into consideration. Specifically, regarding the digital signature Sphincs+, it was noticed that performance registered was slower than with other algorithms. The use of this type of algorithm will be appreciated in applications where performance is not a high priority. On the other hand, being a hash-based algorithm, Sphincs+ does not have to be implemented in a hybrid mode, because the reliability of this algorithm’s family is well known. In Project Leap, Sphincs+ was configured with hybridisation. Even considering the time taken by the legacy part of the protocol, this algorithm registered longer times.

Testing performed during the first phase of Project Leap needs to be continued to explore more processes. The testing results (see tables in Annex D) demonstrate that there is a wide variation in performance characteristics between different algorithms when setting up the tunnel.

Graph 8 Time needed to set up a post-quantum VPN tunnel between the Deutsche Bundesbank (client) and Bank of France (server)



The blue bar labelled IKE represents the time needed to exchange the asymmetric keys and for the authentication. The orange bar labelled CHILD represents the time needed to exchange keys. These different steps of the protocol are represented in Graph 4 with the superposed layers of the tunnel.

The tunnel's reliability and consistency was tested by recording the time needed to build a new VPN tunnel from scratch. Once data were sent through it, the tunnel was rekeyed in order to be exchange the keys again. Then the process was restarted repeatedly to understand the consequences if the connection was interrupted. At the start of this specific test, the project team noticed that there was no performance impact on the rekey. It was observed that the protocol sends a rekey command, but it was not executed immediately. As soon as the system is informed of the rekey, it sends back a confirmation to say that the command was registered. This is comparable with ticketing an IT system problem. It doesn't mean that the problem is treated and resolved immediately. In this case, the rekey was executed later and could then be measured. With this specific test, it was observed that there was no impact on the performance stability of the tunnel. During the rekey of the tunnel, the impact on performance concerned only the key exchange, being completely asynchronous for the client. This test was repeated 100 times and showed stable results.

The stability of the VPN tunnel was also tested by an hourly verification through a complete working day when the tunnel was still set up. The frequency of the verification can be changed as necessary. The project team considered that a full working day was sufficient to prove that the tunnel was completely functional. The outcome was that the connection proved stable and worked as well as a legacy VPN tunnel.

6.3 Security

Although various authorities such as ANSSI have recommended implementing only the fifth security category, the Project Leap team chose to test several different security categories as defined by NIST. A comparison was done between hybrid implementations and non-hybrid. Using post-quantum cryptography in a hybrid mode mitigates two security-related risks:

- If legacy asymmetric cryptosystems are broken, a post-quantum layer protects data transfer, maintaining the security of the system. Implementing a hybrid mode prevents any regression.
- Hybridisation allows the systems to be agile: it makes it easier to replace traditional schemes as they become outdated.

One of the main conclusions is that there is always a trade-off between performance and security. If the security strength is increased by using an algorithm in its high-level security version, the time needed to set up the VPN tunnel is also increased. That is why the security must be configured according to application requirements, taking into account the importance of processing speed and the frequency at which public keys and ciphertexts need to be operated on. The results of the performance tests registered differences in the range of seconds, although with some exceptions like the post-quantum algorithm Crystals-Kyber, which showed only a minuscule difference in speed between level 3 and level 5. The results of the tests indicated that in use cases with high performance constraints, Crystals-Kyber seems to be better suited than Frodo. The performance difference between Crystals-Dilithium and Falcon was less significant. That said, Falcon demonstrated a better performance. With the latter results, if performance is sought, a combination of algorithms using Crystals-Kyber and Falcon might be preferred, but users should carry out internal tests on their systems first to confirm if they achieve same level of results in their particular setup.

Several types of signature algorithm were tested with the X.509 standard to see if it was possible to identify the certificate in use. In fact, with different possible post-quantum algorithms for digital signatures, it was important to identify it in order to validate the specific algorithm used. Once the certificate is received, the OID (object identifier) describes the algorithm used for the certificate. Hence, with current tools it is possible to identify which OID is used, demonstrating that in post-quantum cryptography it is indeed possible to obtain information about the algorithm being used.

A final test was executed with a fake certificate which had been altered. This underscored the reliability of the protocol: as it was not possible to verify the post-quantum signature, the certificate was rejected.

> **The testing phase underscored the reliability of the cryptographic protocols used, showing that it is key to provide for cryptographic agility. It was possible to verify the algorithm used in this new protocol when in the traditional protocol identifying it was not this important as there was only one used. This series of tests demonstrated the importance of considering the overall effects of cryptographic protocols when using different algorithms.[2]**

[2] More detailed technical information is available in Annex D.

7. Conclusion and next steps

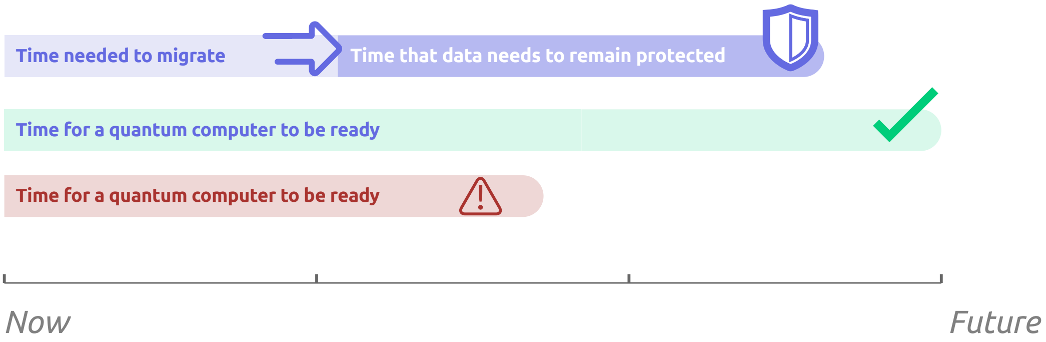
7. Conclusion and next steps

Project Leap has demonstrated that applying post-quantum protocols is already feasible. Hence, it is already possible to starting the migration process. Central banks need to allow for a transition phase in their cyber security roadmaps so that they are prepared once the final standards are published. By providing insights and technical findings, this report paves the way for future cooperation amongst central banks on post-quantum cryptographic protocols. Project Leap started with the implementation of a quantum-safe environment at the network level, building a secure channel of communication to send data as well as payment messages through a post-quantum VPN tunnel. In future phases, additional central bank use cases will be explored with the overall aim of contributing to the work of quantum-proofing the financial system.

7.1 Need for a migration plan

The key question is when quantum computing will become practicable and thus when organisations should be prepared for an attack. Generally, the answer to this question is given in terms of a theorem by Michele Mosca (Mosca (2021)). A migration plan needs to be implemented depending on the following variables (see Graph 9):

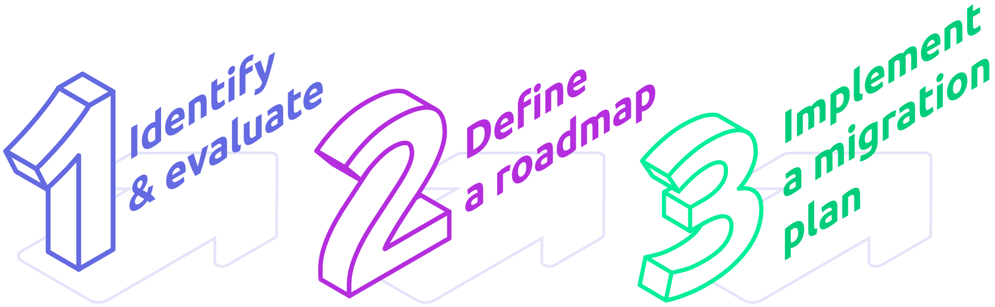
Graph 9 Mosca’s model for a safe transition to post-quantum cryptography


Time needed to migrate
Time that data needs to remain protected
Time for a quantum computer to be ready
Time for a quantum computer to be ready
Now
Future

Once the analysis of these variables is completed, central banks can set out a roadmap for implementing quantum-safe security. This process will start with inventorying their IT systems to identify and evaluate their vulnerabilities and establish which security methods may need to be replaced or upgraded. Processes to enable a continuous monitoring of cryptography should be established as soon as possible (CSA (2021)). Moreover, central banks need to determine whether the cryptographic protocols they are using are protecting confidential data that need to be stored over a long time period, and which might potentially be targeted by an adversary. If it is determined that the information will still have value at a time when traditional cryptography could be defeated, then new encryption systems will need to be deployed. To be effective, this must be done in advance. In particular, the use of potentially weak encryption algorithms such as RSA and ECC needs to be examined, as well as vulnerable protocols using these algorithms (eg VPN IPsec, SSH, TLS, etc).

Once the roadmap is defined, the implementation phase will start, as the infrastructure is upgraded by deploying quantum-resistant encryption.

Graph 10 Steps needed to establish a migration plan



To date, only a few initiatives to test and implement quantum-safe cryptography have been conducted in the central banking community. These new cryptographic protocols represent some challenges and constraints with regards to changing widely deployed cryptographic schemes. Organisations that manage their own cryptographic infrastructure and have a need for long-term cryptographic protection should factor the threat of quantum computer attacks into their long-term roadmaps. By building a secure VPN tunnel to protect communications between two central banks, the collaborative work of Project Leap paves the way for the construction of quantum-resistant infrastructures.

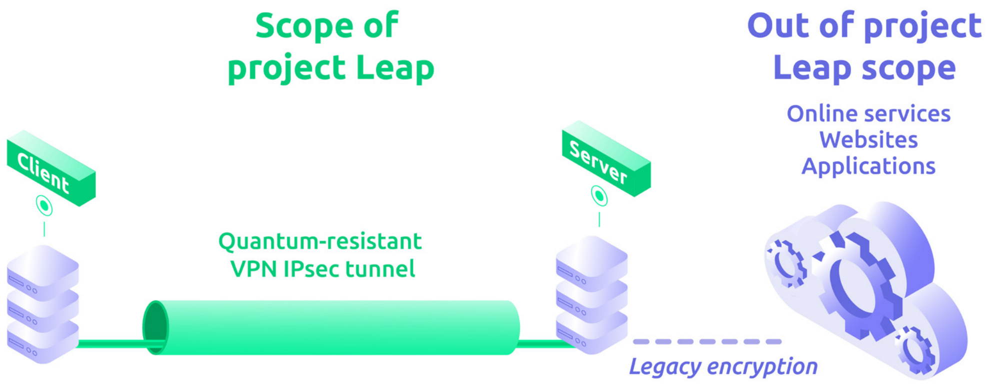
7.2 Deployment challenges

The transition to post-quantum cryptography applications will be a major undertaking. As seen before, the challenge that central banks and all other organisations will face is the need to compile an inventory of the cryptographies currently in use across their IT systems and to identify where the threatened cryptographic schemes are implemented. Once all the systems are reviewed, organisations will have to start replacing vulnerable cryptographic schemes by new quantum-safe cryptographic protocols. Another challenge is the sheer scale of the exercise and the time required. The transition will impact a large range of protocols, schemes and infrastructures. Migrating to new protocols takes time because the replacement of algorithms requires new cryptographic libraries. Not only will hardware be impacted, but operating systems and application code as well. This in turn means updating all the relevant documentation. Last but by no means least is the human resources challenge, something organisations should consider at the very beginning of the process. In today’s labour market, experts with the requisite skills are scarce. Cyber security experts will need to be trained, if demand is to be met. Starting the migration process soon will allow central banks to organise well in advance, giving them time to upgrade the necessary skills in their cyber security departments.

7.3 Next steps

Project Leap showed that implementing post-quantum solutions is already feasible. For a VPN, it was clearly demonstrated that there is no significant impact on performance. Nevertheless, for applications where performance is critical, such as instant payment applications or central bank digital currency (CBDC) systems, a trade-off between security and performance will be necessary. It was also shown that the level of security can be adapted to different central bank processes, and that implementing a strongSwan solution offers enough flexibility for hybridisation. Future work could include testing post-quantum cryptography in a more complex environment, addressing more central banking use cases to secure communications between central banks and other institutions. In quantum-proofing the financial system, quantum-resistant cryptography will need to be implemented not only at the network layer but also at the application and transport layer to build a complete chain of trust (Graph 11).

Graph 11 Next steps of Project Leap



Annexes

Glossary of terms

A

ANSSI: the National Agency for the Security of information Systems is a French authority for the security of information systems.

B

BSI: German Federal Office for Information Security.

C

Child: a phase of the IPsec VPN protocol where there is no need for authentication.

D

DS: a Digital Signature is a cryptographic process used to authenticate a message.

E

ECDSA: or Elliptic Curve Digital Signature Algorithm, is a cryptographically secure digital signature scheme based on the ECC.

ECDH: Elliptic-curve Diffie–Hellman.

ECC: Elliptic-curve cryptography.

I

IKE: a protocol that aims at establishing a secure tunnel (integrity and confidentiality) between two peers.

IKEv2: a standard of internet key exchange protocol on its second version, using key exchange algorithms and digital signatures.

IPsec: a secure architecture for IP traffic allowing the protection of data at the network layer and being transparent at the application layer (OSI model).

K

KEM: key exchange mechanisms (also known as key establishment) allows to exchange keys between two parties by using cryptographic algorithms.

N

NIST: National Institute of Standards and Technology.

O

OID: stands for object identifier, it serves to name almost every object type in X.509 certificates.

P

PKE: public key encryption is a hybrid encryption scheme providing three primitives, a public/private key generation algorithm, an encryption algorithm (using the public key) and a decryption algorithm (using the private key).

Q

Qubit: a quantum bit is the basic building block of a quantum computer.

R

Rekey: during the session of the VPN the key exchange is renewed without the authentication phase.

RSA: a public key cryptosystem for which the acronym stands for Rivest-Shamir-Adleman, the team who devised the algorithm.

S

StrongSwan: is an opensource IPsec-based VPN solution with strong authentication using X.509 certificates.

T

TLS: Transport Layer Security of an architecture.

V

VPN: a virtual private network is a mechanism for creating a secure connection between a server and a client through an insecure network.

References

ANSSI (2022): *ANSSI Views on the post-quantum cryptography transition,* March.

BSI (2023): *Cryptographic mechanisms: recommendations and key lengths,* January.

Castelvecchi, D (2023): "Google's quantum computer hits key milestone by reducing errors", *Nature*, 22 February.

CSA (2021):): *Practical preparations for the post-quantum world,* October.

Eisenbach, T, A Kovner and M Lee (2021): "Cyber risk and the US Financial System: a pre-mortem analysis", Federal Reserve Bank of New York, *Staff Reports,* n° 909, May.

Financial Stability Board (FSB) (2017): *Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices*, October.

Preskill, J (2018): "Quantum computing in the NISQ era and beyond", *Quantum Physics*, Cornell University, July.

Mosca, M and M Piani (2021): *Quantum threat timeline report, Global Risk Institute*, January.

NIST (2016): *Submission requirements and evaluation criteria for post-quantum cryptography standardization process,* December.

——— (2021): *Migration to post-quantum cryptography*, August.

——— (2023): *Migration to post-quantum cryptography: preparing for considering the implementation and adoption of quantum safe cryptography*, April.

Scopus (2021): *Quantum computing research trends report, Elsevier,* February.

White House, *Memorandum for the heads of executive departments and agencies*, November 2022.

World Economic Forum (WEF) (2022): *The Global Risks Report 2022,* 17th edition.

Yan, B, Z Tan, S Wei, H Jiang, W Wang, H Wang, L Luo, Q Duan, Y Liu, W Shi, Y Fei, X Meng, Y Han, Z Shan, J Chen, X Zhu, C Zhang, F Jin, H Li, C Song, Z Wang, Z Ma, H Wang and G-L Long (2022): "Factoring integers with sublinear resources on a superconducting quantum processor", *Quantum Physics*, Cornell University, December.

Annex A Technical boxes

Box 1 - Quantum computing

Despite the challenges they pose to our intuitive understanding of the world, the laws of quantum theory are fundamental and apply, to the best of our current knowledge, to every physical object. However, if materials are composed of numerous elementary components, more intuitive laws can be used to describe their collective behaviour. These laws are known as classical laws, and these are the laws exploited by our day-to-day computers. The term quantum computer refers to a device that uses the quantum behaviour of matter rather than the classical laws to make calculations. The quantum objects manipulated in a quantum computer are called "qubits", a contraction of the term "quantum bit". Quantum computers today are still an emerging technology and a research endeavour rather than an established engineering discipline.

The term quantum computing is not to be confused with quantum computer technology. The quantum computing approach is a completely new approach to algorithmics involving algorithms that can be executed only on quantum computers. Quantum computing requires a device that can leverage and manipulate the quantum behaviour of some physical objects. It was surprising at first that the laws of physics cannot be ignored when designing algorithms. However, once this conceptual barrier was overcome, the development of quantum computing began. Just as algorithms preceded modern digital computers, quantum algorithms have also preceded quantum computers. Quantum computing is based on the assumption that the qubits of future quantum computers could be observed in two values only, in an analogous way that bits can be either 0 or 1.

Quantum computing is often reduced to the concept of superposition, which is misleading. Quantum theory is a mathematical construct that places observation at its core. Some properties of a quantum object are only observed in a finite number of values, called pure states. A fundamental property of quantum theory is superposition, which allows a quantum object to evolve into a state that is a mixture of pure states. Whenever a qubit is placed in a state of superposition, a measure or observation of its value will give 0 or 1. The superposition cannot be seen directly but it can be inferred through probabilistic behaviour. Therefore, superposition for a qubit means that the observed state will be 0 with a certain probability P, and 1 with a probability 1-P. The uncertainty is not an experimental limitation of the quantum computer or the observer, but instead a fundamental property of the quantum nature of the object. Using a state of superposition for a qubit, it is possible to perform a similar computation on both pure states in one execution only. This approach is similar to executing the same code on a classical multiprocessor computer in parallel with different inputs. But the benefit of superposition would be marginal if it were only able to halve the execution time of an algorithm.

Superposition is only the first behaviour that makes quantum computing so efficient. The concept of entanglement is a second one that has no equivalent in our classical conception of the world. This law makes it possible for two quantum objects to be entangled in a way such that the resulting compound cannot be described as a combination of each individual object. As the saying goes: the whole is greater than the sum of the parts. This enlarged set of potential configurations exponentially increases with the number of entangled qubits and allows a natural parallelisation unattainable with classical computers.

This is the combination of superposition and entanglement which allows quantum algorithms to perform some computational tasks so efficiently.

Having discussed the advantages of the quantum behaviour of matter when it comes to computation, it is also important to mention its constraints. The most significant challenge when working with quantum computing, and when building quantum computers, is related to observation or measurement. In general, at a microscopic scale, it is assumed that the state of an object we have just observed will be preserved. The situation in the quantum world is completely different. As mentioned before, only the pure states are observed even when a quantum object is in a state of superposition. Moreover, after the observation, the object is no longer in the superposition state but has collapsed to the pure state observed. In the quantum world, "observing is perturbing" to quote the astrophysicist and ecologist Hubert Reeves. For quantum computing, the consequences are severe. It means that no intermediate results from a computation can be observed without perturbing the end results. It is even possible to demonstrate that it is impossible to make a copy of a quantum superposition state.

This rule, known as the measurement postulate, also poses major challenges for the construction of a workable quantum computer. Specifically, the interaction with external particles is a potential measurement that could affect the algorithm, by terminating its execution. In order to perform as expected, quantum computers therefore require a strictly isolated environment and quantum algorithms will certainly require demanding error correction steps. Due to the nature of measurement in quantum theory, it is unlikely that quantum computers will replace our classical computers in all classes of applications, especially those heavily relying on copying and storing information. Quantum computing will likely remain a tool for the resolution of certain computationally intensive tasks.

Quantum theory preserves information. This additional property requires quantum algorithms to always be reversible. The term "reversibility" in this context means that there is no single step in the algorithm that erases information, and that the output of a computation should be sufficient to rebuild the input. When it became increasingly difficult to cool down microprocessors, reversible classical computers were contemplated. Since erasing information increases the temperature, a reversible computer will not heat up as quickly as a classical computer. The knowledge gained from the study of reversible computers was useful during the development of the first quantum algorithms.

Box 2 - RSA and Shor's algorithm

The RSA methodology is a public key cryptographic schema based on the idea that a message can be encrypted with one key (the encryption key) but only decrypted with a different key (the decryption key). Number theory, among other things, provides practical schemas for implementing such encryption mechanisms.[1]

The typical RSA methodology relies on two large prime numbers. Using those two primes, a first clock is defined with a periodicity that corresponds to the product of the two primes. Another clock is then defined with the product of those two primes, from which 1 has been removed. Encryption is the process of taking the digitalised version of a message to the power of the public encryption key. The calculation is performed on the first clock, so the periodicity of the first clock must also be made public. The public encryption key needs to conform to certain mathematical properties, but it can be considered almost discretionary.

The decryption key is determined by the encryption key and the second clock. In the modular arithmetic of the second clock, the decryption key is the inverse of the encryption key. The message is decoded by taking the encoded message to the power of the decryption key on the first clock.

Knowledge of the encoded message, the public encryption key and the periodicity of the first clock are all that is needed to decrypt the message. The procedure is quite simple: decompose the periodicity of the first clock into the two original primes; remove 1 from those two primes and multiply them to obtain the periodicity of the second clock. Using the second clock and the public encryption key it is possible to determine the decryption key.

While the procedure may be straightforward, the first step – the factorisation of a number into the product of the two primes it is comprised of – is a very time-consuming process. As of today, there are no known algorithms that can perform such decomposition efficiently for large numbers. The absence of such an algorithm is what makes RSA so reliable and robust.

However, there is a quantum algorithm that would allow for efficient factorisation of large numbers. Known as Shor's algorithm, the algorithm and its numerous variants are based on the idea that one can determine the periodicity of the second clock by evaluating all powers of the encoded message on the first clock.

[1] The approach adopted in RSA is based on modular arithmetic, which is simply the arithmetic of the clock. Using traditional arithmetic, 11+2 equals 13. However, when considering a traditional clock, and assuming it is now 11 am, adding two hours gives 1 pm, not 13. While traditional clocks reset the counting at 12, it is possible to design countless modular arithmetic using any other natural number. This is called the modulus or periodicity.

Shor’s algorithm has four main steps, which are:

- First, through the use of the principle of superposition on the entangled qubits, it is possible to bring the system into a state that represents a large sequence of natural numbers in their binary representation.

- Second, an arbitrary number needs to be raised to the power of all the natural numbers represented in the first step. Because they are in a state of superposition, it is necessary to make only one pass through this second step. At this stage, we know that the qubits represent a complicated but periodic function.

- Third, a measure is taken such that the system is forced to settle at one value of this periodic function. The function is simpler now that its state has collapsed to only a small subset of powers, but it is still not useable

- Finally, the fourth step is to transform this function with a classical procedure, called the (discrete) Fourier transformation, which will identify the periodicity. Knowledge of this periodicity allows the large periodicity of the first clock to be factored and the periodicity of the second clock to be deduced. It must be said that this procedure does not work all the time. In cases where it does not, a different arbitrary number must be chosen at the second step of this algorithm.

Given knowledge of the periodicity of the second clock and of the public encryption key, the message is no longer protected. Adaptations of the Shor algorithm could also make other public key cryptography schemes vulnerable.

Annex B Classification families of post-quantum algorithms

- Lattice-based algorithms:
  Lattice-based algorithms are built on the complexity of finding vectors that are the shortest vector problem or the closest vector problem. Lattice-based signature schemes use lattices that have been specifically built to contain private short vectors and Learning With Errors (LWE) or Module Learning With Errors (MLWE) schemes which use specific classes of random lattices.

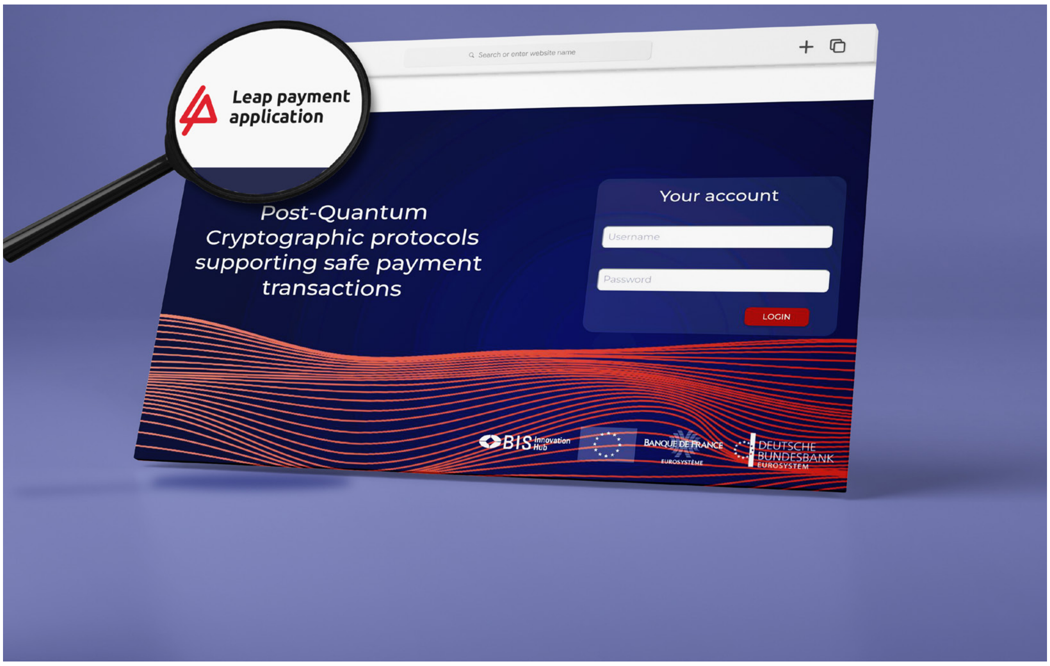
- Code-based algorithms:
  Code-based algorithms are based on the science of designing encoding schemes that let two parties communicate over a noisy channel. The sender encodes a message so that the receiver can decode it even if bounded noise has been added by the channel. It is known that, for certain encoding schemes, the best decoding algorithm takes exponential time on a classical computer. Moreover, the decoding problem appears to be difficult even for a quantum computer.

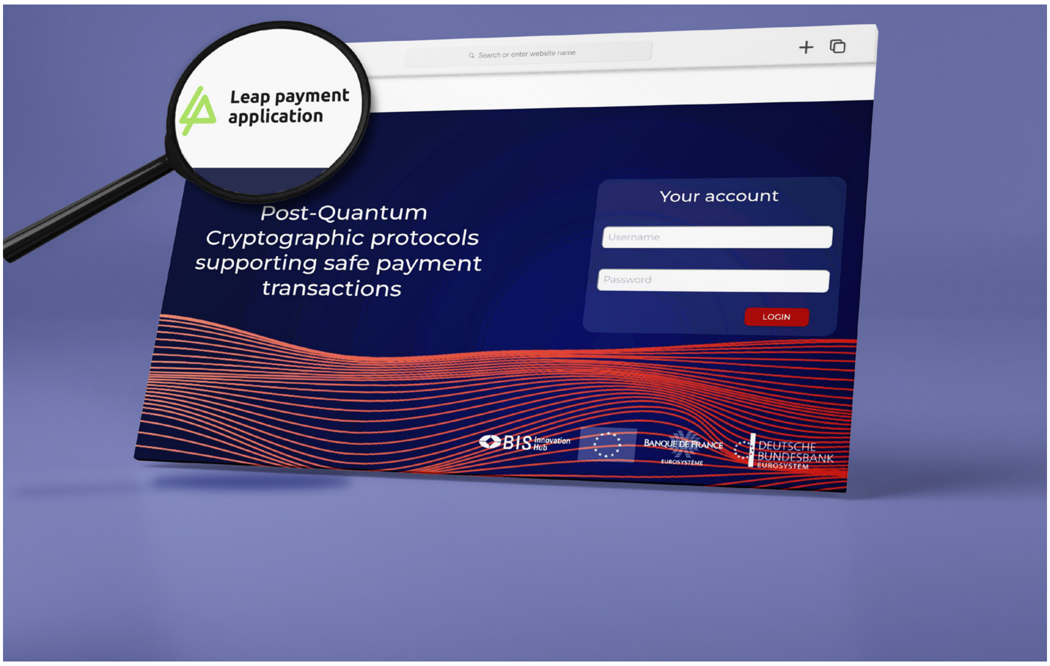
- Hash-based algorithms:
  Hash-based functions allow an important message with gigabytes of data to be computed as input and output as a short hash value. Hash functions are widely used for password management or on the blockchain. One of the most used hash functions, SHA256, outputs a 256-bit hash value, independently of the size of the input. It is not expected that hash functions would be threatened by quantum computers, but depending on the size of the key, and advances made in quantum computing, hash-based functions could be attacked by applying Grover's algorithm.

- Multivariate-based algorithms:
  The security of multivariate-based algorithms depends on the difficulty of solving systems of multivariate polynomials. Multivariate cryptography is used in the construction of digital signatures, rather than in PKE schemes or KEMs.

- Isogeny-based algorithms:
  The security of these schemes relies on the difficulty when recovering an isogeny between a pair of elliptic curves. As opposed to multivariate schemes, isogeny-based schemes are more suited for PKE schemes and KEMs.

Annex C Screenshots of Leap payment application home page


Search or enter website name
Leap payment application
Post-Quantum Cryptographic protocols supporting safe payment transactions
Your account
Username
Password
LOGIN
BIS Innovation Hub
BANQUE DE FRANCE EUROSYSTÈME
DEUTSCHE BUNDESBANK EUROSYSTEM


Search or enter website name
Leap payment application
Post-Quantum Cryptographic protocols supporting safe payment transactions
Your account
Username
Password
LOGIN
BIS Innovation Hub
BANQUE DE FRANCE EUROSYSTÈME
DEUTSCHE BUNDESBANK EUROSYSTEM

Annex D Technical description of tests

Test protocol

Tools used for the testing

- A strongSwan version including a post-quantum library designed by the solution provider (C-QST-STR).
- OpenSSL and Open Quantum Safe (OQS) OpenSSL were used to analyse post-quantum (PQ) certificates.
- Vendor Quantum Safe Library (C-QSL).
- strongSwan PKI tool was implemented to generate post-quantum keys and certificates.

Operation performed during one test of each performance tests:

- Ping vpn ip before: KO
- strongSwan start Charon
- strongSwan init IKE
- strongSwan init nit child all
- Ping vpn after: OK
- Download 1MB file (wget): OK
- Send file 1 Mb file (scp): OK
- strongSwan Rekey chilld all
- strongSwan Rekey ike
- strongSwan Terminate IKE
- strongSwan Terminate child
- strongSwan kill Charon
- Ping after closing: KO

For each test, the algorithm, the security strength category and the size of key was verified in the logs file, as well as the strongSwan control commands (charon daemon).

Each test was executed 100 times and performed in a row for each algorithm.

When the AES version of FrodoKEM was tested on in-premises infrastructure without hardware acceleration, the performance was affected.

Tests executed

- Establishing a VPN between the Bundesbank and the Bank of France including the generation of the PQ key and exchange of the certificate.
- Connexion to a web portal through a post-quantum VPN.
- Testing different algorithms.
- Testing reliability and consistency of the VPN.
- Testing stability of the VPN during a 24-hour connection (with automatic rekey).
- Testing in a could on the Deutsche Bundesbank side and on premises of the Bank of France (a VPN was set up between the two central banks as well as inside their own IT environments).
- Testing a false certificate.

Limitations identified

The time records were registered via the Linux command “date” right before and after execution of the command, meaning that it does not reflect the computing time of the algorithm. It shows the time needed by the software to fully process the operation.

To register the computing time would have required a modification of the strongSwan library.

Certain operations are asynchronous in strongSwan, such as the rekey. Consequently, it was not possible to record rekey timing. Nevertheless, it pointed out the fact that this specific operation has no impact for the client.

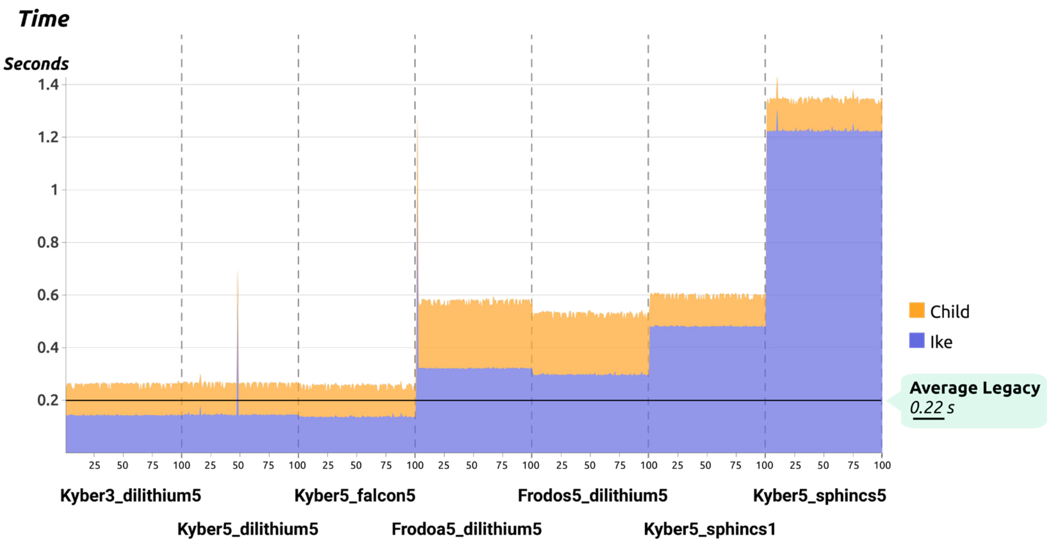
Due to the size of the signature Sphincs+, the size of the packet and fragment Sphincs+ was increased.

Data and information collected

The results showed consistency in every test performed, even when comparing the results of the Bank of France and Deutsche Bundesbank's specific IT environments.

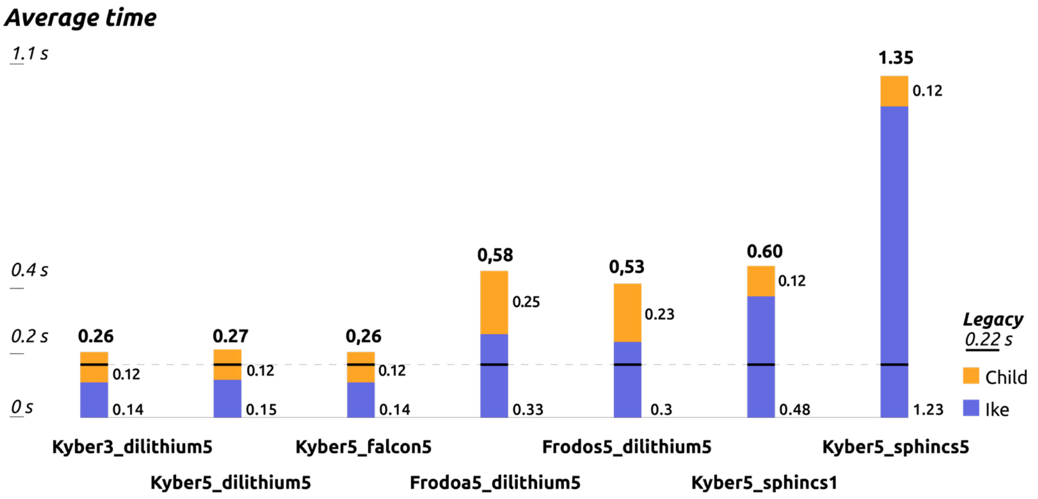
Graph A: The time needed to set up a VPN tunnel on Bank of France system cumulating IKE and CHILD layers. Except from the combination of Crystals-kyber and Sphincs+, this took less than one second.

Graph A



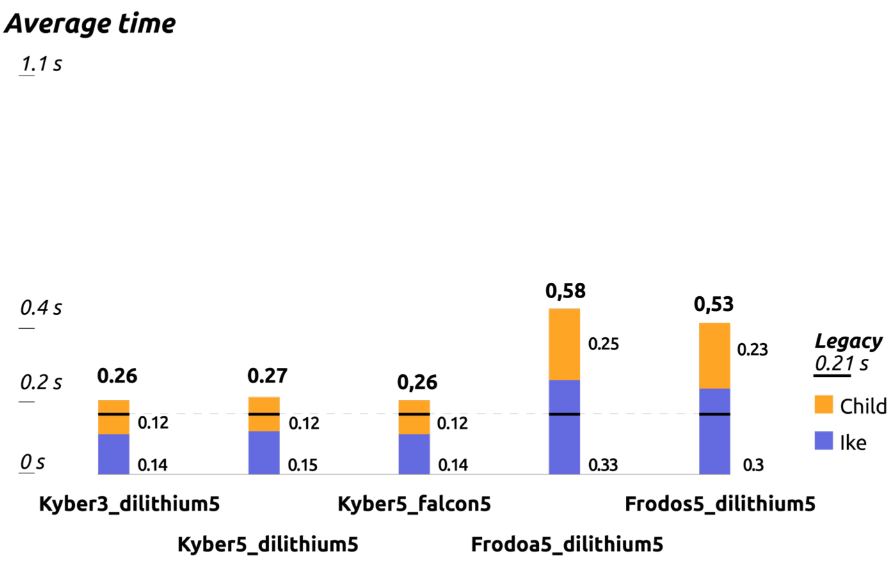
Graph A shows consistent results for each algorithm that was tested (each combination of algorithms was tested 100 times).

Graph B



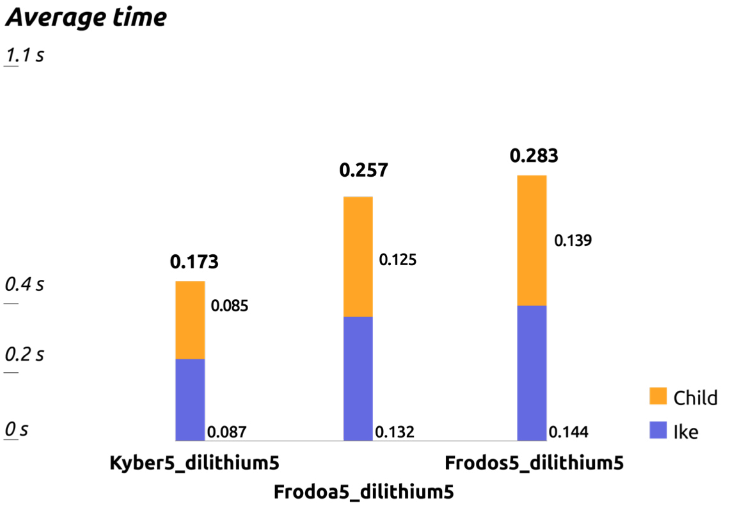
Graph B shows the impact on performance when using Sphincs+5 in comparison with another algorithm.

Graph C Local Bank of France time measurements without the combination of Crystal-Kyber and Sphincs+



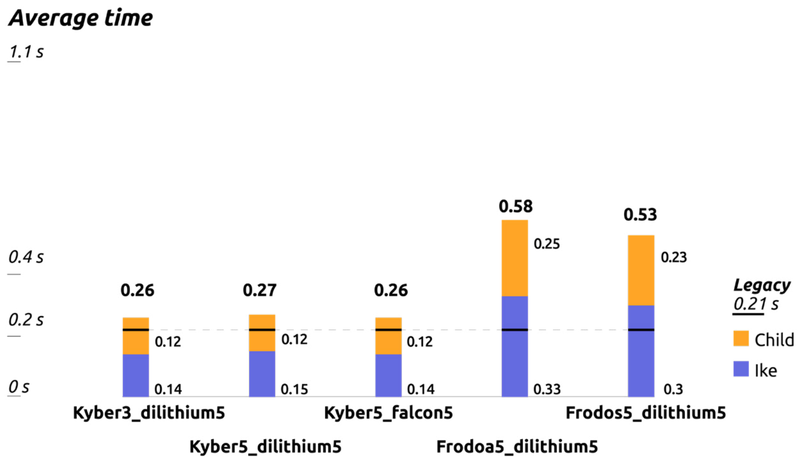
Graph C shows the difference of performance between FrodoKEM and Crystals-Kyber.

Graph D.1 Frankfurt local time measurements comparing FrodoKEM AES and FrodoKEM Shake



Graph D.1 shows measurement with AES acceleration realised on Bundesbank servers.

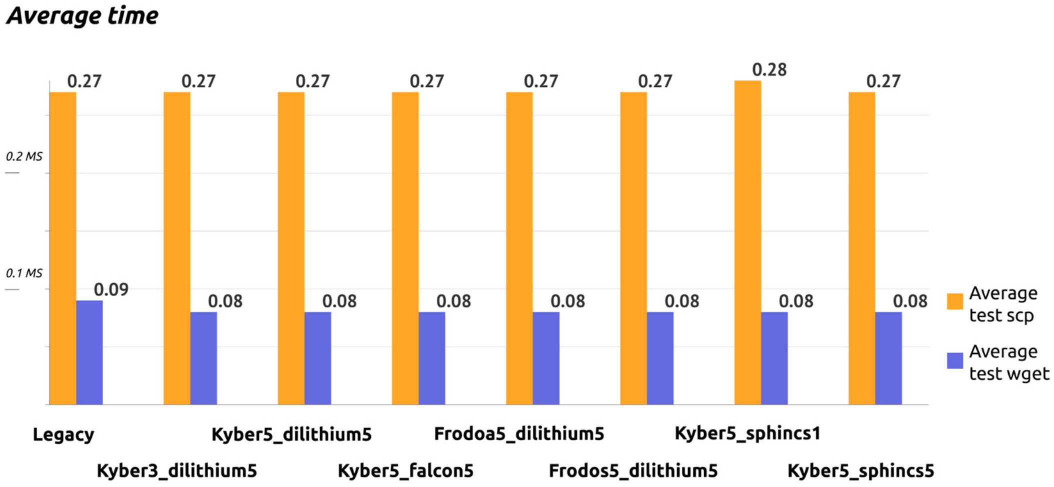
Graph D.2



In Graph D.2, the tests realised on the Bank of France server without hardware acceleration showed that shake was faster than AES, so that we can expect that, once hardware acceleration is available for the Shake protocol, better performance results should be observed.

FrodoKEM AES took more than 0.3 seconds for the IKE layer on the Bank of France side, when it took less than 0.14 seconds on the Deutsche Bundesbank side. A difference is also observed for the Child layer.

Graph E Average time to send and receive data



As expected, applying post-quantum cryptography had no impact on the performances of sent data as it was encrypted with a symmetric protocol (AES-256).

Table of OID Certificates

Algorithm	OID (display by OpenSSL)	OID (display by OQS OpenSSL)
FALCON_LEVEL5	1.3.9999.3.4	1.3.9999.3.4
DILITHIUM_LEVEL5	1.3.6.1.4.1.2.267.7.8.7	dilithium5
SPHINCS+_LEVEL1	1.3.9999.6.7.4	sphincsshake256128fsimple
SPHINCS+L_LEVEL5	1.3.9999.6.9.3	sphincsshake256256fsimple

A modified certificate was tested in order to break the signature of the certificate. To create such a fake certificate, a bit was modified.The intention was to confirm that an invalid certificate could not be identified as a real one.

The certificate was not verified by OpenSSL due to the fact that this tool is not configured to identify the algorithm. But, with OQS OpenSSL version the certificate could be identified.

Technical findings

A successful testing phase showed that implementing post-quantum algorithms without any serious drawback is possible.

Cryptographic agility:

- The key exchange is well managed by the key proposal.
- Currently there is no mechanism for a signature proposal, so the client must know the algorithm used or try a different one.

Performance:

Sphincs+ is among the digital signatures tested that performed less well in time and size. This algorithm is also, for now, the only one that is based on a non-lattice problem, offering a valuable backup solution. Including Sphincs+ in the libraries would seem prudent.

As expected, Crystals-Kyber showed better performance than FrodoKEM which is also acceptable for many use cases. It could be preferred for applications with high security level requirements.

Even though the Falcon signature size is smaller than that of Crystals-Dilithium, there was no significant impact on the performance record. Falcon will probably be preferred for applications that require a significant number of signatures to be stored.

The rekey is asynchronous and transparent for the transitioning data.

Annex E Project participants and acknowledgements

BIS Innovation Hub

Raphael Auer, Eurosystem Centre Head
Angela Dupont, Adviser and Project Lead
Andras Valko, Adviser

BIS Subject matter experts

David Whyte, Head of Cyber Resilience Coordination Centre
Christophe Laforge, Head of Finance Operations

Bank of France

Marc Fasquelle, Senior Manager
Olivier Lantran, Senior Manager
Benjamin Delpy, Senior Manager, Cyber security expert
Nicolas Margaine, Manager, Cyber security expert
David Viatgé, Consultant, Cyber security expert
Erwann Legeleux, Developer
Blandine Leal, UI Designer

Deutsche Bundesbank

Julia Biesen, Senior Manager
Thomas Kraus, Senior Manager
Florian Stock, Senior Manager
Henrieke Grimm, Innovation Manager, Agile Coach
Max Grytz, Innovation Manager
Vasileios Rentoumis, Innovation Manager

European Central Bank

Sjoerd Van der Vaart, International Innovation Manager

Vendor

Jean-Charles Faugere, Founder & Chief Technical Officer
Christian d'Orival, Chief Revenue Officer
Pascal Maudet, Professional Services Director
Julien Prat, Senior Cryptography Engineer

Acknowledgements

The authors are grateful to Christophe Laforge for his contributions to this report, and to Miguel Diaz and Baltazar Rodriguez, David Whyte, and the project's private sector partner CryptoNext Security.

Bank for International Settlement (BIS)

ISSN 978-92-9259-661-3 (Online)