IDEMIA

Anticipating the Post Quantum era security challenges

An update from the cryptography experts at IDEMIA Secure Transactions

PAYMENT CONNECTIVITY

POSTED ON 11.18.24

In just a few years, quantum computers have emerged as what could be one of the most transformative technologies in the years to come. Quantum technologies hold great potential for many industries. In the field of cryptography, one of the foundations of security at the core of the products and systems we use every day, the emergence of these technologies is reshuffling the deck. Between risks and opportunities, experts in the field have been preparing for years. Here's an update on the current situation and their recommendations for tackling this unprecedented challenge.

Quantum computers: an increasing development and industrialization momentum

By making it possible to solve problems that were previously unsolvable with today's most powerful conventional computers, quantum computers present exciting prospects—from the discovery of new materials or the synthesis of new pharmaceutical components to the optimization of logistics, telecoms networks and electrical infrastructures. They should also help drastically reduce the resources needed to carry out the increasingly complex calculations performed by artificial intelligence tools, which are already pushing to the limits the largest Cloud infrastructures (whose resources were once thought to be unlimited).

As more and more concrete applications for quantum computers are identified, the quantum community is growing and investments are increasing rapidly. According to a 2023 PwC study on emerging technologies, 29% of CEOs were already planning to invest in quantum technologies as a matter of priority in 2024[1]. Many sectors hope that quantum computers will soon become an industrial reality thanks to current scientific and technical breakthroughs and growing investments, even though no one can truly predict how long it will take or what their actual capabilities will be.

The major advantage of quantum computers lies in their ability to perform certain calculations at an incomparable speed compared to that of current computers. This will be very useful in certain fields, but it also comes with a risk: in the medium or long term, could they enable malicious actors to break the algorithms and security protocols we have trusted for decades? There is no way to know for sure the scope of the impact that quantum computers could have on current security systems, but no matter how hypothetical the risk may be, one thing is clear: our societies absolutely cannot afford to take it.

> *This acceleration in investment and technical advances in the quantum field, against a backdrop of growing international sovereignty and cybersecurity concerns, is creating a real state of urgency for all security players around the world.*
>
> Paul Dischamp, Cryptography Lab Director at IDEMIA Secure Transactions

Post-quantum security: a present-day matter

Thinking that the risk is still a long way off would be misguided. The threat posed by advances in quantum technologies to the cryptography that currently protects our data and transactions is already here. Security professionals cannot afford to ignore this threat. Finding a solution is a responsibility for all players in the security industry.

Many around the world have rolled up their sleeves and, fortunately, did not wait for the quantum threat to hit the headlines before taking the measure of what is at stake. IDEMIA Secure Transactions is one of them.

The most pressing issue is that of “harvest now, decrypt later,” an attack strategy in which fraudsters obtain encrypted data and hold it until quantum capabilities become available that will enable them to decrypt it. Another risk, which may not immediately spring to mind, is the risk associated with the billions of connected objects that make up the Internet of Things, with a lifespan of up to 15 or 20 years (connected cars, smart meters, payment terminals, etc.). If quantum computers capable of breaking current cryptosystems emerge while these devices are still in use, their security will be significantly compromised.

> *Providers of critical services must begin the migration to post-quantum cryptography now, as transitioning an entire ecosystem to new technologies is a time-consuming process. It’s not just the algorithms that need to be updated, protocols and various devices must also be adapted. The sooner this migration will be completed, the sooner the long-term security of infrastructures will be ensured.*
>
> Christophe Giraud, Cryptography & Product Security Group Manager at IDEMIA Secure Transactions

Stay agile: be ready never to be fully quantum-ready

Shortly after reaching the final selection round for standardization of quantum-resistant cryptographic models launched by the NIST (National Institute of Standards and Technology) in 2016, one of the first candidate models was broken—not by a quantum computer but by a conventional computer. This came as no surprise to cryptography experts, as it is the normal course of events: rigorous scrutiny and continuous analysis are essential to confirming (or refuting) the robustness of a cryptographic solution.

This example shows that the ‘quantum threat’ must not cause us to lower our guard in the face of the means already available to attackers. It also shows the degree of uncertainty about the robustness of any new cryptographic algorithm against current and future threats.

Confidence in the algorithms and cryptographic solutions we use today was not established overnight. Similarly, while we already have a good level of trust in the post-quantum cryptography algorithms and protocols that have just been standardized, it will take ten, or even twenty, years to ensure their robustness. This gradual process is normal in ensuring long-term security.

Emmanuelle Dottax, Cryptography Architect at IDEMIA Secure Transactions

The necessary maturation time for post-quantum cryptography technologies is a factor that has been taken into account from the very beginning by the experts who opened this new field of research. This is the reason why the main institutions responsible for defining security standards are advocating for a hybrid approach which involves combining traditional cryptography with post-quantum cryptography. In other words, rather than replacing the old lock (classical cryptography) with a new one (post-quantum cryptography), it is better to add the new lock to the old one.

As new post-quantum cryptographic standards continue to evolve, crypto-agility – i.e. the ability to remotely change all or part of a cryptographic solution already deployed in the field – is also part of the prerequisites. It is the key to being able to update defenses in real time, as soon as a vulnerability is discovered—without shutting down systems or recalling all chip-equipped devices. This proactive approach ensures continuous security and adaptability, keeping systems resilient and up-to-date.

Preparing for post-quantum security means building in flexibility now, so we're ready to update and respond seamlessly to future challenges. As cryptographic standards evolve, crypto-agility will be essential to maintain trust in security systems.

Luk Bettale, Cryptography Group Manager at IDEMIA Secure Transactions

While in a highly flexible and connected environment (like a server), this type of upgrade will not present any real technical difficulties, it will be a far more delicate operation in environments with limited resources and low connectivity, such as the secure element of a smart card. This is why the experts in chip design and secure OS development at IDEMIA Secure Transactions are hard at work defining products with the most flexible architecture possible and integrating the latest security features to protect these particularly sensitive operations.

Getting ready: standardization of new cryptographic algorithms

Just recently (in August 2024), after 8 years of research and evaluation, a first set of standards based on 3 algorithms (one for key establishment, the other two for digital signatures) has just been finalized by the NIST. While the organization keeps investigating additional algorithms to strengthen and complement this first line of defense, it is already urging the entire IT community to implement them without delay.[2]

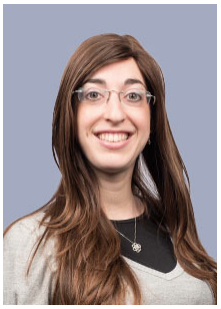
Besides actively contributing to NIST research and standardization efforts, IDEMIA Secure Transactions is already making progress on deploying the first standards available—which is not as straightforward as one may think. In practice, for these new post-quantum defenses to become a reality, one of the challenges is the effectiveness of the implementations. The critical aspect is to carry these out correctly, taking into account the use cases and the specificities of each environment.

The new algorithms standardized by NIST were not originally designed for embedded systems, which impose specific constraints. One of the priorities is to make the implementations of post-quantum algorithms resistant to side-channel and fault injection attacks, to which embedded systems are particularly vulnerable. The implementation techniques

used to secure classical algorithms are not always suitable for post-quantum algorithms. Therefore, new methods must be found to protect them. This can sometimes be a real challenge, but it is absolutely essential. Well-versed in this area, the cryptography team at IDEMIA Secure Transactions makes significant contributions to the development of these new methods, including several publications at top-tier conferences in the field of embedded cryptography – with a specific focus on the implementation of the algorithms selected by the NIST (ML-DSA, ML-KEM).[3]

Alongside these security specificities, there are also considerations related to the inherently limited computing power and memory space of the secured elements. Post-quantum protocols must be designed to ensure the same level of functionality as classical cryptography, even under this high level of constraints. For example, at the 5th post-quantum standardization conference organized by the NIST this year, one of the doctoral students from IDEMIA Secure Transactions presented a technique to streamline the key generation process for a digital signature in an embedded environment.[4]

> *Beyond the search for cryptographic algorithms that can theoretically withstand the computing power of quantum computers, it is also essential to ensure that their implementations combine security with performance optimization for real-life applications.*
>
> Rina Zeitoun, Cryptography Engineer at IDEMIA Secure Transactions



Looking at the big picture: from theory to real-life post-quantum cryptography applications

On all fronts, IDEMIA Secure Transactions experts are busy implementing the first post-quantum cryptographic defenses. The mission is formidable: safeguard credentials, ensure data integrity, guarantee the reliability and confidentiality of transactions, but also protect the privacy of users and prevent security breaches that could damage the reputation of companies providing essential services around the world.

> *The challenge of post-quantum cryptography knows no borders, and all countries must prepare for the advent of the quantum computer. In addition to our contributions to the standardization efforts led by the NIST in the United States, we are committed to advancing post-quantum cryptography worldwide.*
>
> Marc Bertin, Chief Technology Officer at IDEMIA Secure Transactions

Ensuring the performance of post-quantum cryptographic models in real-life conditions requires the coordinated efforts of many players in the security chain. That's why IDEMIA Secure Transactions works not only with security agencies, but also with its customers, other security players as well as start-ups to test real-life applications.

IDEMIA Secure Transactions' proofs of concept focus on two key priorities: safeguarding data against the 'harvest now, decrypt later' threat, and supporting customers and partners in preparing for post-quantum migration at the ecosystem level.

Ensuring data protection with advanced encryption is at the core of the company's expertise. Early in 2019, IDEMIA was one of the first companies to announce the development of a quantum-resistant smart card. Two years later – in anticipation of new ETSI and GSMA standards – IDEMIA Secure Transactions was already proactively testing the integration of the first post-quantum algorithms into its Quantum-Safe 5G SIMs with Telefónica España to protect subscriber privacy. More recently, IDEMIA Secure Transactions also trialed with success the protection of data in transit

to an IoT device using the first quantum-safe Transport Layer Security (TLS) connection based on a crypto-agile eSIM.

IDEMIA Secure Transactions is also working on in-depth data protection against quantum threats beyond its traditional activities, leading the Hyperform consortium funded by France 2030 and the European Union, alongside other French cybersecurity leaders. This consortium explores end-to-end data protection for complex IT ecosystems (data storage in the cloud, document archiving and online collaboration), relying on a smart card crypto-agility capabilities to maintain post quantum security over time.

> *Cryptography is everywhere, and it is at the heart of our activities. We have an enormous amount of work ahead of us to identify and explore all the different use cases of post-quantum cryptography. This requires the involvement of the entire security ecosystem, as well as real-life trials, in close collaboration with our customers.*
>
> Olivier Nora, Chief Open Innovation at IDEMIA Secure Transactions

As a frontrunner in the global ecosystem post quantum migration, IDEMIA Secure Transactions is actively involved in the migration of edge devices connected to digital services: payment cards, vehicles, IoT devices such as smart meters... This migration will need to happen before quantum computers have sufficient capabilities to break classic cryptography. It needs to be anticipated as early as possible. Partnering with research institutes, solution providers and clients on end-to-end implementations, IDEMIA Secure Transactions is assessing system-wide impacts and helps define the research activities necessary to prepare products and digital solutions to be crypto agile.

In 2022 already, IDEMIA Secure Transactions cryptography team dedicated a paper to the integration of post-quantum cryptography into card payment protocols.[5] This article helped identify the challenges that need to be addressed to maintain the same level of functionality for offline payments as the current EMV protocols. With this end-to-end approach, IDEMIA Secure Transactions has also recently positioned itself as a pioneer in offline CBDC payments (Central Bank Digital Currency) with the demonstration of a post-quantum resistant transaction using a new public key cryptographic solution.

In the IoT ecosystem, IDEMIA Secure Transactions explores the migration path for critical devices that have a long shelf life, are resource constrained and are not designed to be crypto agile. As part of its collaboration with Telefónica and Quside, IDEMIA demonstrated how, in a foreseeable future, eSIM crypto-agility capabilities could be leveraged to securely upgrade a device operating system to offer quantum-safe services —achieving seamless transition from classic cryptography to post quantum cryptography with no impact on the IoT hardware. This partnership is a first step towards the deployment of new cryptographic services for IoT developers through the GSMA Open Gateway platform.

These proofs of concept activities complement IDEMIA's contributions to global research and standardization efforts. Besides participating to NIST initiatives, IDEMIA is also involved with the GSMA, ETSI, GlobalPlatform and FIDO Alliance as well as with several standardization bodies and organizations in the telecoms and IoT fields in India. IDEMIA Secure Transactions has also set up post-quantum research partnerships in Europe with INRIA and CEA, as well as a strategic research partnership with the Indian Institute of Technology Hyderabad (IIT Hyderabad).

Post-quantum security challenges are a reality, and it is urgent to act, while remaining aware that agility will be decisive in maintaining the security of transactions and data over time. Security players are well aware of their responsibilities, and are all hands on deck. Active collaboration and investments of companies that depend on cryptography to secure their products and services is now crucial to developing and deploying tomorrow's cryptographic solutions. This new era of cryptography is also a tremendous opportunity to rethink and enhance the security of the products and services we use every day, taking into account new considerations, such as enhanced privacy protection, for example.

[1] https://www.pwc.com/us/en/tech-effect/emerging-tech/emtech-survey.html
[2] https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
[3] Publications related to securing post-quantum cryptography implementations in embedded environments:
– ML-DSA (ex-Dilithium): https://dblp.org/rec/journals/tches/CoronGTZ23a.html , https://dblp.org/rec/journals/tches/CoronGLTZ24.html
– ML-KEM (ex-Kyber): https://dblp.org/rec/journals/tches/CoronGMZ22.html , https://dblp.org/rec/journals/tches/CoronGMZ23.html
– NTRU: https://dblp.org/rec/journals/tches/CoronGTZ23 ; https://dblp.org/rec/conf/cardis/BettaleEMRS22.html
[4] https://csrc.nist.gov/csrc/media/Presentations/2024/antrag-simplifying-and-improving-falcon/images-media/nguyen-antrag-pqc2024.pdf
[5] https://csrc.nist.gov/csrc/media/Events/2022/fourth-pqc-standardization-conference/documents/papers/post-quantum-protocols-for-banking-applications-pqc2022.pdf