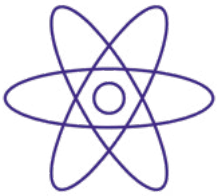
WHITE PAPER



Quantum SAFE SIM

Securing telecommunication in the quantum era through SIM cryptography evolutions

IDEMIA

A new era is dawning: the advent of quantum computers will revolutionize our lives. Quantum computers are expected to perform calculations much more efficiently than any existing supercomputer, enabling new technological applications. While this is good news for most fields, it is not the case for cybersecurity—the power of quantum computers can also be used for security attacks.

In this white paper, we explore why and how this technological advancement affects security, and why we need to prepare our industry for the quantum age today. We will also analyze the importance of researching, implementing, and deploying quantum safe technology—more specifically, a quantum safe SIM and its evolution in eUICC or iUICC.

Contents

1 What is quantum computing?

Second quantum revolution

In the first half of the 20th century, scientists realized that classical physics did not fully represent all physical behaviours because it could not describe certain occurrences, such as the radiation emanating from the stars. Decades of research enabled scientists to understand the phenomena involved and to formulate the core principles of quantum physics: wave/particle duality, the fact that particles can exist in a superposition of different states until an observation occurs, the tunnelling effect, and the fact that particles can be connected at a distance, i.e. entanglement.

Understanding quantum physics had a major impact. It has allowed scientists to build devices that followed these rules and is the basis for crucial inventions such as global positioning systems (GPS), magnetic resonance imaging (MRI), and transistors—more generally electronic semi-conductors. This advancement in technology is often referred to as the "first quantum revolution", as it drives the computer chip industry and the "Information Age".

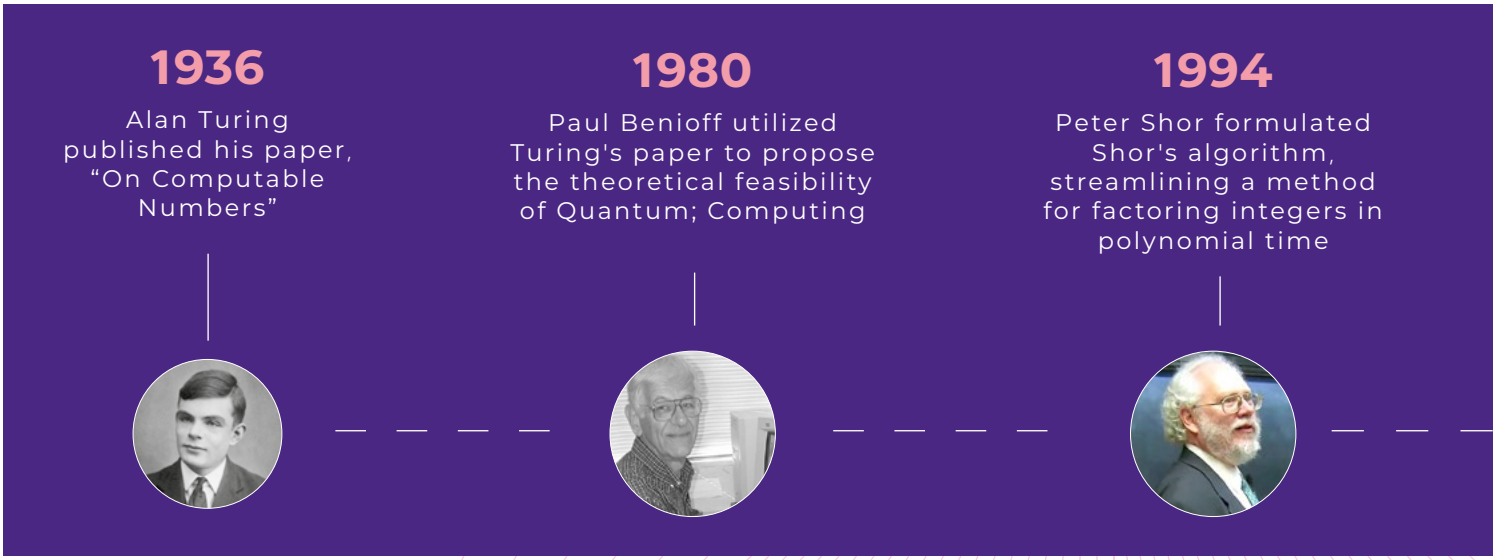
Scientists have succeeded in explaining quantum behaviour, but they have not yet been able to manipulate that behaviour. This challenge constitutes the next step: to use quantum mechanics to manipulate it, create, and harness the power of unnatural quantum states. This will open the door for new technologies that will achieve unprecedented efficiency and levels of miniaturization—paving the way for the "second quantum revolution".

History and principles

In 1936, Alan Turing published a paper titled "On Computable Numbers" that laid the foundations for classic computer science as we know and use today. In 1980, Paul Benioff provided the counterpart to Turing's paper for quantum computing: he introduced a theoretical model for a quantum computer that demonstrated the possibility of quantum computing in general. Among other things, this ground breaking work established the field of quantum computing.

Quantum computers take advantage of several quantum phenomena—super-position and entanglement properties as well as interference—and implement a different computational model that

Figure 1: Quantum Computer Milestones



can be exponentially more powerful than classical computers. However, quantum computers should not be seen as supercomputers as they do not allow significant speed-ups for all problems. In fact, it is necessary to have an efficient quantum algorithm for a given problem, i.e. a program that takes advantage of quantum properties to solve the problem. For example, in 1984, Peter Shor published a quantum algorithm for factoring numbers that performs exponentially faster than any known classical program. For its part, the quantum search program proposed by Grover in 1996 provides a quadratic speed-up when searching a random database. Many other quantum algorithms have been found for various problems. This field is still very active, and new algorithmic methods and development tools are expected to emerge.

Since the early 1990's, great strides have been made to show how a quantum computer could speed up the resolution of some intractable numerical problems. In 1998, Jonathan A. Jones and Michele Mosca first demonstrated the execution of a quantum algorithm; that is, an algorithm meant to run on a quantum computational model. In 2011, the Canadian company D-Wave Systems was the first to market a quantum computer, and in 2019, Google made the controversial statement claiming to have achieved quantum supremacy as shown in Figure 1.

Meanwhile, there are worldwide efforts to build quantum computers, and there have been numerous announcements in the last two years that illustrate the acceleration of quantum computer development. While the path to a general-purpose quantum computer is still long and uncertain, powerful machines for specific purposes may emerge in coming years.

2 The quantum threat

Quantum computers are expected to have a significant impact in the field of chemistry to simulate interactions between molecules for new materials, drugs, etc. Predicating the behaviour or optimizing complex systems, such as those found in climatology or logistics, will become manageable.

1998

Jonathan A. Jones and Michele Moscal marked the first demonstration of a quantum algorithm

2011

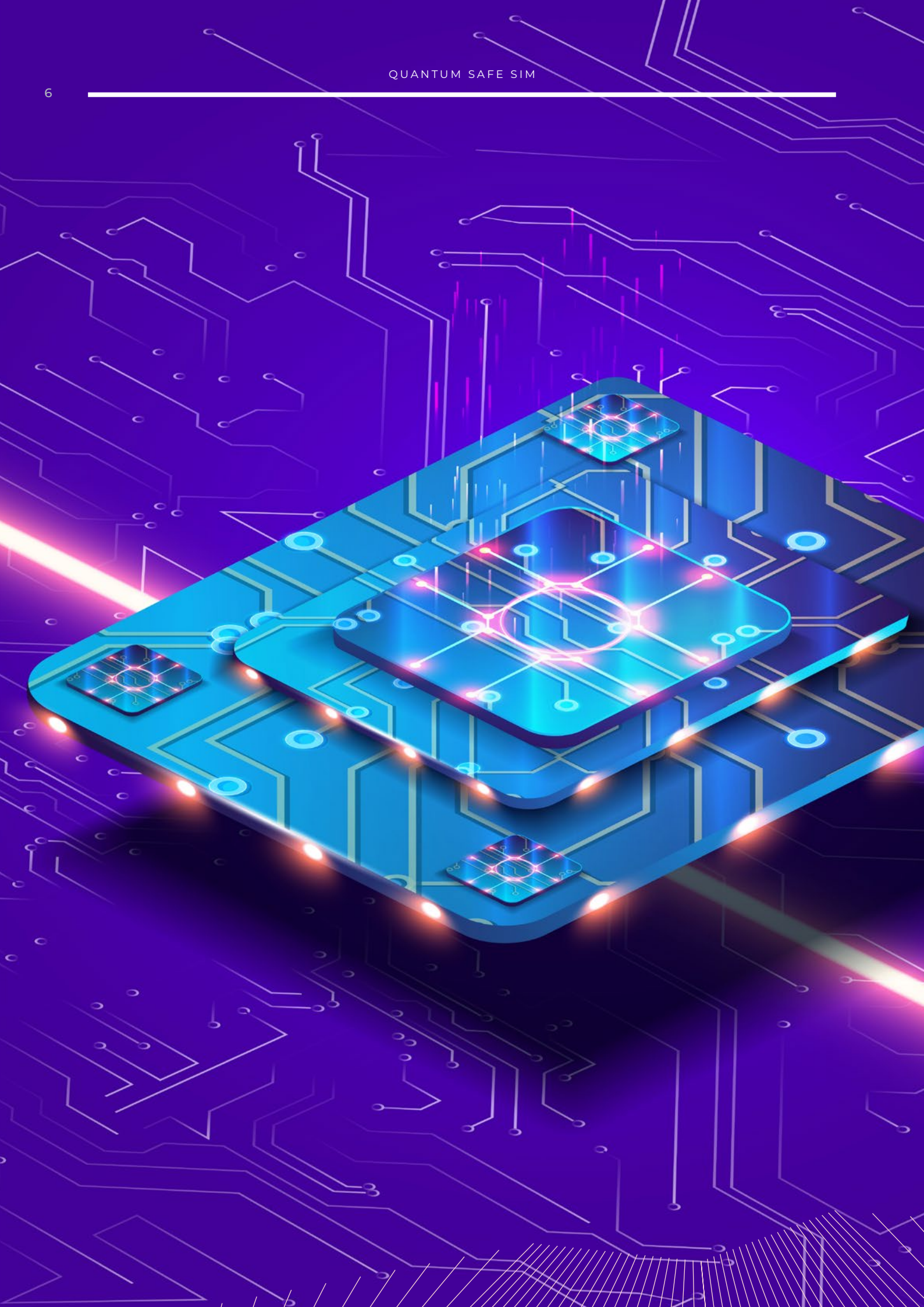
D-Wave Systems of Burnaby in British Columbia became the first company to sell a quantum computer commercially

D-Wave The Quantum Computing Company™

2019

"Google claims to have reached quantum supremacy with an array of 54 qubits out of which 53 were functional, which were used to perform a series of operations in 200 seconds that would take a supercomputer about 10,000 years to complete" although still controversial statement

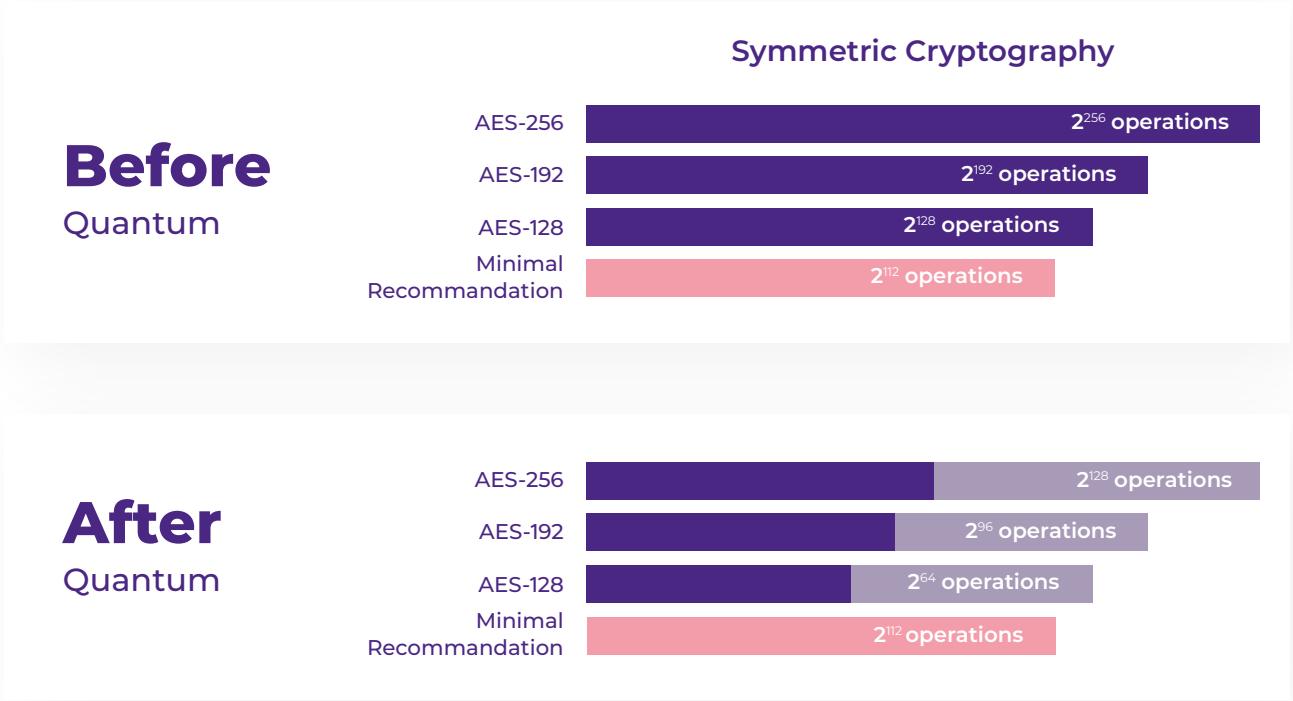
Google



Albeit in a very different way, another area impacted by quantum computers will be cryptography. Cryptography is the foundation of all security applications we use today: mobile and Internet communications, payment and mobile payment, and electronic documents such as passports, etc. Symmetric (or secret key) cryptography is used to protect communications once there is a shared secret with an interlocutor. Asymmetric (or public key) cryptography is used as a preliminary step when there is not a common secret in order to create one. It has revolutionized the field since its invention in the 1970s, and has enabled the widespread use of cryptography in our lives.

The security of cryptography is based on the difficulty of solving problems. Unfortunately, some of these problems become easier for a quantum computer. With the Grover algorithm, mentioned above, a brute force attack on any secret key can be performed much more efficiently than with a classical computer. Consequently, a quantum computer would weaken symmetric cryptography. However, since the gain is only quadratic, the use of larger keys is sufficient to thwart this threat. In fact, some state-of-the-art algorithms used with their highest security parameters are already quantum-safe. Figure 2 shows the impact on the current standard in symmetric cryptography: while the 128-bit key version of AES can potentially be broken, switching to the 256-bit key version is sufficient to regain the recommended level of security as defined by NIST.

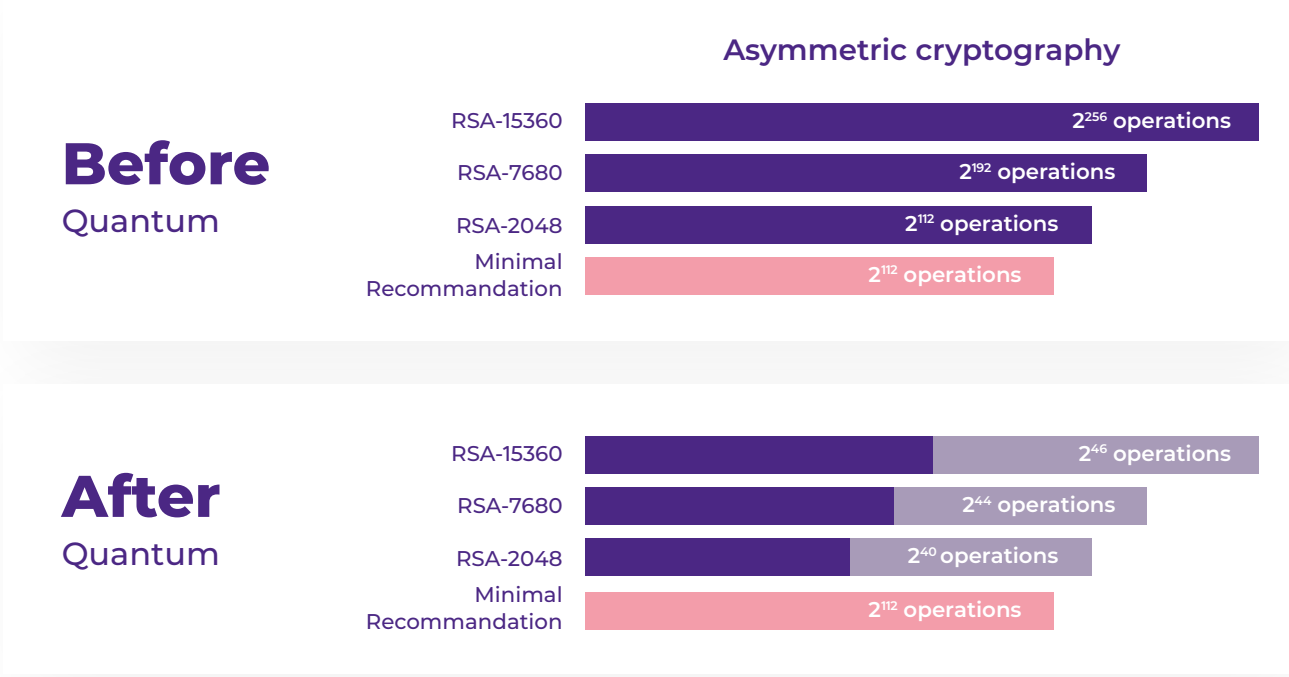
Figure 2: Quantum computers threat – Symmetric cryptography



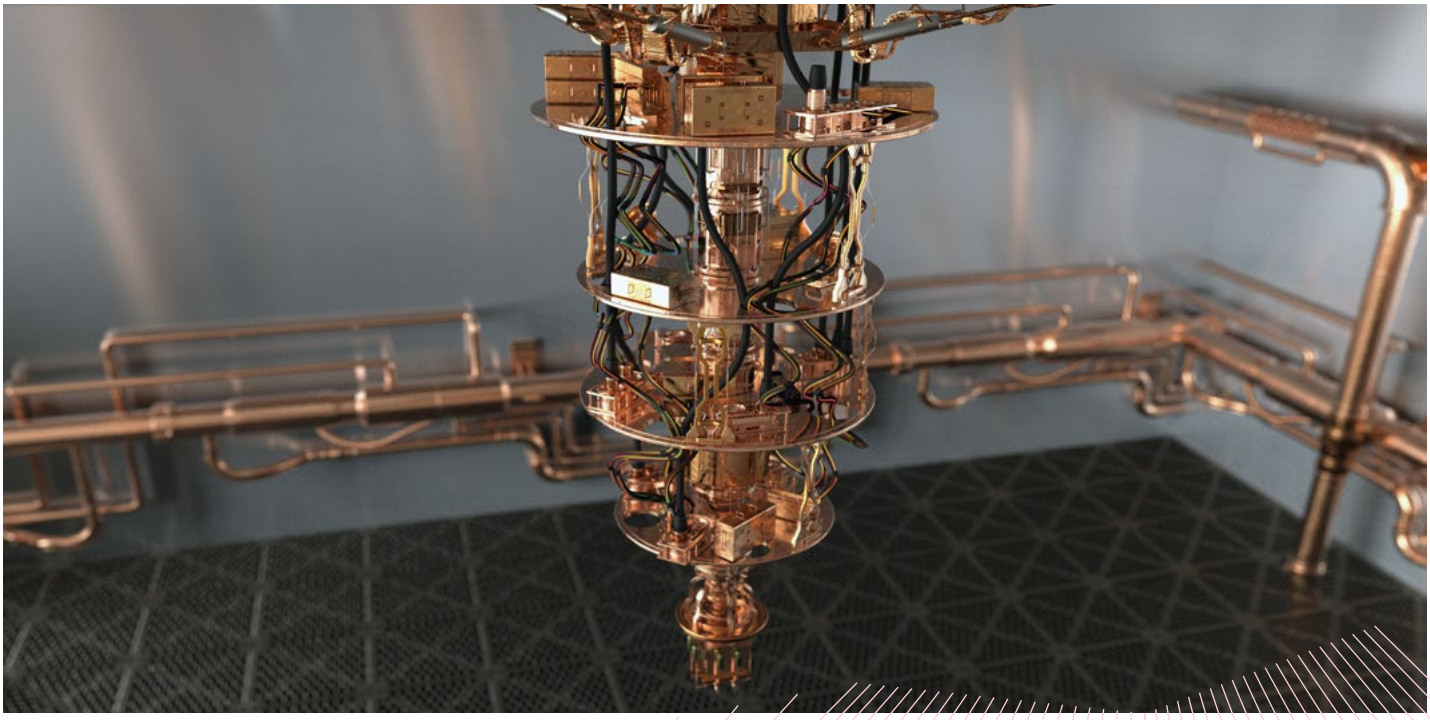
From 100 000 billion years to less than
a week for a brute force attack

In contrast, Shor's algorithm is a real game-changer. The difficult problems on which asymmetric cryptography is based today would be surprisingly easy to solve. In fact, the gain here is exponential, so these algorithms would no longer be secure even with keys millions of times larger. Figure 3 illustrates this fact: RSA would be impossible to repair since lengthening the key would provide virtually no security. This is also true for cryptography based on elliptic curves.

Figure 3: Quantum computers threat – Asymmetric cryptography



From 1.5 billion years to a few minutes



Cellular telecommunications case

In cellular telecommunications, symmetric cryptography is used to authenticate the subscriber to the network and to protect communications between the mobile and the network. The SIM is the heart of this process: it contains the subscriber's identity and secret key, and implements the AES-based algorithm milenage to perform authentication and generate keys for communication protection. This algorithm is used in 3G, 4G, and 5G networks. As we have seen above, this can be made quantum-safe by adjusting the length of the keys involved.

In order to recover the secret key of a given subscriber, the network must first determine their identity—the IMSI (International Mobile Subscriber Identity). Until 5G, the IMSI was sent in clear text. This allowed attackers to track users using "IMSI-catchers". These devices are widely available on the Internet at an affordable price, putting the basic privacy of citizens at risk.

In order to protect the subscriber identity, a new feature has been introduced with 5G: the SIM encrypts the IMSI before it is sent over the air. This feature uses asymmetric cryptography based on elliptic curves—which would be completely broken by quantum computers, as mentioned earlier.

Another aspect affected by the same threat is the remote management of UICCs in general, and eUICCs in particular. Indeed, it is possible to communicate with these elements over-the-air, to update the software, or to import data. For eUICCs, these mechanisms are essential because they allow loading of the profile for each new subscription. The protocols used rely partly on symmetric cryptography, but also on asymmetric cryptography. For example, each profile is signed in order to guarantee its authenticity. Moreover, the network behind this system includes many different actors , that communicate with one another over secure TLS channels, the latter also relying on asymmetric cryptography.

The cryptographic community's answer

If we want to continue enjoying the benefits of digitalization in the post-quantum era while maintaining security, we need to somehow replace the current asymmetric algorithms. To this end, new mathematical problems must be considered that are difficult to solve even with a quantum computer. A new family of cryptographic algorithms must be developed that run on classical devices and are simultaneously secure against both classical and quantum computers. This is known as "post-quantum cryptography".

3 When will the threat occur?

No one can predict when a quantum computer will be available that is powerful enough to threaten cryptography in practice. However, even if quantum computers do not pose a threat to cryptography now or in the immediate future, post-quantum cryptography must be developed and built starting from now. Designing, secure algorithms, standardizing them, developing them, deploying them widely, etc., may take years or decades. Moreover, data that is encrypted today must remain secure for a relatively long time for some applications. Thus, to be secure in the distant future and avoid the threat of "record now, decrypt later", such sensitive data must be protected with quantum-safe techniques as soon as possible. This is especially true for private data transmitted on cellular networks. Data must remain protected in the future to guarantee the citizen's right to privacy.

To this end, the NIST has initiated a standardization process for post-quantum cryptography. Its goal is to update asymmetric cryptography standards to include post-quantum algorithms. The process began in late 2017 as an open and transparent "competition" with 69 candidates participating in the first round. Algorithms were submitted by different teams composed of cryptographers from all parts of the world, often involving both academics and the industry. There are now 7 "finalists" and 8 "alternates" remaining for the third round, which began in July 2020. The end of this standardization process was initially planned for 2022/2024, but the timeline may be affected by research progress.

The standardization bodies of the cellular world are also working on securing the future of telecommunication,

- The 3GPP plan is to migrate to 256-bit key length version of milenage after release 17
- ETSI has launched a Quantum Safe Cryptography working group
- Global Platform is also studying the topic

We recommend preparing the industry now to seed quantum-safe algorithms and create the associated protection while protecting society against this type of attack in the short, mid, and long term.

4 To go deeper in challenges

Moving to post-quantum cryptography will not be a simple plug-and-play process. Even if all aspects of security and standardization of the new algorithms are settled, some challenges for the security community will remain. We can already foresee that post-quantum algorithms will differ from classical algorithms in some aspects such as:

- Functionalities: Since post-quantum resistance requires a change in fundamentals (the mathematical problems), cryptographers will again need to build cryptosystems that exploit these problems via ad hoc constructions. For this reason, the landscape of post-quantum algorithms is not equivalent to the classical one.
- The size of keys and programs: the underlying problems identified so far generally have a negative impact on the size of the keys, i.e. they are larger. In some algorithms, the public key can reach several hundred kilobytes, which is disproportionate to with the sizes for classical algorithms in use today.
- The underlying mathematical computations: the new problems serving as a basis for post-quantum algorithms imply different low-level mathematical operations that often consume more resources. This means that the development chain will be impacted from the lowest layers with performance also affected.
- The security level: in the family of post-quantum problems, some are quite recent and need to be studied further by the community to assess their long-term security, while others rely on more mature problems, even if not widely used until now.

These differences will have impacts at different levels.

First, the security protocols (i.e., the sequence of cryptographic methods used to perform a security-related functionality, given the key material available to the parties) that we use today will most certainly need to be adapted. The selection of the most appropriate algorithms must be done taking into account the characteristics mentioned above and require studies for each use-case. In particular, for algorithms relying on young problems, ANSSI and NIST recommend/require that it be used in combination with a classical algorithm. In this way, we avoid a breach if the new problem is broken, while taking advantage of it if not.

This leads us to the next challenge: performance. As mentioned earlier, the nature of the computations is different—the keys and software are larger, and we need to use both post-quantum and classical algorithms in the same protocols. To achieve acceptable timing, we must work on optimizations at all levels; in software as well as hardware.

In fact, cryptography embedded in current chips used, for instance, in a SIM, include specific pieces of hardware with the sole purpose of accelerating mathematical operations for crypto. As the operations change, those accelerators must be redesigned.

While we expect new algorithms to bring resistance from a theoretical point of view, cryptography—when deployed on actual material—has to resist other threats. Threats come from attackers who can spy on or influence the behaviour of the machine that performs the computations with the secret keys which can include spying on power consumption, the timing of execution, or the results of erroneous computations. This is known as Side-Channel and Fault Analysis, and is a very active field for attackers that is often less expensive than trying to crack the protocol itself. Protecting an implementation from these threats is done by applying countermeasures at the very low level of computation (in both software and hardware) by essentially randomizing computations in a clever way. Crypto developers must adapt this principle to new mathematical operations while trying to limit the impact on performance.

5 〉IDEMIA – our Quantum SAFE SIM

As a leader in technology and innovation in biometrics, cybersecurity and as a SIM supplier, IDEMIA has years of experience in optimizing protocols and implementations to meet increasingly demanding requirements such as contactless banking transactions. We take the quantum threat very seriously, which is why our cryptography experts are actively conducting research in this area and participate in standardization efforts.

As we have seen, protecting data transiting over the cellular network is crucial for subscriber privacy and management of (e)UICCs on the field. IDEMIA is working to shape the future and secure credentials in the quantum era.

Conclusion

Quantum computing is a real threat to the world of cellular networks. As we have seen, current standardized and deployed cryptography is not resistant to quantum attacks, and is already exposed to the "record now, decrypt later" attack. Considering the time needed to design new protocols, standardize them, achieve secure and performant implementations, and deploy new products — which is several years — we need to explore quantum-safe technology now. This is essential to meet the quantum-era challenge successfully.

The telecommunications community is taking actions to prepare for this necessary evolution and IDEMIA is in the forefront of innovation to support its customers and the industry in this journey.

We invite you to participate (if you are not already a participant), in our Quantum SAFE SIM and network testing initiative, and we will continue to work with mobile network operators to secure their business and their subscribers' data.

Acronyms

3GPP	3rd Generation Partnership Project
AES	Advanced Encryption Standard
ECC	Elliptic-curve cryptography is modern family of public-key cryptosystems and tends to be widely used for secure data transmission
ETSI	European Telecommunications Standards Institute
eUICC	Embedded Universal Integrated Circuit
GP	Global Platform
IMSI	International Mobile Subscriber Identity
iUICC	Integrated Universal Integrated Circuit
NIST	National Institute of Standards and Technology is a physical sciences laboratory and non-regulatory agency of the United States Department of Commerce
RSA	Rivest–Shamir–Adleman is a public-key cryptosystem that is widely used for secure data transmission computers that are a real threat for the cellular network world due to the current cryptography deployed
SUCI	Subscriber Unique Concealed Identity


IDEMIA

Securing **mobility** and **beyond**

idemia.com/solution/connectivity

IDEMIA

Join us on

www.idemia.com