WHITE PAPER

Post-Quantum Cryptography

How to protect existing systems against future quantum computing threats

Post-quantum cryptography (PQC) is the field of cryptography that deals with cryptographic primitives and algorithms that are secure against an attack by a large-scale quantum computer. While this area gained widespread attention among academics, it has been largely overlooked by industry. As we will see in this white paper, this is indeed a matter that industry should take seriously.

Quantum Computers

A quantum computer operates on the basis of the quantum mechanical principles superposition and quantum entanglement. The unit of information in a quantum computer is called qubit. In contrast to classical bits, which either have the value 1 or 0 and are therefore in one state or the other, a qubit is a superposition of these states. This means that it is both 0 and 1 at the same time and assumes both states. The phenomenon of quantum entanglement is the second principle of quantum mechanics that applies to qubits. This principle allows qubits to interact and influence one another regardless of the distance and medium between them.

Combined with other properties of quantum computers, these principles make it possible to calculate specific problems much more efficiently than with conventional computers. The main advantage of a quantum computer is its ability to simulate the physical micro-world much more accurately. As our world is governed by quantum

mechanics at atomic level, a computer that understands and uses these same phenomena can much better approximate quantum behaviours than a traditional computer.

Research on quantum computers has gained much traction in recent years. With a quantum computer, it is much faster to run simulations and perform certain calculations. Therefore, it can be used to optimise various applications and products in the pharmaceutical, chemical, and other industries. A rather negative side effect of quantum computers is their ability to solve the mathematical problems on which today's cryptography is based very efficiently.

Quantum Computers and Cryptography

Small-scale quantum computers have already been created by large companies and organisations around the world. These computers are expanding rapidly, and the goal of a large-scale quantum computer seems within reach in the not-too-distant future. When these computers become available, current public-key cryptosystems like RSA or elliptic curves will become insecure. Shor's algorithm [Sho94] shows how, using a quantum computer, the prime factorisation of a large number and the calculation of discrete logarithms can be done in polynomial time.

Additionally, symmetric encryption algorithms and hash functions that are not directly tied to a mathematical problem are also at risk, as Grover's algorithm [Gro96] shows. In this case, the impact is not as devastating as in public-key cryptography, but the time it takes to break a symmetric scheme or a hash function through a brute-force attack or an exhaustive search is reduced by almost half.

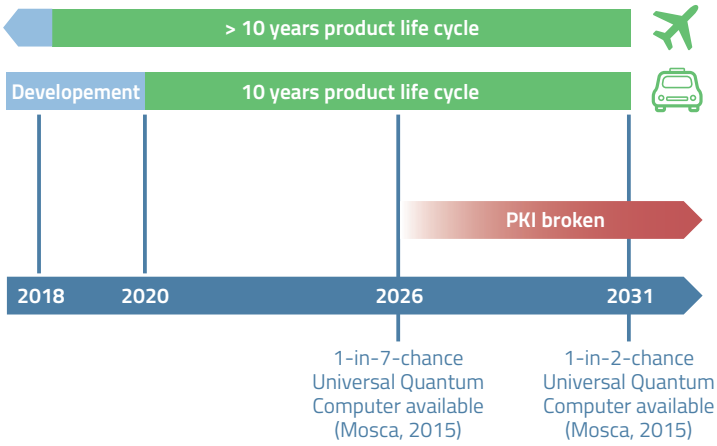
Type	Algorithm	Key Strength Classic (bits)	Key Strength Quantum (bits)	Quantum Attack
Asymmetric	RSA 2048	112	0	Shor's Algorithm
	RSA 3072	128		
	ECC256	128		
	ECC 521	256		
Symmetric	AES128	128	64	Grover's Algorithm
	AES 256	256	128	

Source: isara.com

The solution to the latter problem is considered easy, since the security parameters of the cryptographic functions can be increased with relatively little effort. To solve the first problem however, it is necessary to select new mathematical problems that are not vulnerable to quantum computers and to design, analyse, and implement new cryptographic schemes based on these mathematical problems.

Who is affected

The probability to break RSA 2048 by 2031 is estimated at 50 % [Mos15]. Complex software solutions and products usually entail long and arduous product development processes. Additionally, many industries like automotive, aerospace, transportation, public and critical infrastructure and others, design and produce products today that will be on the market for the next 20 to 50 years.



Another interesting aspect of these industries is their reliance on pre-orders that are produced now, but delivered far off in the future (+10 years). These products will most certainly face the threat of quantum computers. Consequently, it is essential to plan ahead and integrate the required protection mechanisms in the design and production processes that take place today.

How to avoid this danger

The good news is that there already are cryptographic systems that offer protection against strong quantum computers. The scientific field dealing with this aspect is called post-quantum cryptography. It focuses on the creation and deployment of what is known as post-quantum cryptosystems. But as discussed above, this is no longer a mere scientific issue. There are cryptographic algorithms based on mathematical problems that cannot be easily solved by a quantum computer.

These algorithms fall into five categories.

> **Hash-based**
> **Code-based**
> **Lattice-based**
> **Multivariate**
> **Supersingular isogeny-based**

Each category focuses on a different set of mathematical problems, some of them as old, mature, and well understood as the mathematics of today´s public-key cryptography, and others newer, more performant but yet untested in practice.

The diversity of the PQC ecosystem can create uncertainty about the security promises of these schemes. Academia and industry both agree that the way to tackle this issue is through the use of hybrid schemes.

Hybrid Schemes

A hybrid scheme is a combination of a traditional and a post-quantum scheme, meaning that the resulting scheme is at least as secure as one of the schemes used. In the example of key exchange, this would translate into performing two independent key exchanges, one with a traditional scheme like Diffie-Hellman and one with a post-quantum scheme. The two resulting keys are then combined (e.g. with an XOR operation) to create the final secret key that was exchanged.

Now, imagine what would happen if strong quantum computers come into widespread use and Diffie-Hellman becomes insecure. The security of the key would remain as strong as that of the quantum key exchange scheme that was used, and it could therefore still be used and considered secure. On the other hand, if the chosen post-quantum scheme was proven to be faulty or to contain errors, the security of the exchanged key would be reduced to that of Diffie-Hellman, which is still what is considered secure and state of the art today.

The use of hybrid schemes can therefore protect against more types of future dangers and threats. It is highly recommended in order to ease the transition into the post-quantum era.

Current Standardisation Activities

A major issue for post-quantum cryptography is the lack of standardisation, making a widespread deployment of PQC difficult and impractical. Luckily, large standardisation organisations have already started working on it.

NIST, the National Institute of Standards and Technology in the USA, has made a call for proposals for cryptosystems that are secure against quantum computers [NIST]. The 69 submitted algotithms will be evaluated and some of them will be standardised.

The European Standards Organization ETSI has also started research in this area with some preliminary publications [ETSI]. Furthermore, the IETF (Internet Engineering Task Force) has already published a standard for the post-quantum stateful hash-based XMSS scheme (eXtended Merkle Signature Scheme) [XMSS] and is planning to release more soon.

However, standardisation takes time and it will be years before the international community implements these standards. Industries and governments that need to integrate PQC into their products, processes, and infrastructures today should start addressing this issue as soon as possible. The longer they wait, the greater the danger of finding themselves unprepared in the post-quantum era.

Sources:
[Shor94] P. W. Shor, Algorithms for quantum computation: Discrete logarithms and factoring, Proc. 35nd Annual Symposium on Foundations of Computer Science (Shafi Goldwasser, ed.), IEEE Computer Society Press (1994), pp. 124-134
[Grover96] L. K. Grover, A fast quantum mechanical algorithm for database search, STOC 96 Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, pp. 212-219
[Mosca15] https://eprint.iacr.org/2015/1075.pdf
[NIST] https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf
[ETSI] https://www.etsi.org/technologies-clusters/technologies/quantum-safe-cryptography
[XMSS] https://tools.ietf.org/html/rfc8391

MTG AG · Dolivostr. 11 · 64293 Darmstadt · Germany
Tel +49 6151 8193-0 · contact@mtg.de · **mtg.de**