White Paper

Post-quantum cryptography: Secure encryption for the quantum age

Technology based on quantum computers has the potential to revolutionize a wide range of different fields of IT and industry—in the positive as well as negative sense. A significant increase in computing power delivers more capacity for analyzing and processing large quantities of data, therefore opening up new findings, application areas and business models. However, that also means more computing power to break today's security mechanisms. The rollout of quantum computers will impact IT security and, in particular, encryption mechanisms. It will invalidate some of the most-used current encryption algorithms. That's because their security is essentially predicated on the fact that they take too long to be decrypted by current computers with their present computing capacity.

That's no longer the case with quantum computers. Migrating cryptographic algorithms that are currently secure to quantum-safe algorithms may be a very time-consuming process. That's especially true if they're used in industries and application areas where products, such as smart meters and vehicles, are being developed now and will still be on the market in ten or 15 years' time. That's why it is important for users of cryptographic algorithms to set great store on crypto agility now, in particular for products with long life cycles. "Crypto agility" denotes the ability to replace currently used algorithms with quantum-safe ones—including in products already on the market. Utimaco's Hardware Security Modules and flexible Software Development Kit are especially suited for that task—and are also used by leading experts in the field of post-quantum cryptography.

Introduction: What is post-quantum cryptography?

A new generation of computers has entered the arena in the shape of quantum systems. They don't use bits, i.e. they don't know just the states 0 and 1 like conventional computers do. Instead, quantum computers use quantum bits (qbits) with three states:
0, 1 and one in between, termed the superposition. Unlike bits, a quantum bit can assume any states simultaneously. As a result, such a computer is able to carry out far more computing operations concurrently. Researchers estimate that a quantum system is about 1,000 times faster[1] than today's supercomputers.

Unfortunately, this computing power can also be used to compromise existing encryption methods. Consequently, these technologies have to be modified to withstand attacks from quantum computers. That requires post-quantum cryptography (PQC). PQC methods are encryption systems (cryptosystems) that can be used on conventional computers, such as PCs and mobile devices, and can withstand attacks by quantum computers.

The opportunities quantum technology opens up: current application scenarios

Of course, quantum computers were not conceived per se as "cyber weapons". Such systems give companies, researchers and public institutions new options. Thanks to their huge computing power, they can carry out complex calculations several thousand times faster than conventional systems. However, that's not true for all types of computational task.

Quantum systems are especially efficient if a task contains a large number of possible combinations. That's the case in calculating traffic flows, for example. Automotive companies and urban planners are already using early versions of quantum systems to analyze traffic in cities and reveal the best ways to manage it. In the financial sector, quantum computers might help compile an ideal stock portfolio for a customer. Also, manufacturers and logistics providers can use these systems to optimize delivery routes. Other application areas include searching for new drugs, examining software and training neural networks used in the field of machine learning.[2]

The dark sides of quantum technology

Yet the availability of quantum computers also entails risks—and the more so when such systems are provided over the cloud in the future. IBM already offers researchers and scientists access to a quantum computer in the cloud. Companies like Google, IBM and Amazon Web Services will follow. That means quantum computers will be available to a wide range of users—including those who use these systems to break encryption methods. Researchers expect that quantum computers will be available on a largish scale in around ten to 15 years.

There is also an additional consideration for companies from high-tech countries, like Germany, who may have to assume that government agencies elsewhere will use quantum computers to steal business secrets and research results. According to the German Federal Association for Information Technology, Telecommunications and New Media (BITKOM), more than 53 percent of German companies were the victim of industrial espionage and data theft in 2016 and 2017. The preferred prey was e-mails, financial data, and information from research and HR departments.

If German companies don't want to get left behind economically due to the outflow and theft of know-how, they will have to encrypt sensitive information so that it can't be compromised using quantum systems.

[1] http://www.datasciencecentral.com/profiles/blogs/understanding-the-quantum-computing-landscape-today-buy-rent-or-w

[2] https://www.dwavesys.com/sites/default/files/D-Wave%202000Q%20Tech%20Collateral_0117F.pdf
https://www.accenture.com/t00010101T000000__w__/br-pt/_acnmedia/PDF-45/Accenture-Innovating-Quantum-Computing-Novo.pdf

Quantum systems and IT security

The key problem of quantum computers in connection with encryption is that conventional encryption techniques can be broken with them. They include methods based on elliptic curves (Elliptic Curve Digital Signature Algorithm (ECDSA)) that are used to protect blockchain keys, for example.

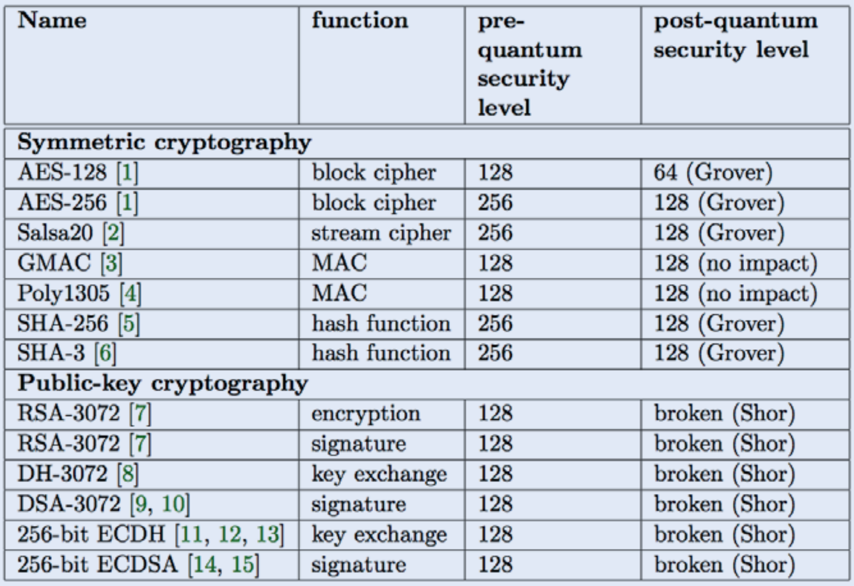
Asymmetric encryption techniques that use a public and private key (public key infrastructure (PKI) systems) are also at risk. That includes the widespread RSA method. Its security to date has been based on the fact that it's difficult for a conventional computer to factorize products of large prime numbers into their individual component primes.

For example, any PC can multiply 2,803 by 4,219 in a very short space of time. However, breaking down the result (11,825,857) into the two initial numbers requires immense computing power.

Quantum computers manage such tasks far faster than conventional computers. The American Peter W. Shor presented such an algorithm back in 1994. Experts predict that, from 2019 on, we can expect to see quantum computers that can crack RSA encryption. The same goes for methods based on Diffie-Hellman (DH) and the Digital Signature Algorithm (DSA).

Symmetric encryption methods such as AES (Advanced Encryption Standard) and SHA (Secure Hash Algorithm) will lose a large part of the protection they offer as a result of quantum computers.

Researchers like Daniel L. Bernstein and Tanja Lange have ascertained that, for instance, AES with 256-bit keys will in future only be as secure as current AES encryption with 128-bit keys.



Name	function	pre-quantum security level	post-quantum security level
Symmetric cryptography			
AES-128 [1]	block cipher	128	64 (Grover)
AES-256 [1]	block cipher	256	128 (Grover)
Salsa20 [2]	stream cipher	256	128 (Grover)
GMAC [3]	MAC	128	128 (no impact)
Poly1305 [4]	MAC	128	128 (no impact)
SHA-256 [5]	hash function	256	128 (Grover)
SHA-3 [6]	hash function	256	128 (Grover)
Public-key cryptography			
RSA-3072 [7]	encryption	128	broken (Shor)
RSA-3072 [7]	signature	128	broken (Shor)
DH-3072 [8]	key exchange	128	broken (Shor)
DSA-3072 [9, 10]	signature	128	broken (Shor)
256-bit ECDH [11, 12, 13]	key exchange	128	broken (Shor)
256-bit ECDSA [14, 15]	signature	128	broken (Shor)

The level of security offered by encryption methods—with and without quantum computing (source: Daniel J. Bernstein/ Tanja Lange, 2016)

[3] https://www.bitkom.org/Presse/Presseinformation/Spionage-Sabotage-Datendiebstahl-Deutscher-Wirtschaft-entsteht-jaehrlich-ein-Schaden-von-55-Milliarden-Euro.html

Action needs to be taken now

Even though quantum systems are not expected to be available to everyone for ten to 15 years, IT managers and managing directors have to put the issue of "post-quantum cryptography" on their agenda now. One reason is that it takes time to put existing encryption methods on a new foundation. The Cloud Security Alliance (CSA)[4] assumes five to ten years, for example.

A further point is that data encrypted with older methods is prone to quantum attacks. As a result, attackers can gain access to such data. Companies and public institutions must therefore ensure that all confidential data at risk is protected against such attacks by PQC methods. That involves a lot of time and effort—from capturing and categorizing such information resources to encrypting it again using PQC solutions.

However, one of the most vital factors requiring post-quantum cryptography is digitization. Concepts such as industrial IoT (also referred to as Industry 4.0), digital retailing, smart metering, autonomous driving and the Internet of Things are predicated on secure communication. If hackers succeed in paralyzing factories, traffic control systems or power stations, the consequences may be disastrous. Yet equipping such facilities with hardened IT security and encryption technology requires several years of preliminary work.

Coexistence of new and existing environments

One key point must be remembered when switching to a quantum-resistant cryptosystem environment at companies and public institutions: It's usually not possible to implement everything at once and start with a blank slate. That would be the case if only solutions, algorithms, methods for exchanging key material and certificates designed for the PQC age were used.

The American National Institute of Standards and Technology (NIST) assumes that algorithms resistant to attacks by quantum computers will be published in 2023.[5] However, replacing existing keys

> ”
>
> Companies and public institutions should now start addressing the fact that conventional encryption methods will be obsolete in a few years' time as a result of quantum computers. That's because switching to post-quantum cryptography costs time and needs good preparation.
>
> *Malte Pollmann, CEO of Utimaco*

[4] https://downloads.cloudsecurityalliance.org/assets/research/quantum-safe-security/applied-quantum-safe-security.pdf

[5] https://csrc.nist.gov/CSRC/media/Presentations/Update-on-the-NIST-Post-Quantum-Cryptography-Proje/images-media/2_post-quantum_dmoody.pdf

> ”
>
> Crypto agility is a must for future-proof cryptography solutions that also want to survive in the age of quantum computers. Hardware Security Modules and flexible software development kits play a key role in such solutions.
>
> *Malte Pollmann, CEO of Utimaco*

and cryptomaterials with new versions involves a lot of time and effort. That means different types of cryptosystems will coexist in practice—those that support post-quantum cryptography and those that don't.

There's a further aspect: the varying development times and periods of use for products. There are considerable differences in this respect. Development cycles of two to four years are customary in industry, the energy sector and the automotive sector. The lifecycle of machinery and vehicles is usually seven years or more.

That means a cryptography solution has to be adaptive to new requirements, such as post-quantum encryption solutions. That's only possible at acceptable cost and effort if a cryptography environment is agile, i.e. supports crypto agility.

Why crypto agility is important

Crypto agility means that applications, end-user devices and Hardware Security Modules in the field of encryption should use flexible, "agile" protocols and update methods that enable a switchover to post-quantum cryptographic primitives, for example. That has to be quick and easy so as to reduce the attack surface and limit the time and effort involved for users.[6]

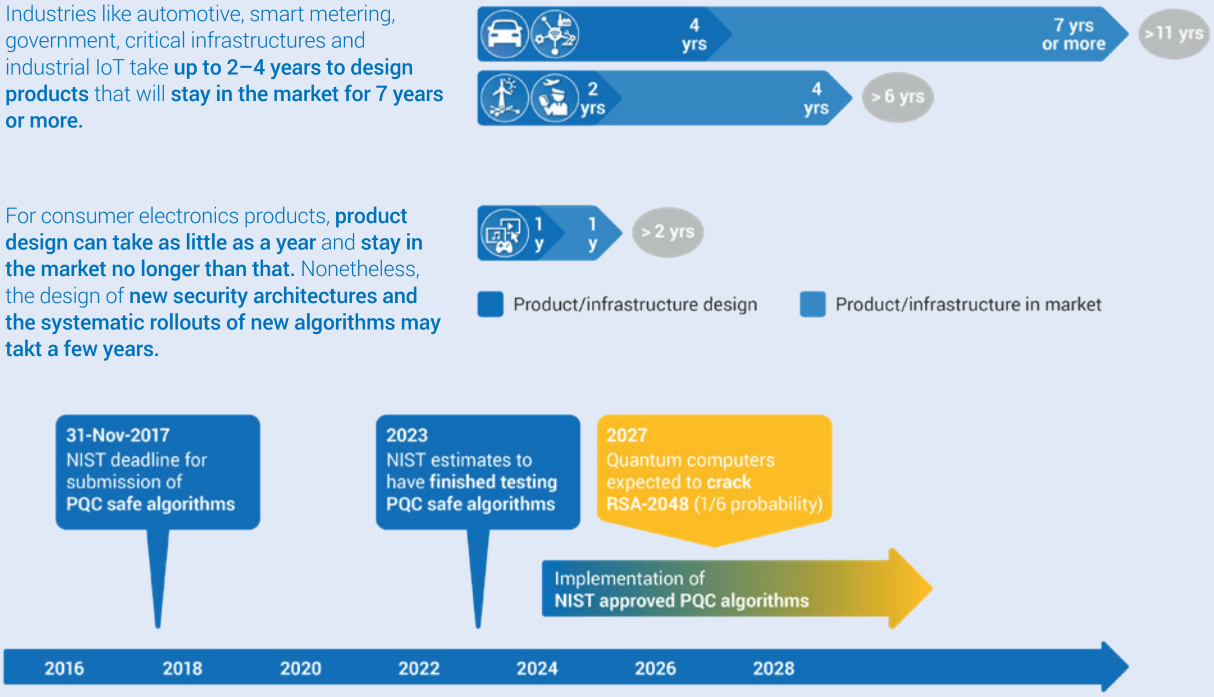
The German Federal Office for Information Security (BSI) also advises ensuring that new standards and algorithms in the field of encryption can be implemented immediately for new and further developments of products and services.[7] The background: In view of the rapid advances in quantum computers, the BSI has confined its recommendations in the Technical Guideline TR-02102-1 (Cryptographic Mechanisms: Recommendations and Key Lengths) to the period up to 2024. It is anticipated that, as of then, quantum computers will render at least some of the common encryption technologies obsolete.

Crypto agility also offers a further advantage: It bridges the gap between encryption techniques that are not yet "quantum-safe" and those that already meet the new requirements. That goes for chips, secrets and software code. Initial hybrid approaches that use PQC and common cryptography methods to date are being developed. Google has chosen this approach for its PQC algorithm New Hope.

[6] https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Practical.PostQuantum.Cryptography_WP_FraunhoferSIT.pdf?_=1503992279

[7] https://www.bsi.bund.de/DE/Publikationen/BSIForumkes/forumkes_node.html;jsessionid=84FC91445F5B5E029EC976F5CF4A882C.2_cid341

Product life cycles typically vary per industry



Industries like automotive, smart metering, government, critical infrastructures and industrial IoT take **up to 2–4 years to design products** that will **stay in the market for 7 years or more.**

For consumer electronics products, **product design can take as little as a year** and **stay in the market no longer than that.** Nonetheless, the design of **new security architectures and the systematic rollouts of new algorithms may takt a few years.**

4 yrs
7 yrs or more
>11 yrs
2 yrs
4 yrs
>6 yrs
1 y
1 y
>2 yrs
Product/infrastructure design
Product/infrastructure in market

31-Nov-2017 NIST deadline for submission of **PQC safe algorithms**

2023 NIST estimates to have **finished testing PQC safe algorithms**

2027 Quantum computers expected to **crack RSA-2048** (1/6 probability)

Implementation of **NIST approved PQC algorithms**

Maximum crypto agility is necessary, if only because of the highly differing product cycles. (Photo source: Utimaco)

Key role of software development kits

Yet the question is: How can crypto agility be put into practice? One problematic aspect, for example, is that much of the encryption hardware on the market does not enable flexible adaptation to new circumstances. Installation of new firmware or implementation of new algorithms is not possible or is possible only at great cost and effort.

The Hardware Security Modules from Utimaco in conjunction with the Utimaco Software Development Kit (SDK) prove that this doesn't have to be the case. Such a development environment already enables solutions that are suitable for the post-quantum era to be created.[8]

Users can create their own algorithms, tailor-made key derivation or complex protocols with the SDK. New PQC algorithms and appropriate keys can also be integrated in a Hardware Security Module – a flexible and future-proof approach. That's one of the reasons why large enterprises use Utimaco's solutions.

The bottom line is that a software development kit is vital against the backdrop of post-quantum cryptography. That goes for environments where symmetric encryption is used, as well as those which use asymmetric methods.

[8] https://hsm.utimaco.com/solutions/applications/post-quantum-crypto-agility/

In symmetric cryptography, a large number of keys have to be administered and key derivation functions (KDFs) implemented in a secure environment. The latter can be best achieved with an SDK. One example of such an environment is the home location register (HLR) in mobile communications, where key derivations are implemented in the HSM with the aid of the SDK. In order to make such symmetric cryptographic methods fit for the PQC era, the key lengths must be doubled at the least.

There is still no standardized PQC solution available for asymmetric encryption methods. It's expected that it will not be until 2023 that new algorithms are identified as "secure" by NIST. Companies that use public key infrastructures (PKIs) in order to identify and authenticate their IoT devices will (have to) use keys based on current and future, quantum-safe algorithms in parallel for some time. That demands flexibility at multiple levels—and that's offered by, among other things, the Utimaco Software Development Kit and associated scripting solution, which can be used to implement new algorithms in HSMs that are being used.

> ”
>
> Our HSMs are future-proof because they permit simple upgrading with new encryption technologies and algorithms. That also goes for methods that are resistant to attacks from quantum computers.
>
> *Malte Pollmann, CEO of Utimaco*

Application scenario: PQC and Hardware Security Modules

Microsoft has presented an application scenario for a post-quantum cryptography solution in conjunction with Hardware Security Modules (HSMs).[9] It's based on Microsoft's signature scheme Picnic and Utimaco's HSM solution. Two software components were used:

- A host application on a Windows PC and
- Firmware modules from Microsoft in an HSM from Utimaco's SecurityServer Se50 LAN V4 series.

In a research project on quantum-safe algorithms, Microsoft succeeded with the aid of these elements in creating a public key infrastructure (PKI) with signatures which cannot be compromised by

The Hardware Security Modules from Utimaco in conjunction with a Software Development Kit (SDK) already enable solutions that are suitable for the post-quantum era to be created. (Photo source: Utimaco)

[9] https://github.com/Microsoft/Picnic/blob/master/spec/design-v1.0.pdf

quantum computers. The use of new keys and signatures created using an innovative algorithm was no problem for the HSM.

One great advantage of Utimaco's solution proved to be that firmware from external vendors like Microsoft can be installed on the systems. That makes it possible to implement new cryptographic algorithms as and when required. If, for instance, certain encryption keys prove to be prone to attacks with quantum computers, new firmware modules with appropriate software can be installed on the hardware.

Would you like to learn more about post-quantum cryptography?

If this white paper has aroused your interest and you'd like to learn more about post-quantum cryptography, crypto agility and the implementation of new algorithms in the HSM, then read our book "Post-Quantum Crypto for Dummies."

It will be available on April 16, 2018, at the RSA Conference in San Francisco or a little later on our website at hsm.utimaco.com/downloads/.

Would you like to try out our HSM or implement new algorithms yourself?

Then get started by downloading our simulator. You can find it by going to: hsm.utimaco.com/downloads/utimaco-portal/hsm-simulator/

Ready to take off?
Download our HSM simulator!

Register for free

Take me there