THALES

www.thalesesecurity.com

‹Thales eSecurity›

CRYPTOGRAPHY FOR A POST-QUANTUM ERA

Thales eSecurity's crypto agility strategy for post-quantum computing data security

White Paper

Contents

Cryptography for a Post-Quantum Era

Quantum computing is an exciting new computing paradigm and is expected to solve complex problems that require far more computational power than what is possible with current generation of computer technologies. Advance research in materials science, molecular modelling, and deep learning are a few examples of complex problems that quantum computing can solve. Quantum computing, in essence, is the ultimate in parallel computing, with the potential to tackle problems conventional computers can't handle.

There is significant research, investment & momentum in Quantum Computing both in the industry and academia. And although still in the early stages of having commercially viable, affordable and deployable Quantum Computers, companies such as D-Wave systems already sell Quantum Computers to solve certain class and scale of complex problems.

It is also predicted that Quantum computers will be able to break several of today's cryptographic algorithms that are used to secure communications over the internet, provide root of trust for secure transactions in the digital economy and encrypt data. To protect against attacks from Quantum Computers, vendors of security products and service providers must constantly assess the risk associated with the choice of crypto algorithms. The choice of algorithms will have to evolve from those that are quantum resistant to entirely new algorithms for the post-Quantum world.

This whitepaper discusses the threat posed by quantum computing and the actions being taken by Thales eSecurity to ensure our customers continue to have the security they expect from our products. This paper provides a brief overview of how quantum computing impacts cryptographic algorithms then discusses standards related activities and how Thales eSecurity is preparing for quantum secure computing.

Quantum Computing – The threat to security

Cryptographic systems are built upon complex mathematical problems, which can only be solved if you have knowledge of some secret data; typically a very large number. Without these numbers, it is impossible to reverse-engineer encrypted data or create a fraudulent digital signature. These numbers are what we know as our cryptographic keys.

For instance, the RSA algorithm works by using pairs of very large prime numbers to generate public and private keys. The public key can be used to create a mathematical challenge that can only be solved by someone who holds the private key. Attempting to guess the answer, by way of a brute-force search, would take thousands of years using contemporary computers.

Unlike their classical counterparts, quantum computers will be able to solve these mathematical problems incredibly quickly. The asymmetric algorithms we use today for digital signatures and key exchange will no longer be strong enough to keep data secret once a sufficiently powerful quantum computer can be built. This means that core cryptographic technologies that we have to rely on, RSA and elliptic curve cryptography, will become insecure. These asymmetric algorithms underpin the majority of our security systems today, including everything from web browsing to financial transactions.

By contrast, symmetric algorithms and hash functions are only partially affected by quantum computers – the best quantum algorithms are about twice as fast as their classical counterparts, so key lengths and hash sizes will need to double. But we can still continue to use the same families of symmetric algorithms (such as AES) without concern.

No-one really knows when a sufficiently powerful quantum computer will be produced, however most estimates place this at least a decade or two away. Before this moment arrives, all security systems will need to be updated to use algorithms that are strong enough to withstand attacks from both classical and quantum computers.

Standards activities and industry support

The academic community has been studying the impact of quantum computers on cryptography for years and several new families of algorithms have emerged as potential replacements for RSA and ECC.

From a standardisation perspective, NIST has taken the lead in organising a competition to interrogate these candidates and identify the strongest and most suitable choices. The winners of this competition will almost certainly be adopted across industry. This is similar to the competitions in the seventies and late nineties that led to the development of DES and AES algorithms. Dozens of submissions were received before the 2017 deadline and are now being subjected to analysis and scrutiny, which will take at least five years. This means the winners can be expected in 2022-2024.

From the beginning, Thales eSecurity has been an active participant in the **NIST workshops** around post-quantum cryptography and continue to monitor and follow global efforts to standardize and promote the adoption of post-quantum cryptography. In order to ensure we have a broad, global vision of the state of the art, we have been closely monitoring the activities, progress, and conclusions being published by the following global working groups and organizations:

- European Telecommunication Standards Institute (ETSI) working group for Quantum-Safe Cryptography **(WG QSC)**
- The Internet Engineering Task Force (IETF) RFCs influencing protocols such as IKEv2 (**Hybrid PKQE**, **Auxiliary Exchange**, and **Pre-shared Keys**), and Cryptographic Message Syntax (Hash based signature schemes such as **MTS** and **CBOR**, as well as **Pre-shared Keys**)
- Post-Quantum Cryptography for long-term security (**PQCRYPTO ICT-645622**), to include their publication titled **"Initial Recommendations of long-term secure post-quantum systems"**, as well as their **annual conferences**
- American National Standards Institute (**ANSI**) X9F Quantum Computing Study Group and the TR-50 Quantum Techniques in Cryptographic Messaging Syntax
- International Telecommunications Union Telecommunications Sector (ITU-T), Study Group 17 (**SG17**)

Thales eSecurity taking action

Our research and security teams have been actively participating and following the developments of post-quantum cryptography. The Thales eSecurity CTO office has been conducting experiments and building prototypes to assure our products will address the future risks that our customers may encounter. In 2017 we implemented leading candidate algorithms and added them to popular open source crypto applications. Our experience taught us that these algorithms are not fundamentally more complex than existing classical algorithms. We released some of this research work publically; you can check our **GitHub account** for examples. Our ongoing research is now focusing on accelerating the different families of algorithms using our existing hardware platforms.

Crypto-Agility

Across our product range, in both hardware and software, we are preparing for the forthcoming changes by ensuring we are crypto-agile. Crypto agility is the ability to easily substitute one type of algorithm for another, without requiring expensive and time-consuming product changes. This refers mainly to our use of algorithms to secure the operation of the products, such as the signature schemes that enable our access control schemes, but of course it also applies to the algorithms we offer to our customers to use.

Fortunately, this is not the first time cryptographic standards have changed. In the past two decades we've seen the deprecation of a number of schemes, most notably in the hashing space. Our previous experience in migrating away from SHA-1 hashing primitives and adopting stronger asymmetric primitives such as ECC, has paved the way for an architecture that can adapt quickly to change.

Specifically, the product teams have been improving their commitment to the crypto-agile approach through the more frequent use of longer symmetric algorithm key lengths, the use of symmetric integrity protection over asymmetric, supporting data-driven algorithm selection, and introducing dual-signature mechanisms with updatable trust models, with redundant recovery mechanisms.

In the meantime, our **CodeSafe technology** allows any cryptographic algorithm to be implemented in a secure manner using our nShield range of hardware security modules. If your company is planning to make an early leap into post-quantum algorithms, before the industry has settled on its preferred candidates, CodeSafe can help secure your implementation to ensure private key material is not leaked into server memory.
For further assistance in this area, please contact our **Advanced Solutions Group.**

Our Customers

Our customers trust us as a security partner and we are frequently asked how best to prepare for the quantum security threat.

We've **written about this subject before** and the main points can be summarised quite succinctly. As a user of cryptography, you must consider where your use of cryptography today may leave you exposed once we pass the point of quantum computer supremacy.

In almost every situation, the good news is that quantum-resistant algorithms are going to arrive in time to save the day. The NIST competition will finish perhaps even a decade before the first quantum computers can pose a danger to our data, so there is plenty of time to make adjustments. However, you should be following our lead and working to ensure your products and services can cope with a switch of algorithm without causing you downtime (or undue delay).

In some rare cases, such as those companies who are deploying IoT hardware into the field that might need to last thirty years without further modification, there is additional complexity to consider. Here it is important to consider how to support in-field upgrades of algorithms – particularly those relating to secure boot – to allow your infrastructure to defend itself against quantum adversaries. It's difficult to advise in a general sense how to secure these sorts of deployments because every deployment has its unique architecture, however, we are here to help and getting in touch with us to discuss your specific use case.

Summary

At Thales eSecurity we are optimistic about the future of post-quantum cryptography. Our products and services are preparing for the necessary changes, while the industry as a whole is on track to identify the safest algorithms to use way ahead of the pending danger. Our research work further reassures us that a post-quantum world is reassuringly similar to our current methods and tactics. It is our belief that:

- Crypto agility research is ahead of post quantum crypto attacks
- It will be more than a decade before asymmetric crypto based on today's algorithms can be compromised with quantum computing
- The industry should continue to work with NIST and other standards bodies
- Quantum Computers will be leveraged to develop sophisticated malware that attacks AI/deep learning algorithms

If you have specific questions or concerns about the impact of quantum computers on the security of our products or your deployments, please don't hesitate to get in touch at **sales@thalesesec.com.**

THALES

www.thalesesecurity.com

About Thales eSecurity

Thales eSecurity is a leader in advanced data security solutions and services that deliver trust wherever information is created, shared or stored. We ensure that the data belonging to companies and government entities is both secure and trusted in any environment – on-premises, in the cloud, in data centers or big data environments – without sacrificing business agility. Security doesn't just reduce risk, it's an enabler of the digital initiatives that now permeate our daily lives – digital money, e-identities, healthcare, connected cars and, with the internet of things (IoT), even household devices. Thales provides everything an organisation needs to protect and manage its data, identities and intellectual property, and meet regulatory compliance – through encryption, advanced key management, tokenization, and privileged-user control and high-assurance solutions. Security professionals around the globe rely on Thales to confidently accelerate their organization's digital transformation. Thales eSecurity is part of Thales Group.

Follow us on:

Americas – Thales eSecurity Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel:+1 888 744 4976 or +1 954 888 6200 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com