Firmware integrity in the quantum age

www.infineon.com/OPTIGA-TPM-SLB9672

Contents

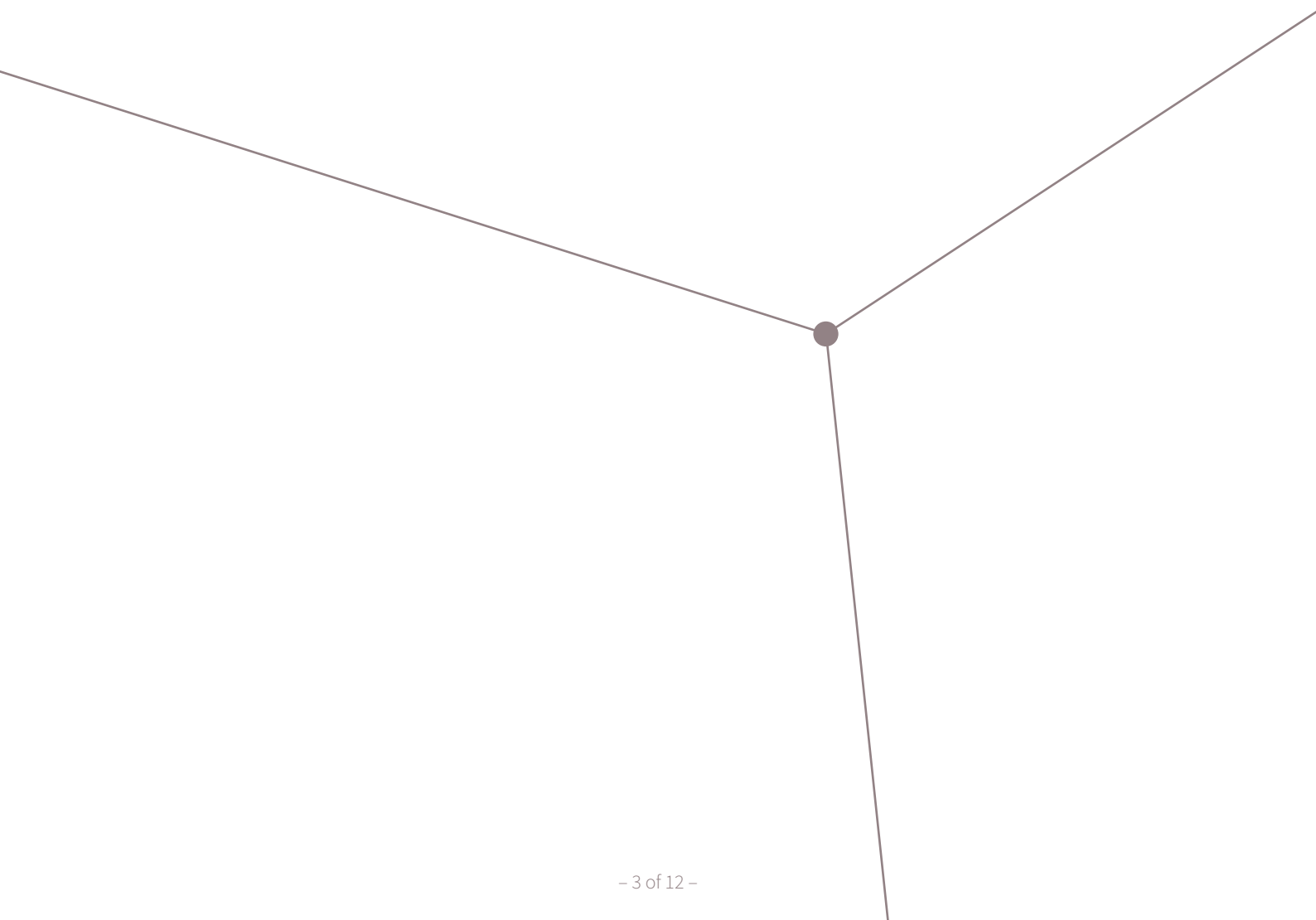
Introduction

As we entrust more aspects of our lives to the digital world, security is a fundamental need of society with increasing importance. The connected world in which we live is constantly expanding to encompass more ‘things’, further driving the demand for security. The ability to update these things over-the-air (OTA) is a huge benefit – and a risk as malicious code can be injected allowing third parties to take control.

Cryptographic techniques including public and private keys used in conjunction with hardware devices such as TPMs have provided strong security, allowing users to be confident that attacks are unlikely to be successful.

However, things are changing with the research on quantum computers – machines that use quantum mechanical phenomena to solve mathematical challenges that are very hard to solve with conventional computers. With this level of computing power, quantum computers would be able to break today’s common public key cryptography, seriously compromising the confidentiality and integrity of all forms of digital communications.

In this technical white paper, Infineon will look at the threat posed by quantum computing and discuss how cryptography will evolve to provide security and trust in a post-quantum world.



The threat from quantum computers

Quantum computers are a new breed of highly powerful computing devices that use quantum mechanical phenomena to solve mathematical challenges that are very hard to solve with conventional computers. Using a set of quantum bits known as 'qbits', a quantum computer is able to perform exponential parallel computations on a single piece of quantum hardware.

The disruptive nature of quantum computing technology has already been proven, at least on a small scale. In practice, continued research and development, both in academic circles and in industry, is slowly but surely increasing the size of quantum computers. While currently, the size remains limited, there is broad agreement among experts that a universal quantum computer will exist around 2040. Quantum computing is significantly funded including EUR 1 billion from the EU and EUR 650 million in Germany while the US has assigned $1.2 billion to boost US quantum tech. Research firm, ResearchAndMarkets estimates that the market for QC hardware will be over USD 6 billion by 2025.

Positive benefits of large-scale quantum computing will include breakthroughs in artificial intelligence, chemical simulation, optimization and cryptography. However, the disruptive potential of these machines to break current cryptographic algorithms is a global threat to computer and internet security.

Using an appropriate quantum computer, today's commonly used asymmetric cryptosystems, especially RSA and ECC can be completely broken using Shor's integer factorization algorithm. At a relatively simple level this technique was demonstrated by IBM and others as early as 2001. RSA is based upon the assumption that factoring large integers is computationally highly difficult and, while this remains valid for non-quantum computers, Shor's algorithm shows that factoring integers is efficient in an ideal quantum computer. Mitigating techniques such as increasing the key length of these algorithms does not result in a significantly higher security, meaning that new and / or alternative asymmetric algorithms are needed.

Alternatively, the effect of quantum computing technology on most symmetric cryptographic algorithms is not as dramatic. Currently, the best-known attack is Grover's key search algorithm, devised by Lov Grover in 1996. Unlike other quantum algorithms, which provide exponential speedup over their classical counterparts, Grover's algorithm only provides a quadratic speedup. Grover's algorithm could brute-force a 128-bit symmetric cryptographic key in approximately 264 iterations, or a 256-bit key in around 2128 iterations.

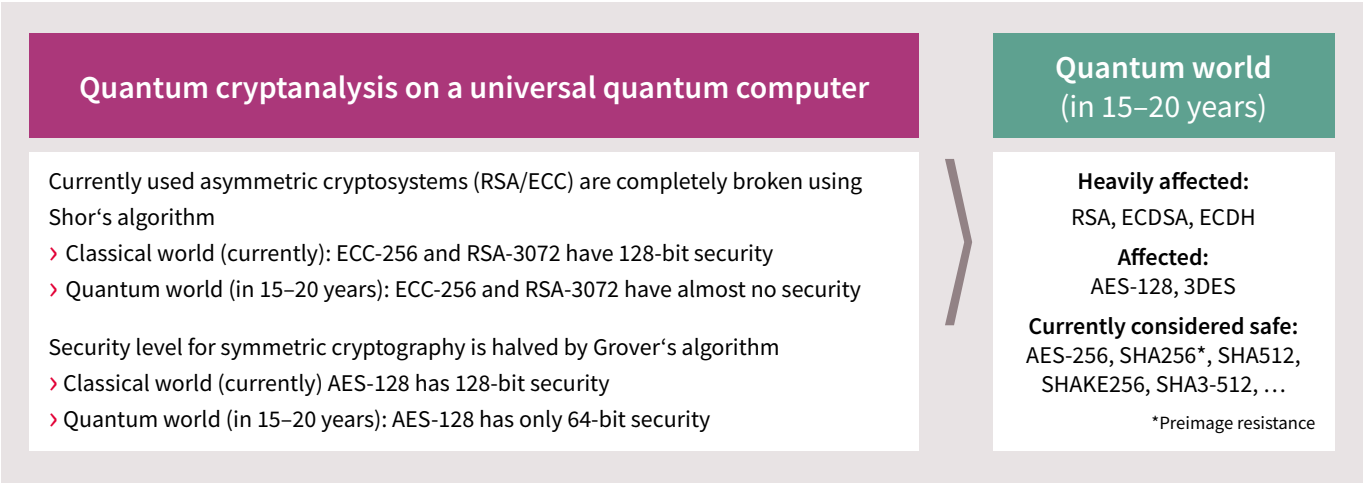


Figure 1: Quantum computing poses a significant threat to current cryptosystems, especially asymmetric

As a result of Grover's algorithm, the bit security of commonly used symmetric algorithms such as AES, SHA-2 or SHA-3 is halved. Therefore, AES-256 and SHA-256 can continue to be considered appropriately secure.

Why do we need to act now?

The timescales may seem far off and with the high costs involved, quantum computers are unlikely to be commonplace, so at one level there seems little need for urgency. Certainly, for many consumer type devices such as smartphones, tablets and bank cards, the expected useful lifetime is well within the timescales being discussed, so at a first glance there is little urgency here as current products will be obsolete before any meaningful quantum computers appear.

It should be noted, however, that all data that has been encrypted using today's encryption schemes may be stored and decrypted at a future point in time. This means that even some of today's data may be at risk tomorrow. Furthermore, large capital installations such as those associated with national infrastructure (power stations, air traffic control, large factories) would be expected to still be operational after quantum computers are able to be deployed.

Modern vehicles are becoming increasingly connected to receive updates over-the-air as well as to infrastructure (V2I) and to each other (V2V) presenting a multitude of potential attack surfaces, some of which could take control of the vehicle. These vehicles are right on the cusp, with estimated lifetimes of around 15 years, so there is also significant urgency here for a solution to security in the post-quantum world.

At this time the threat is 'emerging' and, as such, there is much work to be done particularly in the area of standards for security. The threat will continue to adapt and develop over time, in much the same way that computer viruses have. This means that there will be no 'total' solution, but companies – especially those producing products that will be in operation post-2035 – need to act now to mitigate as many risks as possible.

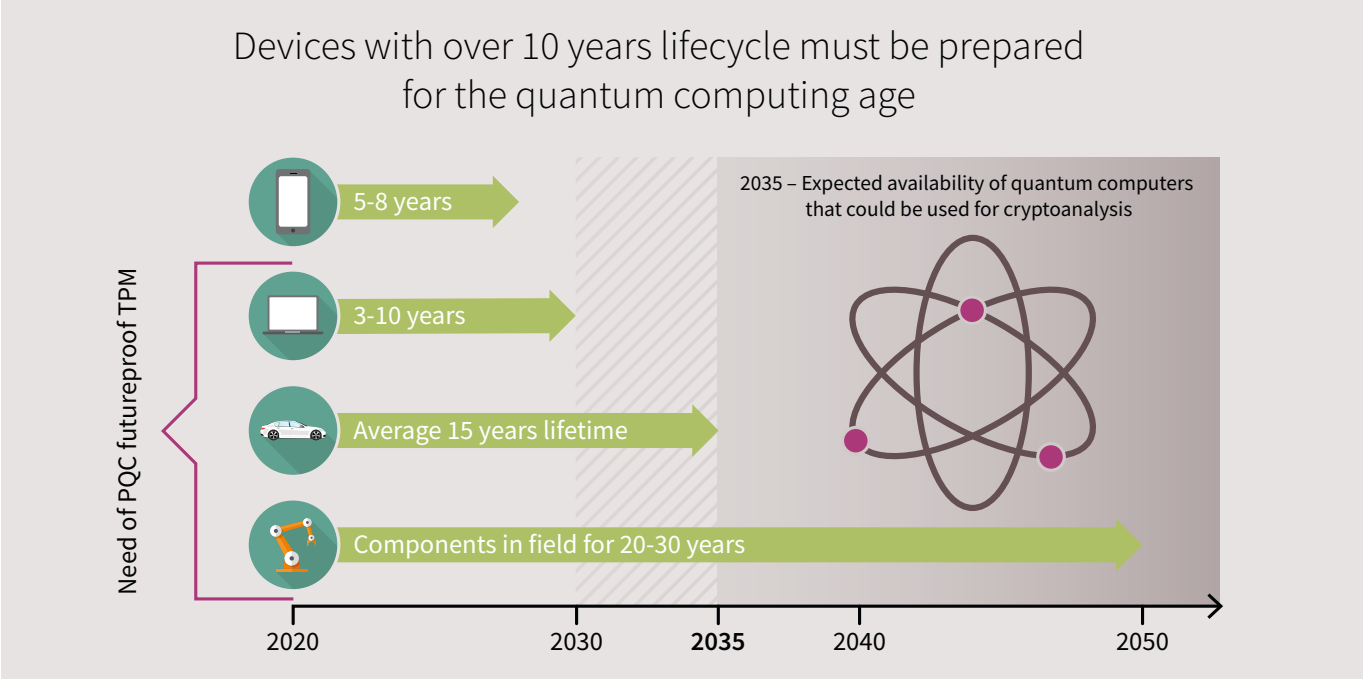


Figure 2: It is important to act now, particularly for large infrastructure that will be deployed for decades

Developing post-quantum computing standards

During 2017 the US National Institute of Standards and Technology (NIST) started a long-term process with the intention of eventually establishing agreed standards for security in a post-quantum computing (PQC) world. Similar to the approach taken with AES and SHA-3, NIST invited proposals for quantum-safe public-key encryption, key-exchange and digital signatures – although this time the call was much broader.

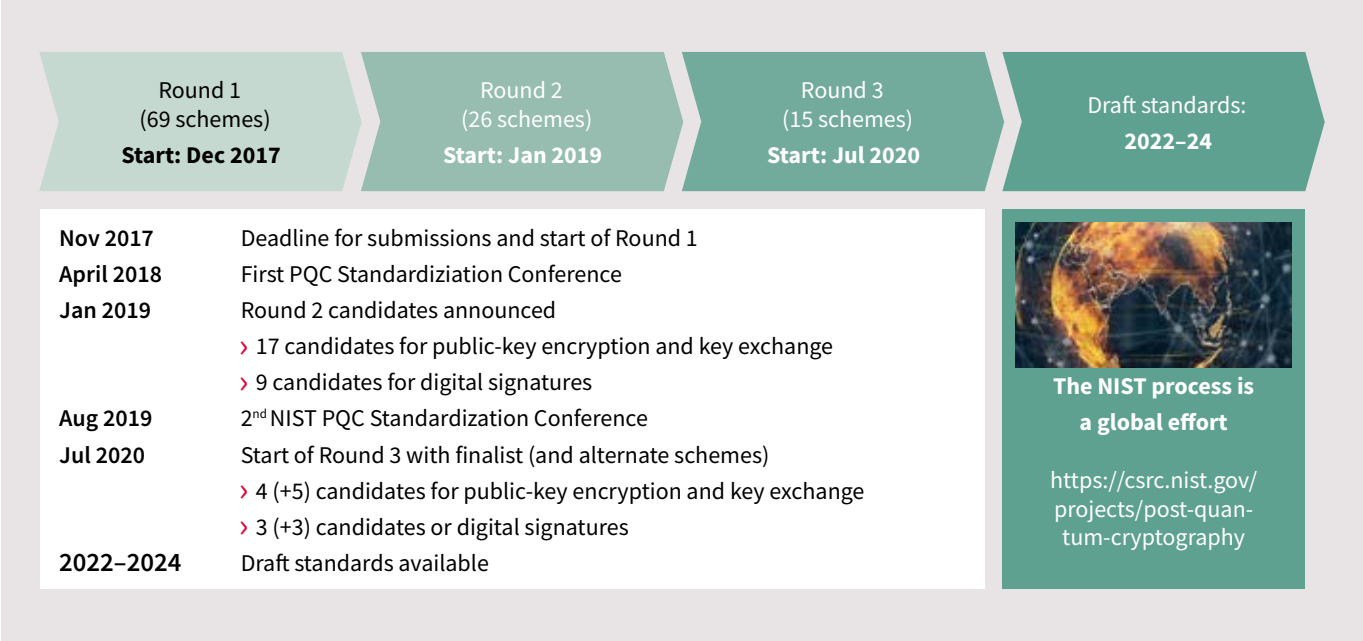


Figure 3: NIST is leading efforts to develop security standards for a PQC world

NIST received a total of 69 submissions during the first round, although many of these proposals were dismissed as the schemes were completely broken or significantly attacked within a short time. Following a PQC standardization conference in April 2018, NIST selected the most promising 26 schemes to advance into Round 2.

Authors were permitted to merge or revise submissions in between rounds, so that they could benefit from know-how gained during the process. There was a second standardization conference in August 2019 and, as a result, and in July 2020 NIST announced the third (and final) round with 15 schemes. Since many schemes are slow and demand high levels of processing, NIST is also evaluating the performance of software and hardware implementations.

The last round of the competition already contains many promising candidates. However, it is not yet fully decided whether NIST will select a single winner or whether they will propose standardizing several alternate approaches. The whole process is planned to deliver draft standards by 2024, although the initiative is likely to continue beyond this to keep pace with developments in quantum computing.

As the process is ongoing and no consensus has yet been reached, if a PQC scheme is required today it is unclear which algorithm(s) to choose. An alternative interim solution could be stateful hash-based signatures.

Stateful Hash-based Signatures

Hash-based signatures (HBS) are asymmetric post-quantum cryptographic schemes that are readily available today. HBS rely on the preimage resistance of a hash function, which is a well understood property and considered to be more robust than the assumptions used by RSA and ECC. The other main difference when compared to RSA and ECC is that most HBS are stateful, meaning that it is essential that the number of signatures that can be generated with a private key is limited, requiring tracking of previously used keys.

Hash-based signatures have a long history stretching back to 1979 although, most recently, two stateful HBS schemes LMS and XMSS were published in 1995 and 2011. These two schemes were standardized by the IETF in RFC 8554 and RFC 8391 and then, in October 2020, NIST finalized their PQC standard SP800-208 based on a subset of the parameters in the RFCs.

The main hash functions used by LMS and XMSS are SHA-256 or SHAKE256 giving a HBS with post-quantum security of 128 bits. With the smallest parameter set, the signature size is around 2.5 kB for both schemes and the public key is about 60 bytes. The private key size depends on the performance trade-off used for signing as faster algorithms increase private key sizes to a few kB.

On embedded devices, verification takes a few hundred milliseconds while signing takes seconds. Key generation can take minutes or even hours, depending on the number of required signatures. However, a cryptographic hash accelerator may significantly improve the performance.

HBS have many advantages, most notable being considered as quantum resistant and, therefore, future proof. The main drawback is their statefulness as re-using the same private key for several different messages means that the scheme can be trivially broken. As a result, careful state management is essential with any used private key being reliably deactivated before the corresponding signature is released.

Figure 4: Hash-based signatures contain many useful features

From a performance perspective, key generation is the most critical step as a huge hash tree has to be computed to determine the public root key which, depending on the parameters, can result in several hundred million hash computations. The same is true for the signature generation if no time-memory trade-off is implemented. In practice, signing algorithms reuse the intermediate results that were stored during key generation, although this does increase the size of the private key.

Stateful HBS are ideal for embedded platforms as was shown in 2012 when a preliminary, adapted version of XMSS was implemented on a 16-bit Infineon SLE78 smartcard. As verification is fast and does not involve secrets, implementation is possible on resource constrained devices. The signing algorithm is also well suited to embedded devices, especially those with security controllers where the private keys and the state of the used private key can be securely controlled.
When looking at the properties of stateful HBS it is clear that these PQC schemes are very well suited to firmware updates, especially as they are the only asymmetric PQC algorithms currently standardized.

What is the role of a TPM?

A typical embedded processor will usually be susceptible to attacks, as standard hardware is not optimized for security applications. The complex host software is executed on the same processor as the security code and will, inevitably, share resources such as memory, thus leaving the system vulnerable to threats and bugs. The situation is even more critical when considering physical attacks, which can be rendered fairly easily. These attacks may include ‘micro probing’ the chip, observing the power usage or just injecting spikes to change operation and reveal weaknesses in the code execution.

Incorporating a dedicated security processor offers protection against the types of attack outlined above. The security processor has its own dedicated resources, including protected memory that allows code to be executed completely internally, removing some of the key vulnerabilities of the software approach. Also, it is designed to securely store sensitive data and the hardware is optimized to protect data inside the chip from being accessed by the outside world.

While this approach adds another component, it also significantly simplifies things as the secured code is completely separate and does not have to be ‘woven into’ the general operating code or executed on shared resources.

A good example of such a security processor is the Trusted Platform Module (TPM). These devices have been used successfully to provide security in PCs for years and are becoming more common in embedded systems. A TPM can be thought of as a ‘safe’ within the system as it is capable of resisting both logical and physical attacks - its shielded environment protects confidential data and cryptographic secrets.

TPMs support a wide variety of use cases including basic device authentication and protection of system integrity via remote verification. These functionalities offer high levels of flexibility thereby enabling dynamic security enhancements. ‘On-the-fly’ updates can be used to add the higher levels of future protection that embedded systems require, hence allowing TPM-based systems to address short-term security requirements as well as new use cases.

The evolutionary path

Clearly, moving from the current world of classical computing to the PQC world will be a journey, with mitigation steps being developed in parallel with the work being carried out to develop standards for the threats currently envisioned.

Based upon the idea that the security of the application cannot be higher than the security of the firmware update mechanism – or put another way, if the firmware update is weak, the whole system is weak – HBS standards will be applied to the firmware update mechanism now.

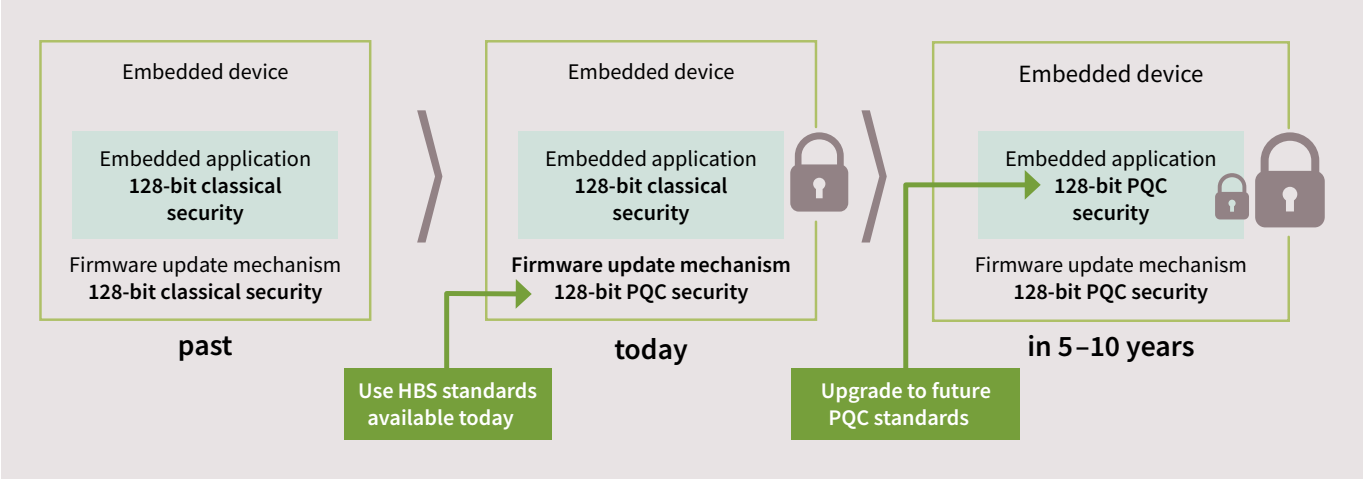


Figure 5: Using HBS today will allow critical firmware updates to be protected from quantum computing

Looking to the future, as PQC standards are developed and released (by NIST and other similar bodies) then these will be applied to the embedded application, thereby providing 128-bit PQC security throughout the embedded system.

A TPM for the PQC world

Infineon's OPTIGA™ TPM SLB 9672 includes a PQC-protected firmware update mechanism and is the first device to be independently security evaluated and certified to meet the Common Criteria international standard. In fact, the new device is an official TPM product listed at the Trusted Computing Group (TCG) as being compliant to their TCG 2.0 rev. 1.59 specification.

Additionally, the OPTIGA™ SLB 9672 already meets the forthcoming Microsoft Windows requirements that are due to become effective in April 2023 and is compliant with the new NIST standard, SP 800-90B. FIPS 140-2 certification is pending.

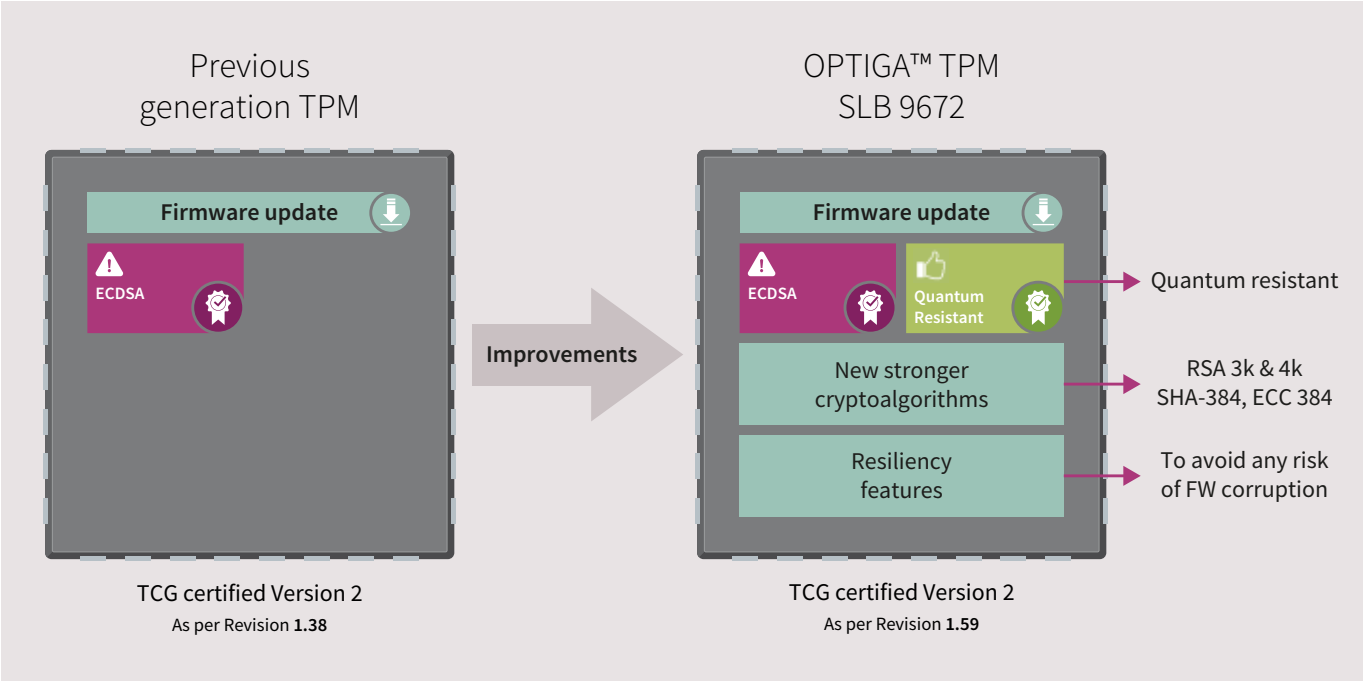


Figure 6: The new OPTIGA™ TPM SLB 9672 offers specific PQC-resistant features

The new device includes a number of important features including new stronger cryptographic algorithms such as RSA 3k & 4k, SHA-384 and ECC 384. The firmware update mechanism in the OPTIGA™ SLB 9672 is quantum resistant due to its ability to handle XMSS signatures and it includes a number of additional resiliency features to avoid any risk of firmware corruption.

The Infineon update authority is now able to handle the statefulness of XMSS keys thereby providing secured firmware update operations allowing clear business continuity. In the field, the OPTIGA™ SLB 9672 is able to transparently check the XMSS signature and therefore validate (or not) the transferred payload.

The OPTIGA™ SLB 9672 meets requirements for demanding applications with an operating temperature range of up to -40°C to +85°C. It currently supports 192-bits key length although this will be extended to 256 bits via a firmware update which is in preparation.

The device includes three GPIO lines and a 51kbyte non-volatile user memory that can be used to store keys or data.

Applications for the new TPM include servers and PCs as well as general computing and data storage. It will also support a wide range of network infrastructure including gateways, routers, wireless access points, network interface cards and switches. The OPTIGA™ SLB 9672 is compatible with Intel x86, ARM and other platforms.

Infineon support for TPM development

Infineon's OPTIGA™ TPM 2.0 Explorer is a GUI-based tool for users to familiarize themselves with TPM 2.0 quickly and easily using a Raspberry Pi®. In addition, the software platform demonstrates how the OPTIGA™ TPM 2.0 can be used to increase security and trust in applications. Using this tool, designers can experience the benefits that TPMs bring to smart home devices and network equipment.

Designers benefit from the tool as they are able to explore OPTIGA™ TPM 2.0 features and learn use cases faster by simply selecting a button to call the relevant function or task. The tool provides immediate visual feedback so that commands run and corresponding responses can be reviewed.

Using the tool allows designers to initialize a TPM 2.0 and display all of the defined properties as well as performing a full reset when required. It is also possible to manage the non-volatile memory and handle PCR indexes as well as defining how the system enters and recovers from a lockout event.

The comprehensiveness and simplicity of the GUI tool makes it possible for all users, regardless of their experience or knowledge, to access and explore the features of OPTIGA™ TPMs.

Summary

Quantum computing may pose a significant threat to security, especially to devices and systems that are able to receive remote firmware updates. The incredible computing power of quantum computers will allow conventional asymmetric encryption to be broken with ease and symmetric encryption keys will be significantly weakened.

While the threat from quantum computers is a decade or more in the future, designers need to act now, especially for large infrastructure projects that will still be in use (and require secured operation) in the age of quantum computing. The challenge for designers is meeting a threat that is not (yet) fully defined and while standards remain in development.

Existing technology such as the well-known stateful hash-based signatures have been shown to offer protection in the PQC world as they are based on the preimage security of the hash function. This means that they can, at least, enable that all firmware updates remain appropriately secure.

TPMs provide essential hardware support and Infineon's OPTIGA™ TPMs are well known and respected, being incorporated in half of the world's business PCs. Infineon began work on PQC solutions in 2017 and the OPTIGA™ TPM SLB 9672 is one of the first results of those endeavours. This is the world's first TPM with a PQC-protected firmware update mechanism and, as such, goes a long way towards enabling data security in the PQC age.

www.infineon.com

Published by
Infineon Technologies AG
Am Campeon 1-15, 85579 Neubiberg
Germany

Document number: B185-I1252-V1-7600-EU-EC
Date: 02/2022

Please note!
This Document is for information purposes only and any information given herein shall in no event be regarded as a warranty, guarantee or description of any functionality, conditions and/or quality of our products or any suitability for a particular purpose. With regard to the technical specifications of our products, we kindly ask you to refer to the relevant product data sheets provided by us. Our customers and their technical departments are required to evaluate the suitability of our products for the intended application.

We reserve the right to change this document and/or the information given herein at any time.

Additional information
For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices, please contact your nearest Infineon Technologies office (www.infineon.com).

Warnings
Due to technical requirements, our products may contain dangerous substances. For information on the types in question, please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life-endangering applications, including but not limited to medical, nuclear, military, life-critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.