Latest Trends in Post Quantum Cryptography

Daisuke Moriyama, Automotive System Security Department, Automotive Core Technology Development Division, Automotive Solution Business Unit, Renesas Electronics Corporation

Introduction

Most Cryptographic experts and leading governmental agencies are predicting that existing cryptographic algorithms that are widely used today will be vulnerable when quantum computing becomes more readily available. Many leading companies are anticipating this "Post Quantum" era and requiring algorithms that are secure against quantum computers. This white paper explains how the security of current cryptography is evaluated and how powerful quantum computers can break it. We also introduce the latest status of post-quantum cryptography standardization projects and global trends to adopt the post quantum cryptography initiated by several companies and governmental organizations.

Background

Cryptographic technology is all around us, even if we don't realize it. When we access a website with a PC or smartphone, almost all web servers enable secure communication by default. Most modern web browsers provide a visual indication, such as a closed lock icon, when a secure connection is established. In this case, the browser is using Hypertext Transfer Protocol Secure (HTTPS), an extension of the Hypertext Transfer Protocol (HTTP). In 2018, only 27% of web servers used HTTPS by default. However, by 2022 that number increased to 80% [1]. To establish secure communication, it is necessary to confirm that the server is authentic. A digital signature is used to determine authenticity. Signatures can be transported in digital certificates, which define the structure for communicating cryptographic information. Along with digital signatures and the server's public key, certificates also contain information about which cryptographic algorithm was used to generate the signature. The client can verify the server's authenticity based on the defined cryptographic algorithm. For example, when you access https://www.renesas.com, you can see that the digital certificate associated with this website was generated with the RSA and SHA-256 cryptographic algorithms, as shown in Figure 1.

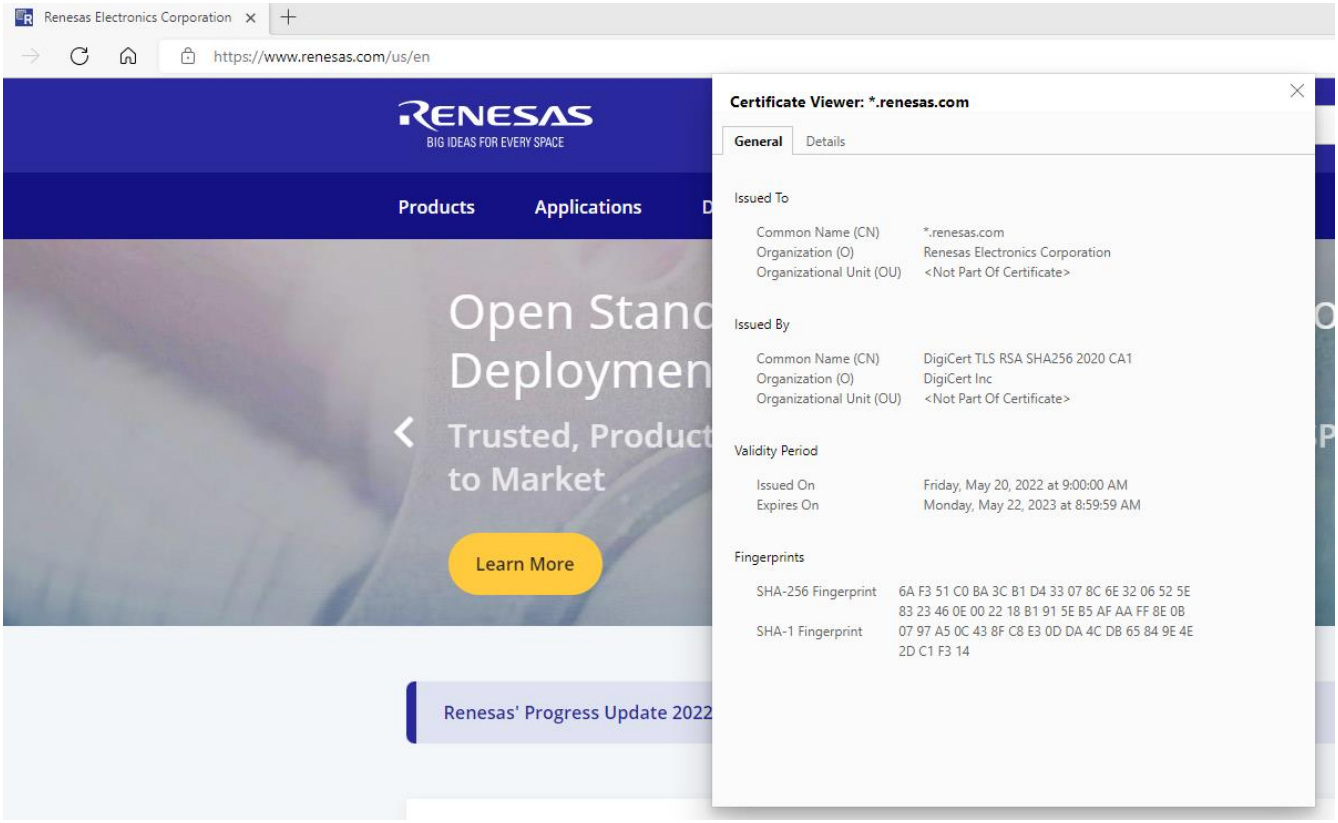

Figure 1. Certificate information in Renesas Electronics website

When web servers and clients securely exchange specific data, Transport Layer Security (TLS) provides a mechanism to derive a shared secret key. This key is generated by two parties using a cryptographically secure key exchange protocol or key derivation scheme. Messages are encrypted and decrypted using a symmetric key encryption algorithm. Secure communication is essential for IoT products, which is why Renesas partners with best-in-class solutions providers like wolfSSL [2][3]. WolfSSL supports hardware-accelerated TLS in several Renesas microcontrollers including the RX, RA, and Synergy Families. This combination of public key and symmetric key cryptography is not limited to web browsing; it is deployed for secure communication in a variety of contexts. For example, public key cryptography is used in V2x applications including Vehicle-to-Vehicle (V2V) or Vehicle-to Infrastructure (V2I).

Digital signatures are not only used in network communication, but also inside microcontrollers and PCs. The boot sequence often includes a check to ensure the integrity and/or authenticity of fundamental functions. As part of this procedure, a digital signature is usually stored internally in advance as the Root of Trust. A trusted chain derived from the certificate verifies the authenticity of the next boot target program. This architecture prevents execution of an unauthorized program. The secure boot architecture for automotive products is described in detail in blogs that are available on the Renesas web site [4][5]. We also provide a secure boot mechanism for IoT products. For example, the Renesas Flexible Software Package for RA Family microcontrollers provides an optional secure bootloader [6][7].

As we explained briefly above, public key cryptography and symmetric key cryptography are widely used to support our secure life. Some readers may be surprised to learn that quantum computers are evolving very rapidly and can complete certain computations in just a few seconds that would take classical computers more than ten thousand years to complete. This white paper explains how the security of current cryptography is evaluated, how quantum computers affect current cryptography, what the current development status of quantum computers is, the latest status of post-quantum cryptography, and governmental/industrial announcements and activities.

Security Evaluation of the Current Public Key Cryptography

The security of Public Key Cryptography, including the digital signature scheme and key exchange protocol, relies on mathematical problems that are hard to solve using current computers. The integer factorization problem is a well-known problem, which states that it is hard to compute a pair of prime number $(\boldsymbol{p}, \boldsymbol{q})$ given $\boldsymbol{N} \coloneqq \boldsymbol{p} \times \boldsymbol{q}$. While it is trivial to factor small numbers, such as factoring $\mathbf{21}$ as $\mathbf{7} \times \mathbf{3}$, the problem becomes unmanageable, even when using computers, when the two primes are significantly larger. This mathematical problem is the basis for RSA cryptography. The discrete logarithm problem over a finite field, or elliptic curve, is another famous mathematical problem. Again, the larger the numbers, the more difficult the problem is to solve. DSA and ECDSA are well known digital signature schemes that rely on these problems.

The security strength of the mathematical problem is given by the number of steps needed to solve the target problem, where each step is a single logical operation (AND, OR, XOR, etc.). When a problem requires more than 2^{128} operations to solve, even with the best solving algorithm proposed by researchers, we say that the problem has 128-bit security. For example, the RSA encryption scheme, which relies on the integer factoring problem, provides 128-bit security when the length of N is 3,072 bits and (p, q) is 1,536 bits. Table 1 shows a summary of well-known public key cryptographic algorithms and lengths that provide the specific security strength.

Table 1. Public Key Cryptographic Algorithms and Security Strengths

	Encryption	Signature		Key exchange	
Algorithm	RSA	DSA	ECDSA	DH	ECDH
112-bit security	2,048-bit	2,048-bit	224-bit	2,048-bit	224-bit
128-bit security	3,072-bit	3,072-bit	256-bit	3,072-bit	256-bit
192-bit security	7,680-bit	7,680-bit	384-bit	7,680-bit	384-bit
256-bit security	15,360-bit	15,360-bit	512-bit	15,360-bit	512-bit

To determine the practicality of solving one of these mathematical problems, let's assume that we run 100 million computers whose CPU operates at 4GHz around the clock for a year (24 hours per day, 365 days). In this case, the total computation performed in one year is estimated as $10^7 \times 60 \times 60 \times 24 \times 365 \times 4 \times 10^9 \approx 2^{80}$. Even if we were to continuously run this machine cluster for 1000 years, the total evaluated computational steps is still only 2^{90}, or a bit strength of 90-bit security.

It is desirable to choose a cryptographic algorithm and bit length that are both small enough to be efficiently computed in normal usage and large enough to keep security within a sufficient margin. Since CPU performance is gradually increasing with the development of semiconductor technology, the required bit strength to maintain the same practical level of security is also increasing. A decade ago, 112-bit security was considered as the recommended security strength. However, the National Institute of Standard and Technology (NIST) has announced that 112-bit security is not sufficient after 2030, with a recommendation to increase the security strength to 128-bit security [8]. The Japanese governmental project CRYPTREC gives an estimation that 128-bit security is effective until 2050 against typical computers [9].

Quantum Computer's evolution

The above security estimation is evaluated against traditional computers: PCs, cloud servers, microcontrollers, etc. On the other hand, quantum computers perform computations using physical phenomena based on quantum mechanics, such as quantum superposition and quantum entanglement. Quantum computers are not simply considered to be fast computers in the sense of traditional computers. The concept of a "bit" in traditional computers is treated as "qubit" in a quantum computer. The qubit does not provide a digitalized state of 0 or 1, but rather it satisfies both conditions at the same time. Therefore, N qubits can express 2^N-bit states as they would be represented by a traditional computer. This property can be used to significantly reduce the time required to solve several mathematical problems like those used for RSA and elliptic curve cryptography.

However, this fact does not indicate that current public key cryptography is easily broken when a device has several hundreds of qubits in a quantum computer. All quantum elements in a quantum computer are quite unstable and are exposed to heavy noise, and they cannot be directly used for logical operations such as AND, OR, XOR, etc. This type of quantum element is called a physical quantum bit. To perform a logical operation with physical quantum bits, we need to add a sufficient error correction mechanism and provide enough time for state stabilization. About 1,000 physical quantum bits are required to generate one logical quantum bit for stable operation. A research result in 2019 showed that 2,048-bit RSA encryption can be broken in 8 hours with a quantum computer, but the precondition of this estimation requires that a quantum computer must configure 20 million physical quantum bits [10][11]. For the input length n, they estimate that approximately $3n$ logical qubits are required to solve the integer factoring problem. When we focus on the elliptic curve cryptography over the prime field, another research result show that about $9n$ logical qubits are required to break the discrete logarithm problem [12].

Starting as far back as 2010, several companies have announced they could build a workable quantum computer. The latest news of quantum computer development is that Alphabet™ used a 53-qubit (physical quantum bit) quantum computer in 2019 and IBM® created a 127-qubit quantum computer in 2021 and a 433-qubit quantum computer in 2022 [13][14][15]. In addition, IBM® provides a roadmap of quantum computer development to reach 1,121-qubit in 2023 and 4,158-qubit in 2025 [16] (*1)(*2). It will take a long time to reach 20 million qubits to break public key cryptography as described above, but the recent evolution of the quantum computer is remarkable. Following these technology trends, the White House published a memorandum that federal agencies should strengthen current public key cryptographic algorithms by 2035 to mitigate the risk caused by quantum computers [17]. In 2021, the

European Union Agency for Cybersecurity (ENISA) published that specific countermeasures are required to maintain data confidentiality if the data will be stored over 10 years [18].

(*1) Alphabet is a trademark of Alphabet Inc.
(*2) IBM is a trademark or registered trademark of International Business Machines Corporation in the United States, other countries.

Selection of Post Quantum Cryptography

In 2016, NIST started a standardization project for Post Quantum Cryptography (PQC) to choose the next generation public key cryptography to protect against quantum computer attacks. NIST issued a call for proposals for researchers all over the world to nominate cryptographic algorithms that can replace current RSA and elliptic curve cryptography. As a result, 69 cryptographic schemes were submitted, including the encryption algorithm and the digital signature scheme. After much discussion between NIST and cryptographic researchers, NIST selected 26 algorithms to proceed to the second round of evaluations in 2019, and 15 algorithms (7 finalists and 8 alternate candidates) were chosen as the third-round candidates in 2020. Finally, CRYSTAL-Kyber was selected as the standard public key encryption scheme and CRYSTALS-Dilithium, FALCON, and SPINCS+ were winners for the standard digital signature scheme in July 2022.

When NIST started this standardization project, they requested submissions to provide parameter settings in the specification document such that the proposed algorithm provides 128-bit, 192-bit, and 256-bit security. A unique number is assigned to each algorithm to distinguish each security strength, as shown in Table 2.

The PQC algorithms rely on mathematical problems that are different from RSA or elliptic curve cryptography. One algorithm is based on the shortest vector problem, which finds a lattice point that is the closest to the origin in a vector space. Another algorithm is based on the closest vector problem, which finds a vector that is the closest to a given point in a vector space. While there are many mathematically intractable problems that are resistant to quantum computer attacks, CRYSTALS-Kyber, CRYSTALS-Dilithium and FALCON rely on the security from lattice problems.

Table 2. Post Quantum Cryptographic Algorithms to be Standardized

	Encryption	Signature		
Algorithm	CRYSTALS-Kyber	CRYSTALS-Dilithium	FALCON	SPHINCS+
128-bit security	Kyber512	Dilithium2	FALCON-512	SPHINCS+-128
192-bit security	Kyber768	Dilithium3	(none)	SPHINCS+-192
256-bit security	Kyber1024	Dilithium5	FALCON-1024	SPHINCS+-256

According to NIST recommendations [19], CRYSTALS-Kyber and CRYSTALS-Dilithium will be widely used for various applications. FALCON has the advantage that the signature length is shorter than CRYSTALS-Dilithium, so it will be useful for specific scenarios. The main motivation to select SPHINCS+ is that this algorithm is not based on the same mathematical problem as the other signature schemes, relying on the security of a hash function (collision

resistance). In fact, the lattice problem is a new research topic; therefore, NIST wishes to standardize on multiple algorithms in case a novel solution algorithm is found by researchers.

When NIST published the announcement of the selection of the four initial algorithms, they also announced that they will continue to a fourth round to evaluate additional algorithms. At the time of writing this white paper, four third-round algorithms, called BIKE, Classic McEliece, HQC and SIKE, are the investigation candidates [20]. The security of these algorithms is not based on the lattice problem; therefore, we expect the final list of standardized algorithms may be expanded.

Even though there are many quantum-resistant algorithms, it is important for everyone to align with the defined, standardized algorithms. The main reason is to ensure that we can seamlessly communicate with each other over a secure channel. This requires that the underlying cryptographic algorithms, like AES, SHA, ECDSA, etc., are standardized and all hardware/software implementations are functionally identical.

Post Quantum Security for Symmetric Key Cryptography

As we explained above, quantum computers are effective tools for attacks on current public key cryptography. When we focus on the security of symmetric key cryptography, there is a well-known concept result called Grover's algorithm. This shows that when traditional computers require 2^N computations to perform an exhaustive search, quantum computers perform the same operation in only $2^{N/2}$ steps. For example, AES with a 256-bit secret key provides a traditional security strength of 256 bits, but its post-quantum security strength is only 128 bits. Many symmetric key algorithms provide 128-bit/192-bit/256-bit security against traditional computers, but the post-quantum security for these settings is only 64-bit/96-bit/128-bit respectively. Therefore, it is reasonable for us to select a 256-bit secret key in symmetric key encryption and a 512-bit output for the hash function algorithm to sufficiently keep the security margin even in the post-quantum setting. We summarize well-known symmetric key algorithms and their security strengths in Table 3.

Table 3. Post-Quantum Security of Symmetric Key Algorithms

Type	Algorithm	Secret key length	Output length	Traditional security	Post-quantum security
Encryption	AES	128-bit	128-bit	128-bit	64-bit
		192-bit	128-bit	192-bit	96-bit
		256-bit	128-bit	256-bit	128-bit
Hash	SHA2	-	256-bit	128-bit	64-bit
		-	384-bit	192-bit	96-bit
		-	512-bit	256-bit	128-bit
	SHA3	-	256-bit	128-bit	64-bit
		-	384-bit	192-bit	96-bit
		-	512-bit	256-bit	128-bit

While post-quantum security is completely different between public key cryptography and symmetric key cryptography, it is necessary to compress a message with a hash function to generate a digital signature. CRYSTALS-Kyber and CRYSTALS-Dilithium use the hash

function SHA3 as a building block, and these schemes execute the hash computation multiple times. Therefore, the security of the hash function is also important to ensure that the total security provided by the public key encryption or digital signature scheme is sufficient to protect against quantum computers.

The effectiveness of quantum computer attacks against symmetric key algorithms is quite limited compared to attacks against the current public key cryptography implementations of RSA and elliptic curve cryptography. As explained above, the number of logical qubits to break the current public key algorithms is proportional to the input length. In contrast, exponentially large computational steps are still required to break the symmetric key algorithms. Therefore, NIST is currently focusing on post-quantum cryptography standardization for public key algorithms.

World Trends for Post Quantum Cryptography

Nowadays we can find a lot of open-source projects and open-source software available for both evaluation and use in commercial products. There are several freely available software packages that implement post-quantum algorithms. We can even find a reference implementation written in C from the submitted material uploaded to NIST. One open-source project is the PQClean project, which mainly targets fair evaluation and high-quality source code [21].

The PQClean project was launched in 2019 and provides open-source software for post-quantum cryptography, including the four algorithms selected as the standard by NIST. The main difference from typical open-source projects is that one of the main objectives of this project is the focus on software quality improvement. For example, PQClean states that there are no errors/warnings from well-known C toolchains, no problems reported from static/dynamic analysis, namespaces are unified, etc. Therefore, it is expected to be able to be safely integrated with a higher-layer system, and we can also fairly evaluate which algorithm is suitable among the several standardized algorithms in its system. The source code provided by the PQClean project is integrated into another open-source project called the Open Quantum Safe Project, which provides a prototype of secure network protocol implementations like OpenSSL™ [22] (*3).

Another open-source project is the PQCRYPTO Project, funded by the European Union. This project focuses on a software library of post-quantum algorithms for the Arm® Cortex®-M4 and releases a library called pqm4 (*4). This library enables us to examine several implementations, including a reference implementation submitted to NIST, an optimal C implementation, a ported implementation from PQClean, an assembly implementation using the Cortex®-M4 instruction set, and more. This library will be useful to evaluate the software implementation results for various microcontrollers for IoT products.

Currently, several IT companies provide a library or server-side setting that enables post-quantum cryptography in TLS as a beta version [23][24][25][26]. While we could not find an actual case study from other industries, governmental organizations frequently publish information on their websites. The Cybersecurity & Infrastructure Security Agency (CISA) issued guidance to carefully monitor further technology development and plan to move critical

infrastructures to use post-quantum cryptography if those systems will be used for several decades [27][28]. The European Union Agency for Cybersecurity (ENISA) and Bundesamt für Sicherheit in der Informationstechnik (BSI) suggest to deploy both current public key cryptography and post-quantum cryptography in one system to both maintain backward compatibility and provide future security in case a critical vulnerability is found in the post-quantum cryptography [29][30]. We expect that it will take many years to move to post-quantum algorithms, but it is important for each governmental organization and private sector to prepare to support post-quantum cryptography for ensuing a continuously secure society for the long term.

(*3) OpenSSL is a trademark owned by the OpenSSL Software Foundation.
(*4) Arm and Cortex are registered trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

Conclusion

In this paper, we focused on quantum computers, post-quantum cryptography, and the latest security trends. The security of current public key cryptography is still sufficient against the traditional computers, but it is critically insecure against attacks that utilize quantum computers. Currently, the NIST post-quantum standardization project has selected four algorithms to be standardized, and we expect these algorithms to play a significant role in providing a secure digital society in the near future. Even though technology migration might require a long time, organizations should cooperate to provide a continuously secure environment for consumers of digital services and products. It is particularly important to ensure that a compromise of the current public key cryptography schemes does not directly affect the lifespan of IoT or automotive products. This can be done by supporting post-quantum cryptography for products that are expected to be used by the consumer for a long time. Renesas continuously monitors the standardization progress and market trends related to post-quantum cryptography. While the standardization by NIST has not been finished, each PQC algorithm needs various arithmetic and logical operations, including a hash calculation. Therefore, microcontrollers and System-on-Chip (SoC) have an important role in automotive and IoT products to efficiently calculate them. We intend to provide an efficient PQC hardware/software architecture in the near future so that our customers can implement a secure ecosystem even in the presence of quantum computers.

[References]

[1] https://w3techs.com/technologies/history_overview/site_element/all/y
[2] https://www.renesas.com/us/en/products/microcontrollers-microprocessors/rx-32-bit-performance-efficiency-mcus/rx-partners/wolfssl-embedded-ssl-tls-library
[3] https://www.renesas.com/us/ja/blogs/realizing-secure-and-high-speed-communications-rx-mcu-and-wolfssls-tls-library (Japanese translated version of [2])
[4] https://www.renesas.com/us/en/blogs/introduction-about-secure-boot-automotive-mcu-rh850-and-soc-r-car-achieve-root-trust-1

[5] https://www.renesas.com/jp/ja/blogs/introduction-about-secure-boot-automotive-mcu-rh850-and-soc-r-car-achieve-root-trust-1 (Japanese translated version of [4])
[6] https://www.renesas.com/us/en/software-tool/flexible-software-package-fsp
[7] https://www.renesas.com/us/ja/software-tool/flexible-software-package-fsp (Japanese translated version of [6])
[8] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf
[9] https://www.cryptrec.go.jp/report/cryptrec-mt-1011-2021.pdf (written in Japanese)
[10] https://www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/
[11] https://arxiv.org/abs/1905.09749
[12] https://link.springer.com/chapter/10.1007/978-3-319-70697-9_9
[13] https://www.nature.com/articles/s41586-019-1666-5
[14] https://research.ibm.com/blog/127-qubit-quantum-processor-eagle
[15] https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two
[16] https://www.ibm.com/quantum/roadmap
[17] https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/
[18] https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation
[19] https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms
[20] https://csrc.nist.gov/Projects/post-quantum-cryptography/round-4-submissions
[21] https://github.com/PQClean/PQClean
[22] https://openquantumsafe.org/
[23] https://cloud.google.com/blog/products/identity-security/how-google-is-preparing-for-a-post-quantum-world
[24] https://aws.amazon.com/blogs/security/how-to-tune-tls-for-hybrid-post-quantum-cryptography-with-kyber/
[25] https://www.microsoft.com/en-us/research/project/post-quantum-cryptography/
[26] https://blog.cloudflare.com/post-quantum-for-all/
[27] https://www.cisa.gov/uscert/ncas/current-activity/2022/08/24/preparing-critical-infrastructure-post-quantum-cryptography
[28] https://www.cisa.gov/news/2022/08/24/cisa-releases-new-insight-preparing-critical-infrastructure-transition-post-quantum
[29] https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study
[30] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html

(Rev.1.0 Dec 2022)

IMPORTANT NOTICE AND DISCLAIMER

RENESAS ELECTRONICS CORPORATION AND ITS SUBSIDIARIES (“RENESAS”) PROVIDES TECHNICAL SPECIFICATIONS AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for developers skilled in the art designing with Renesas products. You are solely responsible for (1) selecting the appropriate products for your application, (2) designing, validating, and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, or other requirements. These resources are subject to change without notice. Renesas grants you permission to use these resources only for development of an application that uses Renesas products. Other reproduction or use of these resources is strictly prohibited. No license is granted to any other Renesas intellectual property or to any third party intellectual property. Renesas disclaims responsibility for, and you will fully indemnify Renesas and its representatives against, any claims, damages, costs, losses, or liabilities arising out of your use of these resources. Renesas' products are provided only subject to Renesas' Terms and Conditions of Sale or other applicable terms agreed to in writing. No use of any Renesas resources expands or otherwise alters any applicable warranties or warranty disclaimers for these products.

(Rev.1.0 Dec 2022)

Corporate Headquarters

TOYOSU FORESIA, 3-2-24 Toyosu, Koto-ku, Tokyo 135-0061, Japan
https://www.renesas.com

Contact Information

For further information on a product, technology, the most up-to-date version of a document, or your nearest sales office, please visit:
https://www.renesas.com/contact-us

Trademarks

Renesas and the Renesas logo are trademarks of Renesas Electronics Corporation. All trademarks and registered trademarks are the property of their respective owners.