EINPRESSWIRE

Soft Forum Proposes Hybrid PQC Cryptographic Products in the Age of Quantum Computers

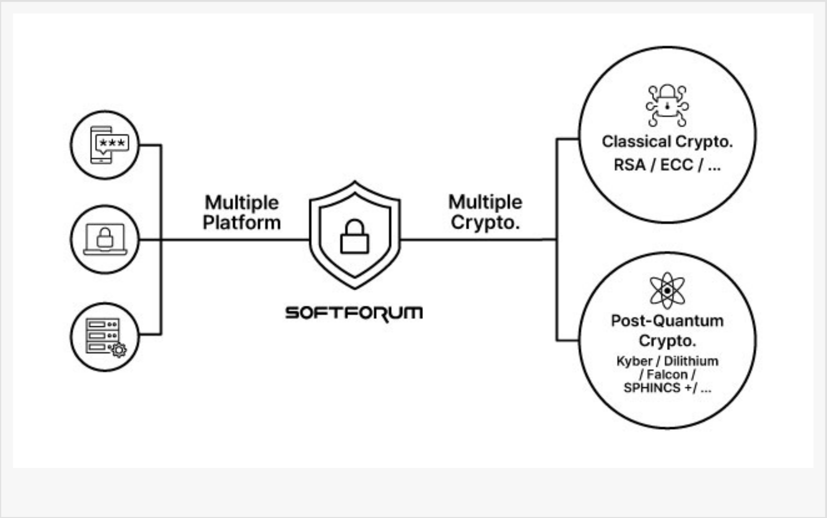
- The current security system can be breached by quantum computer technology
- Committed to preoccupying the next-generation security market with Hybrid PQC

SEOUL, SOUTH KOREA, April 28, 2023 /EINPresswire.com/ -- Security threats in the era of quantum computers have been discussed for 10 years. To this end, the government has started leading the construction of quantum resistant cryptography, and in the case of the United States, it has announced the application of quantum-resistant cryptography to the current security system from 2024 through the roadmap. Various quantum-resistant encryption solutions are being developed to support the current security system, preparing for the future quantum computer era.

Encryption is a basic tool of information security used to protect sensitive information from unauthorized access. It is essential for safeguarding sensitive data such as financial information, health records, and passwords. If the public-key cryptography currently used for such encryption is disabled, the safety is threatened leading to serious consequences.

Approximately 2,000 to 5, 000 units are expected to lead technological innovation in actual industrial sites by 2030, and contributions to finance, energy, pharmaceutical, and chemistry are expected to be significant. Besides these factors of technological innovation, significant risks to the digital economy and national security cannot be ruled out.

If Cryptanalytically Relevant Quantum Computer: CRQC capable of sophisticated cryptanalysis emerges, public key cryptography used in the current digital infrastructures can be decrypted. Direct risks may increase not only in the private sector, but also in communications, major infrastructure, control systems, financial transactions, Internet communications, and authentication in the government and military sectors.



The reason why we need to switch to hybrid quantum-resistant cryptography now

When applying encryption technology, most of the time, the use is classified in consideration of algorithm characteristics such as symmetric keys, public keys, and hash functions and used in combination. A typical combination is a combination of a symmetric key and a public key. Public key cryptography is used to share key information, and symmetric key cryptography with high speed is used for key renewal or message transmission. Moreover, cryptographic algorithms are used in combination with digital signatures, certificates, message authentication codes, and pseudorandom number generators. It is only a matter of time before hackers decrypt the current public key encrypted data if the CRQC emerges.

At the Davos World Economic Forum (WEF) 2022, IBM Chairman and CEO Arvind Krishna estimated that the capability of breaking today’s encryptions is possible in the range of 400-1000 qubits by these high-performance quantum computers.

Hybrid PQC applied products by Softforum

Hybrid PQC encryption products must support the adjustment of security strength based on the data information lifecycle. Furthermore, it is necessary to prepare the following encryption products currently proposed by Soft Forum to be linked to business systems.

- Field-proven hybrid encryption (Post Quantum Crypto)
- Non-face-to-face authentication encryption (Post Quantum Authentication)
- Structured/unstructured data encryption (Post Quantum Data Protection)
- Segment encryption (Post Quantum Network Data Protection)
- De-identification of personal information (Post Quantum Privacy Data Filter)

The common attribute of the quantum-resistant cryptography products by Softforum is that the products are Hybrid PQC which apply both to the current security system and the quantum computer era of the future. Softforum has earned 5 Golds in the 2023 Cybersecurity Excellence Awards and is recognized for its technological expansion worldwide.

In particular, Softforum cryptographic module is a module library that supports the latest quantum-resistant cryptographic algorithms, which can be applied to the next generation of cryptographic systems by supporting CRYSTALS-Kyber, CRYSTALS-Dilithium, Falcon, and SPHINCS+, the final winners of the Post Quantum Encryption Competition held by NIST, as well as the existing symmetric and asymmetric key cryptographic verification algorithms approved by national institutions. Consequently, both the current encryption system and the next-generation quantum-resistant encryption system can be selectively applied depending on the target system. Such versatility is an important factor that can be customized according to the characteristics of each company and played a major role in Softforum's selection as the Most Innovative Cybersecurity Company.

The scope of application of Softforum's Hybrid PQC products continues to expand. It has a wide range of products starting from the most widely used basic non-face-to-face authentication encryption to the products that provide robust security against various types of data encryption for unstructured data, including personal information such as images, voices, videos, logs, etc.

Moreover, privacy de-identification products that require automatic classification processing in real-time according to personal information detection and de-identification policy settings provide a cryptographic process for permission-based user management and access control for transparency and convenience.

Softforum Hybrid PQC product details

A. Non-face-to-face authentication encryption (Post Quantum Authentication)
Supports post-quantum-based storage of biometric information in compliance with the international standard FIDO and processes multi-step non-face-to-face verification based on various biometric authentications.
B. Structured/unstructured data encryption (Post Quantum Data Protection)
Provides strong security with a comparative advantage by using quantum-resistant encryption keys for structured/unstructured data including personal information such as images, voices, videos, and logos.
C. Segment encryption (Post Quantum Network Data Protection)
Hybrid algorithms for end-to-end segment encryption products enable strong encryption communication that is not broken even in the era of quantum computers.
D. De-identification of personal information (Post Quantum Privacy Data Filter)

Along with the de-identification of personal information using PQC, it supports history management, user management, and password access process.

About Softforum

Softforum is a company specializing in next-generation information security solutions in the PQC field and is rapidly emerging and highly evaluated in the global security market.

Softforum was recognized as the “Most Innovative Cybersecurity Company” of Asia in the 2023 Cybersecurity Excellence Awards.

Soyeun Kim
SoftForum Co., Ltd.
+82 1067392217
email us here