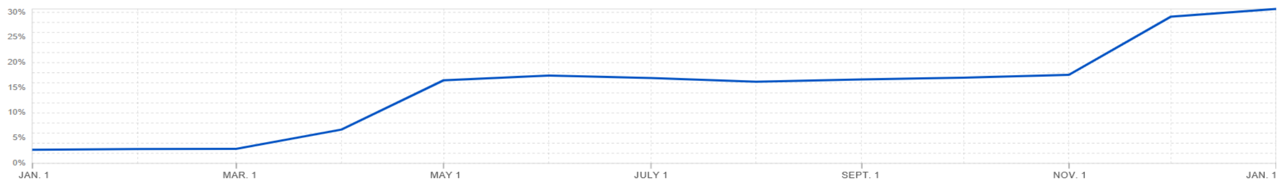
Post-quantum cryptography is here, the death of traditional cryptography is set

Cryptographic algorithms are essential for protecting confidential information from unauthorized access. For decades, both international and China cryptographic algorithms have proven to be strong enough to resist attacks using traditional computers to crack cryptographic algorithms. However, future quantum computing may break these algorithms in seconds, making data and information vulnerable. Fighting this future quantum capability requires new cryptographic algorithms that can protect data from attacks launched using current traditional computers and future quantum computers. These algorithms are called Post-Quantum Cryptography (PQC).

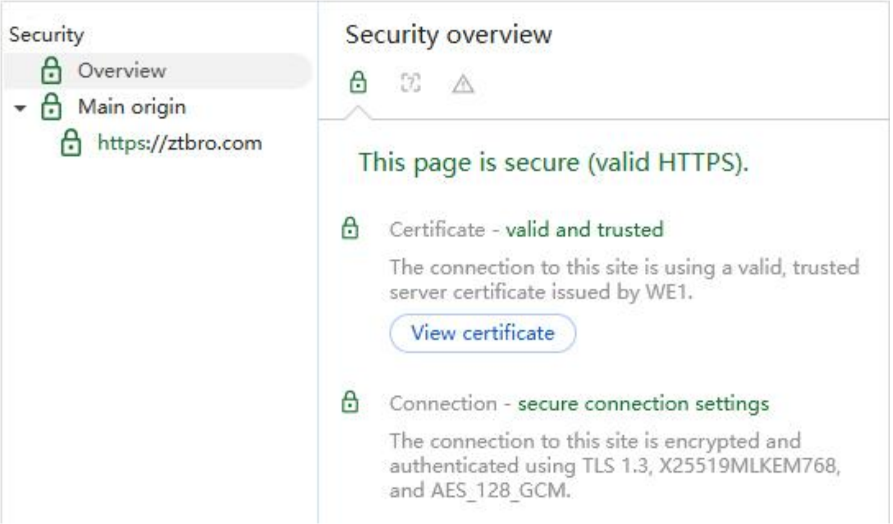
Although the transition to post-quantum cryptography began before the advent of quantum computers, there is still a pressing threat. Attackers collect encrypted data now with the intention of decrypting the data after quantum technology matures. This is the security threat of "harvest now, decrypt later". Because the value of many confidential data often lasts for many years, and some personal confidential data will accompany a person's life, it is crucial to start the transition to post-quantum cryptography now to prevent confidential data from being decrypted in the future. This threat model is one of the main reasons for the urgent transition to post-quantum cryptography.

1. Post-quantum cryptography is here, and it’s coming fast

According to Cloudflare's 2024 annual report, Cloudflare has enabled post-quantum cryptography algorithms by default on its service network since October 2022. After the Google Chrome 124 version released on April 17, 2024 enabled the post-quantum cryptographic protocol by default, PQC cryptographic algorithm traffic increased rapidly from slightly more than 2% of requests to around 12% within a month, and reached 13% at the end of November, and reached 30% on January 1, 2025. This is due to the upgrade of other Chromium-based browsers to version 124, coupled with the default support of Firefox and preliminary testing of Apple's Safari browser, which continues to rise.



This is what the title of this article means, "Post-quantum cryptography is here", and it is coming fast. The popularization and application of post-quantum cryptography in HTTPS encryption will effectively solve the security threat of "harvest now, decrypt later". You can use Google Chrome to check the security overview of ztbro.com, where the connection section shows: The connection to this site is encrypted and authenticated using TLS 1.3, X25519MLKEM768, and AES_128_GCM. This X25519+ MLKEM768 is a post-quantum cryptographic algorithm - a hybrid post-quantum key encapsulation algorithm, which is used for key encapsulation of asymmetric key algorithms, while the website deploys a traditional cryptographic ECC algorithm SSL certificate.



Security overview

This page is secure (valid HTTPS).

Certificate - valid and trusted

The connection to this site is using a valid, trusted server certificate issued by WE1.

Connection - secure connection settings

The connection to this site is encrypted and authenticated using TLS 1.3, X25519MLKEM768, and AES_128_GCM.

ML-KEM-768 is the Module Lattice-based Key Encapsulation Mechanism standard released by the National Institute of Standards and Technology (NIST) on August 13, 2024. It is one of a set of algorithms for key encapsulation mechanisms (KEM) that can be used by communicating parties to establish a shared key on a public channel. The shared key established using KEM can be used with symmetric key cryptographic algorithms to perform basic tasks in secure communications, such as encryption and authentication. The standard specifies a key encapsulation mechanism called ML-KEM. The security of ML-KEM is related to the computational difficulty of the Module Learning with Errors problem. Currently, ML-KEM is considered safe, even in the face of future quantum computers. The standard specifies three parameter sets, in order of increasing security strength and decreasing performance, namely ML-KEM-512, ML-KEM-768, and ML-KEM-1024.

2. **Traditional cryptographic algorithms are set to die, must prepare in advance**

In order to respond to the security threat of "harvest now, decrypt later", the NIST released a draft for public comments on NIST IR 8547 "Transition to Post-Quantum Cryptography Standards" on November 12, 2024. The report describes NIST's expected approach to transitioning from cryptographic algorithms vulnerable to quantum attacks to post-quantum digital signature algorithms and key establishment schemes. It identifies existing quantum-vulnerable cryptographic standards and the current quantum-resistant standards that will be used in the migration. This report informs the efforts and timelines of federal agencies, industry, and standards organizations for migrating information technology products, services, and infrastructure to PQC.

NIST released three PQC standards in August to begin the next important stage of the transition to post-quantum cryptography: FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism, which is the ML-KEM algorithm already in use, FIPS 204, Module-Lattice-Based Digital Signature Algorithm and FIPS 205, Stateless Hash-Based Signature Algorithm. NIST believes that it may take 10 to 20 years from algorithm standardization to full integration into information systems. This timeline reflects the complexity of the industry building algorithms into products and services, procuring these products and services, and integrating these products and services into technical infrastructure.

Once PQC algorithms are standardized, related applications will need to be modified to use them. Many applications include standardized protocols and security components that need to be modified to support the use of PQC algorithms. In addition, applications are built on software cryptographic libraries that either provide implementations of cryptographic algorithms or interfaces to hardware cryptographic modules (HSMs). These software cryptographic libraries and hardware cryptographic modules also need to be modified to support PQC algorithms. Applications may also rely on infrastructure components such as public key infrastructure (PKI), which also need to be updated to support PQC algorithms before applications can use PQC algorithms.

Among the three PQC standards, FIPS 204 and 205 are quantum-resistant digital signature algorithms, and FIPS 203 is a quantum-resistant key encapsulation algorithm. The existing digital signature algorithms ECDSA, RSA, EdDSA, and key encapsulation algorithms based on ECC and RSA algorithms are all easily cracked by quantum computers, but the existing symmetric encryption algorithms are not easily cracked by quantum computers.

That is to say, the existing network protocols and security technology standards based on RSA and ECC algorithms , such as Transport Layer Security (TLS) , Secure Sockets Layer (SSL), SSL VPN, Secure Shell (SSH), Internet Protocol Security (IPsec) and Cryptographic Message Syntax (CMS) , etc., all rely on traditional cryptographic algorithms that are vulnerable to quantum attacks and must be upgraded and updated to support the PQC algorithm , which is critical to maintaining data confidentiality and integrity.

The public key infrastructure (PKI) system, including the CA system, RA system, key management system, and directory service, must update PKI components to issue, distribute, and manage digital certificates using the PQC algorithm, and use the PQC algorithm to issue certificate revocation lists to ensure backward compatibility and interoperability during the transition period, which is critical to maintaining the trust and security of the global Internet.

IT applications and services cover a wide range of software and platforms used by organizations, including web applications, databases, communication tools, cloud services, and enterprise software. These applications rely on cryptographic techniques to protect data, authenticate users, and secure transactions. Applications and services must be modified to support the PQC algorithm for encryption, digital signatures, and key exchange. This requires updating the underlying cryptographic implementation, adapting to changes in key sizes and algorithm performance, and ensuring compatibility with updated protocols and libraries. Developers will need to refactor code, perform extensive testing, and potentially redesign user interfaces to accommodate these changes.

To this end, NIST has listed a timetable for transitioning to the PQC standard, with the goal of reducing quantum risks as much as possible by 2035. As shown in the table below, the currently widely used secure cryptographic algorithms RSA-2048 and ECC-256 will be Deprecated after 2030 and Disallowed after 2035. This is the death date of traditional cryptographic algorithms, requiring the industry to prepare for the migration of all related systems and products to the PQC algorithm in advance.

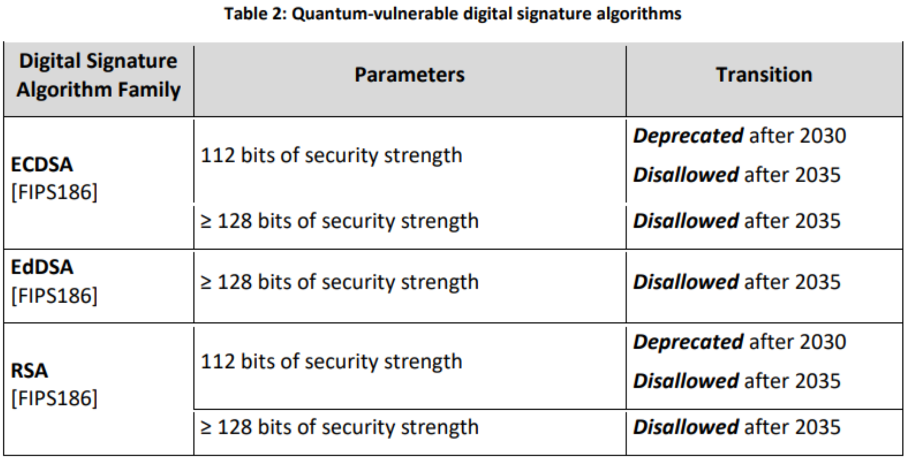


Table 2: Quantum-vulnerable digital signature algorithms

Digital Signature Algorithm Family	Parameters	Transition
ECDSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
EdDSA [FIPS186]	≥ 128 bits of security strength	***Disallowed*** after 2035
RSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035

3. China should release post-quantum commercial cryptography standards and PQC migration plans

The draft of the "Transition to Post-Quantum Cryptography Standards" released by NIST is currently in the public comment stage, with the deadline being this Friday (January 10, 2025). The purpose of writing this article on Monday is to hope that China cryptographic industry will attach great importance to the urgency of the impending death of this traditional cryptographic algorithm developed by the NIST, because China is vigorously promoting the popularization of commercial cryptographic algorithm SM2, which also belongs to the ECC-256 algorithm category, and is a similar algorithm that is planned to be deprecated after 2030 in the NIST report, and there are only 5 years left.

China must not only release post-quantum commercial cryptography standards as soon as possible, but also release an action plan for transitioning to post-quantum cryptography as soon as possible. Once China PQC commercial cryptography algorithm standards are determined, the relevant industry must take immediate action and start the PQC commercial cryptography algorithm migration work, because this migration work may take 10-20 years to complete. It is necessary to complete the PQC algorithm migration work of all related systems before quantum computers are available, and completely disable all traditional cryptographic algorithms. There is a long way to go.

Richard Wang

Jan. 6, 2025
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.
The author has published 84 articles in English (more than 109K words) and 200 articles in Chinese (more than 581K characters in total).