It's time for the mysterious cryptography to enter the public eye

November 3, 2025

The "cryptography" in this article refers to technology, products, and services that use specific transformation methods to encrypt and protect information, and to authenticate securely. It is extremely important because every second we spend online is protected by cryptography for data and network security, yet they are shrouded in mystery, invisible and intangible. ZT Browser globally unique innovation - displaying the cryptography algorithm used by the website in the address bar - brings this highly complex and mysterious technology into the public eye. This is crucial for popularizing the ongoing global technical revolution from traditional cryptographic algorithms to quantum-resistant cryptographic algorithms. ZT Browser's "visualization" bridges the gap between technological elites and public understanding. Only with public understanding and support can the global migration to post-quantum cryptography (PQC) be truly and rapidly completed.

1. Why does this mysterious cryptography need to be brought into the public eye now?

Since its inception, cryptography has been the unseen guardian of Internet security. From the early DES algorithm to today's AES, RSA, ECC, and SM2, confidential data uses complex mathematical transformations to ensure that it is not illegally stolen or tampered with during transmission and storage. However, this secrecy is a double-edged sword: users enjoy a secure online experience but are completely unaware of the underlying algorithms. This is particularly dangerous in the current era of quantum computing, as no one can guarantee that these cryptographic algorithms will withstand attacks from future quantum computers.

The rise of quantum computers will completely revolutionize traditional cryptography. Classical algorithm algorithms like RSA/ECC/SM2 rely on the computational difficulty of large number factorization or discrete logarithm problems, but quantum algorithms such as Shor's algorithm can break them in polynomial time. Therefore, attackers don't need immediate decryption capabilities, they can simply "harvest now, decrypt later" - data encrypted today can be easily cracked tomorrow in the quantum era. Consequently, top global cryptography experts and leading technology giants have acted

swiftly, adopting post-quantum cryptography algorithms based on existing TLS/SSL certificates to implement hybrid post-quantum cryptography HTTPS encryption. According to Cloudflare statistics on November 1st, 47% of global Internet traffic already uses hybrid PQC encryption, and the top eight of the world's ten largest Internet traffic websites support PQC HTTPS encryption. Government websites in the US, UK, and France etc., as well as banks in the US and Europe and top university websites, have also adopted PQC. But how can Internet users be informed about this rapid shift in cryptographic algorithms? Internet users have the right to know whether the websites they visit are "quantum-safe" because all their personal data are online now, and users have the right to know whether it is safe!

Unfortunately, popular browsers like Google Chrome and Microsoft Edge only display a simple Tune or padlock icon, claiming "connection is secure" without revealing the underlying algorithms. This makes PQC migration lack public motivation: website administrators are unwilling to invest, users are unaware of its benefits, and the entire ecosystem stagnates. The mysterious cryptography needs to be brought into the public eye; only by making technology transparent can we inspire public participation. Imagine if everyone could instantly tell whether a website uses quantum-resistant algorithms - this would drive faster website upgrades, creating a feedback mechanism from users to businesses. This is not only a technological revolution but also a science popularization revolution -bringing cryptography from behind the scenes to the forefront, making security common sense.

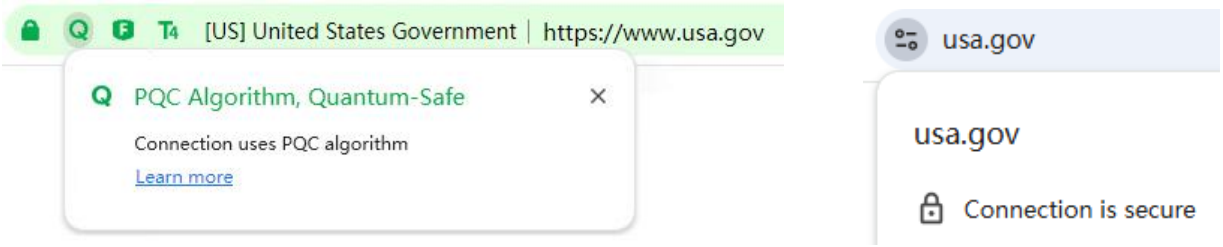
In other words, security should not be a magic trick hidden in a black box, but a transparent and verifiable public service. It requires a shift from a security paradigm of "trusting a specific provider" to one where "everyone can verify it". Therefore, cryptography must move from implicit protection to explicit security, and cryptographic technology must empower the public to protect public data security in a more open and transparent manner.

2. How did ZT Browser bring mysterious cryptography into the public eye?

ZT Browser, one of ZoTrus Technology's flagship products, adheres to the company's positioning as a "cryptographic technology provider based on zero trust principles". In its latest version 137, it features a globally unique and innovative address bar UI that visualizes the HTTPS encryption algorithm. This

isn't just a simple icon stacking; it's an intuitive design based on in-depth technical analysis, helping Internet users clearly understand at a glance whether each website connection is truly secure and what cryptographic algorithm is used to achieve that security. This embodies the "zero trust principle": don't trust the browser's claim of "connection is secure" but rather require the browser to simultaneously disclose the actual cryptographic algorithm used, allowing users to determine for themselves whether the connection is truly secure.

If a website supports PQC HTTPS encryption, a "**Q**" icon will appear after the padlock icon in ZT Browser address bar. Clicking the "**Q**" icon displays the messages "PQC algorithm, Quantum-Safe" and "Connection uses PQC algorithm", clearly informing the user that the website they are visiting guarantees the continued security of their data in the present and the quantum era, as shown in the left image below. This contrasts with other browsers that simply display "Connection is secure" as shown in the right image below. ZT Browser's ingenious UI design is a global first, allowing users to verify a website's resistance to quantum attacks without the need for specialized tools or cryptographic knowledge.



Furthermore, to comprehensively reveal the risks of traditional cryptographic algorithms, ZT Browser has added RSA algorithm (**R** icon) and ECC (**E** icon) algorithm to the existing SM2 algorithm (**m** icon). If a website uses the RSA algorithm (2048-bit key, which has been deprecated due to its inherent risks), it displays the "**R**" icon with a prompt: "RSA algorithm, Publicly Trusted, but does not support quantum-safe" suggesting the website migrate to PQC. If a website uses the ECC algorithm (256 bits key, highly efficient encryption, now the default hybrid PQC scheme), it displays the "**E**" icon with a prompt: "ECC algorithm, Publicly Trusted, but does not support quantum-safe" suggesting the website migrate to PQC. For the now commonly used hybrid PQC algorithm connection, it not only explicitly states "Quantum-Safe" but also indicates the traditional cryptographic algorithm used for website connection authentication (such as ECC/RSA/SM2). These icons are not only intuitive but also

integrate the website's trusted identity (**T**1/**T2**/**T3**/**T4**) and WAF protection (**F**) icons, forming a one-stop security dashboard that allows users to clearly see all the security protection measures adopted by the website.

ZT Browser, by modifying the underlying Chromium UI logic, abandons the vague default "security" label and explicitly emphasizes the urgency of migrating to PQC by informing users whether the current connection encryption uses traditional cryptographic algorithms or post-quantum cryptography. This UI innovation stems from ZoTrus' in-depth analysis of TLS/SSL certificates and TLS protocols, prioritizing the use of the PQC algorithm. This not only ensures the security of users' online browsing but also helps them naturally learn cryptographic knowledge while browsing the Internet, enhancing their online security capabilities.

3. Only after widespread popularization of PQC can the PQC migration be completed smoothly and quickly.

Post-quantum cryptography migration is not a solo act for technical elites, but a global project that requires consensus and action from all netizens. Currently, PQC standardization has been led by NIST in the United States, and algorithms such as Kyber and Dilithium have been integrated into OpenSSL, BoringSSL and TongsuoSSL. American and European countries have already rapidly started PQC migration, but developing countries such as China and all underdeveloped or less developed countries have not yet begun. This necessitates starting with popular science to truly bring the mysterious field of cryptography into the public eye.

ZT Browser's **Q** icon is a powerful tool for popularizing this knowledge. It transforms abstract cryptographic algorithms into visible symbols, driving a change in Internet user behavior: when users see "**Q**", they will proactively choose websites that ensure their data security in the quantum era; when they see "**R**/**E**/**m**", they will proactively report to website administrators, requesting support for post-quantum cryptography. Every Internet user can become a witness and participant in this PQC migration. When users can "**see**" quantum-safe, they will be more consciously "choosing" quantum- safe, thus forming a market force driving the global PQC migration. Similarly, other browsers should emulate this UI design. Global Internet users can accelerate the evolution of the PQC ecosystem by promoting

ZT Browser or advocating for standardization (such as adding PQC visual UI specifications to W3C proposals or pushing browsers to add PQC visual UI proposals in CA/browser Forum).

Only through widespread public education can resistance be overcome. Educating users to understand the security threats of "harvest now, decrypt later" can stimulate demand; allowing businesses to see user preferences can lead to investment in PQC. Ultimately, universal support will drive a seamless migration from traditional cryptography to quantum-resistant cryptography, ensuring the continued security of Internet data in the quantum era. ZT Browser takes this as its mission, acting as a bridge, connecting cryptography experts and the public, and connecting China with the world, through technological transparency. It calls on global developers, users, and regulators to work together to make the **Q** icon a standard feature in the address bar, allowing the cryptographic revolution to benefit everyone globally.

4. The USA and China PQC algorithms standard can serve as backups for each other, working together to ensure the security of global Internet.

The National Institute of Standards and Technology (NIST) of USA released three PQC algorithm standards in August 2024: (1) FIPS-203: It is based on Module Lattice-Based Key Encapsulation Mechanism (ML-KEM), which enables the generation of secure keys for data encryption (such as HTTPS). It is secure against quantum-enabled attacks. It includes ML-KEM-512, ML-KEM-768, and ML-KEM-1024. (2) FIPS-204: A digital signature algorithm based on Module-Lattice (ML-DSA), which uses Fiat-Shamir with Aborts to resist quantum attacks. Its key and signature sizes are moderate, and the signature is fast, and the signature validation is even faster. (3) FIPS-205: A hash-based digital signature algorithm (SLH-DSA) that uses HORST and W-OTS to resist quantum attacks and has the advantage of shorter public and private keys, although the signature is longer than ML-DSA. The most widely used PQC algorithm currently is the ML-KEM-768 algorithm, a hybrid PQC algorithm X22519MLKEM768 used for the HTTPS key exchange. This is a pioneering contribution of the US PQC standard to ensuring global Internet security, and it deserves high recognition.

The China National Institute of Commercial Cryptography Standards (NICCS) announced in October 2025 that it would officially begin accepting proposals for the Next Generation Commercial

Cryptography (NGCC), including public-key cryptographic algorithms, hash algorithms, and block cipher algorithms. This represents a new exploration building upon acquired research achievements in cryptography community, seeking to further stimulate innovation in cryptographic algorithm design and analysis techniques, to enhance the novelty and diversity of cryptographic algorithms (particularly post-quantum public-key cryptographic algorithms), to drive more international academic communications, and to promote the advancement of cryptography. NGCC expects to establish an interoperable cryptographic algorithm suit and facilitate the standardization of the next-generation commercial cryptographic algorithms. According to the "Cryptographic Algorithm Submission Requirements", the algorithms failed in other international standardization activities will not be excluded, but further innovations are expected. And NGCC explicitly does not accept proposals of the same or similar algorithms that have already been standardized by the US NIST.

Given that current post-quantum cryptographic algorithms are only theoretically resistant to quantum attacks and cannot be truly verified (since quantum computers capable of verifying algorithm reliability have not yet been developed), the author believes that to ensure global Internet security, the global Internet not only should quickly adopt the existing US-led PQC standard algorithm to secure global Internet, but also hopes that China-led PQC standard algorithm can be released as soon as possible and become one of the optional algorithms for ensuring global Internet security. Furthermore, the author calls on international organizations such as IANA, IETF, and CA/Browser Forum to actively support the inclusion of China traditional commercial cryptographic algorithms and next-generation commercial cryptographic algorithms (PQC algorithms) into relevant international standards, and to promptly assign relevant protocol numbers so that the Chinese PQC standard can be officially adopted in relevant protocols (such as TLS). This would allow the US-led PQC standard and the China-led PQC standard to serve as backups for each other, and both to be optional PQC algorithms for global Internet users, jointly contributing to the security of global Internet. This is because the threat of quantum computing to traditional cryptographic algorithms is a global and borderless threat, and there is only one Internet in the world.

Richard Wang

November 3, 2025
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.
The author has published 101 articles in English (more than 138K words) and 236 articles in Chinese (more than 701K characters in total).