# Dual hybrid PQC algorithm support is highly significant

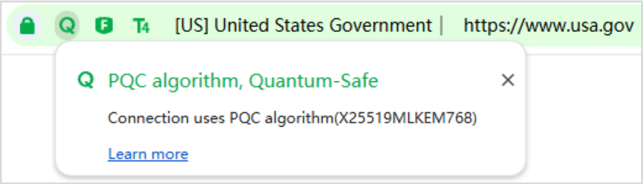
December 15, 2025

On December 12th, ZT Browser released an updated version, V2601, supporting the hybrid commercial cryptography algorithm and post-quantum cryptography algorithm - SM2MLKEM768. This comes less than a month after the Internet Assigned Numbers Authority (IANA) officially assigned TLS Supports Group code point 4590 to SM2MLKEM768 on November 14th, achieving full product support across ZoTrus product line. This is also just two months after ZT Browser released support for the hybrid ECC algorithm and PQC algorithm X25519MLKEM768 on October 11th. ZT Browser and ZoTrus HTTPS Automation Gateway now support both international standard post-quantum cryptography algorithms: X25519MLKEM768 and SM2MLKEM768. This fully demonstrates ZoTrus' exceptional cutting-edge cryptography product development capabilities, representing a significant achievement in China's quantum technology field. This article will discuss this major event in detail.

## 1. The PQC migration international solution is a widely adopted hybrid PQC algorithm - X25519MLKEM768.

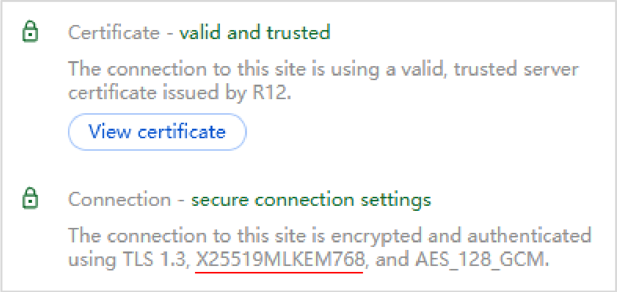
According to statistics released by Cloudflare Radar, as of today, 51% of global Internet traffic is encrypted using post-quantum cryptography HTTPS. This demonstrates that the global industry is rapidly adopting hybrid PQC algorithms to address the existing "harvest now, decrypt later" security threat, ensuring the continued security of this traffic data in the present and the quantum era. This rapid application solution uses the X25519MLKEM768 hybrid algorithm for key encapsulation in SSL certificates based on traditional ECC/RSA algorithms. This is a hybrid algorithm combining the traditional cryptographic algorithm X25519 and the post-quantum cryptographic algorithm MLKEM768. X25519 ensures current compatibility and speed, while MLKEM768 resists quantum attacks.

Users can check whether the website they are visiting supports X25519MLKEM768 using the browser's developer tools. Alternatively, they can use the ZT Browser to check if the address bar displays the "**Q** " icon. Clicking the "**Q**" icon will prompt "PQC algorithm, Quantum-Safe" and display that the PQC hybrid algorithm is X25519MLKEM768.



PQC algorithm, Quantum-Safe

Connection uses PQC algorithm(X25519MLKEM768)


Certificate - valid and trusted

The connection to this site is using a valid, trusted server certificate issued by R12.

Connection - secure connection settings

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

The implementation of this hybrid PQC algorithm technology has progressed very rapidly: On November 12, 2024, Google Chrome version 131 officially supported the use of the hybrid PQC algorithm X25519MLKEM768 in the TLS 1.3 protocol, and Microsoft Edge, Apple Safari, and Firefox browsers subsequently followed suit. On March 17, 2025, Cloudflare announced that it would provide free upgrades to support the hybrid PQC algorithm to all CDN users; on April 8, 2025, OpenSSL 3.5.0 natively supported the NIST released three PQC standards. Starting in August 2025, the US government websites, many government service systems and critical Internet infrastructures (such as important Internet services and online banking systems) have successively adopted X25519MLKEM768 for HTTPS encryption. European countries have also adopted it, and seven national portals in the G20 countries have adopted it, including the United States, the United Kingdom, France, Japan, Australia, Saudi Arabia, and Argentina. Famous universities in Europe and the United States, such as Oxford, Cambridge, and Berkeley, have also adopted it.

## 2. The current solution for migrating PQC in China is to widely apply the hybrid PQC algorithm - SM2MLKEM768.

China started relatively late in the field of post-quantum cryptography HTTPS encryption. Currently, no government website or e-government service system has adopted hybrid PQC algorithm HTTPS encryption, and no bank website or online banking system has used it. Only a few university websites, such as Tsinghua University, have adopted the international solution X25519MLKEM768. This may be related to the fact that China does not yet have its own post-quantum cryptography algorithm, and also to insufficient publicity regarding the importance of post-quantum cryptography migration. This is the main reason why the author has published more than a dozen articles related to post-quantum cryptography HTTPS encryption.

In fact, China cryptography industry has already taken action. Not only has the CACR held several academic conferences related to post-quantum cryptography, but most importantly, the industry has already taken concrete actions, mainly in following four things.

(1) The Tongsuo Cryptography Open-source Community drafted the RFC draft "Hybrid Post-quantum Key Exchange SM2-MLKEM for TLSv1.3" in January 2025, and in July 2025, TongsuoSSL open-source project implemented support for the SM2MLKEM768 hybrid PQC algorithm, which is a milestone achievement.

(2) ZT Browser began developing support for hybrid PQC algorithms in April 2025, and released version 137 in October 2025. It became the world's first browser to simultaneously support the commercial cryptography algorithm SM2 and the hybrid PQC algorithm X25519MLKEM768. It also innovatively added a post-quantum cryptography identifier "**Q**" after the padlock icon in the address bar, allowing users to know at a glance whether a website supports post-quantum cryptography.

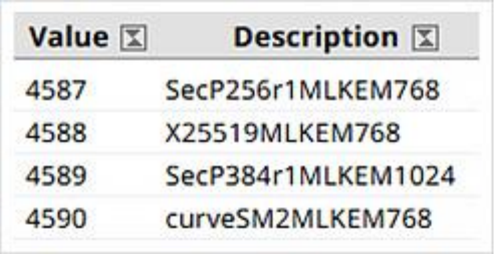
(3) In October 2025, ZT Browser, in conjunction with the Tongsuo Cryptography Open-source Community, applied to the international organization IANA for a TLS Supported Groups code point for the SM2MLKEM768 algorithm. This application was officially approved on November 14, 2025, assigning the number 4590. This signifies that the hybrid protocol of commercial cryptographic algorithms and post-quantum cryptographic algorithms launched by China cryptographic research team has gained recognition from an authoritative international standards organization and has officially become one of the four hybrid PQC protocols in the international standard TLS protocol group.

(4) December 12, 2025, ZT Browser and ZoTrus HTTPS Automation Gateway are the world's first and only browser and gateway to officially release upgraded versions supporting the SM2MLKEM768 algorithm for post-quantum cryptography HTTPS encryption.

With this, China now possesses a complete product line that can be practically applied, simultaneously supporting both the commercial cryptographic SM2 algorithm and the post-quantum cryptographic algorithm MLKEM768. This product can be used for the urgent commercial cryptographic HTTPS encryption transformation and post-quantum cryptographic migrations for Chinas critical information infrastructure systems. This is currently the best solution for PQC migration to HTTPS encryption in China. Once the China post-quantum cryptographic algorithm is officially released, only an algorithm upgrade will be needed to achieve the final PQC migration solution - a hybrid algorithm combining the SM2 algorithm and the China PQC algorithm.

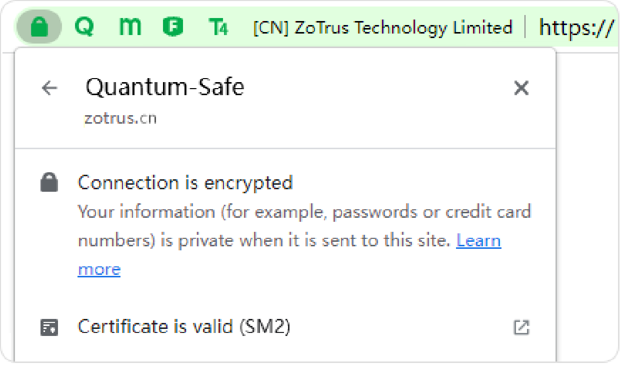
### 3. ZoTrus is the world's first to simultaneously support two hybrid PQC algorithms.

ZoTrus Technology released two product updates this time: ZT Browser has been upgraded to support SM2MLKEM768 with the previous support for X25519MLKEM768, and ZoTrus HTTPS Automation Gateway has also been upgraded to support it. This makes ZoTrus the only product and manufacturer in the world to support two of the four hybrid PQC algorithms approved by IANA.



| Value | Description |
|---|---|
| 4587 | SecP256r1MLKEM768 |
| 4588 | X25519MLKEM768 |
| 4589 | SecP384r1MLKEM1024 |
| 4590 | curveSM2MLKEM768 |

Users can use ZT Browser to visit ZoTrus official website, and click the padlock icon, the SSL certificate algorithm will be displayed using the SM2 algorithm, with an indicating "Quantum-Safe" as shown in the left figure below. Clicking the post-quantum cryptography "Q" icon will display "PQC algorithm, Quantum-Safe" along with "Connection uses PQC algorithm (SM2MLKEM768)," as shown in the right figure below.



[CN] ZoTrus Technology Limited | https://

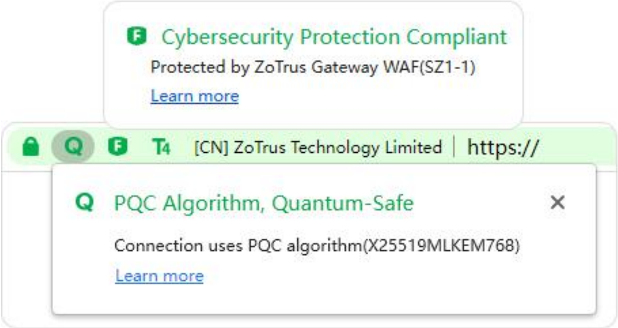
Quantum-Safe

zotrus.cn

Connection is encrypted

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Certificate is valid (SM2)



Cybersecurity Protection Compliant

Protected by ZoTrus Gateway WAF(SZ1-1)

Learn more

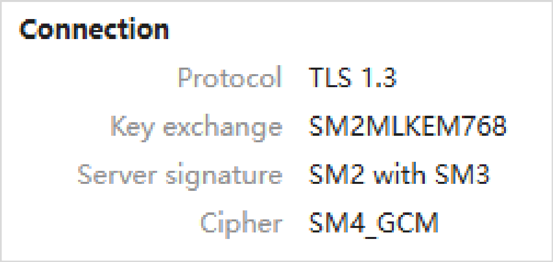
[CN] ZoTrus Technology Limited | https://

PQC Algorithm, Quantum-Safe

Connection uses PQC algorithm(X25519MLKEM768)

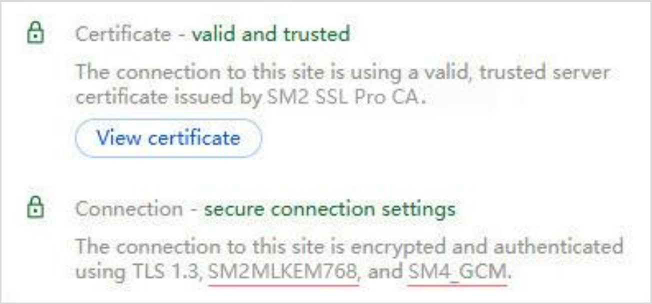
Learn more

Users can also use the developer tools in ZT Browser to view SSL certificate information and network connection information. As shown in the left figure below, the network security connection uses the TLS 1.3 protocol, the key exchange uses the SM2MLKEM768 algorithm, the server signature (SSL certificate) uses the SM2 with SM3 algorithms, and the Cipher algorithm uses SM4_GCM. The three algorithms required for HTTPS encryption are all commercial cryptographic algorithms. As shown in the right figure below, the SSL certificate is SM2 algorithm SSL certificate issued by Guizhou CA. This is a full-stack HTTPS encryption that implements both post-quantum cryptographic algorithms and commercial cryptographic algorithms. As shown in the above right figure, clicking the WAF protection icon "**F**" will display "Protected by ZoTrus Gateway WAF ( )". This also proves that it is the close cooperation between ZoTrus Gateway and ZT Browser that seamlessly achieves the deployment of SM2 algorithm SSL certificate but implements a hybrid PQC algorithm key exchange of SM2 algorithm and PQC algorithm MLKEM768. This is a double achievement, simultaneously completing the post-quantum cryptography migration and commercial cryptographic transformation.



**Connection**

| | |
|---|---|
| Protocol | TLS 1.3 |
| Key exchange | SM2MLKEM768 |
| Server signature | SM2 with SM3 |
| Cipher | SM4_GCM |



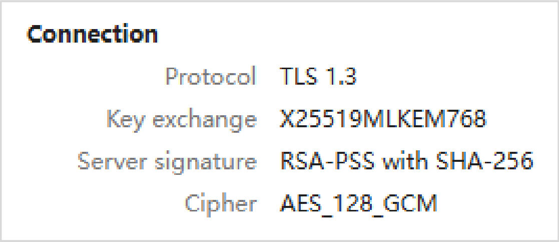
Certificate - valid and trusted

The connection to this site is using a valid, trusted server certificate issued by SM2 SSL Pro CA.

Connection - secure connection settings

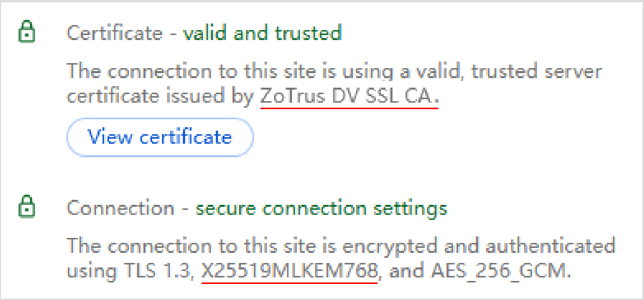
The connection to this site is encrypted and authenticated using TLS 1.3, SM2MLKEM768, and SM4_GCM.

If users use Google Chrome to visit ZoTrus official website, HTTPS encryption is implemented using an RSA/ECC algorithm SSL certificate, as shown in the below left figure of Server signature. Using developer tools, the network connection uses the TLS 1.3 protocol, X25519MLKEM768 key exchange, and AES_128_GCM encryption, as shown in the below right figure. This fully demonstrates that the ZoTrus HTTPS Automation Gateway simultaneously supports both hybrid PQC algorithm - X25519MLKEM768 and SM2MLKEM768 that IANA assigned code point as 4588 and 4590.



**Connection**

| | |
|---|---|
| Protocol | TLS 1.3 |
| Key exchange | X25519MLKEM768 |
| Server signature | RSA-PSS with SHA-256 |
| Cipher | AES_128_GCM |



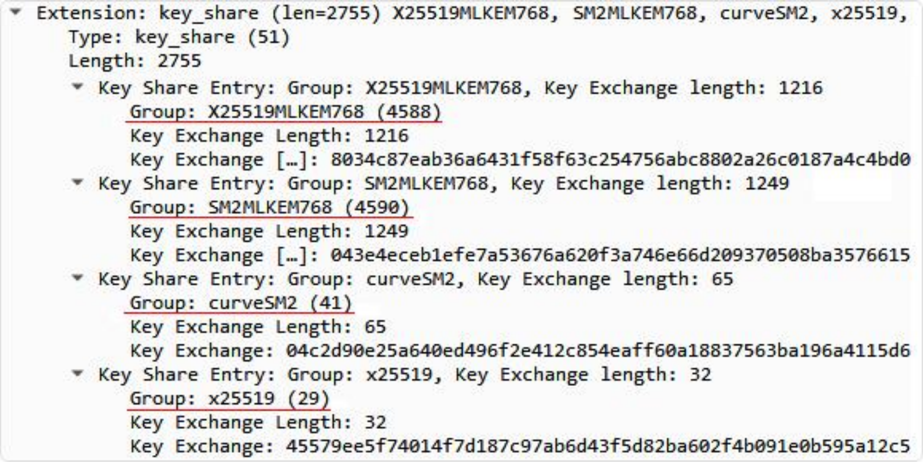
Certificate - valid and trusted

The connection to this site is using a valid, trusted server certificate issued by ZoTrus DV SSL CA.

Connection - secure connection settings

The connection to this site is encrypted and authenticated using TLS 1.3, X25519MLKEM768, and AES_256_GCM.

Of course, users can also use ZT Browser to access other websites that support X25519MLKEM768 algorithm to verify that ZT Browser supports both the X25519MLKEM768 and SM2MLKEM768. ZT Browser prioritizes the SM2MLKEM768 algorithm, if a website only supports X25519MLKEM768, ZT Browser uses the X25519MLKEM768 algorithm to implement HTTPS encryption. And IT engineers can use packet capture software, shown in the figure below, that ZT Browser supports both commonly used traditional cryptographic algorithms (X25519, SM2) and two hybrid PQC algorithms (X25519MLKEM768, SM2MLKEM768).



```
▾ Extension: key_share (len=2755) X25519MLKEM768, SM2MLKEM768, curveSM2, x25519,
    Type: key_share (51)
    Length: 2755
  ▾ Key Share Entry: Group: X25519MLKEM768, Key Exchange length: 1216
      Group: X25519MLKEM768 (4588)
      Key Exchange Length: 1216
      Key Exchange […]: 8034c87eab36a6431f58f63c254756abc8802a26c0187a4c4bd0
  ▾ Key Share Entry: Group: SM2MLKEM768, Key Exchange length: 1249
      Group: SM2MLKEM768 (4590)
      Key Exchange Length: 1249
      Key Exchange […]: 043e4eceb1efe7a53676a620f3a746e66d209370508ba3576615
  ▾ Key Share Entry: Group: curveSM2, Key Exchange length: 65
      Group: curveSM2 (41)
      Key Exchange Length: 65
      Key Exchange: 04c2d90e25a640ed496f2e412c854eaff60a18837563ba196a4115d6
  ▾ Key Share Entry: Group: x25519, Key Exchange length: 32
      Group: x25519 (29)
      Key Exchange Length: 32
      Key Exchange: 45579ee5f74014f7d187c97ab6d43f5d82ba602f4b091e0b595a12c5
```

## 4. The China plan for hybrid PQC algorithms is not only China's, but also the world's.

The above section discussed in detail the international post-quantum cryptography migration scheme and the current China scheme. This separation is for ease of explanation. Since SM2MLKEM768 is one of the four hybrid PQC algorithm options listed by IANA, both solutions are actually available to worldwide users. However, the X25519MLKEM768 scheme was the first proposed and has gained support from common browsers and open-source cryptographic components such as OpenSSL. This allows cloud service providers like Cloudflare and Amazon to provide support, resulting in 51% of global HTTPS encrypted traffic using the X25519MLKEM768 algorithm for quantum resistance protection, although this algorithm is currently still in the RFC draft stage.

The X25519MLKEM768 algorithm RFC draft was proposed in August 2024 and officially became a draft of the TLS working group in March 2025, with the expected RFC standard status being Proposed Standard. The SM2MLKEM768 algorithm has not yet officially become a draft of the TLS working group, and the only driving force for this standardization process is the widespread deployment and use of the SM2MLKEM768 algorithm, just like the X25519MLKEM768 algorithm. This force can first come from the widespread deployment and use by browsers, network security companies, cryptography companies, and internet giants in China. The two core product upgrades released by ZoTrus Technology this time prove that the SM2MLKEM768 algorithm is feasible, browsers support it, and SSL gateways support it. The author would like to once again thank the TongsuoSSL open-source community for its open-source contributions.

As we stated when applying to IANA for the TLS Supported Groups code point for the SM2MLKEM768 algorithm, the global Internet TLS ecosystem needs multiple algorithms to provide better resilience and more options, because no one can guarantee that traditional cryptographic algorithms and post-quantum cryptographic algorithms will be secure in the face of future quantum computers. More choices mean more security. This view has also been supported by ZoTrus' Hong Kong partners, even though the SM2 algorithm is not mandatory in Hong Kong SAR.

For a more secure global Internet in the future, the author urges the global industry to take action together, supporting both hybrid PQC algorithm - X25519MLKEM768 and SM2MLKEM768, to provide better resilience and security for global Internet traffic, because there is only one Internet in the world, and all stockholders should work together to build a global Internet security community with a shared future.

Richard Wang

**December 15, 2025**
**In Shenzhen, China**

Follow ZT Browser at X (Twitter) for more info.
The author has published 105 articles in English (more than 142K words)
and 244 articles in Chinese (more than 723K characters in total).