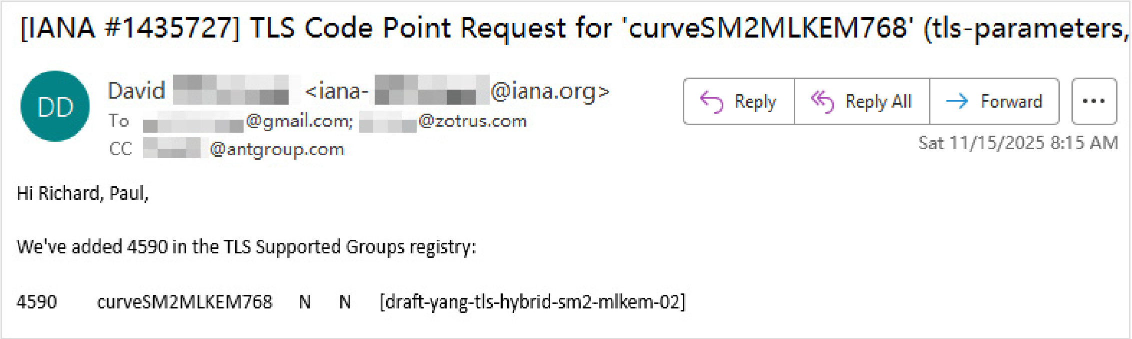
Interpreting SM2MLKEM768 = 4590

November 17, 2025

This is a significant event that occurred on Saturday morning – the IANA (Internet Assigned Numbers Authority) officially assigned the post-quantum cryptography hybrid protocol number - 4590 to the China cryptography research team. This signifies that the China commercial cryptography and post-quantum cryptography hybrid protocol developed by the Chinese cryptography research team has gained recognition from authoritative international standards organizations and has officially become one of the post-quantum cryptography hybrid protocols in the TLS protocol group. This is a big event concerning the security of global internet data in the quantum era; it deserves to be discussed in detail in an article. Even more significant is that this was a friendly interaction and mutual support action between the Chinese and American scientific communities in the development of international TLS standards, worthy of being documented.



[IANA #1435727] TLS Code Point Request for 'curveSM2MLKEM768' (tls-parameters,

David [redacted] <iana-[redacted]@iana.org>
To [redacted]@gmail.com; [redacted]@zotrus.com
CC [redacted] @antgroup.com

Sat 11/15/2025 8:15 AM

Hi Richard, Paul,

We've added 4590 in the TLS Supported Groups registry:

4590 curveSM2MLKEM768 N N [draft-yang-tls-hybrid-sm2-mlkem-02]

1. What is curveSM2MLKEM768?

The SM2 algorithm is an elliptic curve cryptography algorithm developed in China. It belongs to the same class of algorithms as the international standard algorithms ECC and X25519, differing only in curve parameters. MLKEM is a post-quantum cryptography algorithm - FIPS 203 - developed by NIST in the United States. Based on a modular lattice key encapsulation mechanism, it can generate secure keys for data encryption that are resistant to quantum attacks. It is available in three key lengths: MLKEM-512, MLKEM-768, and MLKEM-1024, with MLKEM-768 being the most commonly used. The global Internet is facing a "harvest now, decrypt later" security threat. This means attackers are now collecting encrypted Internet data, which they can then decrypt once quantum computers are available. Therefore, the global internet and cryptography industries have acted swiftly. Since August, government websites in the US and Europe, online banking systems, university websites, and major high-traffic websites have all adopted post-quantum cryptography HTTPS encryption. This encryption method still uses SSL certificates issued with traditional cryptographic algorithms, but the key encapsulation employs both the traditional cryptographic algorithm X25519 and the post-quantum cryptographic algorithm MLKEM768. This is the hybrid algorithm - X25519MLKEM768. The hybrid algorithm design provides "double insurance": X25519 ensures current compatibility and speed, while MLKEM768 resists quantum attacks, ensuring the continued security of confidential data in the present and the quantum era.

China is rapidly implementing SM2 algorithm HTTPS encryption migration. However, even with all systems migrated, the security of confidential data in the quantum era remains unsecure. Furthermore, China's post-quantum cryptographic algorithm has yet to be released. What can be done? Alibaba's Tongsuo SSL, referencing the international standard algorithm X25519MLKEM768, has successfully developed and integrated a commercial cryptographic post-quantum cryptographic hybrid algorithm - SM2MLKEM768, and proposed an RFC draft. This is a hybrid algorithm combining the traditional cryptographic algorithm SM2 and the post-quantum cryptography MLKEM768. It can also be used for key encapsulation in the HTTPS encrypted handshake process based on traditional cryptographic algorithm SSL certificates, thus achieving HTTPS encryption using a hybrid SM2 + PQC algorithm.
Readers should now understand what "curveSM2MLKEM768" is. It is a hybrid algorithm of SM2 and MLKEM768, used in the key exchange process for HTTPS encryption, just like X25519MLKEM768. It simultaneously meets the two urgent compliance and security requirements of China commercial cryptography transformation and post-quantum cryptography migration, making it the best solution at present.

2. What is 4590?

This requires a basic explanation of the TLS parameter registry.
In the digital age of the internet, our daily browsing, shopping, and chatting all rely on an invisible "shield" - Transport Layer Security (TLS). It acts like an "encrypted courier" in the digital world,

ensuring your data is not spied on or tampered with during transmission. TLS's predecessor was SSL (Secure Sockets Layer), and it is now standard on HTTPS websites. However, for TLS to work smoothly across countless devices globally, a unified "rulebook" is needed - TLS Parameter Registry, maintained by IANA, this registry records various key codes and identifiers in the TLS protocol, much like traffic lights, ensuring everyone "speaks the same language." Why are these TLS parameters necessary? Simply put, the Internet is open, if lacks a unified standard, allowing developers to work independently, leading to compatibility issues or security vulnerabilities. These parameters are set to achieve interoperability (seamless collaboration between different systems) and security (preventing the abuse of weak algorithms). What are their uses? From the handshake to establish a connection, to encrypted data transmission, and error handling, these parameters are indispensable.

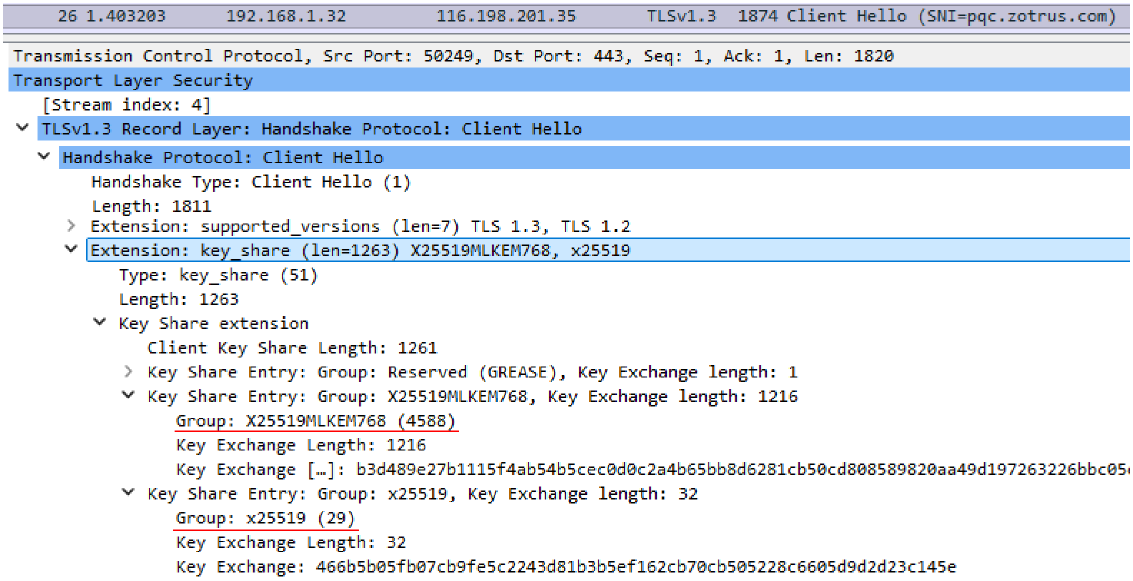
The most prominent parameter in the TLS protocol is the TLS Cipher Suites, the "recipe" for encryption. It defines the specific "recipe" for encrypted communication: the algorithm used for key exchange, the symmetric cipher for data encryption, and the hash function for integrity verification. The registry lists hundreds of suites, ranging from the old, disabled "TLS_RSA_WITH_RC4_128_MD5" (value 0x0004) to modern "TLS_AES_128_GCM_SHA256" (value 0x1301). Why are these parameters set? Because encryption algorithms are constantly evolving, and early algorithms like MD5 have been proven insecure (easily cracked). Therefore, IANA standardizes them through expert review, marking them as "Recommended" (Y), "Not Recommended" (N), or "Deprecated" (D) to prevent developers from misusing weak cipher suites. This ensures the bottom line of security for TLS encryption implementations worldwide. What is its purpose? When a browser accesses a website, the browser and server negotiate a cipher suite via the "ClientHello" message. If the negotiation fails, a secure connection cannot be established.

The second important parameter is the TLS Supported Groups, which specify the mathematical "cornerstone" of key exchange, such as x25519 (No. 29, the recommended curve) or ffdhe2048 (No. 256, the Diffie-Hellman group). Why set these parameters? To lock in the security algorithm. What is its purpose? In modern TLS encryption, it's used for "forward secrecy" (old sessions are secure even if the server key is compromised).

Let's focus on the new IANA support group numbers for post -quantum cryptography algorithm: 512

/ 513 / 514, which correspond to MLKEM512 / MLKEM768 /MLKEM1024 respectively. No. 4587 / 4588 / 4589 represent three hybrid protocols of the traditional elliptic curve cryptography algorithm and the post-quantum cryptography algorithm ML-KEM: SecP256r1MLKEM768 / X25519MLKEM768 / SecP384r1MLKEM1024. The IANA has added entries for post -quantum cryptography to the TLS supported group registry is for implementing hybrid post-quantum cryptography HTTPS encryption. And the commonly used is X25519MLKEM768, numbered 4588, avoids implementation conflicts through IANA standardization. Marked as "Not Recommended" (N), it is still in the experimental stage, but early adoption is encouraged to promote ecosystem migration. What are its uses? In TLS 1.3 HTTPS connections, the client proposes 4588 through the "supported_groups" extension. If the server supports it, a hybrid key is generated during the key-sharing phase: a shared key based on X25519 and a quantum-safe shared key based on ML-KEM. This prevents attackers from decrypting historical sessions using a quantum computer even if they steal the server's encryption key (enhanced forward secrecy). This has become the mainstream solution and de facto standard for browsers. 47% of global Internet traffic already use hybrid post-quantum cryptography HTTPS encryption, ensuring that online privacy data can withstand the "future quantum attack".

Currently, the X25519MLKEM768 protocol, supported by the four major browsers (Google Chrome, Microsoft Edge, etc.) and ZT Browser, can be discovered through packet capture, as shown in the figure below. It can be seen that the hybrid quantum cryptography algorithm X25519MLKEM768 is numbered 4588, while the traditional cryptography algorithm X25519 is numbered 29.



```
   26 1.403203       192.168.1.32          116.198.201.35        TLSv1.3   1874 Client Hello (SNI=pqc.zotrus.com)

Transmission Control Protocol, Src Port: 50249, Dst Port: 443, Seq: 1, Ack: 1, Len: 1820
Transport Layer Security
    [Stream index: 4]
  ⌄ TLSv1.3 Record Layer: Handshake Protocol: Client Hello
    ⌄ Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 1811
      › Extension: supported_versions (len=7) TLS 1.3, TLS 1.2
      ⌄ Extension: key_share (len=1263) X25519MLKEM768, x25519
          Type: key_share (51)
          Length: 1263
        ⌄ Key Share extension
            Client Key Share Length: 1261
          › Key Share Entry: Group: Reserved (GREASE), Key Exchange length: 1
          ⌄ Key Share Entry: Group: X25519MLKEM768, Key Exchange length: 1216
              Group: X25519MLKEM768 (4588)
              Key Exchange Length: 1216
              Key Exchange […]: b3d489e27b1115f4ab54b5cec0d0c2a4b65bb8d6281cb50cd808589820aa49d197263226bbc05
          ⌄ Key Share Entry: Group: x25519, Key Exchange length: 32
              Group: x25519 (29)
              Key Exchange Length: 32
              Key Exchange: 466b5b05fb07cb9fe5c2243d81b3b5ef162cb70cb505228c6605d9d2d23c145e
```

4590 is the IANA approval number for the post-quantum cryptography supported group protocol - curveSM2MLKEM768**.** With this number, the hybrid PQC algorithm SM2MLKEM768, which combines China commercial cryptographic algorithms with post-quantum cryptography, as explained above, truly becomes a usable protocol. In other words, it officially becomes a globally recognizable traffic light, providing a feasible implementation foundation for China to implement HTTPS encryption using a hybrid algorithm of commercial cryptography and post-quantum cryptography based on SM2 algorithm SSL certificates. It also paves the way for the global adoption of TLS 1.3 and post-quantum cryptography algorithms in China's ongoing development of the Transport Layer Cryptography Protocol (TLCP) 2.0.

3. Additional information on RFC 8998 and related IANA numbers.

RFC 8998 was a significant achievement for Alibaba TongsuoSSL in August 2019, but it wasn't until March 2021 that it received official approval from the International Engineering Task Force (IETF) and was assigned the RFC serial number – RFC 8998: ShangMi (SM) Cipher Suites for TLS 1.3. This standard enables commercial cryptographic HTTPS encryption to be implemented using the advanced TLS 1.3 protocol. Why is TLS 1.3 needed? Because TLS 1.3 not only disables insecure static RSA key exchange and supports forward secrecy, but more importantly, its design mechanism follows the principle of "Crypto Agility", providing a foundation for subsequent post-quantum cryptographic algorithms and protocols. Therefore, commercial cryptographic HTTPS encryption must support TLS 1.3. The establishment of RFC 8998 means that the SM2 algorithm has become one of the algorithms supported by the international TLS 1.3 standard, which is the important significance of RFC 8998.

Another important contribution of RFC 8998 is obtaining the IANA-assigned TLS cipher suite numbers for two commercial cryptographic algorithms: TLS_SM4_GCM_SM3 (Value 0x00C6), TLS_SM4_CCM_SM3 (Value 0x00C7), a TLS signature scheme number: sm2sig_sm3 (Value 0x0708), and another is the TLS supported group number for the SM2 algorithm: 41 (curveSM2), which is the same type protocol number as the 4590 allocated this time, used for key exchange. These three numbers enable the TLS 1.3 international standard to truly support the SM2 algorithm to implement HTTPS encryption and lay the standard foundation for the internationalization of China post-quantum cryptography algorithm.

Currently, 360 Browser already supports HTTPS encryption based on the RFC 8998 standard. ZT Browser will also support RFC 8998 while supporting the hybrid PQC algorithm SM2MLKEM768. This is because only commercial cryptographic algorithms that implement RFC 8998 and support TLS 1.3 can achieve HTTPS encryption using the hybrid PQC algorithm SM2MLKEM768.

4. There is great potential for cooperation between the US and China technology communities in the development of TLS standards.

The successful inclusion of the "Chinese solution" to post-quantum cryptography into the international standards system not only demonstrates that the Chinese cryptography community can keep up with cutting-edge international technologies, but it also possesses the capability for original innovation and participation in the formulation of international standards and specifications. This success is a result of multi-party collaboration across related industries: the TongsuoSSL community proposed and drafted the IETF draft of SM2MLKEM768; TongsuoSSL implemented a hybrid key exchange mechanism combining China commercial cryptographic algorithms and American post-quantum cryptographic algorithms according to the draft; and ZT Browser was the first to support this hybrid mechanism for HTTPS encryption using a hybrid algorithm combining commercial cryptography and post-quantum cryptography. This provided a practical application scenario and real standard requirements for the draft standard, which was crucial for passing the IANA expert review, as a standard without practical application needs is worthless. This close collaboration between "open-source cryptography libraries + industrial applications" is a model of how technological innovation ultimately generates value.

More importantly, in our application materials, we emphasized the importance of Sino-US cryptographic algorithms, especially post-quantum cryptography algorithms, serving as backups for each other, from the perspective of safeguarding global internet security. This is because no one can guarantee that post-quantum cryptography algorithms are truly quantum-resistant; current perceptions of security are only theoretical, and no quantum computer can yet be used to verify the security of these algorithms. Therefore, global internet security not only requires US-led post-quantum cryptography algorithms but also a "China solution" to provide valuable technological diversity and more options for global Internet security, greatly enhancing the resilience and security of the global Internet TLS ecosystem, since there is only one Internet in one world. We believe it was this solution, proposed from the perspective of safeguarding global internet security, that impressed the INAN review experts, allowing the "China solution" to successfully become one of the optional solutions for ensuring the security of global Internet TLS traffic. The Sino-US scientific communities have made significant strides in cooperation on TLS standards development.

Richard Wang

November 17, 2025
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.
The author has published 102 articles in English (more than 139K words)
and 238 articles in Chinese (more than 709K characters in total).