IETF 125 Shenzhen 深圳

14 Mar 2026 - 20 Mar 2026

Hybrid Post-Quantum Key Exchange: SM2-MLKEM for TLS 1.3
TLS 1.3商密SM混合PQC RFC草案

Richard Wang 王高华

ZoTrus Technology Limited 零信技术（深圳）有限公司

2026.03.16 11:15-12:15

Agenda

- Introduction & draft status
- Regulatory & quantum threat context (esp. China)
- Why hybrid SM2 + ML-KEM-768?
- Technical specification & design
- IANA assignment & comparison to other hybrids
- Production implementations & ecosystem
- Interoperability & deployment examples
- Security & considerations
- Benefits for global TLS ecosystem
- Next steps & requests to WG
- Q&A

Introduction & Draft Status

- Individual submission: draft-yang-tls-hybrid-sm2-mlkem
- Latest: -03 (published ~November 2025)
- Authors: Paul Yang (Lenovo), etc.
- Defines hybrid key exchange combining CurveSM2 (classic) + ML-KEM-768 (PQ, FIPS 203) for TLS 1.3
- Goal: Regulatory compliance in China + quantum resistance
- Status: Active individual draft, IANA code point assigned
- Seeking: Community feedback, path to Informational or Experimental RFC, discussion on potential TLS WG adoption

Context – China Cryptography Law & Quantum Threat

- China’s Cryptography Law (《密码法》)(effective 2020, enforced for SM2 algorithm HTTPS):
- Mandates SM2 / SM3 / SM4 for classified & critical info infrastructure systems
- Many government, finance, enterprise HTTPS must use SM2 SSL certificate & key exchange
- Quantum computing risk: Harvest-now-decrypt-later attacks threaten long-term confidentiality
- Pure ML-KEM or X25519MLKEM not compliant in regulated sectors → need SM2-inclusive hybrid
- Affects large fraction of Chinese Internet traffic → impacts global routing & CDNs

Why SM2-MLKEM Hybrid?

- Only compliant PQ option for China-regulated traffic
- SM2 (classic) satisfies law today
- ML-KEM-768 adds quantum resistance (level ~ AES-192)
- Cryptographic diversity for the single global Internet
- Complements X25519MLKEM768 (4588), etc.
- Reduces monoculture risk if one curve/KEM family weakened
- Follows established hybrid framework (draft-ietf-tls-hybrid-design)
- Reuses massive existing SM2 deployment (certs, HSMs, libraries in China)
- Reference: RFC8998: ShangMi (SM) Cipher Suites for TLS 1.3

Technical Design – Hybrid Construction

- Concatenation-based hybrid (per hybrid-design draft):
  - Classical: SM2 key exchange (ephemeral, curveSM2)
  - PQ: ML-KEM-768 encapsulation
  - Shared secret = SM2 shared || ML-KEM shared (concat) → input to TLS 1.3 key schedule
- No protocol changes beyond new NamedGroup
- Wire format: Standard TLS 1.3 key_share extension
- Public keys & ciphertexts concatenated in ClientHello/ServerHello

```
ClientHello
  supported_groups incl. 4590
  key_share(4590): SM2_pub || ML-KEM-768_pk
        ↓
ServerHello
  selected: 4590
  key_share(4590): SM2_pub || ML-KEM-768_ct
        ↓
Hybrid Key Exchange:
  SM2_DH(ss_classical)  ||  ML-KEM-768(ss_pq)
        ↓
concatenated_secret = ss_classical || ss_pq
        ↓
HKDF-Extract(concatenated_secret, salt=...)
        ↓
TLS 1.3 key schedule → traffic keys
```

IANA Assignment & Comparison Table

IANA TLS Supported Groups assignment (Nov 2025): Value: **4590** (0x11EE)

Name: curveSM2MLKEM768

DTLS-OK: No | Recommended: No (experimental, encourage adoption)

Reference: this draft

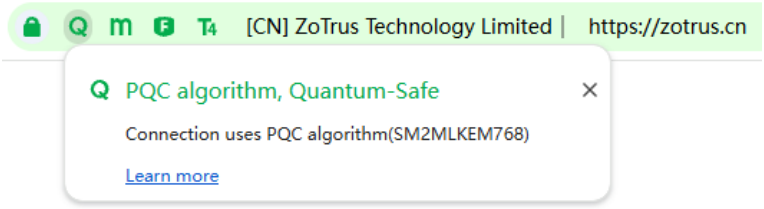
Value	Name	Classical	PQ	Level	Use Case / Notes
4587	SecP256r1MLKEM768	NIST P-256	ML-KEM-768	~192 bit	General purpose
4588	X25519MLKEM768	X25519	ML-KEM-768	~192 bit	Widely deployed (browsers)
4590	curveSM2MLKEM768	SM2	ML-KEM-768	~192 bit	China compliance + diversity

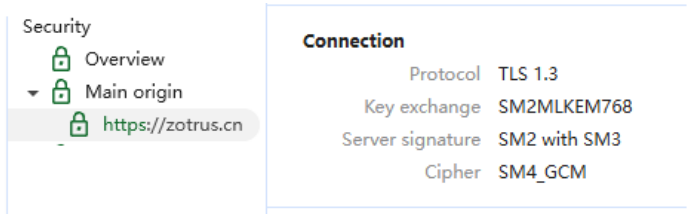
Ecosystem – Server Side

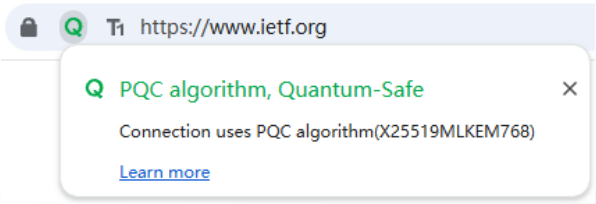
- TongsuoSSL (Alibaba-led OpenSSL branch, widely used in China):
- Supports SM2DH-MLKEM768-hybrid (aligned with draft)
- Compile flags: enable-kyber enable-sm2dh-mlkem768-hybrid
- Command line: -groups SM2DH_MLKEM768_HYBRID
- Production deployments (Alibaba Cloud, etc.)
- Emerging OpenSSL issues 1855: Draft support for RFC8998 curveSM2 + hybrid

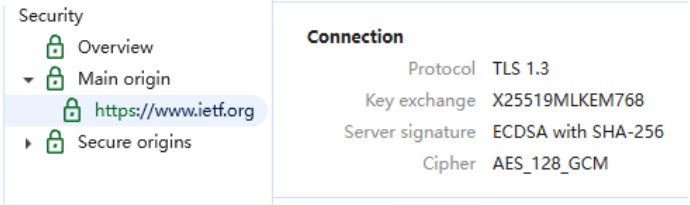
Ecosystem – Client Side (ZT Browser)

- ZT Browser (零信浏览器, by ZoTrus Technology 零信技术):
  - Dual hybrid support: X25519MLKEM768 and SM2MLKEM768
  - Visual indicator: "Q" icon in address bar for PQ connections
  - Shows which hybrid used (helps users/admins verify)







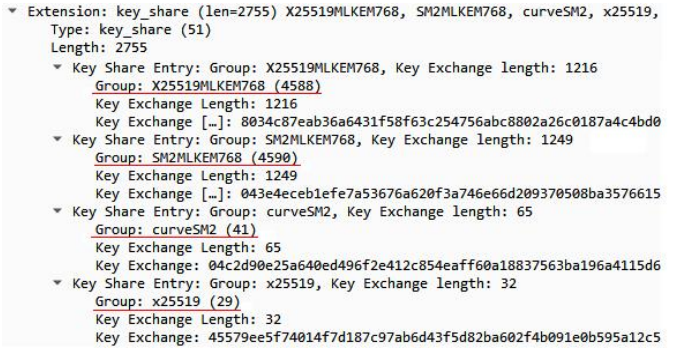


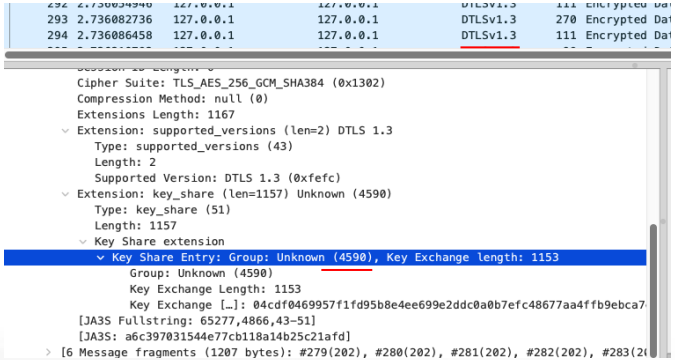
Ecosystem – Gateway / Enterprise

- ZoTrus HTTPS Automation Gateway (零信HTTPS加密自动化网关) (hardware appliance): Transparent front-end TLS termination, SSL acceleration and offloading
- Auto-manages dual SSL certificates (ECC + SM2)
- Enables both X25519MLKEM768 + SM2MLKEM768 hybrids
- No backend server changes required
- Ideal for enterprises migrating to PQ without full re-architecture

Interoperability & Real-World Readiness

- Tested combinations:
  - ZT Browser - TongsuoSSL server(SM2MLKEM768)
  - Wireshark captures show correct group 4590 and 4588, hybrid handshake
- No wire-format issues; follows standard TLS 1.3
- Growing ecosystem: client, server, intermediary already available
- Ready for early adoption in compliant environments
- Now, TongsuoSSL support DTLS v1.3





Security Considerations

- Hybrid security: Falls back to classical if PQ broken; PQ protects if classical broken
- ML-KEM-768: NIST FIPS 203 standardized, well-analyzed
- SM2: Chinese national standard, widely reviewed/deployed
- Concat model: Secure per hybrid-design security proof assumptions
- No downgrade attacks (standard TLS mechanisms)
- Open to further analysis / reviews from crypto community

Benefits for TLS WG & Global Internet

- Addresses real regulatory need → enables broader PQ adoption in large markets
- Increases algorithm diversity → better resilience
- Low risk: Already implemented, IANA assigned, follows WG hybrid framework
- Complements (does not compete with) X25519MLKEM & other WG items
- One Internet → supporting regional requirements strengthens overall security

Next Steps & Requests

- Feedback requested:
  - Technical/design comments on -03
  - Security/deployment concerns
- Path forward:
  - Progression to Informational or Experimental RFC
  - Interest in WG adoption / item?
- Open to: collaboration, testing, co-authors, interop events
- Contact: Richard Wang, richard@zotrus.com
- Thank you for your attention!

References / Backup

- Draft: https://datatracker.ietf.org/doc/draft-yang-tls-hybrid-sm2-mlkem/
- IANA: TLS Supported Groups (4590 = curveSM2MLKEM768)
- Hybrid design: draft-ietf-tls-hybrid-design
- Tongsuo PQC: https://www.tongsuo.net/docs/features/pqc/
- ZT Browser: https://www.zotrus.com/en/blog/ZTBrowser-makes-post-quantum-cryptography-visible.html
- Blog on 4590: https://www.zotrus.com/en/blog/interpret-SM2MLKEM768-and-4590.html

Thank You & Q&A

- Thank you to TLS WG for time & consideration
- Looking forward to your questions, feedback, and guidance
- Send email to: op@zotrus.com, thanks.