ML-KEM in TLS

Ostap Cherkashin

October 31, 2026

Outline

HNDL, MITM, and Other Risks

Lattices and ML-KEM

ML-KEM and TLS

Practical Considerations

HNDL, MITM, and Other Risks

- Shor's algorithm solves integer factorization and discrete logarithm problems in quantum polynomial-time [Sho97]
- Affects traditional asymmetric cryptography: DH, DSA, RSA
  - Confidentiality (DH, RSA): Harvest Now, Decrypt Later
  - Authentication[1] (DSA, RSA): Man-In-The-Middle
- Current estimate for breaking ECDH is 1200 logical qubits [Sch26]

[1] Cannot be attacked retroactively.

Post-Quantum Cryptography

Type	**Signature**	**Key Agreement**	**Hardness**
Codes	LESS [BMPS20]	Classic McEllice [BCC+22]	Syndrome Decoding Problem
Isogenies	SQISign [AAA+26]	CSIDH [CLM+18], MIKE [BDD+26]	Isogeny Problem
Lattices	ML-DSA [FIPS204]	ML-KEM [FIPS203]	Shortest Vector Problem
Multivariate	UOV [BCD+26], MAYO [BCC+26]		Multivariate Quadratic Problem

HNDL, MITM, and Other Risks

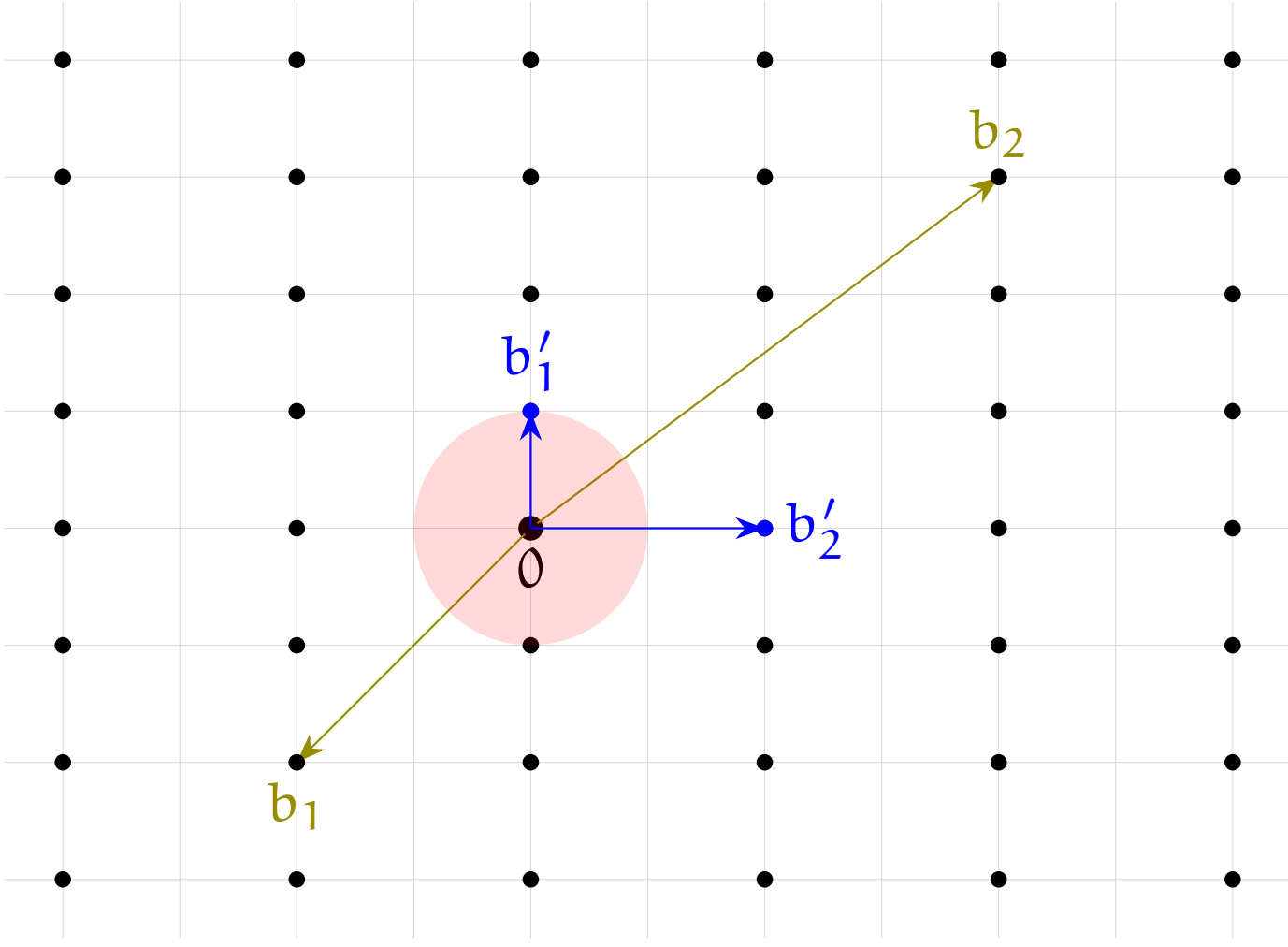
Lattices and ML-KEM

ML-KEM and TLS

Practical Considerations

Lattices

Shortest Vector Problem (SVP)



Lattice $L(b_1, b_2) = \{c_1 b_1 + c_2 b_2 \in \mathbb{R}^2 \mid c_i \in \mathbb{Z}\}$.

SVP: find a shortest vector (NP-hard).

Learning With Errors (LWE)

Short secret version

An *LWE instance* with $m \geqslant n$, prime q, and bound $B \ll q/2$:

1. Choose random $A \in \mathbb{Z}_q^{m \times n}$, $s \in [-B, B]^n$, $e \in [-B, B]^m$
2. Compute $b = As + e$

The *LWE problem* is to find s given (A, b).

Reduces to SVP via bounded distance decoding.

ML-KEM

Presented as Lindner-Peikert encryption[2]

- $\mathsf{KeyGen}() \to ((A, b), s)$
- $\mathsf{Encaps}(A, b) \to c$
  - Generate a shared secret $\mathsf{ss} \in \{0,1\}$
  - Choose random $r, e_1 \in [-B, B]^n$, and $e_2 \in [-B, B]$
  - Return $c = (A^\intercal r + e_1, b^\intercal r + e_2 + \lceil \frac{q}{2} \rfloor \mathsf{ss})$
- $\mathsf{Decaps}(c, s) \to \mathsf{ss}$
  - Parse $c = (u, v)$
  - Return $\mathsf{ss} = \mathrm{Round}_q(v - s^\intercal u)$

[2]ML-KEM uses $\mathbb{Z}_q[x]/\langle x^n + 1\rangle$ instead of Z_q, adds compression, and Fujisaki-Okamoto transform [HHK17] to make it secure to chosen-ciphertext attacks.

HNDL, MITM, and Other Risks

Lattices and ML-KEM

ML-KEM and TLS

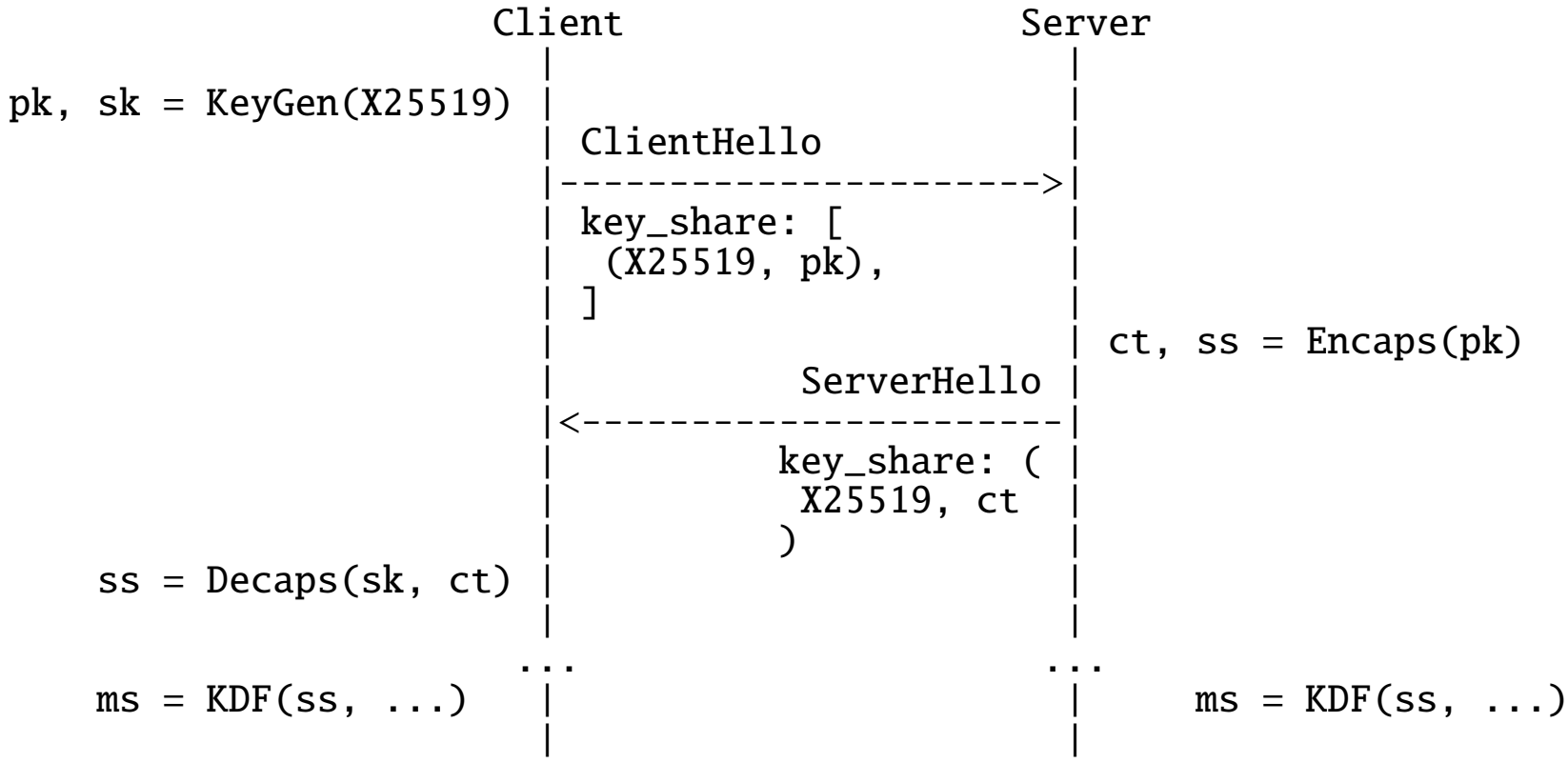
Practical Considerations

Interpreting ECDH as a KEM

For ease of presentation

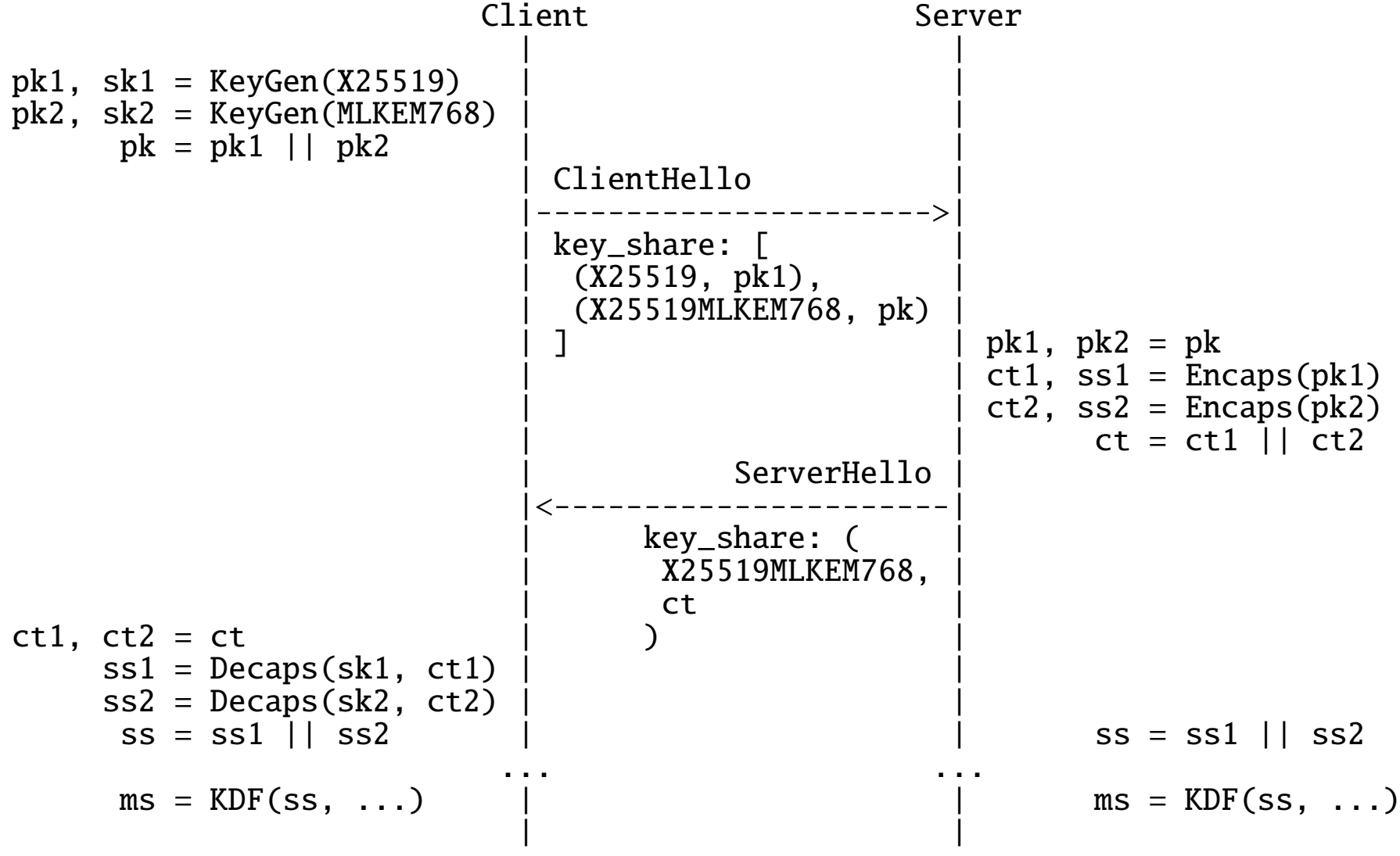
- Elliptic Curve Diffie-Hellman
  - Named group: point Q on curve C
  - Client keys: $c \in \mathbb{N},\ P_c = [c]Q = \underbrace{Q + \cdots + Q}_{c\text{-times}}$
  - Server keys: $s \in \mathbb{N},\ P_s = [s]Q$
  - Shared secret: $\mathsf{ss} = [s]P_c = [sc]Q = [cs]Q = [c]P_s$
- Now as KEM
  - Client runs $(P_c, c) = \mathsf{KeyGen}()$
  - Server runs $(P_s, \mathsf{ss}) = \mathsf{Encaps}(P_c)$
  - Client runs $\mathsf{ss} = \mathsf{Decaps}(c, P_s)$

TLS 1.3 Key Agreement [3]



[3] TLS specification does not use KEM terminology [RFC9846, § 4.2].

TLS 1.3 PQ/T Hybrid Key Agreement [RFC9954]



Hybrid Key Agreement

Notable properties

- Shared secret remains secure even if all but one components are compromised
- Backward compatible: clients and servers can become hybrid-aware independently
- IETF documents
  - Hybrid construction for TLS [RFC9954]
  - ECDH+ML-KEM in TLS [RFC10024]
  - Internet draft for plain ML-KEM [Con26][4]

[4] See also `https://blog.cr.yp.to/20251004-weakened.html`.

HNDL, MITM, and Other Risks

Lattices and ML-KEM

ML-KEM and TLS

Practical Considerations

Performance

- Space: adds ~1200 bytes to ClientHello and ServerHello
- Time[5]: adds microseconds

```
$ openssl speed X25519 ML-KEM-768 X25519MLKEM768
version: 4.1.0
...
                  keygen    encaps    decaps ...
         X25519 0.000015s 0.000035s 0.000019s ...
    ML-KEM-768 0.000022s 0.000015s 0.000023s ...
X25519MLKEM768 0.000039s 0.000049s 0.000042s ...
```

[5] On MacBook Air M4.

Testing for ML-KEM

Passively

1. Capture network packets
2. Inspect ServerHellos[6]

```
$ tshark -r file.pcap -Y 'tls.handshake.type==2' \
        -Tfields -e _ws.col.protocol \
        -e @tls.handshake.extensions_key_share_group \
        -e _ws.col.def_src \
        -e _ws.col.def_dst
TLSv1.3 00:1d   2a03:6000:6e64:611::214 ...
QUIC    11:ec   2606:4700:10::6814:179a ...
```

3. Filter for ML-KEM[7] `11:ec`, `11:eb`, `11:ed`

[6] Set the handshake type to 1 to inspect ClientHellos.

[7] `https://www.rfc-editor.org/info/rfc10024`.

Testing for ML-KEM

Actively

- Use OpenSSL v3.5.0+

```
$ openssl s_client -connect example.com:443 \
        -groups X25519MLKEM768
```

- Write a little program[8]

```
$ ./talks_mlkem x63.ch:443
NO: ML-KEM is not supported
$ ./talks_mlkem example.com:443
YES: connected using X25519MLKEM768
```

- Use a service
  - `https://radar.cloudflare.com/post-quantum`
  - `https://www.ssllabs.com/ssltest/`

[8] `https://x63.ch/files/talks_mlkem.go`.

ML-KEM Support

Cryptographic Libraries and Programming Languages

Name	**Version**	**Affects**[9]
BoringSSL	131 [GOOG]	Chrome, Edge
CryptoKit	macOS 26 [APPL]	Safari, URLSession
Go	1.24 [GO]	Caddy, Traefik
NSS	3.118 [MZLA]	Firefox
OpenJDK	27 [ORCL]	Java
OpenSSL	3.5.0 [OSSL]	Apache, C, C++, HAProxy, Nginx, Node.js, Python
rustls	0.23.22 [RTLS]	Rust, Apache, Nginx
Schannel	W11, WS25 [MSFT]	Windows

[9] Number of X25519MLKEM768 protected HTTPS requests on the internet is growing fast. For instance, CloudFlare reports 72% for human and 48% for bot traffic (`https://radar.cloudflare.com/post-quantum`).

Further Reading

A Gentle Introduction to Lattice-Based Cryptography
by Alfred Menezes [Men26]

Thank You[10]

`https://x63.ch`

[10] **AI disclosure**: Siri AI helped me to draw the lattice on Slide 6. Claude convinced me to use tshark instead of tcpdump on Slide 16. Everything else was done by the author.

Bibliography I

[AAA+26] Marius A. Aardal, Gora Adj, Diego F. Aranha, Andrea Basso, Isaac Andrés Canales Martínez, Jorge Chávez-Saab, Maria Corte-Real Santos, Pierrick Dartois, Luca De Feo, Max Duparc, Jonathan Komada Eriksen, Tako Boris Fouotsa, Décio Luiz Gazzoni Filho, Basil Hess, David Kohel, Antonin Leroux, Patrick Longa, Luciano Maino, Michael Meyer, Kohei Nakagawa, Hiroshi Onuki, Lorenz Panny, Sikhar Patranabis, Christophe Petit, Giacomo Pope, Krijn Reijnders, Damien Robert, Francisco Rodríguez Henríquez, Sina Schaeffler, Benjamin Wesolowski, Giacomo Borin, Thomas Espitau, Riccardo Invernizzi, Marzio Mula, Frederik Vercauteren, Alexandre Wallet, and Wessel van Woerden. *SQIsign: Algorithm Specifications and Supporting Documentation, Version 3.0*. Tech. rep. NIST Post-Quantum Cryptography: Additional Digital Signature Schemes, Round 3. 2026. URL: https://csrc.nist.gov/Projects/pqc-dig-sig/round-3-additional-signatures.

[APPL] Apple Inc. *Transport Layer Security*. https://support.apple.com/en-nz/guide/security/sec100a75d12/web. Jan. 2026. URL: https://developer.apple.com/documentation/cryptokit.

Bibliography II

[BDD+26] Andrea Basso, Pierrick Dartois, Max Duparc, Jonathan Komada Eriksen, Sabrina Kunzweiler, Michael Meyer, Giacomo Pope, Krijn Reijnders, Damien Robert, Ryan Rueger, and Sina Schaeffler. *MIKE: a fast and compact post-quantum NIKE*. Cryptology ePrint Archive, Paper 2026/2377. 2026. URL: https://eprint.iacr.org/2026/2377.

[BCC+22] Daniel J. Bernstein, Tung Chou, Carlos Cid, Jan Gilcher, Tanja Lange, Varun Maram, Ingo von Maurich, Rafael Misoczki, Edoardo Persichetti, Christiane Peters, Nicolas Sendrier, Jakub Szefer, Cen Jung Tjhai, Martin Tomlinson, and Wen Wang. *Classic McEliece: conservative code-based cryptography: cryptosystem specification*. Tech. rep. Oct. 2022. URL: https://classic.mceliece.org/.

[BCC+26] Ward Beullens, Fabio Campos, Sofía Celi, Basil Hess, and Matthias J. Kannwischer. *MAYO Round 3 Version*. Tech. rep. NIST Post-Quantum Cryptography: Additional Digital Signature Schemes, Round 3. 2026. URL: https://csrc.nist.gov/Projects/pqc-dig-sig/round-3-additional-signatures.

Bibliography III

[BCD+26] Ward Beullens, Ming-Shing Chen, Jintai Ding, Boru Gong, Matthias J. Kannwischer, Jacques Patarin, Bo-Yuan Peng, Dieter Schmidt, Cheng-Jhih Shih, Chengdong Tao, and Bo-Yin Yang. *UOV: Unbalanced Oil and Vinegar, Algorithm Specifications and Supporting Documentation, Version 3.0*. Tech. rep. NIST Post-Quantum Cryptography: Additional Digital Signature Schemes, Round 3. 2026. URL: https://csrc.nist.gov/Projects/pqc-dig-sig/round-3-additional-signatures.

[BMPS20] Jean-François Biasse, Giacomo Micheli, Edoardo Persichetti, and Paolo Santini. "LESS is More: Code-Based Signatures Without Syndromes". In: *Progress in Cryptology - AFRICACRYPT 2020*. Ed. by Abderrahmane Nitaj and Amr Youssef. Cham: Springer International Publishing, 2020, pp. 45–65. ISBN: 978-3-030-51938-4.

[CLM+18] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. "CSIDH: An Efficient Post-Quantum Commutative Group Action". In: *Advances in Cryptology – ASIACRYPT 2018*. Ed. by Thomas Peyrin and Steven Galbraith. Cham: Springer International Publishing, 2018, pp. 395–427. ISBN: 978-3-030-03332-3.

Bibliography IV

[Con26] Deirdre Connolly. *ML-KEM Post-Quantum Key Agreement for TLS 1.3*. Internet-Draft draft-ietf-tls-mlkem-11. Work in Progress. Internet Engineering Task Force, Sept. 2026. 9 pp. URL: https://datatracker.ietf.org/doc/draft-ietf-tls-mlkem/11/.

[GO] The Go Authors. *Go 1.24 Release Notes*. Feb. 2025. URL: https://go.dev/doc/go1.24#cryptotlspkgcryptotls.

[GOOG] The BoringSSL Authors. *Enable ML-KEM by default*. Shipped with Chromium 131 https://security.googleblog.com/2024/09/a-new-path-for-kyber-on-web.html. Oct. 2024. URL: https://chromium-review.googlesource.com/c/chromium/src/+/5908098.

[HHK17] Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz. "A Modular Analysis of the Fujisaki-Okamoto Transformation". In: *Theory of Cryptography*. Ed. by Yael Kalai and Leonid Reyzin. Cham: Springer International Publishing, 2017, pp. 341–371. ISBN: 978-3-319-70500-2.

[RFC10024] K. Kwiatkowski, P. Kampanakis, B. E. Westerbaan, and D. Stebila. *Post-Quantum Traditional (PQ/T) Hybrid Key Agreement Mechanisms for TLS 1.3*. RFC 10024. Aug. 2026. DOI: 10.17487/RFC10024. URL: https://www.rfc-editor.org/info/rfc10024/.

Bibliography V

[Men26] Alfred Menezes. *A gentle introduction to lattice-based cryptography*. Cryptology ePrint Archive, Paper 2026/1098. 2026. URL: https://eprint.iacr.org/2026/1098.

[MSFT] Microsoft. *New Windows Features to Secure Today's Data in a Post-Quantum World*. Schannel SSP https://learn.microsoft.com/en-us/windows-server/security/tls/tls-ssl-schannel-ssp-overview. July 2026. URL: https://techcommunity.microsoft.com/blog/microsoft-security-blog/new-windows-features-to-secure-today%E2%80%99s-data-in-a-post-quantum-world/4523370.

[MZLA] The NSS Contributors. *NSS 3.118 release notes*. Nov. 2025. URL: https://firefox-source-docs.mozilla.org/security/nss/releases/nss_3_118.html.

[ORCL] The OpenJDK Contributors. *JEP 527: Post-Quantum Hybrid Key Exchange for TLS 1.3*. Aug. 2026. URL: https://openjdk.org/jeps/527.

[OSSL] The OpenSSL Developers. *Major changes between OpenSSL 3.4 and OpenSSL 3.5.0*. Apr. 2025. URL: https://github.com/openssl/openssl/blob/master/NEWS.md#major-changes-between-openssl-34-and-openssl-350-8-apr-2025.

Bibliography VI

[RFC9846] E. Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.3*. RFC 9846. July 2026. DOI: 10.17487/RFC9846. URL: https://www.rfc-editor.org/info/rfc9846/.

[RTLS] The rustls developers. *Releases / v0.23.22*. Jan. 2025. URL: https://github.com/rustls/rustls/releases/tag/v%2F0.23.22.

[Sch26] André Schrottenloher. *Optimized Point Addition Circuits for Elliptic Curve Discrete Logarithms*. Cryptology ePrint Archive, Paper 2026/1128. 2026. URL: https://eprint.iacr.org/2026/1128.

[Sho97] Peter W. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". In: *SIAM Journal on Computing* 26.5 (1997), pp. 1484–1509. DOI: 10.1137/S0097539795293172.

[FIPS204] National Institute of Standards and Technology. *Module-Lattice-Based Digital Signature Standard*. Tech. rep. Federal Information Processing Standards Publications (FIPS) 204. Washington, D.C.: U.S. Department of Commerce, Aug. 2024. DOI: 10.6028/NIST.FIPS.204. URL: https://csrc.nist.gov/pubs/fips/204/final.

Bibliography VII

[FIPS203] National Institute of Standards and Technology. *Module-Lattice-Based Key-Encapsulation Mechanism Standard*. Tech. rep. Federal Information Processing Standards Publications (FIPS) 203. Washington, D.C.: U.S. Department of Commerce, Aug. 2024. DOI: 10.6028/NIST.FIPS.203. URL: https://csrc.nist.gov/pubs/fips/203/final.

[RFC9954] D. Stebila, S. Fluhrer, and S. Gueron. *Hybrid Key Exchange in TLS 1.3*. RFC 9954. July 2026. DOI: 10.17487/RFC9954. URL: https://www.rfc-editor.org/info/rfc9954/.