ML-KEM is Great! What's Missing?

John Preuß Mattsson, Erik Thormarker, Göran Selander, Santeri Paavolainen,
Sini Ruohomaa, Juha Sääskilahti, Taylor Hartley, Helena Vahidi Mazinani, Mohsin Kahn

Ericsson

Abstract: Post-Quantum Cryptography (PQC) has made significant progress with the standardization of ML-KEM, ML-DSA, and SLH-DSA, paving the way for widespread adoption. However, since many adopters lack expertise in cryptography, it is crucial for specifications and guidance to be concise, accessible, and focused on recommending only secure implementations of PQC and related primitives to minimize the risk of vulnerabilities. Moreover, ML-KEM may not be suitable for all applications, and backup algorithms are needed for cryptographic agility. To address this, we propose several suggestions for NIST's specifications and guidance, including the use of ephemeral keys, hybridization strategies, key combiners, key derivation functions, additional key encapsulation mechanisms, and best practices for asymmetric keying. The transition to quantum-resistant cryptography offers an excellent opportunity to reassess outdated algorithms and practices that no longer provide acceptable security.

Introduction

NIST has done an outstanding job with the standardization of ML-KEM and Post-Quantum Cryptography (PQC) in general. Cryptographers from around the globe have participated and contributed to the PQC project, with discussions being open and public, and all specifications freely accessible. ML-KEM is an excellent general-purpose, single-recipient Key Encapsulation Mechanism (KEM) with exceptional performance in both hardware and software. Ericsson plans to transition all our products and services to ML-KEM as soon as protocol standards and hardened implementations are available.

We greatly appreciate that the ML-KEM family consists of only three algorithms, offers IND-CCA security, ensures the shared secret is derived from randomness contributed by both parties, and produces a uniformly random shared secret that is immediately usable without requiring additional key derivation.

We applaud NIST for mandating the use of SHA-3 in ML-KEM and ML-DSA. SHA-2 has significant problems with side-channels, and SHA-256 and SHA-512 are vulnerable to length-extension attacks. SHA-3 is designed to provide indifferentiability from a random oracle. Ericsson has historically aligned with NSA Suite B and CNSA 1.0, using (HMAC-)SHA-384 whenever feasible. As we transition to PQC, Ericsson plans to adopt the superior SHA-3 family as widely as possible.

The transition to quantum-resistant cryptography presents an excellent opportunity to reassess outdated algorithms and practices that no longer meet acceptable security standards.

Proposals for Quantum-Resistant Key Encapsulation Mechanisms

Below, we present our views on many of the topics NIST requested [1] as well as some additional relevant topics:

- **Limits for use of ephemeral keys**. We strongly support the SP 800-56A [2] requirement that "*An ephemeral private key shall be used in exactly one key-establishment transaction.*" The practice in some security protocols of reusing private keys while still labeling them as ephemeral is deeply problematic and misleading. Users and developers expect that ephemeral keys are used only once and that their security is independent of sessions involving hostile adversaries. The reuse of ephemeral keys, combined with implementation bugs such as the lack of public key validation, has resulted in serious exploitable vulnerabilities. These flaws have allowed attackers to recover the so-called "ephemeral" private key, enabling them to completely compromise sessions between legitimate parties. We strongly recommend that the same requirement "*An ephemeral private key shall be used in exactly one key-establishment transaction*" be included in all NIST specifications on KEMs. Implementation bugs that allow attackers to recover private keys have been well-documented for both ECC and RSA, and similar vulnerabilities are likely for quantum-resistant KEMs. ML-KEM is so fast that reusing private keys to save a few CPU cycles during key establishment is hardly justifiable. Any protocol that reuses private keys should explicitly acknowledge this practice and state that the keys are (semi-)static.

- **Guidance on hybridization.** One implication of NIST IR 8547 [3] is that most industries will go for 100% hybrids aligning with ANSSI's and BSI's requirements that "Post-quantum algorithms must be hybridized" [4] and "PQC only in hybrid solutions" [5]. When SIKE was presented at the first PQC workshop, Shamir said: "*I don't think this should be deployed in the next 20 years*". Similar things can be said about early algorithm implementations, many of which have severe implementation bugs and side-channels. The 2030 deprecation date for ECC means that industry needs to pick the very first available implementations of ML-KEM and use them in production systems, which without hybrid schemes creates unacceptable risks. IETF consensus is very clearly to recommend hybrids. Montgomery curves offer superior security and performance and should be the sole choice for ML-KEM hybridization. Hybrids with X25519 have already become the de facto standard for TLS 1.3, DTLS 1.3, QUIC, SSH, Signal, and Rosenpass with widespread deployments. We think NIST should encourage the use of X25519 and X448 in hybrid schemes. This aligns with de facto Internet standards. Curve25519 and Curve448 are already specified in NIST SP 800-186.

- **Guidance on key combiners.** We welcome NIST's plan [6] to allow hybrid shared secrets of the form $S_1 \| S_2 \| \ldots \| S_t$, where at least one of the shared secrets S_i is NIST approved. We anticipate that hybrid shared secrets consisting of more than two components will be relatively common. For instance, [7], authored by the chief cryptographer of the Swedish NCSA, recommends hybrid keying that integrates symmetric keying, post-quantum secure asymmetric keying, and classically secure asymmetric keying. Both TLS 1.3 and IKEv2 support this type of

hybrid keying. One concrete example is TLS 1.3 resumption with X25519MLKEM768. Additionally, hybrid keying with X25519/X448, ML-KEM, and BIKE/HQC has been proposed as an alternative to FrodoKEM with better performance.

- **Guidance on KDFs.** We do not think that SHA-2 and CMAC should be allowed as KDFs in key combiners. A Key Derivation Function (KDF) should behave as a pseudorandom function (PRF) that maintains collision resistance and preimage resistance, even when the secret is known and not uniformly random. While KMAC and HKDF satisfy these requirements, SHA-2 and CMAC do not and are therefore unsuitable in scenarios where one of the parties can control the input. SHA-256 and SHA-512 are vulnerable to length-extension attacks, while the issues with CMAC are detailed in [8]. We believe SHA-2 should be disallowed as a KDF in all specifications. Systems relying on SHA-2 can use HMAC. Additionally, we emphasize that NIST should discuss length-extension attacks in FIPS 180-5, as suggested in [10]. Although SP 800-108 [9] proposes a potential solution for AES-CMAC, it is lacking both motivation and proof [8]. We argue that CMAC should not be permitted as a KDF unless it can be proven that a specific construction and input formatting ensure collision resistance and preimage resistance, even when the key is known. As (HMAC-)SHA-2 and AES have significant problems with side-channels, NIST should recommend the use of KMAC as the first-hand choice whenever possible.

- **A backup KEM suitable for ephemeral-ephemeral key exchange.** Cryptographic agility is the ability to switch between cryptographic primitives without the need to modify or replace the surrounding infrastructure. The importance of cryptographic agility has been emphasized by several US agencies. A necessity for cryptographic agility is having a cryptographic primitive to switch to, and ML-KEM is currently the only NIST-approved quantum-resistant KEM. BIKE and HQC are good backup algorithms to ML-KEM for ephemeral-ephemeral key exchange. Additionally, hybrid approaches such as X448+ML-KEM+BIKE and X448+ML-KEM+HQC offer significant performance and size advantages comparable to X448+FrodoKEM, while adhering to a comparably conservative design. See Tables 1 and 2 for size and performance comparisons. We are not currently planning to use BIKE or HQC, but we would like to see a standardized backup algorithm for ML-KEM implemented in case theoretical or implementation vulnerabilities are found. Such a backup algorithm should have a different construction than ML-KEM. The practice of implementing independent cryptographic backup algorithms in advance has long been a guiding principle in the telecom industry. We think NIST should standardize BIKE or HQC.

- **A conservative KEM with strong performance for static-ephemeral key exchange.** We strongly think NIST should standardize Classic McEliece, which has properties that makes it the best choice for many different applications. We are planning to use Classic McEliece. Classic McEliece is the most conservative KEM and Classic McEliece category 5 is the best option for protecting various other keys (ML-KEM, ML-DSA, SLH-DSA, FN-DSA, LMS, XMSS, etc.) in transit and storage. Classic McEliece occupies a role similar to SLH-DSA, providing a very conservative security assurance. The small ciphertexts and good performance makes Classic McEliece the best choice for many applications of static encapsulation keys of which there are many (WireGuard, S/MIME, IMSI encryption, File encryption, Noise, EDHOC, etc.). For such applications, key generation time is not important, and the public key can be provisioned out-of-band. When the public key is provisioned in-band, Classic McEliece has less overhead

than ML-KEM at the same security level after just a few hundred encapsulations, see Figure 1. The small ciphertexts of Classic McEliece increase the likelihood that messages fit within a single packet, providing substantial benefits beyond what a simple count might suggest. Users might be comfortable with a lower security category for Classic McEliece compared to ML-KEM, given its attack complexity has remained stable for decades. For static encapsulation use cases where ML-KEM provides the best performance, Classic McEliece is the best backup algorithm. The memory requirement can be kept low by streaming the key. Classic McEliece has already seen significant deployment by e.g., Rosenpass, Mullvad VPN, and Crypto4A. We think NIST should standardize mceliece348864 (category 1), mceliece460896 (category 3), and one of mceliece6688128, mceliece6960119, and mceliece8192128 (category 5). 261 kB and 524 kB encapsulation keys can be used where 1 MB keys cannot.

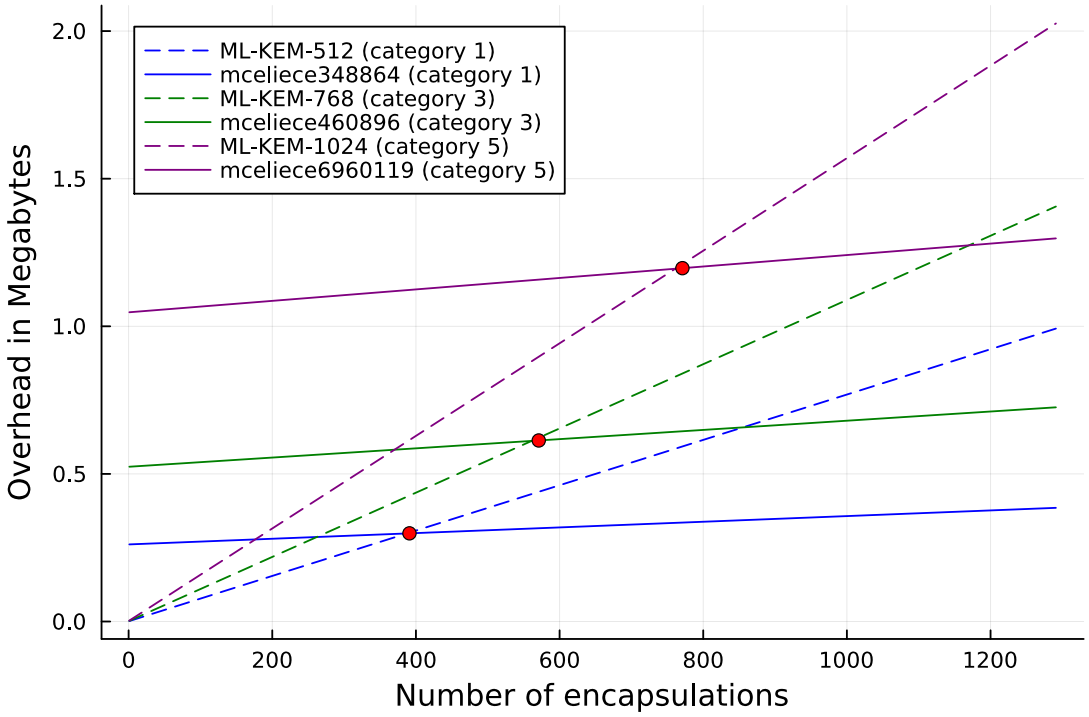

Figure 1. Overhead of the static encapsulation key and ciphertexts in ML-KEM and Classic McEliece as a function of the number of encapsulations.

- **A KEM with small sizes and an algorithm suitable for static-static key exchange.** Constrained radio networks such as Low Power Wide Area Networks (LPWANs) represent a rapidly growing market projected to reach 400-7600 billion USD globally by 2030 [12–13]. The sixth generation of cellular networks, 6G, which will be deployed around 2030, will include both enhanced LPWAN technologies and ultra-constrained zero-energy devices [14]. Constrained radio networks are not only characterized by very small frame sizes on the order of tens of bytes transmitted a few times per day at ultra-low speeds, but also high latency, and severe duty cycles constraints. Due to its large public-key and ciphertext sizes, and the lack of Non-Interactive Key Exchange (NIKE), ML-KEM is unusable in many IoT systems using very constrained radio networks. Using ML-KEM instead of ECDH would in many cases increase the number of bytes with several thousand percent. Due to duty cycles, the increase in "time

to completion" is often even larger. The size of the messages sent over radio is the single most important factor for power consumption and battery lifetime in IoT systems using radio [15]. Static-static key exchange using Diffie-Hellman is specified in SP 800-56A [2] and widely deployed, but NIST has not specified a PQC migration path for such systems. At the PKI Consortium PQC Conference 2025, Cisco asked NIST regarding its plans for quantum-resistant static-static key exchange. Very constrained radio networks cannot migrate to ML-KEM, as doing so would result in completely unacceptable performance, and make the systems unusable. Many deployments will likely continue using ECC until the risk of CRQC attacks on their system (based on lifetime and value) becomes imminent. If NIST disallow ECC, constrained radio networks wanting to be NIST compliant are forced to migrate to symmetric group keys without Perfect Forward Secrecy (PFS) and identity protection. In such scenarios, a compromised node can passively intercept communications between other group members or actively impersonate them to inject malicious messages into the network. NIST should announce that, if practical candidates for standardization emerge, it will initiate the standardization of additional KEMs and NIKEs with small public keys and ciphertexts. This would significantly encourage well-needed research in KEMs and NIKEs suitable for constrained radio networks.

- **Always use asymmetric keying whenever feasible.** NIST should take inspiration from [7] and recommend always hybridizing symmetric keying with post-quantum secure asymmetric keying wherever possible. Asymmetrically distributed keys can be refreshed at very frequent intervals to enhance security. 6G, the sixth generation of cellular networks, is expected to incorporate Authentication and Key Agreement (AKA) augmented with quantum-resistant KEMs [16–17], effectively preventing passive eavesdropping on U.S. mobile communications by foreign nation-states that have compromised the symmetric keys. Agencies in some countries have historically favored weaknesses in standards and implementations, such as cleartext identifiers, the lack of PFS, and the absence of end-to-end encryption, as a means to enable interception. However, these vulnerabilities can be exploited by nation-state threat actors [18–22]. NIST should recommend continuously re-negotiating encryption keys, and chaining the negotiations, so that an adversary has to record and store an uninterrupted sequence of negotiations, and then break them in sequence [7].

Summary and Conclusions

ML-KEM is an excellent KEM with exceptional performance in both hardware and software. However, it is not suitable for all applications, and backup algorithms are needed for cryptographic agility. The transition to quantum-resistant cryptography presents an excellent opportunity to reassess outdated algorithms and practices that no longer provide acceptable security. Based on the discussion above, we recommend that NIST standardize Classic McEliece alongside BIKE or HQC. Additionally, NIST should encourage research into KEMs and NIKEs with smaller public keys and ciphertexts for potential future standardization. Furthermore, NIST should strongly recommend the use of quantum-resistant asymmetric keying whenever possible and uphold the current requirement that ephemeral keys be used only once. For the PQC transition, NIST should recommend the use of the SHA-3 family as the first-hand choice whenever possible. For ML-KEM hybridization, NIST should recommend X25519 and X448, aligning with de facto Internet standards.

Table 1. Public key and ciphertext sizes in bytes. Total size is public key size plus ciphertext size, which is a relevant measure when KEMs are used for ephemeral key exchange in protocols like TLS 1.3 and IKEv2.

Name	Category	Public key	Ciphertext	Total
ML-KEM-512	1	800	768	1568
BIKE-L1	1	1541	1573	3114
ML-KEM-512+BIKE-L1	1	2341	2341	4682
HQC-128	1	2249	4481	6730
ML-KEM-512+HQC-128	1	3049	5249	8298
FrodoKEM-640	1	9616	9720	19336
ML-KEM-768	3	1184	1088	2272
BIKE-L3	3	3083	3115	6198
ML-KEM-768+BIKE-L3	3	4267	4203	8470
HQC-192	3	4522	9026	13548
ML-KEM-768+HQC-192	3	5706	10114	15820
FrodoKEM-976	3	15632	15744	31376
ML-KEM-1024	5	1568	1568	3136
BIKE-L5	5	5122	5154	10276
ML-KEM-1024+BIKE-L5	5	6690	6722	13412
HQC-256	5	7245	14469	21714
ML-KEM-1024+HQC-256	5	8813	16037	24850
FrodoKEM-1344	5	21520	21632	43152

Table 2. Performance in cycles on 2023 AMD Ryzen 7 7700 from eBACS [11]. The numbers represent the median (50%) of many speed measurements. Total is cycles for key gen + encapsulation + decapsulation.

Name	Category	Key gen	Encapsulation	Decapsulation	Total
ML-KEM-512 (kyber512)	1	15420	24443	18693	58556
HQC-128 (hqc128round4)	1	61311	170433	283249	514993
ML-KEM-512+HQC-128	1	76731	194876	301942	573549
BIKE-L1 (bikel1)	1	459202	83286	1069392	1611880
ML-KEM-512+BIKE-L1	1	474622	107729	1088085	1670436
FrodoKEM-640 (frodokem640shake)	1	2084314	2265633	2222733	6572680
ML-KEM-768 (kyber768)	3	26537	36373	27911	90821
HQC-192 (hqc192round4)	3	145927	388479	616013	1150419
ML-KEM-768+HQC-192	3	172464	424852	643924	1241240
BIKE-L3 (bikel3)	3	1276234	177463	3365184	4818881
ML-KEM-768+BIKE-L3	3	1302771	213836	3393095	4909702
FrodoKEM-976 (frodokem976shake)	3	4272608	4592978	4483035	13348621
ML-KEM-1024 (kyber1024)	5	34305	48320	38330	120955
HQC-256 (hqc256round4)	5	295441	733761	1192579	2221781
ML-KEM-1024+HQC-256	5	329746	782081	1230909	2342736
BIKE-L5	5	N/A	N/A	N/A	N/A
ML-KEM-1024+BIKE-L5	5	N/A	N/A	N/A	N/A
FrodoKEM-1344 (frodokem1344shake)	5	7309062	7857621	7702139	22868822

References

[1] Call for Submissions - NIST Workshop on Guidance for KEMs
https://csrc.nist.gov/csrc/media/Events/2025/workshop-on-guidance-for-kems/documents/call-for-submissions-kems-feb-2025.pdf

[2] Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf

[3] Transition to Post-Quantum Cryptography Standards
https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf

[4] ANSSI plan for post-quantum transition
https://pkic.org/events/2023/pqc-conference-amsterdam-nl/pkic-pqcc_jerome-plut_anssi_anssi-plan-for-post-quantum-transition.pdf

[5] Post-Quantum Policy & Roadmap of the BSI
https://pkic.org/events/2023/pqc-conference-amsterdam-nl/pkic-pqcc_stephan-ehlen_bsi_post-quantum-policy-and-roadmap-of-the-bsi.pdf

[6] Recommendations for Key-Encapsulation Mechanisms
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-227.ipd.pdf

[7] On factoring integers, and computing discrete logarithms and orders, quantumly
http://kth.diva-portal.org/smash/get/diva2:1902626/FULLTEXT01.pdf

[8] Ericsson Comments on SP 800-38B
https://csrc.nist.gov/csrc/media/Projects/crypto-publication-review-project/documents/initial-comments/sp800-38b-initial-public-comments-2024.pdf

[9] Recommendation for Key Derivation Using Pseudorandom Functions
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-108r1-upd1.pdf

[10] Ericsson Comments on FIPS 180-4
https://csrc.nist.gov/csrc/media/Projects/crypto-publication-review-project/documents/initial-comments/fips180-4-initial-public-comments-2022.pdf

[11] ECRYPT Benchmarking of Cryptographic Systems
https://bench.cr.yp.to/results-kem/amd64-hertz.html

[12] Low-Power Wan Market Size & Share Analysis - Growth Trends & Forecasts (2025 - 2030)
https://www.mordorintelligence.com/industry-reports/low-power-wan-market

[13] Low Power Wide Area Network Market- Global Industry Analysis and Forecast (2024-2030)
https://www.maximizemarketresearch.com/market-report/global-low-power-wide-area-network-market/7252/

[14] Designing a sensor-driven world: the research take on zero-energy devices
https://www.ericsson.com/en/blog/2023/5/zero-energy-devices-sensor-driven-world

[15] Constrained Radio Networks, Small Ciphertexts, Signatures, and Non-Interactive Key Exchange
https://csrc.nist.gov/csrc/media/Events/2022/fourth-pqc-standardization-conference/documents/papers/constrained-radio-networks-pqc2022.pdf

[16] Forward Secrecy for the Extensible Authentication Protocol Method for Authentication and Key Agreement (EAP-AKA' FS)
https://datatracker.ietf.org/doc/html/draft-ietf-emu-aka-pfs

[17] Enhancing Security in EAP-AKA' with Hybrid Post-Quantum Cryptography
https://datatracker.ietf.org/doc/html/draft-ar-emu-pqc-eapaka

[18] The Great SIM Heist
https://theintercept.com/2015/02/19/great-sim-heist/

[19] DHS says unauthorized Stingrays could be in D.C. area
https://cyberscoop.com/stingrays-dc-area-dhs-ron-wyden/?utm_source=chatgpt.com

[20] Spy ring plotted to obtain details from phones of Ukrainians at US airbase in Germany
https://www.theguardian.com/uk-news/2024/dec/03/spy-ring-plotted-to-obtain-details-from-phones-of-ukrainians-at-us-air-base-in-germany-uk-court-hears?utm_source=chatgpt.com

[21] A Systematic Analysis of the Juniper Dual EC Incident
https://eprint.iacr.org/2016/376.pdf

[22] Former White House tech advisor on data-centric security in the wake of Salt Typhoon
https://www.techradar.com/pro/security/former-White-House-tech-advisor-on-data-centric-security-in-the-wake-of-Salt-Typhoon