



Post-Quantum Key Exchange Overhead on Low-Power Wireless Sensor Networks

Beatriz Desai^{1*}, Dana Pavlovic², Tariq Tremblay³

¹Department of Computer Science, Tamiraparani Institute for Advanced Computer Science, Barbados

²Department of Computer Science, Ebro Center for Computer Science, Serbia

³Department of Computer Science, Irrawaddy University Centre for Computer Science, Qatar

Article Info

Volume 1, Issue 1, 2026

[doi: 10.62715/ijcser.2026.v1.i1.pp25-28](https://doi.org/10.62715/ijcser.2026.v1.i1.pp25-28)

Received: 14 October 2025

Accepted: 19 December 2025

Published: 04 March 2026

Abstract

Sensor networks that establish keys with elliptic-curve Diffie-Hellman will need a replacement that resists quantum attack, and the first standard for one, the module-lattice key-encapsulation mechanism ML-KEM, is now published. This communication considers what the change costs a low-power wireless node. It does not present measurements. It reasons from the published parameter sizes of the schemes, the frame size of IEEE 802.15.4 radios and the classes of constrained device defined by the Internet Engineering Task Force, together with the existing literature on implementing these schemes on microcontrollers. The argument is that the computational cost of lattice-based key exchange is modest on 32-bit microcontrollers and that the burden falls on communication: a public key that fitted in a single frame is replaced by one that must be fragmented across many, on links where each additional fragment costs energy and raises the chance that the whole exchange fails. Memory is a secondary constraint that matters chiefly on the smallest devices. The communication outlines mitigations, including less frequent key establishment, placement of the heavier role on a gateway, hybrid schemes during transition and protocol designs that tolerate fragment loss, and lists the questions that field measurement would need to settle.

Keywords: Post-quantum cryptography, ML-KEM, Wireless sensor networks, IEEE 802.15.4, Key establishment, Constrained devices

© 2026 Beatriz Desai et al. This is an open access article under the CC BY license (<https://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

1. Introduction

The public-key algorithms used to establish session keys today, Diffie-Hellman over finite fields and elliptic curves, depend on the hardness of the discrete logarithm problem. [Shor \(1997\)](#) showed that a sufficiently large quantum computer would solve that problem in polynomial time. No such machine exists yet, but recorded traffic can be stored and decrypted later, and the time needed to replace deployed cryptography is long. [Mosca \(2018\)](#) put the point as an inequality: if the period for which data must stay secret plus the time needed to migrate exceeds the time until a capable quantum computer appears, action is already overdue. Sensor networks score badly on that test. Nodes are installed for many years and are seldom updated once in the field.

* Corresponding author: Beatriz Desai, Department of Computer Science, Tamiraparani Institute for Advanced Computer Science, Barbados.
E-mail: beatriz.desai@tamiraparani.edu

© 2026 Beatriz Desai et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Replacements are available. After a public evaluation, the United States National Institute of Standards and Technology standardised ML-KEM, a key-encapsulation mechanism derived from CRYSTALS-Kyber (Bos et al., 2018; NIST, 2024). The question for sensor networks is what adopting it costs on hardware and radios chosen for frugality. This communication sets out where the overhead arises, using published parameters and standards, and reports no new measurements.

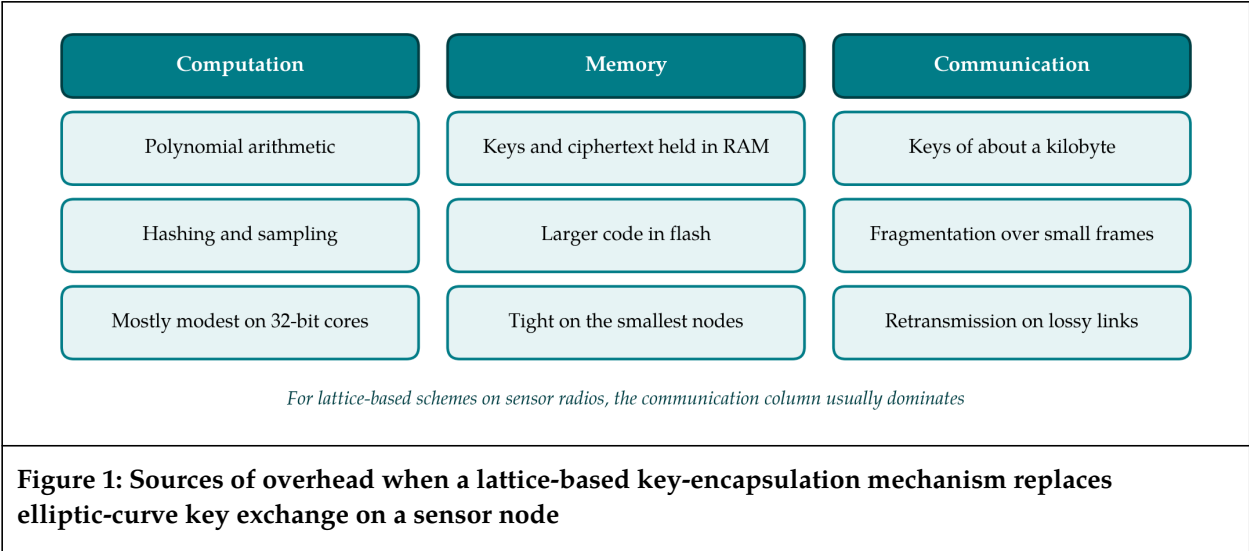
2. The Constraints of Sensor Platforms

The Internet Engineering Task Force classifies constrained nodes by memory. A class 1 device has on the order of 10 kibibytes of data memory and 100 kibibytes of code memory, and a class 2 device roughly five times the data memory (Bormann et al., 2014). Radios conforming to IEEE 802.15.4 carry at most 127 bytes in a physical-layer frame (IEEE, 2020), and after link-layer and adaptation headers a good deal less is left for the application. Larger datagrams are split by the 6LoWPAN adaptation layer into fragments, and in its original form the loss of any one fragment causes the whole datagram to be discarded (Montenegro et al., 2007).

Energy is the binding resource. Early work on public-key cryptography for sensor nodes established that elliptic-curve methods were affordable on 8-bit microcontrollers where RSA was not, and that the energy of a handshake has to include the radio as well as the processor (Wander et al., 2005). Elliptic-curve key exchange suits the radio very well, since a public value of 32 bytes on a modern curve occupies part of one frame.

3. Where the Overhead Arises

Post-quantum schemes change the proportions of the handshake more than its total computational cost. Figure 1 separates the overhead into three components, which are discussed in turn.



Computation is the smallest concern. ML-KEM works with polynomials whose coefficients are small integers, multiplied by a number-theoretic transform, plus hashing with SHA-3 functions. Benchmarking of the candidate schemes on the ARM Cortex-M4 showed lattice-based encapsulation mechanisms to be among the fastest in the field, with running times of the same order as an elliptic-curve scalar multiplication on comparable hardware (Kannwischer et al., 2019). On 8-bit and 16-bit microcontrollers the picture is less favourable and less well documented.

Memory comes next. Keys and ciphertexts of around a kilobyte must be held in RAM while they are processed, along with intermediate polynomials, and the code is larger than a compact elliptic-curve library. On a class 2 device this is comfortable. On a class 1 device that also runs a network stack it competes with packet buffers, and care in implementation matters.

Communication dominates. Table 1 gives the sizes fixed by the standards. The smallest ML-KEM

parameter set has an encapsulation key of 800 bytes and a ciphertext of 768 bytes, against 32 bytes each way for X25519. Neither message fits in an 802.15.4 frame, and each needs at least seven frames before any header is counted. Every fragment costs transmit and receive energy, lengthens the time the radio is awake, and on a lossy multi-hop path adds to the probability that the datagram must be sent again in full.

Table 1: Sizes of the values exchanged in key establishment, as fixed by the cited specifications

Scheme	Public or encapsulation key	Response or ciphertext	Remark
X25519	32 bytes	32 bytes	Elliptic curve; not quantum resistant
ML-KEM-512	800 bytes	768 bytes	Lattice based; lowest security category of NIST (2024)
ML-KEM-768	1184 bytes	1088 bytes	Lattice based; middle parameter set
ML-KEM-1024	1568 bytes	1568 bytes	Lattice based; highest parameter set
Code-based KEMs	Very large	Very small	Key too large to send over sensor links; could be pre-installed

The other families of post-quantum scheme do not offer an easy way out. Code-based mechanisms of the McEliece type have short ciphertexts but public keys far too large to transmit over such links, and hash-based constructions provide signatures, not key exchange ([Bernstein and Lange, 2017](#)). Isogeny-based key exchange once looked ideal for sensor networks because its keys were small, until the SIDH construction was broken by a classical attack ([Castricky and Decru, 2023](#)). That episode is a reminder that compactness and confidence do not always arrive together.

4. Options for Reducing the Burden

Several mitigations follow from the analysis. The first is to perform key establishment less often: derive long-lived link or session keys from one exchange and refresh them by symmetric means, so that the fragmented handshake is paid for at commissioning and rarely afterwards. The second exploits the asymmetry of the mechanism. In a star or tree topology the mains-powered gateway can generate the key pair and the node can encapsulate, which spares the node key generation and decapsulation, though it must still receive the key and send the ciphertext.

Third, during the transition a hybrid exchange that combines an elliptic-curve secret with an ML-KEM secret protects against failure of either, at the cost of a little more data on top of an already fragmented message. Fourth, the protocol can be designed around fragments. Lightweight exchanges for constrained networks such as EDHOC were specified with elliptic curves and message sizes that fit a few frames ([Selander et al., 2024](#)). Carrying a lattice-based mechanism in such a protocol calls for block-wise transfer or fragment-level acknowledgement so that one lost frame does not void the exchange.

5. Open Questions

The reasoning above rests on sizes and published benchmarks, and it leaves questions that only measurement on deployed hardware can answer. The total energy of a complete post-quantum handshake on common sensor platforms, radio included, under realistic loss rates and duty cycling, is not well characterised in the open literature. Nor is the behaviour of multi-hop networks when many nodes rejoin at once after an outage and their fragmented handshakes contend for the channel. Implementations hardened against power and timing side channels, which matter for devices an adversary can handle, cost more than reference code, and the size of that penalty on small cores needs reporting. Finally, authentication is a separate problem: post-quantum signatures are larger still than the key encapsulation messages discussed here, and designs that avoid sending them deserve attention.

6. Conclusion

For low-power wireless sensor networks, the overhead of moving to standardised post-quantum key exchange lies mainly in the radio. Lattice-based encapsulation is computationally affordable on 32-bit microcontrollers, and its keys and ciphertexts are several times larger than the frames that carry them. Designs that establish keys rarely, give the heavier role to the gateway and tolerate fragment loss can contain the cost. How large that cost is in the field remains to be measured, and those measurements are the most useful next contribution.

Conflict of interest

To be declared by the author(s) before publication.

Funding

To be declared by the author(s) before publication.

References

- Bernstein, D.J. and Lange, T. (2017). [Post-quantum cryptography](#). *Nature*, 549: 188-194. <https://doi.org/10.1038/nature23461>
- Bormann, C., Ersue, M. and Keranen, A. (2014). [Terminology for constrained-node networks](#). RFC 7228. Internet Engineering Task Force. <https://doi.org/10.17487/RFC7228>
- Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Schwabe, P., Seiler, G. and Stehlé, D. (2018). [CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM](#). *Proceedings of the 2018 IEEE European Symposium on Security and Privacy*, 353-367. <https://doi.org/10.1109/EuroSP.2018.00032>
- Castruck, W. and Decru, T. (2023). [An efficient key recovery attack on SIDH](#). In: *Advances in Cryptology - EUROCRYPT 2023*. Lecture Notes in Computer Science 14008. Springer, Cham, 423-447.
- IEEE (2020). [IEEE Std 802.15.4-2020, IEEE Standard for Low-Rate Wireless Networks](#). Institute of Electrical and Electronics Engineers, New York.
- Kannwischer, M.J., Rijneveld, J., Schwabe, P. and Stoffelen, K. (2019). [pqm4: Testing and benchmarking NIST PQC on ARM Cortex-M4](#). IACR Cryptology ePrint Archive, Report 2019/844.
- Montenegro, G., Kushalnagar, N., Hui, J. and Culler, D. (2007). [Transmission of IPv6 packets over IEEE 802.15.4 networks](#). RFC 4944. Internet Engineering Task Force. <https://doi.org/10.17487/RFC4944>
- Mosca, M. (2018). [Cybersecurity in an era with quantum computers: Will we be ready?](#) *IEEE Security & Privacy*, 16(5): 38-41. <https://doi.org/10.1109/MSP.2018.3761723>
- NIST (2024). [Module-Lattice-Based Key-Encapsulation Mechanism Standard](#). Federal Information Processing Standards Publication 203. National Institute of Standards and Technology, Gaithersburg, MD. <https://doi.org/10.6028/NIST.FIPS.203>
- Selander, G., Preuß Mattsson, J. and Palombini, F. (2024). [Ephemeral Diffie-Hellman Over COSE \(EDHOC\)](#). RFC 9528. Internet Engineering Task Force. <https://doi.org/10.17487/RFC9528>
- Shor, P.W. (1997). [Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer](#). *SIAM Journal on Computing*, 26(5): 1484-1509. <https://doi.org/10.1137/S0097539795293172>
- Wander, A.S., Gura, N., Eberle, H., Gupta, V. and Shantz, S.C. (2005). [Energy analysis of public-key cryptography for wireless sensor networks](#). *Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications*, 324-328.

Cite this article as: Desai B., Pavlovic D. and Tremblay T. (2026). [Post-Quantum Key Exchange Overhead on Low-Power Wireless Sensor Networks](#). *International Journal of Computer Science Engineering and Research*. 1(1), 25-28. doi: 10.62715/ijcser.2026.v1.i1.pp25-28