
The Importance of Standards in the Adoption of Quantum-Resistant Technologies

Matthew Campagna

Amazon Web Services Inc, USA, Chair of ETSI Cyber Quantum Safe Cryptography Working Group
E-mail: campagna@amazon.com

Received 12 August 2026; Accepted 12 August 2026

Abstract

The emergence of large-scale quantum computing poses a concrete threat to the public-key cryptographic algorithms widely used in today's information technology systems. Over the past three decades, post-quantum cryptography (PQC) and quantum key distribution (QKD) have been proposed to protect against this threat. This article traces the formation and output of research and standards organizations that made these technologies viable for deployment, with particular attention to ETSI, and the NIST Post-Quantum Cryptography standardisation initiative. The article argues that necessity and standardisation, rather than any single technical contribution, was the decisive factor in taking this research from academia and laboratories into an interoperable ecosystem now reaching production deployment. The article further conjectures on reasons why PQC will see much broader adoption than QKD based on some basic principles of adoption of standardized technologies.

Keywords: Post-quantum cryptography, quantum key distribution, standardisation, economics of standards, NIST, ETSI, network effects.

1 Introduction

Since the publication of Shor’s algorithm in 1994, it has been known that a large-scale quantum computer would break the traditional public key algorithms we use today [27]. Since then the cryptographic community has developed or revisited quantum-resistant alternatives. These fell into two distinct categories. The first were new cryptographic algorithms, designed to run on existing hardware systems based on alternative hard mathematical problems, so-called post-quantum cryptography (PQC), lattice-based constructions such as NTRU [15], code-based constructions tracing back to McEliece, [5, 18], and hash-based approaches [17, 19]. The second was quantum key distribution (QKD), an early proposal by Bennett and Brassard to use the effect of quantum mechanics to establish keys over a quantum channel [3].

These early proposals saw limited adoption. Two primary factors thwarting adoption were a sense of urgency and broad industry consensus on the security of these solutions. These conditions have changed over the past 30 years. There have been significant advancements in the development of quantum computing. In addition to regular improvements in the development of quantum computers, we have seen the number of qubits required to run Shor’s algorithm reduce to 10s of thousands of bits [6]. At the same time, we have seen an increase in the effort to research and standardize these alternative quantum-resistant solutions, leading to greater assurance in the algorithms today.

The community working in this space today is vast, but much of this work stemmed from just a handful of efforts consisting of PQCrypto, ETSI and NIST. This article provides an account of these efforts and connects them to the economics of standards to highlight why we are seeing broad adoption today of PQC and limited adoption of QKD [28].

2 The PQCrypto Academic Community

Following Shor’s result there were individual efforts to propose and even standardize quantum-resistant schemes, like NTRU. Ultimately, these saw limited adoption, but a community did emerge that focused on the fundamental research around developing post-quantum cryptography. The term “post-quantum cryptography” is attributed to Professor Daniel Bernstein and has persisted as the most common name for cryptographic algorithms designed to resist quantum attack. Bernstein coordinated the initial PQCrypto workshop

in 2006 [1], held at Katholieke Universiteit Leuven. This international workshop series is organized under the European Network of Excellence for Cryptology (ECRYPT). The workshops focused on the design, analysis and performance of alternative cryptographic algorithms. The archives can be found at [4]. It established post-quantum cryptography as a distinct field of study in cryptology. A broader academic community came to recognize this body of work. At the same time industry struggled to migrate from RSA to elliptic curve cryptography (ECC) as part of NSA's Suite B [21] algorithms. Deprecation of weak algorithms like MD5, SHA1, RC4 and DES turned out to be an arduous task in modern information technology systems. There is no compression algorithm for the cycle of research, conjecture, publication and analysis that leads to consensus that a new technology is secure and so worthy of being a candidate of such a migration. The output of PQCrypto and the industry observation around the development, deployment and deprecation cycle led to the establishment of the ETSI and Institute of Quantum Computing (IQC) at the University of Waterloo Quantum Safe Cryptography Workshop.

3 ETSI TC CYBER Working Group on Quantum Safe Cryptography

The ETSI technical group on Quantum Safe Cryptography (QSC) is a direct result of the ETSI IQC Quantum Safe Cryptography Workshop [13]. In 2013, Professor Michele Mosca of the IQC gathered participants from ETSI, NIST, NICT, IQC, KU Leuven, TU Darmstadt, BlackBerry, and Toshiba, including Bernstein, to establish this workshop. Its central finding was that the research, standardisation, and global deployment of new high-assurance cryptographic algorithms would require approximately twenty years, a timeline comparable for when we expected such a large scale quantum computer that would break the traditional public key cryptosystems. The workshop output was captured in a 2014 whitepaper publication [7] that identified sensible starting points for standardisation, including engagement with NIST and the European Union Agency for Cybersecurity (ENISA) for defining standards and requirements on post-quantum algorithms. The report also suggested the use of hybrid key establishment as a near-term mechanism for both long-term confidentiality and evaluating new quantum-resistant technology. While the workshop includes both QKD and PQC, the ETSI technical group on QSC focuses primarily on PQC, and QKD is the focus of the Industry Specification Group (ISG) of the same name (ISG-QKD).

The ISG-QSC became a working group of the Technical Committee on cybersecurity (TC CYBER) in 2017 and meets four times per year in Sophia-Antipolis, France. Its work program is defined by industry participants who propose and adopt New Work Items based on demonstrated need, surveying activities at NIST, ISO/IEC, and IETF to avoid duplication.

Notable deliverables include ETSI TS 103 744, “Quantum-safe Hybrid Key Establishment” [9], ETSI TR 104 016, “A Repeatable Framework for Quantum-Safe Migrations” [10], and ETSI TR 103 967, “Impact of Quantum Computing on Symmetric Cryptography” [11].

4 NIST Post-Quantum Cryptography Standardisation Initiative

NSA announced the Commercial National Security Algorithms (CNSA) 1.0 in 2015 which made clear their intention to deprecate traditional public key algorithms and transition to new quantum-resistant algorithms [20]. NIST kicked off their post-quantum cryptography initiative in April 2015, hosting the Workshop on Cybersecurity in a Post-Quantum World [25]. The workshop brought together academic researchers, and industry and government stakeholders for the stated reason that “NIST seeks to discuss issues related to post-quantum cryptography and its potential future standardisation.”

In 2016, NIST issued a formal Call for Proposals for quantum-resistant algorithms, receiving 69 complete submissions covering both key encapsulation mechanisms (KEMs) and digital signature schemes. NIST is one of the few bodies with the standing and reach to engage the broader cryptographic research community on the task of reaching consensus on the assurance and suitability of new cryptographic algorithms.

The evaluation proceeded through three public selection rounds from 2017 to 2022, each accompanied by standardisation conferences where submitters and the community presented analyses and attacks. In July 2022, NIST announced the selection of four algorithms: CRYSTALS-Kyber (now ML-KEM) for key encapsulation, and CRYSTALS-Dilithium (ML-DSA), FALCON, and SPHINCS+ (SLH-DSA) for digital signatures [23]. On August 13, 2024, NIST published the first three finalized Post-Quantum Cryptography standards: FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA) [24]. FALCON is still pending finalization and is expected to be published as FIPS 206 (FN-DSA). A fourth round continued to evaluate additional KEM candidates, with HQC selected for future standardisation.

5 ETSI Industry Specification Group on Quantum Key Distribution

Prior to both the ETSI's QSC and NIST PQC initiatives, ETSI's Industry Specification Group on Quantum Key Distribution (ISG QKD) was established in 2008. The formation of the working group coincided with the SECOQC project's multi-node QKD network demonstration in Vienna in autumn 2008 [26]. The report highlighted the need for standards. It signified that QKD was moving beyond the laboratory and that common specifications were required for interoperability, security evaluation, and integration with existing telecommunications infrastructure.

ETSI's ISG-QKD consisted of QKD device manufacturers, telecom operators, national research laboratories, and academic institutions. Its principal output is the GS QKD series of Group Specifications, covering application interfaces, component characterization, security proofs, and module security. ETSI GS QKD 016 defines a Common Criteria Protection Profile for pairs of prepare-and-measure QKD modules [8]. Certification to a Common Criteria Protection Profile raises the overall assurance in available certified products.

6 Adoption of Quantum-Resistant Technology

There is a wealth of information to be found in Swann's "The Economics of Standardisation" and its update [28, 29]. Anyone working in standards would benefit from reading this work. The initial work identifies four types of standards, not mutually exclusive. The standards in PQC and QKD really overlap into all four of these types: compatibility/interface, minimum quality/safety, variety reduction/focusing devices, and information/measurement.

One basic economic effect is that formal standards reduce the cost of coordination between implementors, provide a basis for certification and compliance, and can create an ecosystem of interoperable products that favour the consumer. In the case of post-quantum cryptography, the publication of FIPS 203, 204, and 205 has enabled secondary standards. The IETF has advanced work across most of its cryptographic protocol specifications to provide quantum-resistant options. We have seen new FIPS 140 certified cryptographic modules [24] become freely available. This all leads to an ecosystem of interoperable implementations: vendors can build products knowing they interoperate with a larger ecosystem, and consumers face lower costs because of the competition that interoperability fosters.

The most common approach for PQC deployment has been to adopt hybrid key establishment, pairing a traditional algorithm such as Elliptic

Curve Diffie-Hellman with a post-quantum key encapsulation method such as ML-KEM [16]. Hybrid schemes reduce the risk of new implementations failing under future analysis. The security of the combined key material is no weaker than the stronger of the two components.

We have seen that, for the most part, PQC fits into the existing interfaces that secure protocols, applications, and data stores through direct algorithm substitution. QKD, by contrast, is a point-to-point key establishment mechanism bound to a specific network link [7]. Further, QKD systems still require a traditional authentication mechanism for practical use. It does not benefit from the network effect of vendor interoperability or direct integration into existing telecommunication interfaces, like TLS. The security of stored data, multi-hop routing, cloud workloads, and asynchronous messaging falls outside QKD's operational model. This means, for most end-to-end communication channels, information transiting over a QKD link does not maintain the security properties of that link over the communication path. We have seen that, for the most part, PQC fits into the existing interfaces that secure protocols, applications, and data stores through direct algorithm substitution. QKD, by contrast, is a point-to-point key establishment mechanism bound to a specific network link [6]. Further, QKD systems still require a traditional authentication mechanism for practical use. It does not benefit from the network effect of vendor interoperability or direct integration into existing telecommunication interfaces, like TLS. The security of stored data, multi-hop routing, cloud workloads, and asynchronous messaging falls outside QKD's operational model. This means, for most end-to-end communication channels, information transiting over a QKD link does not maintain the security properties of that link over the communication path.

This distinction has practical consequences for both risk management and the economics of adoption. PQC fits into existing network and compliance frameworks without structural change: FIPS 203, 204, and 205 provide algorithm-level assurance that integrates into certificate hierarchies, TLS handshakes, and code-signing workflows, allowing migration through software updates. QKD requires separate physical infrastructure and an authentication mechanism. This dependency means QKD cannot stand alone as a complete security solution, and deployment cost is not shared across a broad ecosystem. Another headwind on adoption for QKD has been a lack of a clear requirement to deploy QKD. The UK National Cyber Security Centre and France's ANSSI have both published guidance positioning PQC as the primary mitigation for the quantum threat, with QKD acknowledged as a complement for specific high-assurance use cases [2, 22].

An argument can be made that key-establishment is more sensitive to passive attacks, like harvest now decrypt later. QKD provides information-theoretic security guarantees for point-to-point links. More recent work under Specialist Task Force 648 [14] will produce ETSI TS 104 146, “Authenticated Quantum-Safe Hybrid Key Establishment,” which integrates PQC techniques with optional QKD-derived keying material [12]. This specification represents an attempt to bring QKD within the same standards-driven economic model that has accelerated PQC adoption.

7 Conclusion

The threat from large-scale quantum computing to traditional public-key cryptography has been well known. What has changed in recent years is an improvement on the conjectured number of qubits to run Shor’s algorithm and the availability of standardized solutions that work within existing frameworks. The standardisation work described in this article, by NIST, ETSI ISG-QKD and ETSI TC CYBER WG QSC, has produced the specifications, evaluation frameworks, and algorithm selections that allow downstream standards organizations and technology providers to migrate to quantum-resistant technology. The standards have transitioned research into coordinated interoperable solutions. This has lowered the switching costs of adoption, and reduced the risks of cryptographic failure and improved interoperability between vended solutions.

PQC and QKD are complementary solutions, but the economics of standardisation favor PQC as the more prevalent solution. PQC operates at the protocol and application layer through algorithm substitution within existing software frameworks. Each new implementation extends the network of interoperable systems, lowering costs while increasing the scale of adoption. QKD, by contrast, is bound to the physical layer and to the specific links it spans. Its infrastructure requirements and per-link deployment model limit the network effects. For most organizations, PQC provides the more complete and economical path to quantum resistance.

No doubt that this collection of how we arrived at these new standardized technologies is incomplete. Regardless, the standards that foster broad adoption are nearly complete, the migration path is mostly understood, and the frameworks and migration guides continue to provide the necessary guidance for institutions to confidently migrate to quantum-resistant solutions.

References

- [1] “PQCrypto 2006: International Workshop on Post-Quantum Cryptography,” 23–26 May 2006, Katholieke Universiteit Leuven, Belgium. Available: <http://postquantum.cr.yp.to/pqcrypto2006record.pdf>.
- [2] ANSSI (2024) (France), “Avis relatif a la migration vers la cryptographie post-quantique,” <https://messervices.cyber.gouv.fr/guides/avis-de-lanssi-sur-la-migration-vers-la-cryptographie-post-quantique>.
- [3] Bennett, C.H., Brassard, G., “Quantum Cryptography: Public Key Distribution and Coin Tossing,” in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984, pp. 175–179. <https://doi.org/10.1016/j.tcs.2014.05.025>.
- [4] Bernstein, D.J. and Lange, T., “Post-Quantum Cryptography - Conferences,” pqcrypto.org, accessed 3 August 2026. Available: <https://pqcrypto.org/conferences.html>.
- [5] Bernstein, D.J., Lange, T., Peters, C., “Attacking and Defending the McEliece Cryptosystem,” in Post-Quantum Cryptography (PQCrypto 2008), Lecture Notes in Computer Science, vol. 5299, pp. 31–46. Springer. <https://eprint.iacr.org/2008/318.pdf>.
- [6] Cain, M., Xu, Q., King, R., Picard, L.R.B., Levine, H., Endres, M., Preskill, J., Huang, H.-Y., Bluvstein, D., “Shor’s algorithm is possible with as few as 10,000 reconfigurable atomic qubits,” arXiv:2603.28627 [quant-ph], 30 March 2026. <https://arxiv.org/abs/2603.28627>.
- [7] Campagna, M., Chen, L. et al., “Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges,” 2014. Available: https://docbox.etsi.org/Workshop/2013/201309_CRYPTO/Quantum_Safe_Whitepaper_1_0_0.pdf.
- [8] ETSI GS QKD 016 V2.1.1, “Quantum Key Distribution (QKD); Common Criteria Protection Profile - Pair of Prepare and Measure Quantum Key Distribution Modules,” January 2024. Available: https://www.etsi.org/deliver/etsi_gs/QKD/001_099/016/02.01.01_60/gs_QKD016v020101p.pdf.
- [9] ETSI TR 103967 V1.1.1, “Cyber Security (CYBER); Quantum-Safe Cryptography (QSC); Impact of Quantum Computing on Symmetric Cryptography,” January 2025. <https://cdn.standards.iteh.ai/samples/64860/b4aa090bec73481db535d075f687dfa8/ETSI-TR-103-967-V1-1-1-2025-01-.pdf>.

- [10] ETSI TR 104016 V1.1.1, “CYBER; Quantum-Safe Cryptography (QSC); A Repeatable Framework for Quantum-Safe Migrations,” 2024. https://www.etsi.org/deliver/etsi_tr/104000_104099/104016/01.01.01_60/tr_104016v010101p.pdf
- [11] ETSI TS 103744 V1.2.2, “CYBER; Quantum-Safe Cryptography (QSC); Quantum-safe Hybrid Key Establishment,” March 2025. https://www.etsi.org/deliver/etsi_ts/103700_103799/103744/01.02.02_60/ts_103744v010202p.pdf
- [12] ETSI TS 104146 (in development), “Cybersecurity (CYBER); Quantum-Safe Cryptography (QSC); Authenticated Quantum-Safe Hybrid Key Establishment,” STF 648, 2026.
- [13] ETSI, “e-Proceedings: 1st ETSI/IQC Quantum Safe Cryptography Workshop,” September 2013. Available: https://docbox.etsi.org/Workshop/2013/201309_CRYPT/e-proceedings_Crypto_2013.pdf.
- [14] ETSI, “Specialist Task Force 648: Quantum-Safe Cryptography – Authenticated Hybrid Key Establishment and Secure Implementation Guidance,” ETSI Portal. Available: <https://portal.etsi.org/STF/STFs/STFHomePages/STF648>.
- [15] Hoffstein, J., Pipher, J., Silverman, J.H., “NTRU: A Ring-Based Public Key Cryptosystem,” in Buhler, J.P. (ed.) *Algorithmic Number Theory (ANTS-III)*, Lecture Notes in Computer Science, vol. 1423, 1998, pp. 267–288. Springer, Berlin, Heidelberg. <http://csclub.cs.sjsu.edu/faculty/pollett/masters/Semesters/Spring21/michaela/files/Hoffstein97.pdf>.
- [16] Kampanakis, P., Kwiatkowski, K. et al., “Post-quantum hybrid ECDHE-MLKEM Key Agreement for TLSv1.3,” IETF Internet-Draft, draft-ietf-tls-ecdhe-mlkem-02, November 2025. Available: <https://datatracker.ietf.org/doc/html/draft-ietf-tls-ecdhe-mlkem-02>.
- [17] Lamport, L., “Constructing Digital Signatures from a One-Way Function,” SRI International, Technical Report CSL-98, October 1979. <https://di-mgt.com.au/docs/Lamport79-Constructing-Digital-Signatures-from-a-One-Way-Function.pdf>.
- [18] McEliece, R.J., “A Public-Key Cryptosystem Based On Algebraic Coding Theory,” DSN Progress Report, 42–44, 1978, pp. 114–116. <https://ntrs.nasa.gov/api/citations/19780016269/downloads/19780016269.pdf#page=123>.

- [19] Merkle, R.C., “Secrecy, Authentication, and Public Key Systems,” Ph.D. dissertation, Stanford University, 1979. (Reprinted as Technical Report No. 1979-1, Information Systems Laboratory, Stanford.) <https://www.proquest.com/openview/1ae50982b34bee7e3f1b8e232bb98e42/1?pq-origsite=gscholar&cbl=18750&diss=y>.
- [20] National Security Agency, “Commercial National Security Algorithm Suite,” Information Assurance Directorate, 19 August 2015. Available: <https://apps.nsa.gov/iaarchive/programs/iad-initiatives/cnsa-suite.cfm>.
- [21] National Security Agency, “Fact Sheet NSA Suite B Cryptography,” 16 February 2005. Available: http://web.archive.org/20051128182632/www.nsa.gov/ia/industry/crypto_suite_b.cfm.
- [22] NCSC (UK), “Quantum Security Technologies,” Guidance, 2025. <https://www.ncsc.gov.uk/paper/quantum-security-technologies>.
- [23] NIST, “NIST Announces First Four Quantum-Resistant Cryptographic Algorithms,” July 5, 2022. Available: <https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms>.
- [24] NIST, “NIST Releases First 3 Finalized Post-Quantum Encryption Standards,” August 13, 2024. Available: <https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards>.
- [25] NIST, “Workshop on Cybersecurity in a Post-Quantum World,” April 2–3, 2015, Gaithersburg, MD. Available: <https://csrc.nist.gov/Events/2015/Workshop-on-Cybersecurity-in-a-Post-Quantum-World>.
- [26] Poppe, A., Peev, M., Maurhart, O., “Outline of the SECOQC Quantum-Key-Distribution Network in Vienna,” arXiv:0804.0122, 2008. Also published in *International Journal of Quantum Information*, 6(2), 209–218. <https://doi.org/10.1142/S0219749908003529>.
- [27] Shor, P.W., “Algorithms for quantum computation: Discrete logarithms and factoring,” *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124–134. doi: 10.1109/SFCS.1994.365700.
- [28] Swann, G.M.P., “The Economics of Standardisation,” Report for the Department of Trade and Industry, London, 2000. Available: <https://webarchive.nationalarchives.gov.uk/ukgwa/20070628230000/http://www.dti.gov.uk/files/file11312.pdf>.

- [29] Swann, G.M.P., “The Economics of Standardisation: An Update,” Report for the Department of Business, Innovation and Skills, BIS Occasional Paper No. 2, London, 2010. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/32444/10-1135-economics-of-standardization-update.pdf

Biography

Matthew Campagna is a Sr. Principal Engineer & Cryptographer for Amazon Web Services Inc. He oversees the design and analysis of cryptographic solutions across AWS. He is a member of the ETSI Security Algorithms Group Experts (SAGE), and Chair of ETSI TC CYBER Quantum Safe Cryptography working group. Previously, Matthew managed Certicom/BlackBerry’s Cryptography Research Group focused on the development of IP and standardisation for elliptic curve cryptography. He studied Mathematics at Wesleyan University and Fordham University. <https://www.linkedin.com/in/matt-campagna/>.

