The Post-Quantum Apocalypse Is Already Upon Us

Michael B. Jones[1]

[1]*Self-Issued Consulting, LLC, Redmond, Washington 98053, United States of America*

Abstract

"The future is already here — it's just not evenly distributed" is an apt description of the impact of quantum computers on cryptography and its use in our identity systems. We all know that quantum computers are predicted to be able to break the cryptographic algorithms used in today's identity systems (RSA, Elliptic Curve, etc.) at some unknown point in the future. But this possibility has huge implications *right now*. "Disruptive" is an understatement. *Every* piece of software using cryptography has to be updated *before* Cryptographically Relevant Quantum Computers (CRQCs) are created (and we don't know when that will be). "Store now — decrypt later" attacks require action now, not later. Are you using software and protocols that may never be updated for the post-quantum world (such as SAML)? Are you comfortable with your migration path to fully quantum-safe software? This position paper will help you evaluate what you need to do when and how and why to avoid being a victim of the Post-Quantum Apocalypse.

Keywords

Quantum-Resistant Cryptography, Post-Quantum Cryptography, Cryptographic Vulnerabilities, Updating Software and Systems, X.509, OpenID Federation, OpenID Connect, SAML

1. The Impact of Quantum Cryptography and Call to Action

William Gibson observed: "The future is already here — it's just not evenly distributed". That's an apt description of the impact of quantum computers on cryptography and its use in our identity systems.

The future impacts the present. Quantum computers are predicted to be able to break the cryptographic algorithms used in today's identity systems: RSA, Elliptic Curve, etc. We don't know when. This possibility has huge implications now. All software using cryptography has to be updated before Cryptographically Relevant Quantum Computers (CRQCs) [1] are created. Saying that this is disruptive is an understatement!

Long-lived digital signatures are another reason action is needed now. Signed code [2], particularly for Internet of Things (IoT) devices, uses long-lived digital signatures. In some cases, this code may not be able to be updated. Signed trust anchors, for example, for PKI certificate chains [3] and federations [4], use long-lived digital signatures. Any signatures you want to be able to determine validity of in the future need to use post-quantum-safe algorithms now.

2. Two Kinds of Post-Quantum Algorithms

There are two kinds of post-quantum cryptographic algorithms: pure post-quantum algorithms and hybrid post-quantum algorithms.

- Pure post-quantum algorithms are designed to resist attacks by Cryptographically Relevant Quantum Computers on their own. For instance, ML-DSA [5] for signatures and ML-KEM [6] for encryption are pure post-quantum algorithms.
- Hybrid algorithms combine a pure post-quantum algorithm and a classical algorithm. For instance, ML-DSA-44 [5] combined with ECDSA P-256 [7] is a hybrid signature algorithm, which is currently undergoing standardization in the IETF [8]. For hybrid algorithms, the hybrid combination is unbroken unless both of the algorithms combined are broken.

TDI 2026: 4th International Workshop on Trends in Digital Identity, April 20–21, 2026, Verona, Italy

mike@self-issued.consulting (Michael B. Jones)

https://self-issued.consulting/ (Michael B. Jones)

2.1. Arguments for Pure Post-Quantum Algorithms

Switching to pure post-quantum algorithms is a "straightforward" application of algorithm agility. For instance, one can replace RSASSA-PKCS1-v1_5 [9] with ML-DSA-44 [5] and RSA-OAEP-256 [9] with ML-KEM [6]. This avoids the additional complexity of hybrid algorithms. It also avoids the size and computation time penalty of using two algorithms.

2.2. Arguments for Hybrid Post-Quantum Algorithms

Using both a pure post-quantum algorithm and a classical algorithm mitigates risk of the pure post-quantum algorithm being broken. Pure post-quantum algorithms are new. Vulnerabilities may be found.

We can't know, for instance, whether ML-DSA-44 or ECDSA P-256 will be broken first. Hybrid combinations are not vulnerable unless both algorithms are broken. Also, the hybrid approach is required in some jurisdictions (for instance, in the EU [10]).

3. Caveats

I am not a cryptographer. I'm therefore not going to critique the proposed post-quantum algorithms themselves. I will not be commenting on validity or strengths of particular post-quantum algorithms. I will not be recommending which post-quantum algorithms to choose in what cases, for instance, making tradeoffs between ML-DSA and SLH-DSA [11]. I assume you will consult cryptographers and engineering experts to choose appropriate post-quantum algorithms for your uses.

I do not have a crystal ball. I'm therefore not going to predict when Cryptographically Relevant Quantum Computers (CRQCs) will be developed. NIST, EU, others have done risk assessments and produced post-quantum migration recommendations based on them. I assume you will utilize these professional assessments and resulting recommendations and legislation to inform your decision making.

4. Costs to Note When Planning Your Migration

Post-quantum algorithms have different sizes and performance than classical algorithms. For instance, ECDSA P-256 has a public key size of 64 bytes, a private key size of 32 bytes, and a signature size of 64 bytes. Whereas ML-DSA-44 has a public key size 1,312 bytes, a private key size of 2,560 bytes, and a signature size 2,420 bytes. The larger sizes may exceed buffer limitations in some software and protocols. Computational speed is another important factor to compare.

Choosing the right post-quantum algorithms to deploy for particular applications involves weighing important engineering tradeoffs. Which algorithms to use for your use cases is out of scope for this paper.

5. State of the Standards

Many nations and regions have developed or are developing and are standardizing post-quantum cryptographic algorithms for national use. Some of these are being used broadly and internationally.

5.1. US Standards

The US National Institute of Standards and Technology (NIST) has taken the lead on developing post-quantum standards for use within the United States. This has been done through multiple rounds of public algorithm submissions and reviews of the submissions. Many other countries are also referencing the NIST algorithms.

Some of the NIST algorithms are completed standards. For instance, ML-DSA [5] and SLH-DSA [11] for signatures and ML-KEM [6] for encryption are done. Other proposed NIST algorithms, such as FN-DSA, which will be FIPS 206 (formerly known as "Falcon") [12], are still works in progress.

Evaluation of new rounds of submissions are also in progress. For more on the NIST post-quantum effort, see the NIST post-quantum cryptography information site [13].

5.2. Non-US Standards

Multiple countries and regions around the world are also developing post-quantum algorithms and guidance for national and regional use. The European Union has a "A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography" [14]. China has the Next-generation Commercial Cryptographic Algorithms Program (NGCC) [15], which is accepting and evaluating public submissions. Others, including Russia, Japan, and South Korea also are determining national post-quantum algorithm standards [16].

5.3. IETF Post-Quantum Standardization

The Internet Engineering Task Force (IETF) is actively standardizing the use of post-quantum algorithms in Internet protocols. This work is happening in many working groups, including TLS, LAMPS, COSE, JOSE, IPSecME, CFRG, HPKE, Plants, and PQuip.

The TLS working group is standardizing both pure [17] and hybrid post-quantum [18] algorithms for use in the Transport Layer Security (TLS) protocol (a.k.a. HTTPS). The LAMPS working group is standardizing post-quantum certificate formats for X.509 [19], which supports the TLS work.

The JOSE and COSE working groups are standardizing multiple signature and encryption algorithms for their respective cryptographic formats. For instance, the COSE working group just finished standardizing how to use ML-DSA signatures for both COSE and JOSE [20]. A lot has already been completed in the IETF but a lot remains to be done.

The IETF working groups spend a fair amount of energy debating which hybrid combinations to standardize. There's a general consensus to standardize only a small number of code points that make sense – not the full combinatorial combination of possibilities. In theory, for instance, one could standardize all combinatorial combinations of 3 ECDSA (with the P-256, P-384, and P521 curves) or 2 EdDSA (with the Ed25519 and Ed448 curves) classical algorithms with 3 ML-DSA (ML-DSA-44, ML-DSA-65, ML-DSA-87) post-quantum algorithms. The result would be 15 hybrid combinations; but that's not going to happen, since implementers want fewer choices and only those that make practical sense. Deciding which hybrid combinations make sense is a significant focus of IETF post-quantum standardization work.

6. Early Post-Quantum Deployments

"The future is already here — it's just not evenly distributed" is certainly an apt description of the state of post-quantum deployments. Rollouts are gated by standards progress and standards adoption. We're certainly in the very early stages of deployments.

On the other hand, there are surprising areas of significant progress already using completed standards. At IETF 123 in July 2025, John Preuß Mattsson reported "40% of HTTPS client requests use PQC" [21]. This is possible because the TLS and X.509 standards are done and Google and others proactively deployed them in Chrome and other software. This is already putting a dent in the harvest-now/decrypt-later attacks on the Internet. Yubico has prototype FIDO authenticators using ML-DSA [22].

7. Call to Action

The time to act to prepare for the advent of cryptographically relevant quantum computers is now. Here's the steps I recommend.

7.1. Inventory software you're responsible for and make a plan

All software using cryptography has to be updated before Cryptographically Relevant Quantum Computers (CRQCs) are created. Understand your exposure and responsibilities. Your platform vendors will update some of it. For example, Chrome is already there.

Some software and standards are no longer maintained. Many SAML2 implementations are unsupported. There isn't a post-quantum plan for XMLDSIG. Determine what you need to update and/or replace in your environment and make a plan.

7.2. Understand what's truly hard about this

There are many aspects of preparing for a post-quantum future that are hard:

- *Developing post-quantum algorithms is hard* – but that's what cryptographers do.
- *Creating standards for using post-quantum algorithms is hard* – but that's what standards professionals do.
- *Updating software to use post-quantum standards is hard* – but that's what responsible maintainers do.
- *Deploying the updated software in your environment and replacing that which will not be updated is very hard* – doing that is your responsibility.

Acting in the presence of uncertainty can be the hardest thing of all. Will you and your organization step up to the challenge and do what's necessary to prepare for the coming post-quantum future?

8. Conclusion

The post-quantum apocalypse is already upon us. It's time to prepare and act.

Acknowledgments

This work was supported by Fondazione Bruno Kessler (FBK).

Declaration on Generative AI

The author has not employed any Generative AI tools.

References

[1] M. Ivezic, Cryptographically Relevant Quantum Computers (CRQCs), 2023. URL: https://postquantum.com/post-quantum/crqc/.

[2] Multiple Authors, Code signing, Wikipedia, 2026. URL: https://en.wikipedia.org/wiki/Code_signing.

[3] S. Boeyen, S. Santesson, T. Polk, R. Housley, S. Farrell, D. Cooper, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 5280, RFC Editor, 2008. doi:10.17487/RFC5280.

[4] R. Hedberg, M. B. Jones, A. Å. Solberg, J. Bradley, G. De Marco, V. Dzhuvinov, OpenID Federation 1.0, 2026. URL: https://openid.net/specs/openid-federation-1_0.html.

[5] National Institute of Standards and Technology, Module-Lattice-Based Digital Signature Standard, FIPS 204, NIST, 2024. doi:10.6028/NIST.FIPS.204.

[6] National Institute of Standards and Technology, Module-Lattice-Based Key-Encapsulation Mechanism Standard, FIPS 203, NIST, 2024. doi:10.6028/NIST.FIPS.203.

[7] National Institute of Standards and Technology, Digital Signature Standard (DSS), FIPS 186-4, NIST, 2013. doi:10.6028/NIST.FIPS.186-4.

[8] M. Ounsworth, J. Gray, M. Pala, J. Klaußner, S. Fluhrer, Composite Module-Lattice-Based Digital Signature Algorithm (ML-DSA) for use in X.509 Public Key Infrastructure, Internet-Draft draft-ietf-lamps-pq-composite-sigs-19, Internet Engineering Task Force, 2026. URL: https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-sigs/19/.

[9] K. Moriarty, B. Kaliski, J. Jonsson, A. Rusch, PKCS #1: RSA Cryptography Specifications Version 2.2, RFC 8017, RFC Editor, 2016. doi:10.17487/RFC8017.

[10] European Commission, Commission Recommendation (EU) 2024/1101 of 11 April 2024 on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography, in: Official Journal of the European Union, 2024. URL: https://eur-lex.europa.eu/eli/reco/2024/1101/oj/.

[11] National Institute of Standards and Technology, Stateless Hash-Based Digital Signature Standard, FIPS 205, NIST, 2024. doi:10.6028/NIST.FIPS.205.

[12] National Institute of Standards and Technology, NIST Releases First 3 Finalized Post-Quantum Encryption Standards, 2024. URL: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.

[13] National Institute of Standards and Technology, Post-Quantum Cryptography, 2026. URL: https://csrc.nist.gov/projects/post-quantum-cryptography.

[14] European Commission, A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, 2025. URL: https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography.

[15] Institute of Commercial Cryptography Standards, Next-generation Commercial Cryptographic Algorithms Program (NGCC), 2025. URL: https://www.niccs.org.cn/niccs/index.html.

[16] M. Ivezic, Sovereignty in the PQC Era: Standards, Trust, and Crypto-Agility, 2025. URL: https://postquantum.com/post-quantum/sovereignty-quantum-pqc/.

[17] D. Connolly, ML-KEM Post-Quantum Key Agreement for TLS 1.3, Internet-Draft draft-ietf-tls-mlkem-07, Internet Engineering Task Force, 2026. URL: https://datatracker.ietf.org/doc/draft-ietf-tls-mlkem/07/.

[18] K. Kwiatkowski, P. Kampanakis, B. Westerbaan, D. Stebila, Post-quantum hybrid ECDHE-MLKEM Key Agreement for TLSv1.3, Internet-Draft draft-ietf-tls-ecdhe-mlkem-05, Internet Engineering Task Force, 2026. URL: https://datatracker.ietf.org/doc/draft-ietf-tls-ecdhe-mlkem/05/.

[19] J. Massimo, P. Kampanakis, S. Turner, B. Westerbaan, Internet X.509 Public Key Infrastructure – Algorithm Identifiers for the Module-Lattice-Based Digital Signature Algorithm (ML-DSA), RFC 9881, RFC Editor, 2025. doi:10.17487/RFC9881.

[20] M. Prorock, O. Steele, ML-DSA for JSON Object Signing and Encryption (JOSE) and CBOR Object Signing and Encryption (COSE), RFC 9964, RFC Editor, 2026. doi:10.17487/RFC9964.

[21] J. P. Mattsson, Migrating Telecom to Quantum-Resistant Cryptography on a Global Scale, Presentation at IETF 123, 2025. URL: https://datatracker.ietf.org/meeting/123/materials/slides-123-ietf-sessd-ietf-123-host-speaker-slides-00.

[22] Cyber News Live, Yubico Showcases Post-Quantum Cryptography & Digital Identity Innovation, 2025. URL: https://cybernewslive.com/yubico-post-quantum-cryptography-digital-identity/.