Moving to a Post-Quantum World

Challenges in Engineering and Deploying Quantum Resistant Cryptography

Alessandro Barenghi[1][0000-0003-0840-6358]

Dipartimento di Elettronica e Informazione - Politecnico di Milano
Piazza Leonardo da Vinci 32, 20133 Milano alessandro.barenghi@polimi.it

Abstract. The continuous efforts in relaizing a large scale quantum computer are in turn obtaining steady, if slow, progress, thanks to the promise of obtaining efficient computational solutions to socially relevant problems, such as computational chemistry ones. It is therefore reasonable to take measures against the only adverse effect of the availability of large scale quantum computers, i.e., the ability to solve the integer factoring problem and the discrete logarithm over cyclic groups. Transitioning the current state of the art cryptographic protocols to the so-called *post-quantum* cryptographic primitives presents a variety of engineering challenges which range from performing proper drop-in replacement, to redesigning the working principles of the protocol when the post-quantum primitives are unavailable or lack the required temporal or spatial efficiency. This short abstracts summarizes the current state of availability of the post-quantum cryptographic primitives and highlights the relevant challenges in the post-quantum transition.

Keywords: Post quantum cryptography · Engineering Cryptography · Post quantum transition

1 Post-quantum cryptographic primitives

The design of post-quantum cryptographic primitives requires to choose computationally hard problems which stay so even when the adversary is equipped with a quantum computer. Designing post-quantum cryptographic primitives concerns asymmetric primitive design, as symmetric primitives, such as block ciphers and cryptographic hashes can be easily adapted to resist attacks with quantum computers by doubling their security parameter (key length or digest). To this end, successful proposals were made considering: the problem of decoding the syndrome of a random error correction code, coming from an error vector with bounded Hamming weight; finding either the shortest or the closest vector in a discrete modular lattice; finding collisions in a cryptographic hash function; finding solutions to multivariate quadratic equations over a finite field and determining an isogeny out of a given set of automorphisms of an elliptic curve.

While most of the aforementioned problems are known to be NP-complete, and thus extremely unlikely to be solvable in asymptotically polynomial time by

a quantum computer, designing sound cryptographic primitives also requires to consider exponential time cryptanalytic algorithms, and determine appropriate parameters (e.g, keypair sizes) for the scheme. Furthermore, it is common to build post-quantum cryptographic primitives upon computationally hard problems by means of combining them with symmetric primitives to achieve strong security guarantees, e.g., the resistance against active attackers.

Efforts towards fostering proposals and cryptanalytic scrutiny took the form of international contests by standardization entities, among which one of with the larger resonance was the one, which was started in 2017 by the United States National Institute of Standards and Technology (NIST). The contest, which has seen four rounds of selection has recently ended up in selecting two Key Encapsulation Methods (KEMs), FIPS 203 (ML-KEM, formerly CRYSTALS-Kyber, a lattice-based scheme) and FIPS 207 (HQC-KEM, a code based scheme) and three digital signatures FIPS 204 (ML-DSA, formerly CRYSTALS-Dilithium, lattice based), FIPS 205 (SLH-DSA, cryptographic hash based), and FIPS 206 (FN-DSA, lattice based). Due to the partially unsatisfactory performance profile of SLH-DSA, and the desire not to hedge all security guarantees of digital signatures only on lattice-based computationally hard problems, NIST has opened an additional call for digital signatures which is currently in its second round of selection. Similar standardization efforts were put forward by China and explicit suggestions made by European national agencies on which ciphers are advisable to be employed.

The general consensus is that the transition to post quantum cryptographic primitives should be completed by 2030 for critical systems, and by 2035. In doing so, some use case scenarios should be prioritized. In particular, replacing key establishment mechanisms (commonly now done via elliptic-curve Diffie-Hellman key agreement) is considered highly critical due to the possibility of *store now, decrypt later* style attacks, i.e., mass gathering of encrypted communications which are to be decrypted whenever a large enough quantum computer is available. Priority should also be given, although less so than key agreements, to the migration of digital signature algorithms employed to provide origin authentication guarantees expected to be long term (e.g, real estate deeds): in such a scenario a transition is due before a large scale quantum computer is available for targeted attacks. Finally, the transition of digital signature mechanisms employed to ensure origin authentication during interactive key establishment is the last scenario to be tackled: indeed, to compromise the security of communications in this case a large scale quantum computer should be available in the precise moment when the key establishment is performed, and is should have enough computational power to complete the attack with a low latency.

Concerning the available post-quantum cryptographic primitives, it's worth observing that currently no post-quantum alternative to the Diffie-Hellman key agreement is available; this in turn calls to providing *forward secrecy* guarantees [7], and performing symmetric key [3] employing only KEMs. It is also worth observing that current post-quantum signatures do not provide the level of efficiency (both computational and in signature size) which was available with

RSA or elliptic-curve DSA signatures. Indeed, there is no post-quantum signature scheme currently providing small signatures and public keys together with low (hundreds of kilocycles) computational latencies. As a final note in the evaluation of primitives available in a post-quantum world, it is useful to know that the concrete computational efforts to be put forward with a quantum computer to breach a 128b symmetric cipher are likely excessive, making the attack unfeasible [2]. Indeed, while Grover's algorithm provides a quadratic speedup in the solution of a key finding problem of this kind, to fully exploit this speedup the computation needs to be sequential, as there is currently no known way of parallelizing Grover's approach without sacrificing its speedup.

2 The forerunners

Some cryptographic protocols have been forerunners in the transition to the use of post-quantum primitives. A prominent example of post-quantum transition is represented by the OpenSSH [8] implementation of the SSH [5] protocol. Indeed, OpenSSH developers employed a post-quantum key agreement by default since release 9.0 (April 2022), deriving the session key with a hybrid approach, i.e., combining the symmetric keys established with a classical and a post-quantum key establishment. The choice of the developers was a hybrid of Streamlined NTRU Prime [1] (`sntrup761`) and X25519 [5] More recently, in OpenSSH 9.9, we have added a second post-quantum key agreement the support for using ML-KEM instead of Streamlined NTRU Prime was added, and became the new default scheme in OpenSSH 10.0 (April 2025). Currently, no post-quantum cryptographic signatures are planned in OpenSSH in the short term, waiting for proposal with a large consensus.

Among the forerunners of the post-quantum transition, prominent instant messaging protocols such as the ones employed by Signal, and the one employed by Apple's iMessage were the first to transition to a post quantum key establishment, following the same hybrid approach as SSH in September 2023 and February 2024, respectively. Concerning the primitives, both Signal and iMessage made the choice to employ CRYSTALS-Kyber with its most conservative parameters, hybridized with X22519.

We observe that, in all the aforementioned cases, the common ground which facilitated the transition was the relatively abundant computational power available in both scenarios, and the relatively little criticality of low latency key establishments (indeed, instant messaging is asynchronous by nature).

3 Transport Layer Security and DNSSec

The Transport Layer Security (TLS) protocol has been the longstanding mainstay of secure communications, since the inception of its predecessor, Secure Sockets Layer, designed to protect HTTP communications. TLS, currently at version 1.3 [6] provides a transparent way of securing TCP communications, regardless of the application level protocol carried by it, and has thus enjoyed

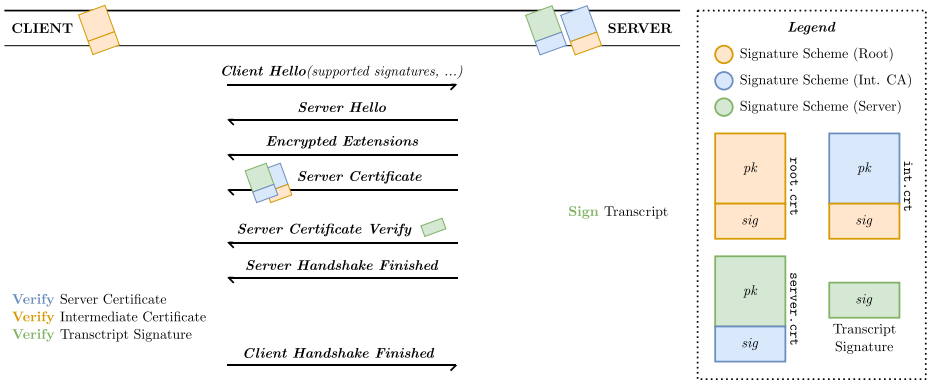

Fig. 1. A summary of a TLS 1.3 connection initiation, together with the cryptographic objects involving asymmetric primitives at play.

success beyond securing HTTP (e.g., in securing e-mail transport and delivery protocols such as SMTP). Transitioning TLS to post quantum primitives starts by reverting a decision made in standardizing version 1.3, i.e. removing the support for the lone KEM which remained, namely, RSA-KEM. RSA-KEM was removed on the grounds that providing forward secrecy with RSA is unfeasible due to its significantly slow key generation process. Adding back KEMs to the protocol is however not expected to be requiring substantial changes; however, providing forward security guarantees without further changes requires a KEM with a fast key(pair) generation algorithm.

A further challenging point in TLS is the embedding of post-quantum signature algorithms. The challenges are best understood when recalling the structure of a TLS connection establishment as depicted in Figure1 The connection establishment procedure sees three signature verification computations, made by the client, and one signature generation, made by the server. Therefore, the benefits of post quantum signatures having a fast verification, at the cost of a slow signature, such as SLH-DSA have no impact on the server side, which is typically the one required to handle the larger amount of connections per second. Focusing now on the spatial constraints, we have that TLS limits the maximum size of the transcript signature in the communication establishment to 64 kiB [6], in turn excluding any signature algorithm with larger signatures. A further constrain comes from the fact that TLS limits the total size of the certificate chain to 16 MiB. While this is not expected to be problematic, even with very large signatures and public keys (a typical, length two certificate chain contains two signatures and two public keys) preliminary experiments have shown that lower, and somewhat arbitrary limits in common software libraries (e.g., OpenSSL) were adopted, and will need revision.

4 Embedded systems

Transitioning highly resource limited platforms, such as microcontrollers, smart cards and RFID tags is expected to present significant challenges. In particular, while some post quantum primitives have larger computational requirements, the main bottleneck is expected to be their memory consumption. As an example, even when considering a very high end microcontroller, such as the STM32L4R5ZI, high end Cortex-M4 has 640kiB SRAM, 2 MiB Flash, selected by the `pqm4` [4] project as the benchmarking platform, as its CPU matches the one suggested by NIST, only 10 out of 14 signatures currently involved in the additional call fit on it (namely, the candidates being CROSS, HAWK, Mirath, MQOM, PERK, RYDE, MAYO, SNOVA, UOV, and FAEST). Typical roadblocks come from the use of a large number of parallel iterations of a zero knowledge identification scheme, together with a Fiat-Shamir transform to turn them into a signature. The computation of such a scheme requires to prepare a large number of commitments, while revealing only some of them. In particular, which commitments should be revealed is pseudorandomly seleted after preparing all of them, in turn forcing implmentors to either keep them all in main memory, or recompute them, a the cost of additional overhead.

5 Concluding remarks

The transition to post-quantum cryptosystem has effectively already begun, and protocols employed in non constrained environments have made significant steps toward its completion already. Fully transitioning other systems will require *cryptographic agility*, i.e., the capability of changing the employed primitives at runtime; indeed, rarely a single cryptographic primitive fits all applicative scenarios. It's worth noting that acquiring this agility may as well pay off twice: once during the current transition, and the second time whenever more efficient post-quantum cryptographic primitives are developed and validated by the community.

6 Acknowledgements

This work was partially supported by project SERICS (PE00000014) under the Italian MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU, and with partial support by the PRIN 2022 project POst quantum Identification and eNcryption primiTives: dEsign and Realization (POINTER) ID-2022M2JLF2. We acknowledge the contribution of Marco Gianvecchio in surveying the concrete state of memory limitations in TLS communications.

References

1. Friedl, M., Mojzis, J., Josefsson, S.: Secure Shell (SSH) Key Exchange Method Using Hybrid Streamlined NTRU Prime sntrup761 and X25519 with SHA-

512: sntrup761x25519-sha512. Internet-Draft draft-ietf-sshm-ntruprime-ssh-05, Internet Engineering Task Force (Aug 2025), https://datatracker.ietf.org/doc/draft-ietf-sshm-ntruprime-ssh/05/, work in Progress
2. Jaques, S.: Quantum Attacks on AES - Keynote talk at CHES 2024 (2024), https://www.youtube.com/watch?v=eB4po9Br1YY
3. Juaneda, J., Dehez-Clementi, M., Deneuville, J.C., Lacan, J.: RHQC: post-quantum ratcheted key exchange from coding assumptions. Cryptology ePrint Archive, Paper 2025/481 (2025), https://eprint.iacr.org/2025/481
4. Kannwischer, M.J., Krausz, M., Petri, R., Yang, S.Y.: pqm4: Benchmarking nist additional post-quantum signature schemes on microcontrollers. IACR Cryptol. ePrint Arch. **2024**, 112 (2024), https://api.semanticscholar.org/CorpusID:267749317
5. Lonvick, C.M., Ylonen, T.: The Secure Shell (SSH) Protocol Architecture. RFC 4251 (Jan 2006). https://doi.org/10.17487/RFC4251, https://www.rfc-editor.org/info/rfc4251
6. Rescorla, E.: The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446 (Aug 2018). https://doi.org/10.17487/RFC8446, https://www.rfc-editor.org/info/rfc8446
7. Schwabe, P., Stebila, D., Wiggers, T.: Post-quantum TLS without handshake signatures. In: Ligatti, J., Ou, X., Katz, J., Vigna, G. (eds.) ACM CCS 2020: 27th Conference on Computer and Communications Security. pp. 1461–1480. ACM Press (Nov 2020). https://doi.org/10.1145/3372297.3423350
8. The OpenBSD foundation: OpenSSH. https://www.openssh.com/