Challenges to migrate to post-quantum: taxonomy

Sofía Celi

July 27, 2022

1 Challenges

Quantum computers fundamentally change the way certain protocols, properties, storage and retrieval systems, and infrastructure need to work. It is not only about swapping algorithms for post-quantum ones but about thinking on the impact that those new algorithms have at the protocol, system and network levels. The known challenges seem to be a these levels:

- Challenges at the Protocols level,
- Challenges at the implementation level,
- Challenges at the standardization level,
- Challenges at the community level,
- Challenges at the research level.

2 Challenges at the Protocols level

- Storage of cryptographic parameters used during the protocol's execution:
  - How are we going to properly store post-quantum cryptographic parameters, such as keys or certificates, that are generated for/during protocol execution (their sizes are bigger than what we are accustomed to)?
  - How is post-quantum cryptography going to work with stateless servers, ones that do not store session state and where every client request is treated as a new one, such as NFS, Sun's Network File System (for an interesting discussion on the matter, see this paper [BL20])?
- Long-term operations and ephemeral ones:
  - What are the impacts of using post-quantum cryptography for long-term operations or for ephemeral ones: will bigger parameters make ephemeral connections a problem?
  - Are security properties assumed in protocols preserved and could we relax others (such as IND-CCA or IND-CPA. For an interesting discussion on the matter, see this paper [HNS+20])?
- Managing bigger keys and signatures:
  - The public key, ciphertext or signature sizes of the majority of post-quantum algorithms are bigger than the classical counter parts (they increase depending on the security level). For some protocols as TLS this means:
    - IP-level fragmentation (which is specially bad in the case of DTLS).
    - DTLS-level fragmentation
    - Extra roundtrips, which will be unworkable in the case of stateless servers.
  - What are the impacts on latency and bandwidth?
  - Does the usage of post-quantum increase the round-trips at the Network layer, for example? And, if so, are these increases tolerable?

  - Will the increased sizes cause dropped or fragmented packets?
  - Devices can occasionally have settings for packets smaller than expected: a router, for example, along a network path can have a maximum transmission unit, MTU (the MSS plus the TCP and IP headers), value set lower than the typical 1,500 bytes. In these scenarios, will post-quantum cryptography make these settings more difficult (one can apply MSS clamping for some cases)?

- Preservation of protocols as we know them:
  - Can we achieve the same security or privacy properties as we use them today?
  - Can protocols change: should we change, for example, the way DNSSEC or the PKI work? Can we consider this radical change?
  - Can we integrate and deploy novel ways to achieve authentication?
  - At the TLS level, can be use something like KEMTLS [SSW20]?

- Hardware (or novel alternative to hardware) usage during protocol's execution:
  - Is post-quantum cryptography going to impact network function virtualization (as used in 5G cellular networks)?
  - Will middleware, such as middleboxes, be able to handle post-quantum cryptography?
  - What will be the impacts on mobile device's connections?
  - What will be the impacts on old servers and clients?

- Novel attacks:
  - Will post-quantum cryptography increase the possibility of mounting denial of service attacks?

3 Challenges at the Implementation level

- Efficiency of algorithms: can we make them faster at the software, hardware (by using acceleration or FPGA-based research) or at an algorithmic level (with new data structures or parallelization techniques) to meet the requirements of network protocols and ever-fastest connections?

- Can we use new mechanisms to accelerate algorithms (such as, for example, the usage of floating point numbers as in the Falcon signature scheme)? Will this lead to portability issues as it might be dependent on the underlying architecture?

- What is the asymptotic complexity of post-quantum algorithms (how they impact time and space)?

- How will post-quantum algorithms work on embedded devices due to their limited capacity (see this paper [BZH+21], for more explanations)?

- How can we avoid attacks, failures in security proofs and misuse of APIs?

- Can we provide correct testing of these algorithms?

- Can we ensure constant-time needs for the algorithms?

- What will happen in a disaster-recovery mode: what happens if an algorithm is found to be weaker than expected or is fully broken? How will we be able to remove or update this algorithm? How can we make sure there are transition paths to recover from a cryptographical weakening?

4 Challenges at the Standards level

- The mathematical base of post-quantum cryptography is an active area of development and research, and there are some concerns in the security they give (are there new attacks in the confidentiality or authentication they give?). How will standardization bodies approach this problem?
- Post-quantum cryptography introduces new models in which to analyze the security of algorithms (for example, the usage of the Quantum Random Oracle Model). Will this mean that new attacks or adversaries will not be noted at the standards level?
- What will be the recommendation of migrating to post-quantum cryptography from the standards' perspective: will we use a hybrid approach?
- How can we bridge the academic/research community into the standardization community, so analysis of protocols are executed and attacks are found on time (prior to being widely deployed)1? How can we make sure that standards bodies are informed enough to make the right practical/theoretical trade-offs?

5 Challenges at the Community level

- What are the needs of different systems? While we know what the needs of different protocols are, we don't know exactly how all deployed systems and services work. Are there further restrictions?
- On certain systems (for example, on the PKI), when will the migration happen, and how will it be coordinated?
- How will the migration be communicated to the end-user?
- How will we deprecate pre-quantum cryptography?
- How will we integrate post-quantum cryptography into systems where algorithms are hardcoded (such as IoT devices)?
- Who will maintain implementations of post-quantum algorithms and protocols? Is there incentive and funding for a diverse set of interoperable implementations?

6 Challenges at the Research level

- Are there any efficient and secure post-quantum non-interactive key exchange (NIKE) algorithms? NIKE is a cryptographic algorithm which enables two participants, who know each others' public keys, to agree on a shared key, without requiring any interaction. An example of a NIKE is the Diffie-Hellman algorithm. There are no efficient and secure post-quantum NIKEs. A candidate seems to be CSIDH, which is rather slow and whose security is debated.
- Are there post-quantum alternatives to (V)OPRFs based protocols, such as Privacy Pass or OPAQUE?
- Are there post-quantum alternatives to other cryptographic schemes such as threshold signature schemes, credential based signatures and more?
- How can post-quantum algorithms be formally verified with new notions such as the QROM?
- What are the challenges of using isogeny-based cryptography?
- Are we sure that there are no quantum or classical attacks that threaten the security of the new proposed algorithms?
- Can security/privacy properties be preserved in secure messaging protocols?

References

[BL20] Daniel J. Bernstein and Tanja Lange. McTiny: Fast High-Confidence Post-Quantum key erasure for tiny network servers. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 1731–1748. USENIX Association, August 2020.

[BZH+21] Gustavo Banegas, Koen Zandberg, Adrian Herrmann, Emmanuel Baccelli, and Benjamin Smith. Quantum-resistant security for software updates on low-power networked embedded devices. *CoRR*, abs/2106.05577, 2021.

[HNS+20] Andreas Hülsing, Kai-Chun Ning, Peter Schwabe, Florian Weber, and Philip R. Zimmermann. Post-quantum wireguard. Cryptology ePrint Archive, Report 2020/379, 2020. https://ia.cr/2020/379.

[SSW20] Peter Schwabe, Douglas Stebila, and Thom Wiggers. Post-quantum tls without handshake signatures. Cryptology ePrint Archive, Report 2020/534, 2020. https://ia.cr/2020/534.