Post-Quantum Cryptography: Migration, Challenges and the role of OpenSSL

Rodrigo Martín Sánchez-Ledesma

rodrma01@ucm.es
Universidad Complutense de Madrid

rmsanchezledesma@indra.es
Indra Sistemas de Comunicaciones Seguras

Table of Contents

Challenges associated to Post-Quantum Cryptography

1. Uncertainty surrounding Post-Quantum Cryptography.

Challenges associated to Post-Quantum Cryptography

1. Uncertainty surrounding Post-Quantum Cryptography.
2. Change of paradigm for Key Establishment.

Challenges associated to Post-Quantum Cryptography

1. Uncertainty surrounding Post-Quantum Cryptography.
2. Change of paradigm for Key Establishment.
3. Size of cryptographic elements of PQ schemes.

Challenges associated to Post-Quantum Cryptography

1. Uncertainty surrounding Post-Quantum Cryptography.
2. Change of paradigm for Key Establishment.
3. Size of cryptographic elements of PQ schemes.
4. Increase in (theoretical) complexity of schemes.

Challenges associated to Post-Quantum Cryptography

1. Uncertainty surrounding Post-Quantum Cryptography.
2. Change of paradigm for Key Establishment.
3. Size of cryptographic elements of PQ schemes.
4. Increase in (theoretical) complexity of schemes.
5. Increase in (practical) complexity of schemes.

Uncertainty regarding PQC

- Derived from the yet-unknown actual capacities and limits of quantum computing.
- (Partial) Novelty of most schemes and underlying hard problems used, along with their understanding.

It represents a challenge to the analysis and selection of cryptographic paradigms, security assumptions and constructions to base primitives on.

Change of Key Establishment paradigm

PQC KE construction are based on KEMs. Some differences include:

1. KEM mechanisms are, in general, *not contributory*, as opposed to KA mechanisms.
2. Public values generated and plausibly exchanged in a key-exchange protocol for establishing a shared key are **not** independent.

These changes can impact the way key establishment protocol are built, and potentially require structural changes to accommodate PQC KEM schemes.

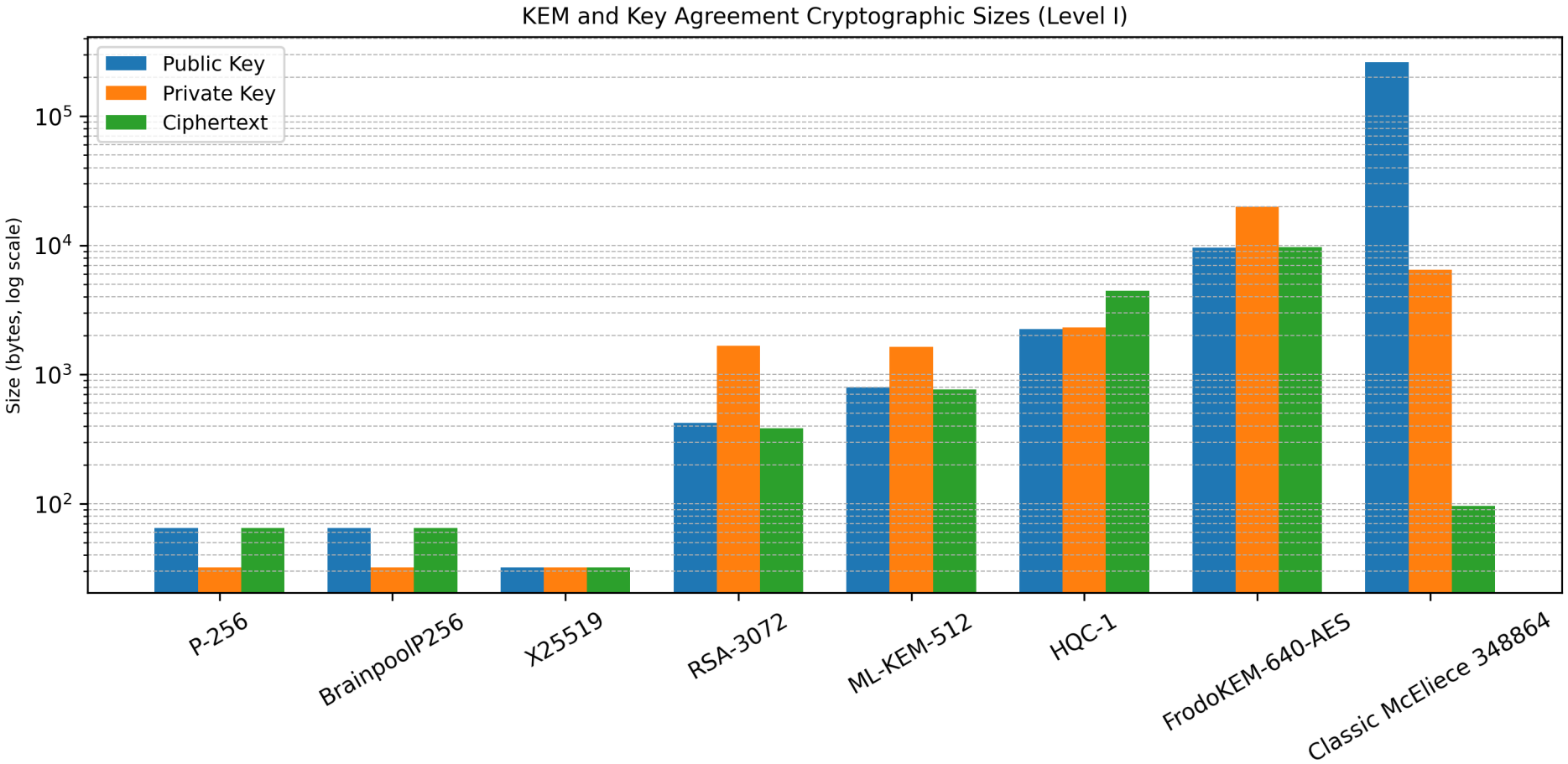
The reality of PQ cryptographic sizes

Post-Quantum schemes have cryptographic sizes of orders of magnitude bigger than traditional cryptography.

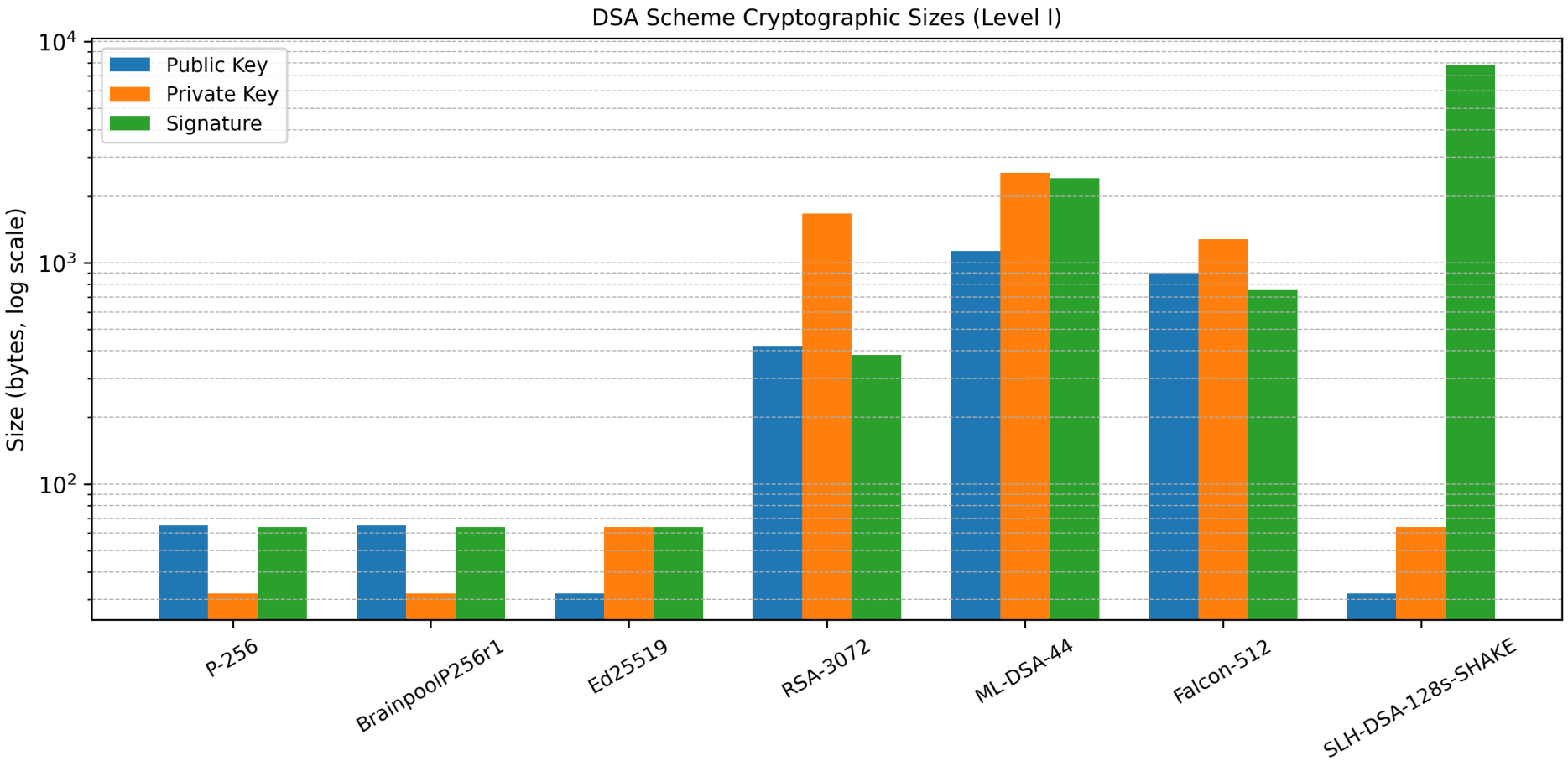
Some consequences include:

- Not all post-quantum primitives will be suitable for every situation.
- Selection of schemes must be done carefully, to minimize impact.

KEM Cryptographic Sizes Comparison



DSA Cryptographic Sizes Comparison



Increase in (theoretical) complexity of schemes

The need for asymmetric primitives that are both quantum-safe and implementable on standard systems requires the use of new, more complex mathematics and cryptography, which means:

- The research needed is much more specialized.
- More resources to perform such research.
- Bigger technical barrier for individuals and organizations.

Increase in (practical) complexity of schemes

Post-Quantum implementations often include:

- Floating-point arithmetic or other non-constant-time-friendly operations.
- Complex probability distributions.
- Decoding / Decryption Failure Rates.
- More complex mathematical structures/routines to implement.

which make secure, leak-free, constant time implementations more difficult to achieve.

Table of Contents

A way to deal with uncertainty: Hybrid approaches

To deal with the uncertainty of PQ security and faulty implementations, the use of hybrid cryptography is deemed as a standard practice.

Hybrid cryptography

The use of two or more cryptographic schemes in a way that the resulting scheme is only vulnerable if every underlying scheme is.

PQC in Protocols and applications

Despite the previous challenges, much work has already been done to adapt standard protocols and applications to the use of PQC:

- TLS: various drafts, repeated shares, KEMTLS, etc...
- X3DH: variants like PQXDH.
- Double Ratcheting: Different proposals like PQ3, Triple Ratcheting, SPQR ...
- MLS: Naturally adapted due to the use of Ratchet KEM Trees
- ... and more!

Handling Post-Quantum sizes

A number of techniques have been employed to alleviate the impact:

- Use of more structured paradigms to help reduce sizes
- Schemes with trade-offs between size and performance, to choose depending upon needs.
- Strong security assumptions to allow for key-reuse and avoid the need of ephemeral procedures.

Post-Quantum scientific development

The raise of Post-Quantum cryptography has brought:

- Overwhelming increase in research, both in cryptography and mathematics.
- Much knowledge about (in)security and its limits has been gained.
- Entirely new or improved cryptographic constructions have surged in recent years.

Post-Quantum implementations

Post-Quantum implementations often enjoy some of the following:

- Use of formal verifiers to study implementations.
- Increase in optimization techniques, to improve performance.
- Condensation of high-profile reference implementation to focus scrutiny.
- Implementation in a variety of languages.

Table of Contents

Steps to undergo PQ migrations

The migration towards Post-Quantum Cryptography will be (one of) the hardest ever undertaken.

Some steps to a successful one must include:

1. Identification of vulnerable cryptography within your organization or product.
2. In-depth study and familiarization with post-quantum cryptography.
3. Early adoption.
4. Plan and prioritize.

Cryptography identification: CBOM to the rescue

The first step towards an analysis of the magnitude of a post-quantum migration is the identification of the cryptography employed within your organization or product.

Cryptographic Bill Of Materials

The use of a CBOM helps keep track of deployed vulnerable cryptography.

Diving into Post-Quantum Cryptography

To plan a PQ migration, once must be familiar with post-quantum schemes and their characteristics, including:

1. Cryptographic sizes and plausible improvements.
2. Performance depending on architecture and use.
3. Mathematical security background: e.g. lattices, codes, multivariate, etc...
4. Cryptographic theoretic security notions: OW-CPA, IND-CCA, etc...

(Not so) Early Adoption: First (NIST) PQ Standards already here!

- FIPS 203: ML-KEM. KEM based on the lattice MLWE paradigm.
- FIPS 204: ML-DSA. DSA based on the lattice MLWE and M-SIS paradigms.
- FIPS 205: SLH-DSA. DSA constructed from various symmetric-based techniques.
- FIPS 206 (WIP): FN-DSA. DSA based on the lattice NTRU paradigm.
- FIPS 207 (WIP): HQC-KEM. KEM based on quasi-cyclic codes.
- SP 800-208: XMSS, LMS. DSA based on stateful hash functions.

(Not so) Early Adoption: First (NIST) PQ Standards already here!

- FIPS 203: ML-KEM. KEM based on the lattice MLWE paradigm.
- FIPS 204: ML-DSA. DSA based on the lattice MLWE and M-SIS paradigms.
- FIPS 205: SLH-DSA. DSA constructed from various symmetric-based techniques.
- FIPS 206 (WIP): FN-DSA. DSA based on the lattice NTRU paradigm.
- FIPS 207 (WIP): HQC-KEM. KEM based on quasi-cyclic codes.
- SP 800-208: XMSS, LMS. DSA based on stateful hash functions.

"Crypto-procrastination time is over!"

Plan and prioritize: Some key aspects

1. Detection of critical areas in which migration must be prioritized.

Plan and prioritize: Some key aspects

2. Following standardization agencies recommendations, including algorithmic recommendations and deployment tactics.

Plan and prioritize: Some key aspects

3. There will not be, in general, a single *"rule them all"*, general purpose scheme. Migration must be planned based on each scenario.

Plan and prioritize: Some key aspects

4. Perform migrations in a *"crypto-agile"* way, i.e. in a way the system is prepared for future updates or changes.

Plan and prioritize: Some key aspects

4. Perform migrations in a *"crypto-agile"* way, i.e. in a way the system is **as** prepared **as possible** for future updates or changes.

Plan and prioritize: Some key aspects

5. Keep in sync with the state of the art. Further optimizations and improvements may appear.

Table of Contents

The role of OpenSSL regarding Post-Quantum Cryptography

OpenSSL is the biggest, most important cryptographic open-source project out there. As such, it must provide:

1. Security and efficiency of the implementations of of PQ schemes for a variety of environments.

The role of OpenSSL regarding Post-Quantum Cryptography

OpenSSL is the biggest, most important cryptographic open-source project out there. As such, it must provide:

1. Security and efficiency of the implementations of of PQ schemes for a variety of environments. 

The role of OpenSSL regarding Post-Quantum Cryptography

OpenSSL is the biggest, most important cryptographic open-source project out there. As such, it must provide:

2. Facilitate the use and adoption of this type of cryptography.

The role of OpenSSL regarding Post-Quantum Cryptography

OpenSSL is the biggest, most important cryptographic open-source project out there. As such, it must provide:

2. Facilitate the use and adoption of this type of cryptography. ✅

The role of OpenSSL regarding Post-Quantum Cryptography

OpenSSL is the biggest, most important cryptographic open-source project out there. As such, it must provide:

3. Provide support for a wide variety of features: hybrid procedures, access independent components, seeds, "derand" interfaces, hybrid combiners and others.

The role of OpenSSL regarding Post-Quantum Cryptography

OpenSSL is the biggest, most important cryptographic open-source project out there. As such, it must provide:

3. Provide support for a wide variety of features: hybrid procedures, access independent components, seeds, "derand" interfaces, hybrid combiners and others.

The role of OpenSSL regarding Post-Quantum Cryptography

OpenSSL is the biggest, most important cryptographic open-source project out there. As such, it must provide:

4. Provide support for standardized PQ algorithms beyond NIST. Algorithms on verge of being standardized include Classic McEliece, FrodoKEM or NTRU.

The role of OpenSSL regarding Post-Quantum Cryptography

OpenSSL is the biggest, most important cryptographic open-source project out there. As such, it must provide:

4. Provide support for standardized PQ algorithms beyond NIST. Algorithms on verge of being standardized include Classic McEliece, FrodoKEM or NTRU.

The role of OpenSSL regarding Post-Quantum Cryptography

OpenSSL is the biggest, most important cryptographic open-source project out there. As such, it must provide:

5. Facilitate collaboration and inclusion of experimental implementations within the ecosystem.

The role of OpenSSL regarding Post-Quantum Cryptography

OpenSSL is the biggest, most important cryptographic open-source project out there. As such, it must provide:

5. Facilitate collaboration and inclusion of experimental implementations within the ecosystem. 

Remarks

Much work has been done, but a lot of it remains ahead...

Remarks

Much work has been done, but a lot of it remains ahead...

Figure: You when realizing the work behind post-quantum migrations

Thank you!