Post-quantum cryptography as an engineering challenge

Project meeting

Secure communication in the quantum era
SPS Project Number: G5448

Pavol Zajac

Institute of Computer Science and Mathematics
Slovak University of Technology

April 02, 2019

Progress report: activities in Slovakia

- research work in progress,
- strong focus on publicity,
- student participation through bachelor and master theses.

Current project related research activities in Slovakia

- continued evaluation of PQ proposals from NIST call,
- theoretical research:
  - hard problems in PQ cryptosystems,
  - attacks on code-based systems,
- implementation and experimental research (student projects)

Project focus by team member

- T. Fabšič: code-based systems (QC-LDPC, QC-MDPC),
- O. Gallo: implementation and side-channel attacks,
- V. Hromada: MQ-based systems,
- P. Špacek: comparative study of PQ proposals with respect to adaptation in TLS-like protocol,
- P. Zajac: design of new protocols and primitives, engineering challenges of PQ systems.

Post-quantum cryptography as an engineering challenge

Main thesis: Post-quantum research is mature enough to be translated into working real-world systems.

There are many challenges:

- update standards and protocols (ongoing with NIST call is only a beginning),
- update available software libraries and hardware components,
- update working systems, including data stores.

All of this in an efficient and secure way...

First step: Understanding

Engineers (and managers) need to understand:

- why post-quantum security is important,
- which cryptographic primitives are potentially compromised and should be replaced,
- which cryptographic primitives can be used instead in selected applications,

Focus of our project: Suitable solution for a post-quantum group communication.

Second step: Implementing the switch

Second step is to adopt quantum-resistant cryptography:

- how to implement new cryptographic primitives in an efficient and secure way,
- how to incorporate new cryptographic primitives in the existing (or planned) applications,
- how to verify the correctness and security of the solution,

An added bonus to our project: runtime verification is a strong domain of our partner from University of Malta.

Third step: Beyond the switch

Post-quantum research can bring new applications, and new challenges to overcome:

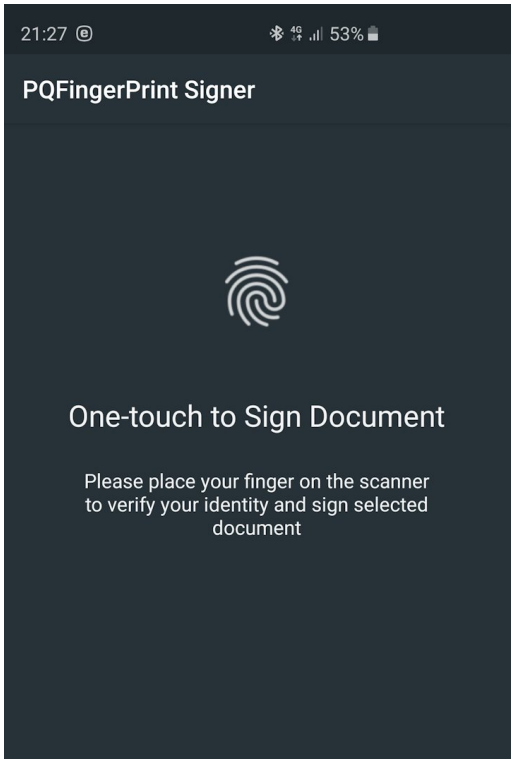
- How to protect legacy applications? (e.g. old blockchains),
- New types of attacks (e.g. post-quantum side-channels),
- ...

Project showcase 1: Post-quantum signatures on Android phones

Diploma project of Ľ. Pernický.

Aim of the project:

Implement an application that allows the user to sign PDF documents on Android phone using PQ signature algorithm.



Project showcase 1: Post-quantum signatures on Android phones

Application features:

- Signature algorithm: SPHINCS-0 from BouncyCastle library (hash-based PQ signature),
- Private key stored on device locked with fingerprint,
- Server side for storing signed documents and backup keys.

Project showcase 1: Post-quantum signatures on Android phones

Efficiency of the application:

- 500 ms to sign, 6 ms to verify signature (Samsung Galaxy S9+/S10+)
- Public Key size: 1kB,
- Signature size: 41 kB,

Project TODOs: non-standard algorithm SPHINCS-0, need to update library to e.g. SPHINCS+.

Project showcase 2: New ways of authenticating ephemeral keys

Project motivation:

- Efficient PQ code-based encryption schemes can have a limited key use due to specific attacks (GJS attack).
- Solution: Ephemeral keys — they also provide forward secrecy.
- Efficient authentication of ephemeral keys: do we really need full signatures?

Project showcase 2: New ways of authenticating ephemeral keys

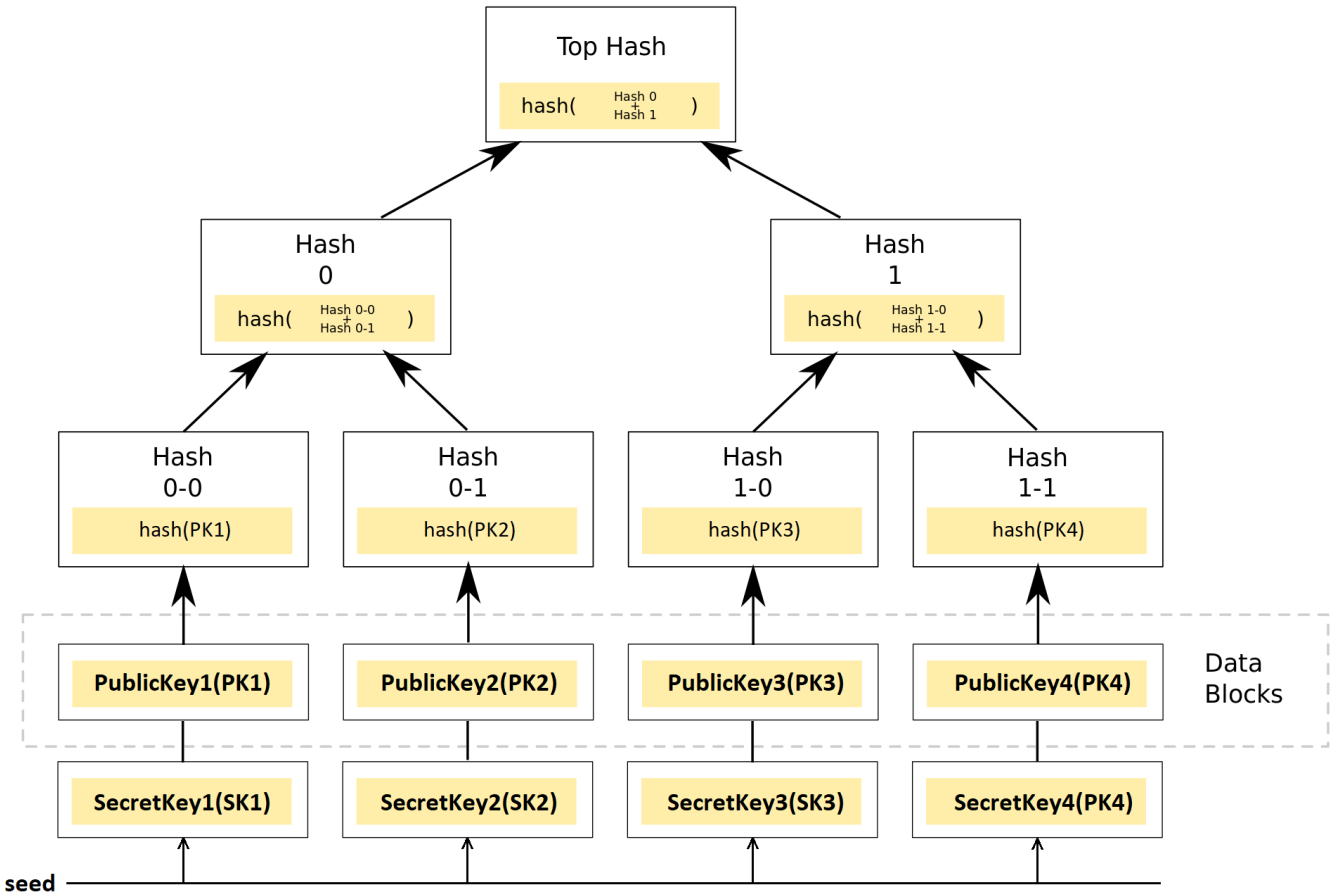
Proposed theoretical solution (P.Zajac):

- Combine ephemeral keys with hash trees (instead of full hash-based signature scheme).
- E.g. replace SPHINCS+ signature (8 kB), with 20-level hash tree (0.6kB): 92.5% saving

Implementation phase (WIP, diploma thesis of M. Novotný):

- Incorporate hash trees and key verification into libraries of the encryption system BIKE (from NIST call).

Project showcase 2: New ways of authenticating ephemeral keys



Project showcase 3: Incorporation of post-quantum primitives into TLS

Main project motivation:

- Recent TLS 1.3 standard supports these handshake algorithms:
  - DHE-RSA,
  - ECDHE-RSA,
  - ECDHE-ECDSA.
- None of them are quantum secure.

Note, that generic quantum-secure TLS can be used to build more advanced schemes (on application layer), including secure group communication.

Project showcase 3: Incorporation of post-quantum primitives into TLS

- Diploma thesis of P. Špaček: McEliece encryption provider for `openssl`
- Aim of the PhD thesis: Identify and implement a suitable set of algorithms to use in TLS-like protocol (compatible with standard TLS libraries).
- Long-term project, currently in evaluation and analysis phase (with respect to NIST call schedule)

Conclusions

- Adaptation of post-quantum cryptography is also an important engineering challenge.
- A lot of effort will be required to prepare post-quantum secure software libraries, and to adapt them in applications,
- Specific properties (key size, signature size, efficiency asymmetry between signatures/verification or encryption/decryption...) of PQ primitives might force us to redesign some applications and protocols.