Efficient and Secured Implementation of Post-Quantum Cryptography

Thomas Pöppelmann
Infineon Technologies AG
Digital Security Solutions
Neubiberg, Germany
thomas.poeppelmann@infineon.com

***Abstract*— Due to their computing power, quantum computers may have the disruptive potential to break various currently used encryption and authentication algorithms within the next 15 to 20 years. Once available, quantum computers would threaten currently used asymmetric algorithms such as RSA and elliptic curve cryptography (ECC). An approach that aims to replace RSA and ECC in next generation security protocols is post-quantum cryptography (PQC). In this work, we show the challenges of implementing PQC on embedded devices and smart cards. One important aspect is the protection of schemes against attacks like power analysis and fault injection and research on this topic is still at a very early stage. Moreover, we describe how existing cryptographic hardware on smart cards or embedded microcontrollers can be used to accelerate post-quantum cryptography.**

Keywords—Post-Quantum Cryptography, Smart Card, Side-Channels

I. INTRODUCTION

With further advances in the construction of quantum computers, it is a possibility that such computers may be able to break cryptographic schemes like RSA or elliptic curve cryptography (ECC) in the next 15 to 20 years. As the confidentiality and authenticity of almost all digital communication relies on the security of RSA or ECC, researchers in academia, industry and government organizations are working on quantum-safe alternative schemes and their standardization.

Such quantum-safe cryptography is often also called post-quantum cryptography (PQC). PQC comprises public-key encryption or digital signature algorithms that rely on the hardness of sophisticated mathematical problems. The underlying assumption is that these problems are intractable for a powerful quantum computer as well as for a classical one. To facilitate the development of new quantum-safe and practical schemes, in 2016 the National Institute of Standards and Technology (NIST) has started a standardization process to find suitable replacements [3].

This work was supported by European Union's Horizon 2020 research and innovation programme under grant agreement No. 779391 (FutureTPM).

In their call for submissions, NIST asked researchers to submit schemes that could become a new standard. This process is open to submitters from all over the world and it follows the spirit of previous competitions that have led to the standardization of the widely adopted block cipher Advanced Encryption Standard (AES) or the recently standardized hash algorithm SHA-3 (SHA, Secure Hash Algorithm). However, for the PQC standardization process a considerable difference to previous competitions is that the scope of the standardization effort is much wider. This is mainly because NIST is asking in parallel for submissions of public-key encryption and digital signature schemes. Moreover, the solution space for PQC algorithms is much broader than for block ciphers or hash functions. Currently, the cryptographic community is considering roughly five classes or families of algorithms to build PQC schemes. These classes are hash-based cryptography, code-based cryptography, multivariate cryptography (MQ), lattice-based cryptography, and isogeny-based cryptography. They all have different characteristics and require specialized techniques for security analysis and implementation. Thus, NIST may alter the rules and selection criteria based on new research and will most likely not pick one winner. Moreover, NIST stated that the process should not be viewed as a competition, but rather as an effort of the community to find several algorithms suitable for future use. Moreover, currently the assessment of the security of post-quantum cryptography schemes is difficult as no practical experience with quantum computers is available and thus a careful study of the diverse underlying mathematical problems is needed. NIST is also explicitly asking the cryptographic community and industry to provide feedback on the suitability of these submissions. This feedback can either be provided over a public mailing list, by submitting presentations, or by approaching NIST representatives during conferences.

II. THE NIST STANDARDIZATION PROCESS: ROUND 1 AND 2

In the first phase of the standardization process in December 2017, NIST has published 69 submissions that are labeled as "complete and proper" and thus meet minimal formal standards. Overall, 278 individual submitters from 25 countries and 6

continents with academic, industry and government affiliations participated. Interestingly, after the first three weeks of round 1 already twelve schemes had been broken or significantly attacked. Such attacks or vulnerabilities in implementations were mostly communicated over the pqc-forum. In addition, the community used the forum to discuss advantages and disadvantages of proposed schemes or their underlying basic mathematical problems as well as practical matters. This makes the forum one of the primary sources on news in academic post–quantum cryptography and allows easy access to statements and contributions of key experts. At the end of round 1 there were over 1000 posts including over 300 official comments on the pqc-forum.

Besides the forum, a major step in the standardization process was the "First PQC Standardization Conference" held in April 2018 in Ft. Lauderdale. The conference gave submitters the opportunity to present the advantages and disadvantages of their proposals. Over 350 participants attended it with background from academia, industry, and government organizations. For the second round of the standardization process, in January 2019 NIST selected the 26 most promising schemes out of the 69 submission. The main selection criteria was cryptographic strength. Minor aspects were cost and performance as well as algorithm and implementation characteristics, e.g., simplicity. For round 2, the selected authors were allowed to submit revised or merged submissions and the submissions were published in April 2019. Many submitters made use of the opportunity to incorporate new research, e.g., on improved parameters or updated their implementations for better performance. To measure the performance NIST has opened the pqc-hardware-forum and stated that the focus for performance evaluation is on general purpose CPUs, Cortex M4-based microcontrollers, and Artix-7 FPGAs.

These works provide important feedback to NIST and the cryptographic community. The implementation of PQC is particularly challenging as microcontrollers and embedded processors usually have a very limited amount of available RAM and storage space to store program code. Moreover, the processing capabilities of 8, 16, or 32-bit architectures are limited. On the other hand, such controllers can achieve energy and real time requirements that can usually not be met by computer systems or high-performance system-on-chips (SoC) with external non-volatile memory or RAM. A special class of constrained devices are smart cards or chip cards, which are used in electronic banking, for secured identification (e.g. passports or ID cards), authentication or transport and ticket applications. Smart cards usually also implement protective mechanisms against a large number of invasive and non-invasive attacks. Moreover, they often have dedicated accelerators to accelerate and protect cryptographic operations (e.g. AES, ECC, or RSA). Such accelerators can be helpful even for the implementation of PQC algorithms as most PQC schemes rely on symmetric functions, e.g., for randomness expansion or hashing.

III. SECOND PQC STANDARDIZATION CONFERENCE

The most recent venue for the discussion of PQC was the "Second PQC Standardization Conference" held in August 2019 in Santa Barbara. The date and location allowed a co-location with the well-known CRYPTO conference and thus enabled interaction with the wider cryptographic community. The conference was attended by over 250 participants and featured presentations by submitters of round 2 schemes and presentations by researchers who reported on advances in implementation, security estimation, or cryptanalysis. Several projects were mentioned or presented that are now aiming at providing a comprehensive overview over the remaining round 2 schemes and their performance on specific devices or in certain applications:

- Open Quantum Safe [4]: The project aims to develop quantum resistant cryptography and prototype integration of such cryptography into protocols like the Transport Layer Security (TLS) protocol. The liboqs library is an open source C library currently containing 7 signatures and 7 key encapsulation mechanisms (KEM) under the MIT License.
- Supercop [5]: Supercop is a system for benchmarking of cryptographic systems and contains a large number of implementation of highly optimized pre- and post-quantum schemes and performance measurements on different architectures (e.g., Cortex-A57, Intel Xeon, Intel CannonLake, AMD Zen).
- mupq [6]: The mupq projects collects and develops PQC implementations targeting the Cortex-M4 as well as RISC-V microcontroller architectures. These implementations are optimized for low memory footprint and are partially written in assembly to make use of the underlying architecture.
- Post-Quantum Crypto Lounge [7]: A collection of searchable data on submissions to the NIST process.

Besides evaluation of individual schemes, the transition to PQC raises also policy related questions. Some of them were addressed in an industry panel with employees from Amazon Web Services, Cisco, Microsoft, IBM, and Cloudflare. Exemplarily, the panel tried to find answers to issues such as:

- How long will it take to introduce PQC into products?
- What are the major barriers to the adoption of PQC?
- How much will IP issues impede adoption of PQC algorithms?

Moreover, at the conference and on the pqc-forum a large number of discussions focused on the assurance of the cryptographic strength of a possible standard. Even though the NIST process has sparked a large number of research, the level of confidence into different primitives or underlying mathematical problems varies a lot. The community and NIST are currently discussing ways to encourage more cryptanalysis to get a better view on the security of PQC schemes. This is also important for parameter selection so that future standards have a suitable but also not too costly parametrization for good performance or acceptable key sizes. Another technical issue is whether NIST should standardize key encapsulation schemes that follow the chosen-plaintext attack (CPA) model or the chosen-ciphertext attack (CCA) model. Schemes in the CPA model usually provide security only when key pairs are not

reused or when ciphertexts send for decryption are appropriately protected from tampering by malicious entities. Schemes in the CCA model are more robust but also more complicated and sometimes slower than their CPA counterparts. This issue is also connected with misuse resistance features of future standards. It is unclear how many tradeoffs should be made (e.g., performance, cryptographic strength) to simplify schemes or to make it harder to implement them in an incorrect manner. Overall, due to the better internal (self-) checking it seems that CCA-secure schemes are less prone to misuse by non-experts in the field of cryptography. Another topic that was excluded from the current standardization process are hybrid schemes and the techniques to securely combine different basic primitives. The rationale is that most likely PQC may be rolled out on top of existing cryptographic protocols and classical schemes. Applications may securely combine keys exchanged with an established classical scheme (e.g., ECC) and a PQC scheme into one session key. During the conference, NIST stated that this topic is under investigation and that NIST may give guidance (e.g., in a standard document) on how an appropriately secure and certifiable combination of classic and PQC schemes may be achieved.

Notably, the overall timeline of the standardization process still stands with the goal of having draft standards available in 2022/2024. However, NIST announced shortly after the conference that a third round is very likely and should start around June 2020. The goal of the third round is to focus further on schemes that are ready for standardization and it is anticipated that NIST will further reduce the pool of candidate schemes. Moreover, NIST stated that they may also select algorithms that are too new or unstable for standardization but still worth further study. In order to allow more focus on few selected schemes, NIST also encourages merging of similar schemes or reduction of parameter sets.

NIST also announced that they are currently working on a draft standard for stateful post-quantum hash-based signatures. Hash based signatures carry strong security arguments as they allow to reduce the hardness of breaking the signature to the hardness of breaking a symmetric hash function (e.g., SHA-256). However, they require the signer to keep a state of the private key and the amount of signatures per public/private key pair is limited. Thus, they are not universally usable and are applicable mainly for limited use-cases, e.g., signing of firmware updates. In December 2018, NIST has published a first version as Draft NIST Special Publication (SP) 800-208 [9].

IV. Other activities

Other standardization bodies involved in PQC are ETSI and ISO who run study groups dedicated to PQC. However, currently it seems that ETSI and ISO will rely on NIST for the initial selection of algorithms. Additionally, several European research projects, e.g., PROMETHEUS and FutureTPM are currently investigating the efficiency, security, and practicability of PQC schemes. Moreover, several PQC-related German funding projects (Aquorypt, QuaSiModO, QuantumRISC, PQC4MED, FLOQI, SIKRIN-KRYPTOV, and KBLS) have recently been started after a call for proposal by the German Federal Ministry of Education and Research had been issued [7].

V. Implementation on Chip Cards

To enable a smooth migration, PQC can be accelerated by using already available RSA/ECC co-processors for (ideal) lattice-based cryptography. The approach is to exploit the availability of fast long integer multiplication on common smart cards that is intended for the acceleration of RSA and ECC. The proof of concept described in [1] is an implementation of a variant of the Kyber Key Encapsulation Mechanism (KEM) scheme on an Infineon SLE78CLUFX5000 chip card. The controller is equipped with 16 Kbyte RAM, 500 Kbyte NVM and a 16-bit CPU running at 50 MHz. The asymmetric co-processor on the SLE78CLUFX5000 allows fast basic long number calculations on integers slightly larger than 2048 bits (addition, subtraction, integer multiplication, modular multiplication). With Kronecker substitution in combination with schoolbook and Karatsuba polynomial multiplication a fast routine for polynomial multiplication can be realized. Moreover, a speed-up of symmetric functions is achieved by using the AES co-processor to implement a PRNG and a SHA-256 co-processor to realize hash functions.

VI. Side-Channel Protection

Besides performance, there are some other challenges when deploying PQC algorithms. For applications that require strong protection against physical attacks, some practical and research problems still need to be solved. This requires the implementation of cryptosystems with protection against active attacks (i.e. adaptive ciphertext attacks) and realization of countermeasures against side-channel analysis [7]. Exemplarily, a sufficient protection of the key and message during decryption requires masking of the computation and new building blocks like a masked binomial sampler. With parameters providing 233 bits of quantum security, an implementation of a lattice-based KEM scheme can be realized that requires roughly 4 million cycles for encryption and 26 million cycles for decryption with masking and hiding countermeasures on an ARM Cortex-M4F microcontroller.

References

[1] Martin R. Albrecht, Christian Hanser, Andrea Höller, Thomas Pöppelmann, Fernando Virdia, Andreas Wallner: Implementing RLWE-based Schemes Using an RSA Co-Processor. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2019(1): 169-208 (2019)

[2] Tobias Oder, Tobias Schneider, Thomas Pöppelmann, Tim Güneysu: Practical CCA2-Secure and Masked Ring-LWE Implementation. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2018(1): 142-174 (2018)

[3] NIST Computer Security Resource Center: Post-Quantum Cryptography, see https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

[4] Douglas Stebila, Michele Mosca. Post-quantum key exchange for the Internet and the Open Quantum Safe project. In Roberto Avanzi, Howard Heys, editors, Selected Areas in Cryptography (SAC) 2016, LNCS, vol. 10532, pp. 1–24. Springer, October 2017. https://openquantumsafe.org

[5] eBACS: ECRYPT Benchmarking of Cryptographic Systems. Unified Performance Evaluation Related to Cryptographic Operations and Primitives: https://bench.cr.yp.to/supercop.html

[6] Matthias J. Kannwischer, Joost Rijneveld, Peter Schwabe, Ko Stoffelen: PQM4: Post-quantum crypto library for the ARM Cortex-M4, https://github.com/mupq

[7] Post-Quantum Crypto Lounge, https://www.safecrypto.eu/pqclounge/

[8] Richtlinie zur Förderung von Forschungsvorhaben zum Thema "Post-Quanten-Kryptografie", https://www.bmbf.de/foerderungen/bekanntmachung-1947.html

[9] Draft NIST Special Publication (SP) 800-208, Recommendation for Stateful Hash-Based Signature Schemes. https://csrc.nist.gov/publications/detail/sp/800-208/draft