Report from Dagstuhl Seminar 23152

Secure and Efficient Post-Quantum Cryptography in Hardware and Software

Thomas Pöppelmann*[1], Sujoy Sinha Roy*[2], and Ingrid Verbauwhede*[3]

1 **Infineon Technologies AG – Neubiberg, DE.** thomas.poeppelmann@infineon.com
2 **TU Graz, AT.** sujoy.sinharoy@iaik.tugraz.at
3 **KU Leuven, BE.** ingrid.verbauwhede@esat.kuleuven.be

Abstract

NIST recently announced the winners of its post-quantum cryptography (PQC) standardization process and outlined the next steps in its ongoing standardization efforts. With fewer algorithms now in the focus of the cryptographic community, the time has come to intensify the investigation of efficiency and physical security aspects of PQC algorithms. This is required to enable PQC in real-life applications and to provide feedback to NIST and submitters before final standardization. To allow widespread adoption, the implementation of PQC in current microchip technologies must be possible within application- or platform-specific constraints such as area, memory, time, power, and energy budgets. Furthermore, more and more PQC use-cases require resistance to physical attacks like power analysis.

The primary aim of this Dagstuhl Seminar was to initiate deeper investigations into secure and efficient implementations of PQC on hardware and hardware/software codesign platforms. In this direction, the seminar brought together researchers in theoretical cryptology, applied cryptography, cryptographic hardware and software systems, and physical security. During the seminar, participants identified new challenges and research directions in PQC, exchanged thoughts and ideas, and initiated collaborations on researching secured and efficient design methodologies for PQC.

Seminar April 10–13, 2023 – https://www.dagstuhl.de/23152

2012 ACM Subject Classification Security and privacy → Public key (asymmetric) techniques; Security and privacy → Hardware security implementation; Security and privacy → Hardware attacks and countermeasures

Keywords and phrases Post-quantum cryptography, secure hardware and software, cryptographic implementations, side-channel attacks, fault attacks, countermeasures against attacks

Digital Object Identifier 10.4230/DagRep.13.4.24

* Editor / Organizer

Secure and Efficient Post-Quantum Cryptography in Hardware and Software, *Dagstuhl Reports*, Vol. 13, Issue 4, pp. 24–39
Editors: Thomas Pöppelmann, Sujoy Sinha Roy, and Ingrid Verbauwhede

Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

1 Executive Summary

Thomas Pöppelmann
Sujoy Sinha Roy
Ingrid Verbauwhede

Our present-day public-key infrastructures primarily rely on RSA and elliptic curve cryptography (ECC). In case a powerful quantum computer is built in the near future, these public-key infrastructures will become completely insecure. Post-quantum cryptography (PQC) aims at developing new cryptographic protocols that will remain appropriately secure even after powerful quantum computers are built.

Even if powerful quantum computers are still far out, replacement algorithms for public-key algorithms need to be developed and implemented now. These algorithms must show appropriate cryptographic security, i.e., resistant to the attacks from quantum and classical computers. On top, their implementations need to be efficient in current microchip technologies, implementable within the constrained area, time, power, and energy budgets. This is very important to enable PQC-based protection of information processed by (battery-powered) Internet of things (IoT) devices or smart cards. At the same time, more and more use-cases require resistance to physical attacks. When an attacker has physical access to a device, the attacker may try to manipulate or observe it during cryptographic operations. The most common physical attacks are side-channel and fault attacks that usually aim to extract a secret key.

The existing PQC algorithms are classified into five categories depending on their underlying hard problems: lattice-based, multivariate polynomial-based, hash-based, code-based, and supersingular isogeny-based. Of them, lattice-based PQC is currently the frontrunner as evident from the fact that the majority of the PQC candidate schemes that were submitted to NIST's Post Quantum Cryptography Standardisation project are lattice-based. A significant volume of research has been performed on studying the security, performance, and application aspects of lattice-based PQC and even more narrowly focused on the algorithms submitted to the NIST call.

There is a need to have a diverse set of algorithms for post-quantum public-key cryptography. One main concern is security and risk management: if a specific class of PQC becomes weaker or is even considered broken in the advent of new cryptanalysis, then there must be other reliable classes of PQC that will offer high security. Indeed the 4th round of NIST's PQC standardization, which will start at the end of the 3rd round, will aim at broadening the set of PQC algorithms. Furthermore, in this direction, NIST indicated that a new call for proposals for PQC signature algorithms (focusing on non-lattice-based algorithms) is planned with a deadline in 2023. Besides the security aspects, each class of PQC has its own advantages. For example, code-based key agreement schemes have small ciphertexts and could be useful in applications where the public keys are known. The isogeny-based key agreement scheme SIKE has the smallest public-key and a small ciphertext size but relatively low performance. In the last few years, several new isogeny-based signature schemes have been developed with small key and signature sizes. Hash-based signature schemes have security guarantees based on hash functions and they have the advantage of (re)using a hash hardware module if the hardware platform has it. Multivariate signature schemes offer fast signing and verifying and very short signatures.

This Dagstuhl Seminar focused on answering the following questions in the context of post-quantum cryptography.

- **Efficiency and correct metrics:** Depending on the application, efficiency can be the area or memory size, throughput or latency, power and energy, or a combination of them. Can we have tailored implementations to satisfy one or several such metrics?
- **HW/SW Co-design:** The right form of interaction of a CPU with HW-based post-quantum acceleration needs to be determined: Options are instruction set extension or usage of domain-specific co-processors. How to determine the splitting of computation tasks between HW and SW?
- **Agility and reuse:** How can complex HW accelerators and controlling SW be reused? For example, can a compact HW accelerator be reused for a high throughput version? And how easy can different processing units, such as polynomial arithmetic or hash modules, support multiple schemes?
- **Physical attacks:** For many use-cases, PQC implementations need to be resistant to side-channel and fault-based attacks. Are low overhead countermeasures feasible? Shall countermeasures be implemented in HW or SW? Can we exploit the mathematical properties of some PQC algorithms to derive low-overhead countermeasures?
- **Proactive security:** Can we construct new PQC algorithms in such a way that they become more resistant to physical attacks and more efficient in HW and SW by design?

To find answers to the above-mentioned questions, the following workgroups were formed:

1. Efficient implementation aspects of PQC
2. Physical security aspects of PQC
3. Theoretical aspects of PQC
4. Application and migration

The time table of the seminar is shown in Fig. 1.

Dagstuhl Seminar 23152 Plan

Time (April)	Monday	Tuesday	Wednesday	Thursday
7:30 - 8:45		Breakfast	Breakfast	Breakfast
9:00 - 10:15		Introduction, goals, and organization. What are you looking for?	Small workgroups	Discussions on research challenges and collaboration ideas.
10:15 - 10:45		Coffee break	Coffee break	Coffee break
10:45 - 12:15		Talk (40 min) on HW/SW Acceleration of Lattice-Based Cryptography (Speaker: Tim Fritzmann) Q&A, discussions, notes.	Short report on work groups. Talk (40 min) on security metrics and certification for PQC (Speaker: Melissa Rossi). Q&A, discussions, notes.	Report of small workgroups, followed by plenary
12:15 - 14:00		Lunch break	Lunch break	Lunch break
14:00 - 15:30		Talk (40 min) on new problems in isogeny crypto. (Speaker: Christophe Petit) Q&A, discussions, notes.	Social activity (hiking and group work)	Conclusion and farewell (30 min)
15:30 - 16:00		Coffee break	Coffee break	
16:00- 17:30	Arrival and Dinner	Talk (40 min) on achieving crypto agility in HW/SW. (Speaker: Matthias Kannwischer) Q&A, discussions, notes.	Discussion, ranking of most challenging topics for research.	
18:00 - 19:00		Dinner	Dinner	
20:00		Evening activity		

Figure 1 Seminar Plan.

2 Table of Contents

3 Overview of Talks

3.1 HW/SW Acceleration of Lattice-Based Cryptography

Tim Fritzmann (Infineon Technologies AG – Neubiberg, DE)

Lattice-based cryptography introduces new mathematical operations that are hard to compute on devices with a low computing power. Therefore, hardware accelerators can be used to meet performance and energy requirements. While previous works focused on standalone hardware solutions for the complete cryptographic scheme, the current trend is to use hardware/software codesigns in order to increase the flexibility of the design. In this context, two types of accelerators can be developed. Loosely coupled accelerators are suitable for large tasks with a low data transfer between main processor and accelerator. In contrast, tightly coupled accelerators are directly integrated into the main processor and avoid any complex bus communication. Experiments have shown that this type of accelerator leads to fast and flexible implementations of lattice-based cryptography.

3.2 New Problems In Isogeny-based Cryptography

Christophe Petit (Université libre de Bruxelles, BE & University of Birmingham, GB)

We give an overview of isogeny-based cryptography, including the main underlying hard problems and existing protocols. We then describe open problems in the field, with a special focus on problems relevant for hardware implementations.

3.3 Implementing the NIST PQC standards on microcontrollers

Matthew Kannwischer (Academia Sinica – Taipei, TW)

In July 2022, the US National Institute of Standards and Technology (NIST) announced the first set of post-quantum schemes to be standardized: Kyber, Dilithium, Falcon, and SPHINCS+. In this talk, I will present the state-of-the-art of those to-be-standardized schemes on the Arm Cortex-M4 which is NIST's primary microcontroller optimization target. I will present the most recent results of the benchmarking framework pqm4 for all four schemes. While for Falcon and SPHINCS+ there has been very little progress in implementation performance lately, recent improvements exist to the speed and memory consumption of Kyber and Dilithium. I will present those new implementation techniques. I will also outline new challenges for implementations on larger Arm processors and the upcoming NIST PQC signature on-ramp in particular with respect to two digital signature submissions that I am involved in: Oil-and-Vinegar and MAYO.

3.4 ANSSI recommendations and brainstorm ideas

Melissa Rossi (ANSSI – Paris, FR)

I presented the PQC transition strategy in France. The first aspect of this transition is the mandatory use of hybridation mode for PQC algorithms. I presented several modes that seem possible solutions. The second aspect is a list of potential good PQC algorithms: Kyber, FrodoKEM, Dilithium, Falcon, XMSS, LMS and SPHINCS+. Finally, I described the certification strategy in France and how it will handle post-quantum products. I concluded the talk with interesting open questions on side-channel and lattices.

4 Working Groups

4.1 Efficient implementations of PQC

Ingrid Verbauwhede (KU Leuven, BE)
Bo-Yin Yang (Academia Sinica – Taipei, TW)
Erkay Savaş (Sabanci University – Istanbul, TR)
Patrick Karl (TU München, DE)
Ahmet Can Mert (TU Graz, AT)

Our work group focused on the implementation aspects of PQC. Initially, we started with a brainstorming session to list some of the important possible research topics/directions related to efficient PQC implementations. After our discussion, we identified the following research questions.

- Implementation aspects of lattice, code, multivariate and isogeny based schemes
- Implementation optimizations targeting memory-constrained devices
- Crypto-agility in HW/SW
- Exploring synergies in different categories of PQC
- New computing paradigms for PQC (i.e., in-memory and approximate computing)
- Automatic tooling, correctness and formal verification
- Standardization of PQC-related operations into RISC-V (i.e., modular arithmetic, butterfly operation, vector operations etc.)

After the initial discussions, the following two main directions were brainstormed by this work group.

4.1.1 Formal verification of PQC implementations

Two approaches for automating the correctness verification process (formal methods) are discussed, model checking by SAT solver and proof assistant. The model checking defines what should or should not happen and then evaluates the given program. The result is either satisfiable, unsatisfiable or non-determine. Domain specific languages can also help in the verification process significantly. We discussed the formal verification tools like CryptoLine [1] which is a language for the verification of low-level mathematical constructions.

Demo. Dr. Bo-Yin Yang provided a demo on how to use CryptoLine and explained basic working principles. CryptoLine uses low-level instruction models for specific micro-controllers provided by Jasmin. It translates each low-level instruction into one or several CryptoLine instructions. Even for complex programs, it takes only couple of minutes for CryptoLine to perform correctness verification.

CryptoLine shows a significant improvement towards tooling/automation of correctness verification. However, there are still challenges such as handling of noise sampling and decryption failures. Verification of floating-point based implementations is also very challenging due to operations like rounding, truncation and overflow. Another important challenge is translating these verification approaches to hardware implementations of PQC.

4.1.2 Exploring synergies in different categories of PQC

NIST finalized its standardization process and announced four candidates (one PKE and three DS) to be standardized. Besides, different cybersecurity agencies have suggested a gradual transition to PQC and some of them selected deployment of a different scheme than NIST's standardization process winners. It is also possible that some of the non-standardized schemes still can find use in some specific platforms and applications. This shows that unified implementations supporting several schemes will be required soon. To that end, it has important significance to find and explore synergies in different PQC schemes.

Our work group started with identifying common arithmetic operations in different PQC categories such as lattice-based and code-based cryptography. Our initial investigation showed that hashing, modular arithmetic and number theoretic transform (NTT) are common operations in most PQC schemes. Our discussion further led to the following research questions/directions.

- Can approximate computing (i.e., allowing errors in computation at the expense of increased failure rate) lead to *super low power* applications?
- Use of erroneous multipliers to improve power consumption.
- Design of hardware modules that lead to some increase in failure rate but allow to reuse them for other schemes, e.g. common multiplier for SABER/Kyber.
- Modelling/Verifying the aforementioned approaches.
- Exploring schemes (mostly non lattice-based) in NIST's additional digital signature call. Since this is very new, this is very unexplored in terms of HW/SW implementations.

Conclusions from this workgroup. (*i*) Recent efforts in formal verification of PQC are promiisng and important; however, there are challenges/limitations such as floating-point arithmetic. (*ii*) This work group will continue collaborative study for exploring synergies in different PQC schemes.

Open problems from this workgroup. (*i*) Translating existing correctness verification approaches/tools to hardware implementations of PQC.

References

1 Yu-Fang Chen, Chang-Hong Hsu, Hsin-Hung Lin, Peter Schwabe, Ming-Hsien Tsai, Bow-Yaw Wang, Bo-Yin Yang, Shang-Yi Yang. *Verifying Curve25519 Software.* ACM SIGSAC Conference on Computer and Communications Security (CCS), pp. 299-309, ACM, 2014.

4.2 Physical security aspects of PQC

Aydin Aysu (North Carolina State University – Raleigh, US)
Ayesha Khalid (Queen's University of Belfast, GB)
Gaetan Cassiers (TU Graz, AT)
Melissa Rossi (ANSSI – Paris, FR)
Peter Pessl (Infineon Technologies AG – Neubiberg, DE)
Prasanna Ravi (Temasek Labs, Singapore & Nanyang Technological University, Singapore, SG)
Simona Samardjiska (Radboud University Nijmegen, NL)
Thomas Eisenbarth (Universität Lübeck, DE)

Our workgroup mainly foccused on the broad topic of physical attacks such as SCA and FIA of PQC schemes. We started by laying out some of the open-problems, that need to be addressed to improve our understanding of the threat of SCA and FIA, as well as implementing efficient PQC designs in a manner resistant to physical attacks. After intense deliberation and discussion, we were able to identify several research questions and open problems that can be split into three broad categories.

- Evaluation of side-channel leakage for practical implementations of PQC schemes.
- Efficient Countermeasures against SCA for Post-Quantum Cryptographic schemes
- Identification of new SCA and FIA on PQC schemes

In the following, we briefly explain the several research questions and discussions that emerged out of the discussion in our work group.

4.2.1 Evaluation of Side-Channel Leakage for Post-Quantum Cryptographic Schemes

We will soon be witnessing wide-scale adoption of lattice-based schemes on embedded devices, and these devices have to be evaluated based on different security certification standards such as FIPS 140-3 [2], Common Criteria [3]. In order to perform side-channel leakage evaluation of PQC schemes, we are not aware of the concrete set of tests that need to be done to certify a given PQC hardware or software against side-channel analysis. Thus, it can be an interesting research direction from the point of view of security certification of PQC HW and SW implementations.

Some of the specific open-problems that we considered during our discussions are as follows:

1. What are the exhaustive set of tests required to test side-channel leakage from all the operations within the decapsulation procedure of IND-CCA secure Key Encapsulation Mechanisms (KEMs). The first challenge towards devising an exhaustive set is the fact that the decapsulation procedure contains three different operations (i.e.) decryption, re-encryption and ciphertext comparison. Thus, it is necessary to device separate tests to test for leakage from each of these three operations separately. While it does not appear to be extremely difficult to arrive at such exhaustive tests for individual post-quantum KEMs, it needs to be analyzed whether they make up the exhaustive set of tests that are sufficient to prove existence of leakage or otherwise.

2. While leakage evaluation tests can help us detect or test for leakage of sensitive variables, it does not necessarily indicate the possibility to perform key recovery. Thus, it is also interesting to ponder upon development of novel techniques that can map available leakage to the most efficient key recovery attack. We are probably not looking at automatic discovery of new attacks based on existing vulnerabilities, but probably estimate the effort required to mount known attacks provided the calculated leakage. This could be particularly interesting for the case of single trace attacks [4, 5], where we can ask the question what is the minimum amount of leakage required to mount a given single trace attack, without explicitly performing the attack itself.
3. Can we develop techniques that can ascertain if certain types of PQC schemes are more difficult to attack through SCA/FIA compared to others? This is for instance, a pertinent question that came up during the NIST PQC process, where NIST was particularly interested in factors that differentiated the different lattice-based schemes in the context of side-channel analysis, given that there were several lattice-based schemes in the NIST PQC standardization process. Development of such analysis techniques can potentially enable us to build leakage resilient schemes that are inherently resistant to SCA [6, 8, 7].

4.2.2 Efficient Countermeasures against Side-Channel Attacks for PQC schemes

1. Masking countermeasures for PQC schemes typically involve a large amount of randomness, especially because they involve computation over large polynomials, matrices or vectors spanning dimensions of the order of a few hundred to few thousand. Obtaining access to a large amount of high quality randomness typically required for masking schemes is particularly challenging, especially when considering constrained embedded devices, which are especially required to be protected against side-channel attacks. These challenges for masking countermeasures gives rise to the following questions.
   a. What is the effect of reusing randomness in masking schemes, tailor made for specific PQC schemes to reduce the true performance overhead of masking countermeasures? This will reduce the randomness requirement, thereby reducing the true performance overhead of masking countermeasures.
   b. What is the impact of using randomness of bad quality in masked implementations of PQC schemes?
2. Masking countermeasures are usually considered to be very expensive, as they have shown to incur a significant overhead in runtime in several prior works [9, 10, 11]. We also observe that PQC schemes involve computation over large polynomials, matrices or vectors spanning dimensions of the order of a few hundred to few thousand. Thus, it is interesting to contemplate use of shuffling countermeasures, exploiting the large dimensions of elements used in PQC based schemes. This is particularly relevant in scenarios where that an attacker is in a restricted setting, limiting him/her with access to "N" traces for a given secret key. In such scenarios, whether shuffling alone is sufficient to provide provable security?
3. Code-based schemes are currently in the spotlight as we expect a code-based scheme to be standardized in the fourth round. Interestingly, there are no systematic measures for SCA protection of these schemes. The decoding algorithms are notoriously difficult to even do in constant time, and the question is whether we can use masking techniques in the decoding algorithms – for instance Reed Muller, Reed Solomon Decoder in HQC, Berlekamp-Massey in Classic McEliece.

4.2.3 Identification of new SCA and FIA on PQC schemes

1. Existing side-channel attacks on lattice-based cryptographic schemes either require the knowledge of inputs/outputs, or require to control the inputs to the DUT [12]. However, it is possible in certain scenarios that the attacker does not directly obtain access to the I/O of the DUT. In such a setting, the attacker only has access to the side-channel traces, and it begets the question if an attacker can still perform key recovery without knowledge of the DUT's inputs/outputs. It is also interesting to explore for which post-quantum schemes this scenario leads to meaningful, exploitable leakage.
2. Several prior works have shown that an attacker can craft malicious inputs to the decapsulation procedure of KEMs to amplify the side-channel leakage of the secret key for efficient key recovery attacks. One of the main downsides of these attacks is that the malformed ciphertexts used for the attack, can be detected with a very high probability. Such chosen-ciphertext attacks using malformed ciphertexts have also been used to target other PQC schemes as well [1]. This makes it natural for a designer to implement a simple protection: refresh the secret key every time he/she observes a decapsulation failure, since decapsulation failures for valid ciphertexts occur with negligible probability. This raises a natural question on whether "it is possible to perform chosen-ciphertext attacks on lattice-based schemes with valid ciphertexts?". This represents a more stealthy approach towards chosen-ciphertext attacks, as valid ciphertexts cannot be detected as malicious by the decapsulation procedure, as they do not trigger decapsulation failures.

Conclusions from this workgroup. During the course of our discussions, we identified several open problems along three axes – SCA/FIA based attacks, Efficient SCA/FIA Countermeasures and the need for comprehensive SCA Leakage Evaluation Techniques of PQC schemes. However, we identified two key components that could foster further research on SCA/FIA of PQC schemes.

1. Development of an open-source implementation framework that allows to run SCA experiments on PQC schemes implemented on commonly used microcontrollers. In this respect, we discussed about the possibility of extrapolating the pqm4 library [13] and integrate with the open-source Chipwhisperer platform [14]. The framework should be developed in such a way that it serves as a library of SCA protected implementations of PQC schemes, and allows for testing for leakage in critical components within implementations of PQC schemes.
2. Development of an open-source database of side-channel traces of implementations of PQC schemes, which can motivate the community towards developing attack techniques as well as novel leakage detection techniques targeting the open-source trace database. While similar open-source side-channel trace database are available for symmetric ciphers such as the ASCAD database for AES [15], we are not aware of similar works for PQC schemes.

Open problems from this workgroup. (i) Development of novel leakage evaluation techniques for PQC schemes, that enables to certify a given PQC implementation as secure or not. (ii) Investigation of the quality of randomness used in masked implementations of PQC schemes. (iii) Development of efficient masking schemes for code-based schemes (iv) Development of novel SCA/FIA for new attack scenarios such as a) Use of Valid Ciphertexts and b) Blind SCA/FIA that work without knowledge of inputs/outputs. (v) Development of open-source implementation framework that enables SCA/FIA evaluation of PQC implementations.

References

1. Ravi, Prasanna, and Sujoy Sinha Roy. *Side-channel analysis of lattice-based PQC candidates.* In Round 3 Seminars, NIST Post Quantum Cryptography. 2021.
2. Schaffer, Kim. *FIPS 140-3 Derived Test Requirements (DTR): CMVP Validation Authority Updates to ISO/IEC 24759. No. NIST Special Publication (SP) 800-140 (Draft)*. National Institute of Standards and Technology, 2019.
3. Boswell, Tony. *Security evaluation and common criteria.* In Secure Smart Embedded Devices, Platforms and Applications, pp. 407-427. New York, NY: Springer New York, 2013.
4. Primas, Robert, Peter Pessl, and Stefan Mangard. *Single-trace side-channel attacks on masked lattice-based encryption.* In Cryptographic Hardware and Embedded Systems-CHES 2017: 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings, pp. 513-533. Springer International Publishing, 2017.
5. Pessl, Peter, and Robert Primas. *More practical single-trace attacks on the number theoretic transform.* In Progress in Cryptology–LATINCRYPT 2019: 6th International Conference on Cryptology and Information Security in Latin America, Santiago de Chile, Chile, October 2–4, 2019, Proceedings 6, pp. 130-149. Springer International Publishing, 2019.
6. Clément Hoffmann, Benoît Libert, Charles Momin, Thomas Peters, and François-Xavier Standaert. *POLKA: Towards Leakage-Resistant Post-quantum CCA-Secure Public Key Encryption*. In Public-Key Cryptography – PKC 2023
7. Jan-Pieter D'Anvers, Emmanuela Orsini, and Frederik Vercauteren. *Error Term Checking: Towards Chosen Ciphertext Security without Re-encryption*. In Proceedings of the 8th ACM on ASIA Public-Key Cryptography Workshop – APKC '21
8. Melissa Azouaoui, Yulia Kuzovkova, Tobias Schneider, Christine van Vredendaal, *Post-Quantum Authenticated Encryption against Chosen-Ciphertext Side-Channel Attacks.* In IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES) 2023
9. Bos, Joppe W., Marc Gourjon, Joost Renes, Tobias Schneider, and Christine Van Vredendaal. *Masking kyber: First-and higher-order implementations.* IACR Transactions on Cryptographic Hardware and Embedded Systems (2021): 173-214.
10. Heinz, Daniel, Matthias J. Kannwischer, Georg Land, Thomas Pöppelmann, Peter Schwabe, and Daan Sprenkels. *First-order masked Kyber on ARM Cortex-M4.* Cryptology ePrint Archive (2022).
11. Bronchain, Olivier, and Gaëtan Cassiers. *Bitslicing arithmetic/boolean masking conversions for fun and profit: with application to lattice-based kems.* IACR Transactions on Cryptographic Hardware and Embedded Systems (2022): 553-588.
12. Ravi, Prasanna, Anupam Chattopadhyay, Jan Pieter D'Anvers, and Anubhab Baksi. *Side-channel and fault-injection attacks over lattice-based post-quantum schemes (Kyber, Dilithium): Survey and new results.* ACM Transactions on Embedded Computing Systems (2022).
13. Kannwischer, Matthias J., Joost Rijneveld, Peter Schwabe, and Ko Stoffelen. *pqm4: Testing and Benchmarking NIST PQC on ARM Cortex-M4.* (2019).
14. O'flynn, Colin, and Zhizhang Chen. *Chipwhisperer: An open-source platform for hardware embedded security research.* In Constructive Side-Channel Analysis and Secure Design: 5th International Workshop, COSADE 2014, Paris, France, April 13-15, 2014. Revised Selected Papers 5, pp. 243-260. Springer International Publishing, 2014.
15. Benadjila, Ryad, Emmanuel Prouff, Rémi Strullu, Eleonora Cagli, and Cécile Dumas. *Deep learning for side-channel analysis and introduction to ASCAD database.* Journal of Cryptographic Engineering 10, no. 2 (2020): 163-188.

4.3 Theoretical aspects of PQC

Jan-Pieter D'Anvers (KU Leuven, BE)
Andrea Basso (University of Bristol, GB)
Thomas Pöppelmann (Infineon Technologies – Neubiberg, DE)
Thomas Prest (PQShield – Paris, FR)
Tobias Schneider (NXP Semiconductors – Gratkorn, AT)
Christophe Petit (UL – Brussels, BE & University of Birmingham, GB)
Sujoy Sinha Roy (TU Graz, AT)

Our workgroup focused on the cost of protecting implementations against side-channel attacks. More specifically, we looked at what design choices can make cryptographic schemes easier to protect against these side-channel attacks. Our brainstorming resulted in three main topics: replacing the FO transformation, improvements to the NIST standard Kyber, and new methods in masking.

The FO transformation is a widely used method to secure schemes actively. However, it comes at a great cost, making ciphertext decryption 2 to 3 times more expensive and making masking harder due to its nonlinearity. We looked at three methods to replace the FO transformation for LWE-based schemes: POLKA [1] and ETC [2] and an ID-based proposal [3]. All these methods are interesting but come with specific preconditions. We looked at the possibility of a more general method and the limitations of what is possible in this space.

Regarding improvements to Kyber, we discussed the possibility of arithmetic hash functions, as other Kyber operations are also arithmetic which could reduce the need for costly conversions between arithmetic and Boolean domains. However, we concluded that this is not trivial due to the inherent conversion between the arithmetic and Boolean domain during the decoding of the message.

In the masking domain, we discussed different security models for probing, which would better mimic existing attacks and subsequently could result in more efficient masking. We also discussed the importance of reducing the randomness cost of masking algorithms. We concluded that this should be a more prominent factor in designing and evaluating these countermeasures. As for existing countermeasures, we looked at improvement possibilities. Notably, the Kavach [4] implementation could benefit from a more efficient Boolean masking of the carry, and the one-hot conversion [5] could benefit from the fact that intermediate variables have constant hamming weight and thus might be better protected against hamming weight leakage.

Conclusions from this workgroup. Using the existing mechanisms, the cost of implementing side-channel countermeasures is quite high, especially when higher order masking are considered. More research is needed.

Open problems from this workgroup. The workgroup will continue working on a concrete idea to replace the FO transformation with a different transformation. The expected result is a shift in cost from decryption to encryption. Other open problems are the improvements of the Kavach, and the one-hot conversion are not planned but left as interesting future work.

References

1 Clément Hoffmann, Benoît Libert, Charles Momin, Thomas Peters, and François-Xavier Standaert. *POLKA: Towards Leakage-Resistant Post-quantum CCA-Secure Public Key Encryption.* In Public-Key Cryptography – PKC 2023

2 Jan-Pieter D'Anvers, Emmanuela Orsini, and Frederik Vercauteren. *Error Term Checking: Towards Chosen Ciphertext Security without Re-encryption.* In Proceedings of the 8th ACM on ASIA Public-Key Cryptography Workshop – APKC '21

3 Melissa Azouaoui, Yulia Kuzovkova, Tobias Schneider, Christine van Vredendaal, *Post-Quantum Authenticated Encryption against Chosen-Ciphertext Side-Channel Attacks.* In IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES) 2023

4 Aikata Aikata and Andrea Basso and Gaetan Cassiers and Ahmet Can Mert and Sujoy Sinha Roy, *Kavach: Lightweight masking techniques for polynomial arithmetic in lattice-based cryptography.* In IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES) 2023

5 Jan-Pieter D'Anvers *One-Hot Conversion: Towards Faster Table-Based A2B Conversion.* In Advances in Cryptology – EUROCRYPT 2023

4.4 Application and migration

Thomas Eisenbarth (Universität Lübeck, Gernany)
Melissa Rossi (ANSSI – Paris, FR)
Rainer Steinwandt (University of Alabama in Huntsville, US)
Marc Stöttinger (Hochschule RheinMain – Wiesbaden, DE)

After initial brainstorming, the discussion focused on the transition phase from traditional public-key solutions to post-quantum solutions. While there is no consensus on the use of hybrid systems as an intermediate step, the interest in such solutions is significant. A common building block for hybrid designs is the use of some form of combiner that is realized with the help of a key derivation function. Depending on the application context, contributing key material may involve a pre-shared key, the outcome of a traditional key establishment, a shared secret from a post-quantum solution, key material derived from a quantum key distribution protocol. Including additional material in the key derivation may be desirable.

We looked at different approaches considered for combining key material from different sources, e.g., by ANSSI (France) [1] and by Germany's Federal Office for Information Security [2]. Aligning with the focus of this Dagstuhl Seminar, our main interest was on possible side-channel vulnerabilities when combining keys from different sources, and we started to discuss if it is realistic and possible to mount such attacks. In addition, we had an initial discussion on attacker models and possible side-channel leakage models. We also formulated the following initial research questions on SCA in combinational functions in hybrid methods:

- What is a typical recommended combiner function and how closely are these related to PRFs, MACs, or hash functions?
- What is a suitable PRF or DualPRF regarding side-channel resistance?
- Is there literature on side-channel attacks on combiner functions used in a hybrid PQC scheme?
- Is there literature on side-channel attacks on PRFs that could serve as a starting point for studying side-channel vulnerabilities in combiner functions?

The following action items have been set up to continue research on this topic even after the Dagstuhl Seminar is over.

- Conducting a literature review will be needed to decide on the next steps.
- Set up follow-up meetings to proceed and exchange on advance with respect to SCA on combiner functions.

Conclusions from this workgroup. The topic SCA on combiner functions will be continued in a collaborative workling group after the Dagstuhl Seminar.

Open problems from this workgroup. Side-Channel Analysis on Combiner Function of Hybrid Schemes.

References

1 Mélissa Rossi. PQC Transition in France; ANSSI views. Presentation at Real World Post-Quantum Crypto, March 2023. Available at `https://www.melissarossi.fr/wp-content/uploads/2023/04/ANSSIs-recommendations-on-the-migration-plan.pdf`.

2 Federal Office for Information Security. Quantum-safe cryptography – fundamentals, current developments and recommendations, May 2022. Available at `https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html`.

Participants

- Aydin Aysu
North Carolina State University – Raleigh, US
- Andrea Basso
University of Bristol, GB
- Gaetan Cassiers
TU Graz, AT
- Jan-Pieter D'Anvers
KU Leuven, BE
- Thomas Eisenbarth
Universität Lübeck, DE
- Tim Fritzmann
Infineon Technologies AG – Neubiberg, DE
- Mike Hamburg
Rambus – Vught, NL
- Matthias Kannwischer
Academia Sinica – Taipei, TW
- Patrick Karl
TU München, DE
- Ayesha Khalid
Queen's University of Belfast, GB
- Ahmet Can Mert
TU Graz, AT
- Peter Pessl
Infineon Technologies AG – Neubiberg, DE
- Christophe Petit
UL – Brussels, BE & University of Birmingham, GB
- Thomas Pöppelmann
Infineon Technologies AG – Neubiberg, DE
- Thomas Prest
PQShield – Paris, FR
- Prasanna Ravi
Nanyang TU – Singapore, SG & Temasek Labs – Singapore, SG
- Mélissa Rossi
ANSSI – Paris, FR
- Simona Samardjiska
Radboud University Nijmegen, NL
- Erkay Savas
Sabanci University – Istanbul, TR
- Tobias Schneider
NXP Semiconductors – Gratkorn, AT
- Sujoy Sinha Roy
TU Graz, AT
- Rainer Steinwandt
University of Alabama in Huntsville, US
- Marc Stöttinger
Hochschule RheinMain – Wiesbaden, DE
- Ingrid Verbauwhede
KU Leuven, BE
- Bo-Yin Yang
Academia Sinica – Taipei, TW