Implementation of a Higher-Order Masked Kyber KEM

Elena Dubrova

1 Project Description

Our daily business relies on the devices that we carry with us, such as medical/bank/transportation cards, car keys and mobile phones. To assure the security and privacy of users, these devices should use secret (cryptographic) keys that are not accessible from the outside. Getting a hold of the key allows a hacker to steal confidential data or take control of a car or a phone. The majority of real-world attacks on security implementations use side-channel analysis, i.e. they measure and process physical quantities, like the power consumption or electromagnetic emanations of a chip, or execution time of a program. Preventing this kind of leakages and side-channel attacks in general remains a great challenge as effective mitigations are often prohibitively expensive in terms of power and energy resources. Moreover, thanks to computing power becoming ever cheaper nowadays, modern adversaries have started using state-of-the-art machine learning algorithms for the attacks.

Another challenge comes from the prospect of quantum computers. If they can be built, most of the public-key cryptosystems used today, like RSA and Elliptic Curve Cryptography (ECC), will be broken. To prevent this, the crypto community is working actively on various aspects of post-quantum crypto. Related to this, the National Institute of Standards and Technology (NIST) launched a Post-Quantum Cryptography (PQC) project [1] which aims to deliver suitable alternatives to classical public-key cryptography (PKC) algorithms that are secure against quantum computer attacks. While the project enters its final stage, many questions are still unanswered, in particular related to efficient implementations of the finalists and their side-channel analysis.

While the NIST PQC project's finalists are designed to resist known mathematical attacks, recent works [2, 3] have shown that their software implementations can be broken by machine learning-based side-channel analysis even if they are protected by countermeasures such as first-order masking and shuffling. This shows that it is necessary to implement stronger countermeasures against side-channel analysis, such as higher-order masking.

The purpose of this project is to implement the first- and higher-order masked Kyber Key Encapsulation Mechanism (KEM) [4]. Kyber is one of the finalists of NIST PQC project. As an example, a C implementation of the first-order masked Saber KEM [5] will be provided to the team. Saber is another finalist of NIST PQC project. It has many common features with Kyber.

2 Project Objectives

The project consists of the following tasks:

- Study different possibilities for implementing the first- and higher-order masking in the Kyber KEM algorithm.
- Analyze and compare different masking approaches with respect to area and performance overhead.
- Implement in C/C++ the selected first- and higher-order masking schemes in Kyber KEM algorithm.
- Compile the resulting protected Kyber implementations on a ARM Cortex-M4.

- Compare non-masked, the first- and higher-order masked Kyber KEM implementations in terms of area and performance overhead.
- Document the resulting implementations and their evaluation results. All relevant parts should be documented, but the project team can choose which part of the documentation should be online-documentation and which parts should be offline documentation in form of a report.
- Create a well-documented project on GitHub, where the source code is licensed under a permissive open source license, like the MIT license.

3 Milestones and Deliverables

The project has the following deliverables, which also serve as milestones. The exact size of the project and the formulation of the deliverables and dates for the milestones needs to be adjusted based on the size and composition of the project group.

D1: Study of approaches for implementing the first- and higher-order masking.

D2: Selection of suitable for Kyber masking approaches and presentation of a proposal for them.

D3: Implementation of the masking approaches selected in D2 in C.

D4: Compilation of the implementations on ARM Cortex-M4 and testing.

D5: Comparison of non-masked, the first- and higher-order masked Kyber KEM implementations in terms of area and performance overhead.

For all parts documentation is required (see previous section).

4 Prerequisites

The project requires competences in computer architecture, hardware design, and embedded software design. The ideal team for this project would be a mixed group with students from the embedded platform and the embedded software tracks.

5 Approximate Team Size

The project proposal has been written for a project group size of 3-4 students, but it can be adapted to a larger team size.

6 Contact

Elena Dubrova, Division of Electronics and Embedded Systems, dubrova@kth.se
Kalle Ngo, Division of Electronics and Embedded Systems, kngo@kth.se

References

[1] NIST, "Post-quantum cryptography," 2021. https://csrc.nist.gov/projects/post-quantum-cryptography.

[2] K. Ngo, E. Dubrova, Q. Guo, and T. Johansson, "A side-channel attack on a masked IND-CCA secure Saber KEM," *IACR Trans. on CHES*, no. 4, 2021.

[3] K. Ngo, E. Dubrova, and T. Johansson, "Breaking masked and shuffled CCA secure Saber KEM by power analysis." Cryptology ePrint Archive, Report 2021/902, 2021. https://eprint.iacr.org/2021/902.

[4] J. W. Bos, M. Gourjon, J. Renes, T. Schneider, and C. van Vredendaal, "Masking Kyber: First- and higher-order implementations," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2021, pp. 173–214, Aug. 2021.

[5] M. V. Beirendonck, J.-P. D'Anvers, A. Karmakar, J. Balasch, and I. Verbauwhede, "A side-channel resistant implementation of SABER." Cryptology ePrint Archive, Report 2020/733, 2020. https://eprint.iacr.org/2020/733.