INDIAN STATISTICAL INSTITUTE, KOLKATA

R. C. BOSE CENTRE FOR CRYPTOLOGY AND SECURITY

KATHOLIEKE UNIVERSITEIT LEUVEN

COMPUTER SECURITY AND INDUSTRIAL CRYPTOGRAPHY

Abstract of Master's Thesis

by Tamas Kanti Garai (CrS2116)

SCA Resistant Implementation of Post-Quantum Scheme: CRYSTALS - Kyber

Advisors: Prof. Dr. Ingrid Verbauwhede & Prof. Dr. Bimal Kumar Roy
Daily Supervisors: Suparna Kundu, Angshuman Karmakar & John Gaspoz

March, 2023

Abstract

The security of most of the widely employed public-key cryptographic protocols depends on the hardness assumption of the integer factorization problem and the elliptic curve discrete logarithm problem. Unfortunately, using Shor's algorithms, one can solve these hard-to-solve problems in the presence of large quantum computers. Although no such powerful quantum computer is available yet, the uninterrupted advancement in the construction of quantum computers poses a threat to the future. As a result of this, together with the announcement by the *National Institute of Standards and Technology (NIST)* to define new standards for digital signature, encryption, and key-establishment protocols, have created significant interest in *Post-quantum cryptography (PQC)*.

Initially, the main focus of the research in *PQC* was the mathematical security of the schemes and the performance of the schemes in the various platforms. In recent years, many works have shown that post-quantum schemes are vulnerable to *Side-Channel Attacks (SCA)* such as timing, power, and electromagnetic attacks. These kinds of attacks exploit the implementations of the mathematically secure scheme by using the leaked information during execution, such as the execution time of the algorithm, the power consumption, or the electromagnetic leakage from the hardware. Masking, shuffling, constant-time implementation, and regular secret-key updates are some of the countermeasures against *SCA*. So far, as a countermeasure against *SCA*, masking post-quantum cryptography has received some attention.

The core idea behind *masking* is to randomly split every sensitive variable X into $d+1$ shares $M_0, ..., M_d$ in such a way that the relation $M_0 \star ... \star M_d = X$ is satisfied for a group operation $\star$ (e.g. the x-or or the modular addition). Usually, $M_1, ..., M_d$ (called the masks) are randomly picked up and M_0 (called the masked variable) is processed to satisfy $M_0 \star ... \star M_d = X$. The parameter d is usually called the masking order.[1]

However, masking a post-quantum scheme causes huge performance and resource overhead. In the thesis, we want to implement *SCA*-resistant implementation of the post-quantum scheme *CRYSTALS - Kyber*, the only *NIST* selected public-key encryption and key-establishment algorithm in the year 2022[2], with reduced performance overhead. For that instead of using just

higher-order masking, we can use another countermeasure called shuffling together with lower-order masking since shuffling is usually significantly less costly than higher-order masking when applied to non-linear layers.

Shuffling consists in spreading the signal containing information about a sensitive variable X over t different signals $S_1, ..., S_t$ leaking at different times. This way, if the spread is uniform, then for every i the probability that S_i corresponds to the manipulation of X is $\frac{1}{t}$. As a consequence, the signal-to-noise ratio of the instantaneous leakage on X is reduced by a factor of t. Applying shuffling is straightforward and does not relate to the nature (linear or non-linear) of the layer to protect.[1]

Then we focus on constructing side-channel resistant implementation of the scheme as efficiently as possible in software by using microcontrollers. Then we can verify the designed protected implementation of the post-quantum algorithm in the *COSIC* state-of-the-art security evaluations lab.

References

[1] Julien Doget Matthieu Rivain Emmanuel Prouff. *Higher-order Masking and Shuffling for Software Implementations of Block Ciphers*. Cryptology ePrint Archive, Paper 2009/420. https://eprint.iacr.org/2009/420.pdf. 2009. DOI: 10.46586/tosc.v2021.i3.137-169. URL: https://eprint.iacr.org/2009/420.pdf.

[2] *Post-Quantum Cryptography: Selected Algorithms 2022*. https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022. Accessed: 2010-03-03.