ERCIM "ALAIN BENSOUSSAN" FELLOWSHIP PROGRAMME

Scientific Report

First name / Family name	Erdem ALKIM
Nationality	Turkey
Name of the *Host Organisation*	Fraunhofer
First Name / family name of the *Scientific Coordinator*	Ruben Neiderhagen
Period of the fellowship	01/09/2019 to 31/08/2020

I – SCIENTIFIC ACTIVITY DURING YOUR FELLOWSHIP

The fellowship project focused on improving the efficiency of cryptographic schemes that are candidates for standardization in the post-quantum cryptography project by NIST. During the fellowship, we mainly focused on cryptographic schemes that are based on lattice problems. Among the lattice-based schemes, the most efficient schemes are using polynomial rings to reduce key sizes and to provide faster implementations.

In [C3], we proposed efficient parameter sets for a provably secure electronic signature scheme that is based on lattice problems. The paper focusses on reducing the key sizes and on providing more efficient implementations compared to the parameter sets provided by the qTESLA submission in the first round of the NIST standardization project while still providing provable security.

As the ring version of lattice problems are used in most of the NIST standardization candidates, we proposed various optimizations for polynomial multiplication on various platforms. As target platforms, we have two different platforms in focus: the first one was a RISC-V based hardware-software co-design, which is a promising candidate for cryptographic accelerators; the second one is the ARM Cortex-M4 based platform, which is one of the official target platforms for embedded systems in the NIST standardization project.

In lattice-based schemes, polynomial rings are defined using two parameters: the degree of the quotient polynomial and the integer ring used for its coefficients. These parameters are usually defined to allow efficient FFT-based polynomial multiplication. Although FFT-based algorithms provide relatively low complexity, they require modular operations since they perform arithmetic in the integer rings.

In [C1], we proposed special instruction extensions for arithmetic operations in selected integer rings. To show the effect of the extensions, we implemented the two NIST candidates, NewHope and Kyber using our extensions. Our results show that the extensions can provide up to 33% performance improvement and up to 61% improvement on the code size for polynomial multiplication. Up to 25% performance improvement can be achieved for the complete schemes using our improved polynomial multiplication.

In [C2], we proposed various optimizations to improve the performance of several lattice-based key encapsulation schemes, namely NewHope, NewHope-Compact and Kyber. In addition to performance optimizations, the paper also proposes techniques to reduce stack usage for these schemes. We show in the paper that our suggested optimizations can result in more than 5% performance and 10% stack usage improvements for all implemented schemes.

In [C5], we proposed various methods to use FFT-based multiplication for polynomial rings that do not naturally support FFT-based multiplication. FFT-based polynomial multiplication provides in-place polynomial multiplication in Z_q/(X^n-1) for selected parameters n and q. Most lattice-based schemes that use the ring version of lattice problems select parameters to utilize this polynomial multiplication algorithm. However, one of the NIST round 3 alternate candidates, NTRU Prime, intentionally selects iparameters that do not support such multiplication. In this paper, we show that even though the parameters are explicitly selected not to support such algorithms, FFT-based polynomial multiplication can still be implemented for those parameters and it can even outperform other approaches. Our results shows that our implementation provides 17% to 28% faster polynomial multiplication and 9% to 15% faster implementations of the entire scheme while requiring 15% to 39% less memory.

Although the main focus of the project was polynomial multiplication in the lattice-based schemes, these schemes need to generate random numbers from special distributions. As the discrete Gaussian distribution is the base for those special distributions, we proposed an efficient hardware implementation for generating samples from discrete Gaussian distribution in [C4]. The paper describes an efficient way to implement a Gaussian sampler that can generate samples for a wide range of the distribution parameters in standard deviations.

II – PUBLICATION(S) DURING YOUR FELLOWSHIP

During the tenure of this fellowship, I have contributed to the publication of papers in international conferences. In addition to this, my co-authors and I submitted two more papers to conferences that are currently in the review process:

C1. Erdem Alkim, Hülya Evkan, Norman Lahr, Ruben Niederhagen and Richard Petri, ISA Extensions for Finite Field Arithmetic: Accelerating Kyber and NewHope on RISC-V, IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020(3), 219-242. 10.13154/tches.v2020.i3.219-242.

C2. Erdem Alkim, Yusuf Alper Bilgin, Murat Cenk, François Gérard, Cortex-M4 Optimizations for {R,M}LWE Schemes, IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020(3), 336-357. 10.13154/tches.v2020.i3.336-357.

C3. Erdem Alkim, Paulo S. L. M. Barreto, Nina Bindel, Juliane Kramer, Patrick Longa and Jefferson E. Ricardini, The Lattice-Based Digital Signature Scheme qTESLA, International Conference on Applied Cryptography and Network Security. Springer, Cham, 2020, Accepted.

C4. Emre Karabulut, Erdem Alkim, Aydın Aysu, Efficient, Side-Channel Resilient, and Flexible Gaussian Sampling Hardware for Lattices, IACR Transactions on Cryptographic Hardware and Embedded Systems, 2021(1), Under Review.

C5. Erdem Alkim, Dean Yun-Li Cheng, Chi-Ming Chung, Hülya Evkan, Vincent Hwang, Trista Ching-Lin Li, Ruben Niederhagen, Cheng-Jhih Shih, Julian Wälde, Bo-Yin Yang, Polynomial Multiplication in NTRU Prime: Comparison of Optimization Strategies on Cortex-M4, IACR Transactions on Cryptographic Hardware and Embedded Systems, 2021(1), Under Review.

III – ATTENDED SEMINARS, WORKHOPS, CONFERENCES

Due to Corona virus, most of the conferences and workshops in related topics were postponed after the end of the fellowship. Therefore, I was not able to attend any conferences.

IV – RESEARCH EXCHANGE PROGRAMME (REP)

I conducted the research exchange programme online with Dr. Ir. Thijs VEUGEN from TNO, the Netherlands. Before the REP, we selected some possible collaboration topics. During the REP, in addition to Dr. Thijs VEUGEN, I found an opportunity to exchange research ideas with two other researchers from TNO. I gave a short talk to introduce my research projects about improving the efficiency of lattice-based cryptographic schemes. We discussed scientific collaboration opportunities and found a topic that both sides are interested in. We were able to build a project around improving a one-year old paper of the TNO team. The project requires to improve the efficiency of securely generating the keys of the Paillier crypto system. Since the REP was done in a period very close to the end of the fellowship and since the project requires a couple of months, we decided to continue working together after the fellowship.