Invited Talk

Department of Computer Science and Engineering

Indian Institute of Technology Kanpur

Date: Friday July 7, 2017

Time: 5 pm

Venue: KD 101

Implementation aspects of ring-LWE-based post-quantum public key cryptography and homomorphic encryption

Sujoy Sinha Roy

Computer Security and Industrial Cryptography (COSIC)

Catholic University of Leuven, Belgium

https://www.esat.kuleuven.be/cosic/people/sujoy-sinha-roy/

Abstract: Shor's algorithm running on a powerful quantum computer would break the RSA and ECC public-key cryptosystems. Keeping in mind the recent progress in quantum computing, NIST has recommended a gradual shift towards quantum-computing-secure public-key cryptography. Post-quantum cryptography refers to cryptographic algorithms that are presumed secure against quantum attacks. Of several candidates, lattice-based public-key cryptography is the most promising one. We investigated implementation aspects of lattice-based post-quantum public key schemes whose security is based on the hardness of the ring-LWE problem. These cryptographic schemes perform arithmetic operations in a polynomial ring and require sampling from a discrete Gaussian distribution. To design a discrete Gaussian sampler that satisfies a negligible statistical distance to the accurate distribution, we analyzed the Knuth-Yao random walk, and proposed an algorithm that is fast and lightweight. For efficient polynomial multiplication, we applied the number theoretic transform and performed computational and architectural optimizations. From these primitives, we designed a compact coprocessor architecture. For a medium security level, the architecture takes only 20/9µs to compute encryption/decryption on a Xilinx FPGA. We also implemented the proposed algorithms on resource-constrained software platforms and found that the ring-LWE-based public-key encryption is roughly 10 times faster than the ECC-based public-key encryption.

Homomorphic encryption enables computation on encrypted data. One application of homomorphic encryption is private cloud computing: a user uploads her encrypted data in the cloud and then computes on the encrypted data. The ring-LWE problem has been used to construct homomorphic encryption schemes. However, software implementations of homomorphic evaluation are very slow due to its arithmetic involving very large polynomials with large coefficients. In this research, we designed a multi-core FPGA-based accelerator for the homomorphic encryption scheme FV. Fast computation time is achieved by implementing

various optimizations on both algorithm and architecture levels. We observe that though the computation intensive arithmetic can be accelerated, the overhead of external memory access becomes a bottleneck. Then we propose a more practical scheme that uses a special module to assist homomorphic function evaluation in less time. With this module, we can evaluate encrypted search roughly 20 times faster than the implementation without this module.

Bio: Sujoy Sinha Roy received the BS degree in Electronics and Telecommunication engineering from the Bengal Engineering and Science University Shibpur (presently known as the Indian Institute of Engineering Science and Technology Shibpur), in 2007 and received the MS degree in Computer Science and Engineering from the Indian Institute of Technology, Kharagpur, in 2012. He received the PhD degree in Electrical Engineering from the Computer Security and Industrial Cryptography group, KU Leuven, in June 2017. His research area has been broadly in the field of efficient implementation of public key cryptography.