Mathematics of Security Analysis for Modern Cryptography

Period：9/20(Wed) - 9/22(Fri)

Venue：JR Hakata City 9F Conference room1

9/20（Wed）

13:00-13:10 Opening

Session 1: Hardware Security

13:10-14:10　Yuichi Hayashi (NAIST)

Mathematics of Electromagnetic Information Leakage Including Modern Cryptography

【Abstract】

This talk focuses on the mechanism of electromagnetic information leakage from hardware, including modern cryptography, and explains the process of leakage of a secret key inside a module to the outside of a device through electromagnetic waves using a mathematical model. The same model can also explain the process of secret key leakage due to intentional electromagnetic interference based on the electromagnetic reciprocity theorem.

14:25-15:25　Rei Ueno　(Tohoku University)

Cryptographic Primitives and Hardware Architecture for Memory Encryption

【Abstract】

Memory encryption is essential to realize the privacy and trust of date stored in main memory, which is placed outside the CPU. Especially in recent years, with the advanced performance and greater capacity of Non-Volatile Memory (NVM), adoption of NVM has grown in data centers, IoT devices, and modern CPUs for power efficiency and performance improvement. However, NVM poses a higher risk of eavesdropping and tampering/data manipulation due to its data non-volatility, than DRAM. Therefore, a memory encryption mechanism, which is capable of encryption and authentication for large-capacity NVM with real-time processing, is strongly demanded. In this presentation, we will provide an overview of cryptographic primitives and its hardware architecture for secure NVM, incorporating the latest findings from the presenters.

15:40-16:40　Abdul Rahman Taleb (CryptoExperts and Sorbonne University)

Towards Achieving Provable Side-Channel Security in Practice

【Abstract】

Physical side-channel attacks are powerful attacks that exploit a device's physical emanations to break the security of cryptographic implementations. Many countermeasures have been proposed against these attacks, especially the widely-used and efficient masking countermeasure. Nevertheless, proving the security of masked implementations is challenging. Current techniques rely on empirical approaches to validate the security of such implementations. On the other hand, the theoretical community introduced leakage models to provide formal proofs of the security of masked implementations. Meanwhile, these leakage models rely on physical assumptions that are difficult to satisfy in practice, and the literature lacks a clear framework to implement proven secure constructions on a physical device while preserving the proven security.

9/21(Thur)

Session 2: Security on Symmetric Key Encryption

10:00-11:00　Akiko Inoue (NEC)

On the security and attacks against mode of operation for authenticated encryption

【Abstract】

Authenticated encryption (AE) is a symmetric key cryptosystem that achieves privacy and authenticity simultaneously. Recent attacks against AE show that secure conventional AE can be broken easily when there is a bug in implementation, or show that some protocols require additional security beyond conventional AE security. This presentation introduces conventional AE, attacks against it, and some AE construction/attacks beyond conventional AE security.

11:15-12:15　Yosuke Todo (NTT)

Security Model for Cache Randomization Function and Design and Security Analysis of SCARF

【Abstract】

Cache attack is a kind of the side-channel attack exploiting the latency difference between the cache and memory accesses. To prevent the cache attack, a cache randomization is promising. At Usenix Security 2023, we proposed the demanded security model for cache

randomization function, the design methodology using the tweakable block cipher, and a specific construction SCARF. In this talk, we first explain this security model. Then, we explain the design process of SCARF and specific discussion about the security of SCARF.

Session 3: Quantum Security

13:45-14:45 Kento Oonishi (Mitsubishi)

Shor's Algorithm Using Efficient Approximate Quantum Fourier Transform

【Abstract】

This presentation shows more efficient Shor's algorithm which solves the integer factoring problem. The integer factorization and discrete logarithm problems are fundamental problems for the security of the current public-key cryptosystems, including the RSA cryptosystems and elliptic curve cryptosystems. Shor's algorithm solves these problems in polynomial time. The evaluation of Shor's algorithm is very important for estimate the time when Shor's algorithm breaks these two public-key cryptosystems. This presentation discusses Shor's algorithm using the approximate quantum Fourier transform. Especially, this presentation discusses the method for minimizing computational cost for Shor's algorithm with fault-tolerance.

15:00-16:00 Junpei Yamaguchi (Fujitsu)

Implementation and analysis of new quantum algorithm SQIF for integer factorization

【Abstract】

In December 2022, a new quantum algorithm called SQIF (Sublinear-resource Quantum Integer Factorization) was proposed, which can factorize integers using fewer qubits than Shor's algorithm. SQIF is based on the difference of squares method, which requires many "relations". SQIF finds a relation by solving a combinatorial optimization problem derived from a lattice problem using the quantum algorithm QAOA. In this talk, we will present the details of our paper, which was published at CSEC in May 2023. First, we will introduce the details of SQIF, and point out the problem that only a few relations can be calculated. Next, we propose an extended version of SQIF that can calculate a sufficient number of relations, and present its experimental results. To scale up the experiments, we used classical annealing computation instead of QAOA and successfully factorized composite numbers from 11 to 55 bits. Finally, we provide an estimate of the number of qubits and computational complexity required for the factorization of a 2048-bit composite number.

16:10-16:40 Ren Taguchi (The University of Tokyo)

Quantum resource estimate for Shor's algorithm for binary ECDLP

【Abstract】

Several study estimates the quantum resources for Shot's algorithm which solves discrete logarithm problems in polynomial time, the quantum inversion computation is dominant for binary elliptic curves. In this talk, we focus on the quantum FLT-based inversion which requires fewer Toffoli gates and the fewer depth. We introduce two quantum FLT-based inversion algorithms which improve the prior works in each and show that we can reduce more qubits.

9/22(Fri)

Session 4: Side-Channel Attack

10:00-11:00 Keita Xagawa (TII)

A survey of side-channel assisted key-recovery attacks against lattice-based key-encapsulation mechanisms

【Abstract】

With the progress in the development of quantum computers, there has been a growing emphasis on standardization and implementation of Post-Quantum Cryptography (PQC) due to the potential impact. Within the NIST's PQC standardization, which holds significant influence, Kyber, a lattice-based cryptosystem, has been selected for key encapsulation mechanisms (KEM) based on criteria such as size, speed, and security. Since standardized KEMs are intended to be implemented in various devices, resistance to side-channel attacks is also crucial. This presentation reviews key-recovery attacks on lattice-based cryptosystems, e.g., Kyber, utilizing side-channel analyses. We focus on the efficiency of these attacks, specifically after constructing a plaintext-checking oracle and a decryption oracle using side-channel analyses.

11:20-12:20 Akita Ito (NTT)

Deep Learning Based Side-channel Attacks and Their Countermeasures

【Abstract】

A side-channel attack is an attack that estimates the secret key in a cryptographic module by using its side-channel information (e.g., power consumption and electromagnetic radiation). In this talk, we will discuss deep-learning-based side-channel attacks (DL-SCAs),

which have attracted much attention in recent years. It is known that deep neural networks enable more powerful attacks than conventional ones by learning the characteristics of side-channel information of the target module in advance. We will also focus on masking countermeasures, a typical countermeasure against side-channel attacks, and explain that masking countermeasures are also effective against DL-SCAs.

12:20-12:30 Closing

13:00-15:00 Free Discussion