高度化する暗号技術と数学的技法の進展

Advances in Sophisticated Cryptography and Mathematical Techniques

アブストラクト

11/7

面 和成（筑波大学）

Title：Blockchain and its applied research

Abstract：Blockchain is a secure distributed ledger system built with digital signatures and cryptographic hash functions that satisfies both tamper resistance and high availability. Blockchain emerged with cryptoassets and is now applied in various fields where data falsification or system crash is critical, such as finance, supply chain, and medical information. In addition, blockchain has a feature that allows programs called "smart contracts" to run by themselves, which opens a wide range of application possibilities. In this talk, I will explain about cryptoassets, blockchain, and smart contracts, and introduce recent applied research on notarization system using individual number card and smart contracts.

吉野 雅之/山本 恭平（日立製作所）

Title：On research of cryptography for secure SaaS: attacks, security requirements and practical solutions

Abstract：The Corona disaster in the 2020s triggered a shift to teleworking in just a few years. SaaS, which allows workers to use a computing environment from home equivalent to the workplace, has become increasingly popular. While the use of data has increased, data management has not been strengthened, and the scale of data leaks has grown over the years. Recent research on multi-party computation and homomorphic encryption has not matured to provide secure SaaS to general users. This presentation will discuss the challenges of realizing secure SaaS and introduce the proposed methods using multiple cryptographic techniques（SSE, TEE, and HE）.

髙橋 朋伽（大阪大学）

Title：On the Weakness of Ring-LWE mod Prime ideal by Trace Map

Abstract：The recent decision by the National Institute of Standards and Technology（NIST）to standardize lattice-based cryptography has further increased the demand for security analysis of it. The Ring-Learning with Error（Ring-LWE）problem is one of the mathematical problems that constitute such lattice cryptography, and it has many algebraic properties because it is considered in the ring of integers R of an algebraic number field K. These algebraic properties make the Ring LWE based schemes efficient, while some of them are also used for attacks. When the modulus q is unramified in K, it is known that the Ring-LWE problem, to determine the secret information s in R/qR, can be solved by determining s (mod p) for all prime ideals p lying over q. The χ2-attack determines s (mod p) by using the χ2-test over a finite field Fq^f, which is improved in the special case where the residue degree f is two, called the two-residue-degree χ2-attack. We extend the two-residue-degree χ2-attack to the prime-residue-degree and composite-number-residue-degree χ2-attack. Our extensions enable the χ2-attack to not only two but also any residue-degree case more efficiently work. As a result, the attack time against a vulnerable field to our proposed attacks with parameter (q,f)=(67,3) took 129 seconds on a standard PC.

11/8

清藤 武暢（有限責任監査法人トーマツ）

Title：Recent Trends on Zero-Knowledge Proof: Theory and its Applications

Abstract：Recently, studies are underway in various fields of organizations to improve internal operations and generate new business values by using data sharing and/or usage platforms. Organizations are focused on privacy-enhancing technologies to guarantee the security of data handled on the above platforms (PETs, for short). And, the zero-knowledge proof is one of the main technology of PETs. This technology can achieve a mechanism that a third party can verify that attributes of data are correct without sharing actual data. In this talk, we will overview the theory and some use cases of the zero-knowledge proof.

松岡 航太郎（京都大学）

Title：Evaluating Boolean circuits over ciphertexts using Fully
Homomorphic Encryption over the Torus

Abstract：In this talk, I will explain how to evaluate Boolean circuits over ciphertexts using Fully Homomorphic Encryption over the Torus (TFHE). By representing privacy-preserving computing as Boolean circuits, we can use conventional logic synthesis tools. TFHE is suitable for the Boolean circuit evaluations because it supports fast Bootstrapping, the heaviest part for deep circuits evaluations. This talk aims to tell how to construct the secure boolean circuit evaluation method from basic mathematics to some technical considerations for performance and security.

小貫 啓史（東京大学）

Title：Recent topics for isogeny-based cryptography

Abstract：Recently, a series of researches gave serious attacks to SIKE, an isogeny-based protocol that is one of the NIST PQC candidates. These attacks highly depend on the design of SIKE, and there are other isogeny-based protocols which are considered to be secure against these attacks. I will give an overview of the attacks to SIKE and show which protocols are still considered to be secure.

渡邉 洋平（電気通信大学）

Title：Recent Progress in Searchable Encryption

Abstract：Consider a two-party information retrieval system where a server stores a database and a client sends the server queries to search the database for the queries. Searchable encryption enables the client to search for a keyword, even if the database is encrypted, without revealing any useful information on the database to the server. In this talk, I focus on searchable symmetric encryption (SSE), one of the active research areas on searchable encryption. I will provide the historical background of SSE research, discuss trade-offs between security levels and efficiency in SSE, and show the state-of-the-art SSE schemes.

11/9

安田 貴徳（岡山理科大学）

Title：Construction of pairing using elliptic curves

Abstract：A practical pairing requires small embedding degrees. It imposes strong conditions for the orders of elliptic curves, and the CM theory is indispensable. Recently, pairing is applied to the zk-SNARKs, which require additional conditions for the elliptic curves from the view of efficiency. Consequently, usable curves for the zk-SNARKs are limited. The construction of a good pairing is even now a problem.

Dung Hoang Duong（University of Wollongong）

Title：Cryptography from group actions

Abstract：Cryptographic Group Actions have been taken a lot of attentions recently, especially in the context of isogeny-based cryptography. In this talk, I will introduce another new research direction on non-commutative cryptographic group actions and their interconnections with other areas of cryptography. I will also introduce some possible cryptographic constructions.