JST (Japan-Taiwan project)

Chang Gung University + Osaka University + JAIST joint work shop

2018/8/23-2018/8/29

This workshop is partially supported by the Japan-Taiwan Collaborative Research Program at Japan Science and Technology Agency,

Contents

1. Location / Flight information

[Location]

Chang Gung University

No. 259, Wenhua 1st Road, Guishan District, Taoyuan City, 台湾 333

http://www.cgu.edu.tw/bin/home.php?Lang=en

[Flight information]

■1 時間 20 分 往復 3,500 円(乗車日より 14 日間有効)

05:50 蛍池駅

|大阪空港・蛍池駅⇔関西空港 リムジンバス

07:10 関西空港第 1 ターミナル

■1 時間 20 分 往復 3,100 円(乗車日より 14 日間有効)

6:00 JR 茨木東口 BR2

6:12 阪急茨木東口 BR1

| JR茨木東口・阪急茨木東口⇔関西空港 リムジンバス

7:20 関西空港第 1 ターミナル

■53 分 3,050 円(乗車券 1,360 円 特別料金 1,690 円)

6:17 新大阪

| JR特急はるか 1 号・関西空港行

7:10 関西空港(鉄道)

7:30 関西国際空港 第 1 ターミナルビル 4F 国際線出発フロア 集合

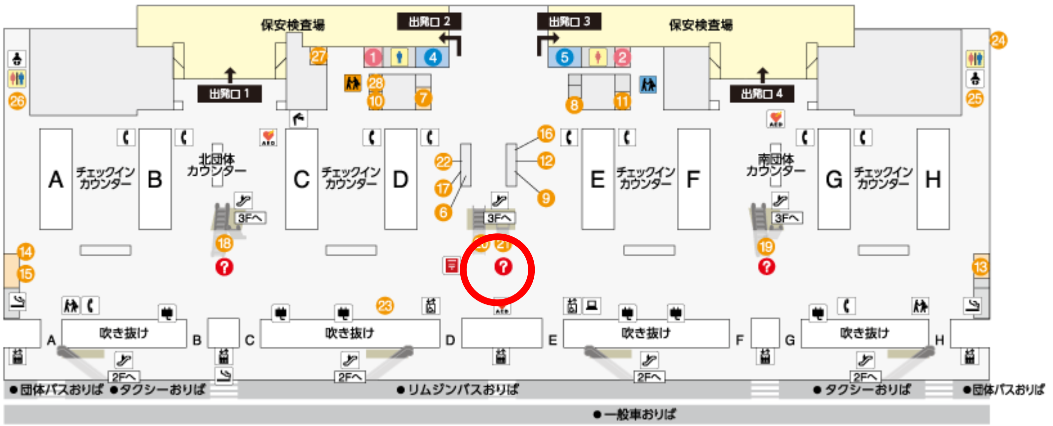

図:関西国際空港 第 1 ターミナルビル 4F(赤マル:中央インフォーメーション辺りに集合)

JL 813S　23AUG　大阪/関空　ー　台北/桃園　09:10 - 11:05

JL 816V　29AUG　台北/桃園　ー　大阪/関空　12:15 - 16:00

2. Purpose

台湾研修の目的は，各人がもつ情報セキュリティの知識を様々な知識を持つ人たちと議論しながら，交換し共有することで，発想の転換方法，コミュニケーション能力を身につけることにあります．

異なる国の人たちと，研究室から場所を変えて議論することは他では得られない経験と自信につながります．また，Chang Gung 大学との交流によるボーダレスな人脈は宮地研修了後にも大きな財産になります．

本研修を通して，社会で活躍する技術者・研究者の基礎素養に，問題発見・解決能力，try and error のサイクルの縮小化を支えるコミュニケーション能力，ダイバーシティ力を身につけるとともに，楽しい経験を積むことを期待しています．

3. Freshener’s talk and Discussion 8/24 (Fri.)

In this session, students present their research background and target for the first time.

We know each research topics in this session.

09:00-09:10	Welcome Remark　Opening (Prof. Chien-Lung Hsu)
09:10-10:25	Session A: Chebyshev chaotic map, symmetric cipher, solver (Chair: Prof. Chien-Lung Hsu)
	Chebyshev chaotic map-based protocols for multi-server environments Tzu-Wei Lin (CGU)* **Solving polynomial system with characteristic set algorithms** Tomoya Nishiguchi (Osaka univ.) **Revisited Diffusion Analysis of Salsa and ChaCha** Yusuke Matsuoka (Osaka univ.)
10:25-10:35	Break
10:35-11:50	Session B: Data sharing (Chair: Prof. Kuo-Yu Tsai)
	Blockchain-enabled genomic data sharing and analysis platform Le Tuan Vinh (CGU)* **Hidden Vector Encryption and its application**

	Motoi Hayashi (Osaka univ.)
	Degree-3 CRH and its application to string commitment
	Hideaki Miyaji (Osaka univ.)
11:50-13:20	Lunch Break
13:20-14:35	Session C: Secure protocol
	(Chair: Prof. Atsuko Miyaji)
	Multiparty Private Set Operation over public network
	Katsunari Shishido (Osaka univ.)*
	Attribute-based encryption scheme with selective attribute revocation
	Guan-Lin Cheng (CGU)
	On Efficient Privacy enhanced technology ZK-SNARK and its application to Zerocash
	Yuki Sugitani (Osaka univ.)
14:35-14:45	Break
14:45-16:00	Session D: Distributed/multi server environment/attack
	(Chair: Prof. Chen-Mou Cheng)
	Security analysis on ECDLP based on index calculus algorithm
	Kenta Kodera (Osaka univ.)*
	The Distributed Ledger of Blockchain for Digital Evidence Preservation
	Wei-Xin Chen (CGU)
	User authentication protocols with three factors and key agreement for multi-server environments
	Mei-Chen Hsieh (CGU)
16:00-16:10	Break

3. First Group Discussion 8/24 (Fri.)

In this session, students share each research topics, discuss what you do not understand each other.

16:10-16:50	Group discussions
17:00-	Welcome party

4. Outside Exchange 8/25 (Sat.)

In this session, we know each other and communicate outside.

8:00	明徳寮 1 階集合—出発 Meet at 1F, Ming-De Building (Dorm 3)	
8:25-8:40	長庚大学→長庚医院 CGU→Chang Gung Memorial Hospital	シャトルバス Shuttle bus
9:00-9:34	A8 長庚医院駅→A1 台北駅 A8 Chang Gung Memorial Hospital Station→A1Taipei Main Station	桃園 MRT Tauyuan Metro
9:45-10:15	R10 台北駅→R08 中正紀念堂 R10 Taipei Main Station→R08 Chiang Kai-Shek Memorial Hall	台北 MRT Taipei Metro
10:15-10:35	朝食 Breakfast	
10:35-11:20	中正紀念堂観光 Visit Chiang Kai-Shek Memorial Hall	
11:20-11:30	R08 中正紀念堂→R07 東門 R08 Chiang Kai-Shek Memorial Hall→R07 Dongmen	台北 MRT Taipei Metro
11:30-14:00	昼食 Lunch	ディンタイフォン(永康街) Din Tai Fung (Yongkang Street)
14:00-14:15	R07 東門→ R03 台北 101/世界貿易センター	台北 MRT

	R07 Dongmen →R03 Taipei 101/World Trade Center	Taipei Metro
14:15-15:30	台北 101 Taipei 101	マンゴーかき氷 Mango shaved ice
15:30-16:30	R03 台北 101/世界貿易センター→R22A 新北投 R03 Taipei 101/World Trade Center →R22A Xinbeitou	台北 MRT Taipei Metro
16:30-17:30	温泉 Hot Spring	北投青磺名湯 Qinghuang Hot Spring
17:30-18:10	R22 北投→ R15 剣潭 R22 Beitou→ R15 Jiantan	台北 MRT Taipei Metro
18:10-20:50	夕食 Dinner	士林夜市 Shilin Night Market
20:50-21:15	R15 剣潭→ R10 台北駅 R15 Jiantan → R10 Taipei Main Station	台北 MRT Taipei Metro
21:22-21:50	A1 台北駅→A8 長庚医院駅 A1 Taipei Main Station→A8 Chang Gung Memorial Hospital Station	桃園 MRT Tauyuan Metro
22:40-23:00	長庚医院→長庚大学 Chang Gung Memorial Hospital→ CGU	シャトルバス Shuttle bus

5. Faculty’s talk 8/27 (Mon.)

In this session, faculties present recent their interested researches, where they are base of student researches. Thorough faculty’s talk, students understand general background and research target in each research group.

09:30-09:40	Welcome Remark (Chair: Prof. Kuo-Yu Tsai)
09:40-10:40	Faculty’s talk (Chair: Prof. Shinya Okumura)
09:40-10:10	**Title: Hierarchical Group Secure Communication Protocol with Anonymous Authentication for IoT-Based and Community-based Healthcare Environments** Prof. Chien-Lung Hsu
10:10-10:40	**Title: Lightweight Authentication Schemes for IoT Applications** Prof. Kuo-Yu Tsai
10:40-10:50	Break
10:50-12:20	Faculty’s talk (Chair: Prof. Chien-Lung Hsu)
10:50-11:20	**Title: Efficient Elliptic Curve Scalar Multiplication** Prof. Atsuko Miyaji
11:20-11:50	**Title: On the use of Frobenius map to accelerate polynomial multiplication with Cantor FFT** Prof. Chen-Mou Cheng
11:50-12:20	**Title: Characteristics of Hardware Accelerators for Elliptic Curves Cryptography** Prof. Kiyofumi Tanaka
12:20-13:10	Lunch break
12:20-13:10	Faculty Lunch meeting

6. Research Discussions 8/27

In this session, understand other researches and improve your knowledge. Let us focus on one important (key) research of team members or researches that you like. Through discussion, understand your own research building blocks well.

13:10-14:50	Understand other researches and improve your knowledge
14:50-15:00	Break

15:00-17:00	Present other researches (Chair: Prof. Chen-Mou Cheng)
15:00-15:30	**Team A: Chebyshev chaotic map, symmetric cipher, solver** Tzu-Wei Lin→Tomoya Nishiguchi → Yusuke Matsuoka→ Tzu-Wei
15:00-15:10	Tzu-Wei Lin present Yusuke Matsuoka research
15:10-15:20	Tomoya Nishiguchi present Tzu-Wei Lin research
15:20-15:30	Yusuke Matsuoka present Tomoya Nishiguchi research
15:30-16:00	**Team B: Data sharing** Motoi Hayashi →Le Tuan Vinh→Hideaki Miyaji→Motoi
15:30-15:40	Le Tuan Vinh present Motoi Hayashi
15:40-15:50	Motoi Hayashi present Hideaki Miyaji research research
15:50-16:00	Hideaki Miyaji present Le Tuan Vinh research
16:00-17:00	Present other researches (Chair: Prof. Shinya Okumura)
16:00-16:30	**Team C: Secure protocol** Yuki Sugitani→Guan-Lin Cheng →Katsunari Shishido →Yuki
16:00-16:10	**Katsunari Shishido presents Guan-Lin Cheng research**
16:10-16:20	Guan-Lin Cheng presents Yuki Sugitani research
16:20-16:30	Yuki Sugitani presents Katsunari Shishido research
16:30-17:00	**Team D: Distributed/multi server environment/attack** Kenta Kodera→Mei-Chen Hsieh→ Wei-Xin Chen→Kenta
16:30-16:40	Kenta Kodera presents Wei-Xin Chen research
16:40-17:50	Mei-Chen Hsieh presents Kenta Kodera research
16:50-17:00	Wei-Xin Chen presents Mei-Chen Hsieh research

7. Final presentation 8/28 (Tue)

In this session, we combine each researches, focus on a key or your favorite research of team members, think use cases of these. We can pose a problem that we need to solve, or expose problems of your research.

08:30 - 08:40	Welcome Remark Opening (Prof. Chien-Lung Hsu)
08:40 - 09:30	Preparation
09:30 - 10:00	Session A: Chebyshev chaotic map, symmetric cipher, solver (Chair: Prof. Chien-Lung Hsu)
09:30 - 09:40	Tzu-Wei Lin*
09:40 - 09:50	Tomoya Nishiguchi
09:50 - 10:00	Yusuke Matsuoka
10:00 - 10:30	Session B: Data sharing (Chair: Prof. Kuo-Yu Tsai)
10:00 - 10:10	Le Tuan Vinh*
10:10 - 10:20	Motoi Hayashi
10:20 - 10:30	Hideaki Miyaji
10:30 - 10:40	Break
10:40 - 11:10	Session C: Secure protocol (Chair: Prof. Chen-Mou Cheng)
10:40 - 10:50	Katsunari Shishido*
10:50 - 11:00	Guan-Lin Cheng
11:00 - 11:10	Yuki Sugitani
11:10 - 11:40	Session D: Distributed/multi server environment/attack (Chair: Prof. Shinya Okumura)
11:10 - 11:20	Kenta Kodera*
11:20 - 11:30	Wei-Xin Chen
11:30 - 11:40	Mei-Chen Hsieh
11:40 - 11:50	Closing (Prof. Atsuko Miyaji)

7. Abstract

7.1 Freshener’s talk

(1)Speaker: Tzu-Wei Lin (CGU)*

Title: Chebyshev chaotic map-based protocols for multi-server environments

Abstract: Multi-server environments have a property called mobility which means users can pass through multiple access point while maintaining ongoing connections. This kind of network can provide users more diversified service. Namely, user can login different servers through the Internet to obtain diversified service. A password authenticated key exchange scheme can be used to authenticate users' legitimacy and establish a secure communication between user and server through his own password. Users can access Internet services from multiple servers. However, it is difficult for users to manage passwords and secret keys securely. If utilizing traditional password-based authenticated key exchange scheme to ensure security of multi-server wireless network, we might face some problems: (i) Users should manage more than one pairs of identifiers and password which might increase user's load and risk of managing passwords. (ii) In general cases, if users utilize one single password to login different servers, we will need a registration center. The chaotic system is characterized by sensitive dependence on initial conditions, pseudo-randomness and ergodicity. These features have excellent properties of diffusion and confusion which are important to cryptography, especially secret key cryptosystems. In this talk, we will introduce the concept of multi-server environments, Chebyshev chaotic map applied in cryptosystem and some previous related works. We will also propose a password authenticated key exchange scheme for multi-server environments based on Chebyshev chaotic map.

(2)Speaker: Tomoya Nishiguchi (Osaka univ.)

Title: Solving polynomial system with characteristic set algorithms

Abstract: Elliptic curve cryptography is a widely used public-key cryptosystem. When we use index calculus to analyze the security of elliptic curve cryptography, the dominant computation is polynomial system solving. We experimentally evaluate how efficiently these polynomial systems can be solved using a characteristic set method, a form of depth-first search on some binary tree.

(3)Speaker: Yusuke Matsuoka (Osaka univ.)

Title: Revisited Diffusion Analysis of Salsa and ChaCha

Abstract: Both ChaCha and AES are standardized as symmetric ciphers in TLS 1.3; AES is a block cipher, whereas ChaCha is a stream cipher. The security of AES has been studied by many researchers. ChaCha, however, needs more security analysis because it has been proposed more recently, compared with AES. Furthermore, ChaCha is improved from Salsa from the point of view of diffusion and thus, diffusion analysis of Salsa and ChaCha is important to understand their security-design criteria. In this study, we revisit diffusion analysis and investigate weak bits and weak columns of Salsa and ChaCha. To the authors' knowledge, this is the first detailed diffusion analysis of Salsa and ChaCha.

(4)Speaker: Le Tuan Vinh (CGU)*
Title: Blockchain-enabled genomic data sharing and analysis platform
Abstract: The first human genome was sequenced in 2001 at a cost of $3 billion. Today, human genome sequencing costs less than $1000, and in a few years the price will drop below $100. Thus, personal genome sequencing will soon be widely adopted as it enables better diagnosis, disease prevention, and personalized therapies. Furthermore, if genomic data is shared with researchers, the causes of many diseases will be identified and new drugs developed. These opportunities are creating a genomic data market worth billions of dollars. Nebula Genomics seeks to lead this emerging market by understanding and overcoming key obstacles. We will spur genomic data growth by significantly reducing the costs of personal genome sequencing, enhancing genomic data protection, enabling buyers to efficiently acquire genomic data, and addressing the challenges of genomic big data. We will accomplish this through decentralization, cryptography, and utilization of the blockchain.

(5)Speaker: Motoi Hayashi (Osaka univ.)
Title: Hidden Vector Encryption and its application
Abstract: There are many cases that the recipient does not want to give server his full private key, but wants server to decrypt ciphertext partially. To solve this problem, searchable encryption is proposed, which generate token to decrypt the ciphertext that satisfies designated conditions from master key. For example, this technology is useful when the recipient want the mail server to discard the e-mail that satisfies some predicates, such as spam-mail. Using searchable encryption, the mail server can only distinguish spam-mail from normal mail with a token. We introduce Hidden Vector Encryption (HVE), which enables to compare conjunctive queries with

polynomial order of ciphertext size and token size.

(6)Speaker: Hideaki Miyaji (Osaka univ.)
Title: Degree-3 CRH and its application to string commitment
Abstract: Hash functions are functions that shrink a long input into a shorter output. That constructions are not so difficult to make, but it includes a lot of mathematical technics to keep its safety, for example, lattice problems to bind and hide their feature. I am now studying Hash which is composed two ways. It first expands the input bits and then, it shrinks it as output bits. This expansion achieves its locality to be constant. If its locality is constant, calculation time will be smaller because the locality and degree is in relevant. Achieve constant locality and degree is very important things and, I am forecasting how it is able to do. There are ways to do degree to 3 by using "Perfect randomized Encoding." I will make a bit commitment by using degree-3 hash functions and prove its safety.

(7)Speaker: Katsunari Shishido (Osaka univ.)*
Title: Multiparty Private Set Operation over public network
Abstract: Both scalability and flexibility have become crucial for privacy-preserving protocols in the age of big data. Multiparty private set intersection (MPSI) and Multiparty private set union (MPSU) are important privacy-preserving protocol. In our study, consider a method over public network, i.e. all parties have no shared key among parties. We have proposed a construction of MPSI and MPSU. MPSI consists of Additive homomorphic encryption and Bloom Filter. We implement our construction of MPSI. We will show an integration of medical data from distributed data-set by using our implementation. MPSU can be able to use even multiset. In order to apply MPSU in the multiset, we propose a new duplicated Bloom Filter to increase the chances of computing the number of duplicates correctly.

(8)Speaker: Guan-Lin Cheng (CGU)
Title: Attribute-based encryption scheme with selective attribute revocation
Abstract: Cipher text policy attribute-based encryption (CPABE) is a cryptography that could provide access control to cloud storage system. By utilizing this protocol, each data user has a secret key with his own attributes. Each data user utilizes the access structure and data user’s attributes to encrypt data. As the consequence, if data user’s attributes correspond to the data owner’s access structure, the data user can decrypt the cipher text and use this data. However, attribute revocation phase and update

phase of such kind of protocol consume a bunch of computation cost. In this study, we propose an attribute-based encryption scheme with selective attribute revocation and time bound which provides the data user’s attribute secret keys with time bound. We utilize time-stamp to embed into cipher test and user’s attribute secret key. If the data user’s secret key is out of date, the secret key would be discharged. Moreover, the scheme could achieve convenience of managing cipher text and user’s attribute secret key.

(9) Speaker: Yuki Sugitani (Osaka univ.)
Title: On Efficient Privacy enhanced technology ZK-SNARK and its application to Zerocash
Abstract: Bitcoin is the most widespread cryptocurrency in the world. While payments are conducted between pseudonyms, it has significant limitations regarding privacy: all transaction log is completely public. Zerocash is a practical scheme offering strong privacy guarantees and it's already implemented in Ethereum. ZK-SNARK is the main idea to protect each user's privacy used in Zerocash scheme.

(10) Speaker: Kenta Kodera (Osaka univ.)*
Title: Security analysis on ECDLP based on index calculus algorithm
Abstract: Elliptic curve cryptography (ECC) is in the spotlight due to their significantly smaller key size compared to other public-key cryptography. The security of ECC is based on the complexity of solving the elliptic curve discrete logarithm problem (ECDLP). Recently, there is a line of research on index calculus algorithms for ECDLP started by Semaev, Gaudry, and Diem. Index calculus is originally applied to discrete logarithm problem over a finite field (DLP). Under certain heuristic assumptions, such algorithms could lead to subexponential attacks to the ECDLP in some cases. This talk starts from basic ideas of index calculus algorithms over ECDLP to recent results including our analysis on difference of complexity of solving ECDLP for elliptic curves in various forms.

(11) Speaker: Wei-Xin Chen (CGU)
Title: The Distributed Ledger of Blockchain for Digital Evidence Preservation
Abstract: The utility of digital evidence is facilitated through digital forensic and preservation while providing evidence. However, it is difficult to preserve archives effectively for organizations which lacks management with specified mechanisms or specification. To ensure that digital evidence is credible in court, there is a need to

establish standards operational procedures for preserving digital evidence and to enhance digital forensic findings through standards and certification. In this study, we propose a blockchain the consistency of distributed ledger mechanism to achieve file consistency. We apply the consistency of distributed ledger mechanism in blockchain for data preservation. If the file is not strictly managed by system, it may suffer from file tampering, file loss, and other related issues. Therefore, we ensure the file-related maintenance through the consistency of distributed ledger mechanism.

(12) Speaker: Mei-Chen Hsieh (CGU)
Title: User authentication protocols with three factors and key agreement for multi-server environments
Abstract: Traditional password-based user authentication protocols authenticate the legitimacy of the user by checking user's valid password and identity. However, the password is either a long meaningless string, which is difficult for user to memorize, or a short easily-memorized password, which is easily suffered from password guessing attacks. In this paper, we propose a new user authentication protocol with three factors, which are smart card, user's biometric characteristics, and a password for multi-server environments based on protocol of Fan et al. which is designed for single server. We allow the user to register and login several servers by memorizing only one password. This protocol is secure against some potential attacks and impersonation attack plotted by any malicious server manager.

7.2 Faculty's talk

(1) Speaker: Prof. Chien-Lung Hsu (CGU)
Title: Hierarchical Group Secure Communication Protocol with Anonymous Authentication for IoT-Based and Community-based Healthcare Environments
Abstract: The Internet of Things (IoT) is an attractive technology to integrate a large number of connected objects that are communicating with each other via wireless communication networks. IoT innovative applications can make our life easier and smarter. Recently, many smart healthcare applications are based on IoT technology for people and caregivers to automatically monitor and collect personal health information such as ECG, temperature, moisture, heartbeat, behavior and etc. Such applications can provide precision Medicare, Medicaid, and Healthcare. IoT-based and community-based healthcare is to provide healthcare services including home support, nursing, physiotherapy, and rehabilitation services with integrated IoT technologies for people with all ages. Since such information is very sensitive for

people, security and privacy protection of IoT-based and community-based healthcare systems should be applied or enhanced. This paper will propose a hierarchical group secure communication protocol with anonymous authentication. Contributions of this paper are given below: (i) It is designed for hierarchical community-based healthcare services, which is suitable for long-term care community-based healthcare services. (ii) All IoT devices can be dynamically grouped hierarchically according to community-based healthcare services. (iii) All hierarchical grouped IoT devices can be anonymously and recursively authenticated for preserving user privacy, which will not be intercepted by adversaries for analyzing social behaviors. (iv) Secure communications will be achieved according to hierarchical groups to withstand potential attacks. That is, each subgroup IoT devices can have their own secure communication and they also can have one with all IoT devices. The proposed protocol can have hierarchical secure communications for community-based healthcare services or applications. (v) The proposed protocol is a lightweight security protocol, which is very suitable for IoT-based applications.

(2)Speaker: Prof. Kuo-Yu Tsai (Chinese Culture University)
Title: Lightweight Authentication Schemes for IoT Applications
Abstract: With the development of Information and communication technology, IoT (Internet of Things, IoT for short) applications can improve the quality of life and productivity of enterprises. However, privacy, security, and authentication issues in some applications are critical, such as in healthcare applications. In this research, we propose a lightweight authentication scheme for IoT applications. A dynamic hashing chain is applied to design an authentication mechanism for nodes in the proposed scheme. The proposed scheme can not only achieve low computation and storage costs, but also provide various security properties, such as anonymity, confidentiality, unforgeability, resistance to impersonation attacks, and resistance to replay attacks.

(3)Speaker: Prof. Atsuko Miyaji (Osaka University/JAIST/CREST, Japan)
Title: Efficient Elliptic Curve Scalar Multiplication
Abstract: Elliptic curve cryptosystem is the most attractive public key cryptosystem since it achieves the high security with a small key size. This is why elliptic curve cryptosystems are currently attracting a great deal of attention from a low power machine such as a smart card. Furthermore, a new tool from elliptic curve cryptosystems, called a bilinear pairing, cast a new light on various problems on

cryptology. Thus, important applications in cryptography have been constructed by using elliptic curves.

The dominant part of efficiency of elliptic curve cryptosystems is the elliptic scalar multiplication. From the point of view of security, researches on elliptic scalar multiplication are also important since naive scalar multiplications may be vulnerable against the side channel attacks. Elliptic curve scalar multiplications have been researched for a long time, but still new techniques are proposed.

In this talk, we will present various techniques on elliptic curve scalar multiplications, and investigate how we combine these different techniques to realize an efficient elliptic curve scalar multiplication.

(4)Speaker: Prof. Chen-Mou Cheng (Osaka univ.)

Title: On the use of Frobenius map to accelerate polynomial multiplication with Cantor FFT

Abstract: The discrete Fourier transform evaluates a polynomial on roots of unity in a field, possibly of nonzero characteristic. As it turns convolution into pointwise multiplication, one important application of the discrete Fourier transform is thus to multiply polynomials, especially with coefficients in a finite field Fq. When q is small, say 2, we need to go to an appropriate extension field F to find enough roots of unity to work with. In this case, we typically use the Kronecker segmentation technique to encode the multiplicand polynomials in F[t]. In 2017, van der Hoeven and Larrieu showed how to avoid the factor-of-two overhead of Kronecker segmentation by embedding, rather than encoding, the multiplicand polynomials into F[t]. Specifically, they restrict the evaluation to a cross section of the set of roots of unity and then use the Frobenius map to recover the results outside of it. In this talk, I will show that this idea beautifully generalizes to a class of "additive" Fourier transform first developed by Cantor and subsequently optimized by Gao-Mateer for an important special case. I will characterize in detail the interaction between Cantor FFT and the Frobenius map, as well as explicitly construct a cross section, as suggested by van der Hoeven and Larrieu.

(5)Speaker: Prof. Kiyofumi Tanaka (JAIST)

Title: Characteristics of Hardware Accelerators for Elliptic Curves Cryptography

Abstract: Elliptic Curve Cryptography (ECC) is a predominant cryptographic system for key agreement and digital signatures. It provides security level comparable to RSA, even with smaller keys and with significantly less complex operations. However, it still involves complex modular arithmetic, which is a major burden for not-powerful/resource-limited processing devices/microcontrollers such as smart cards. To alleviate the overhead of processing, several cryptographic hardware accelerators for ECC have been proposed. Many of them are implemented on reconfigurable devices, FPGA. In this talk, I show the characteristics of them and possibility of further acceleration by investigating inherent parallelism in the algorithm.

8. Attendance List

Taiwan

Prof. Chien-Lung Hsu (CGU)
Prof. Kuo-Yu Tsai (Chinese Culture University)
Guan-Lin Cheng (CGU)
Le Tuan Vinh (CGU)
Mei-Chen Hsieh (CGU)
Tzu-Wei Lin (CGU)
Wei-Xin Chen (CGU)

Japan

Prof. Atsuko Miyaji (Osaka univ./JAIST)
Prof. Chen-Mou Cheng (Osaka univ.)
Prof. Kiyofumi Tanaka (JAIST)
Prof. Shinya Okumura (Osaka univ.)
Katsunari Shishido (Osaka univ.)
Kenta Kodera (Osaka univ.)
Hideaki Miyaji (Osaka univ.)
Motoi Hayashi (Osaka univ.)
Tomoya Nishiguchi (Osaka univ.)
Yuki Sugitani (Osaka univ.)
Yusuke Matsuoka (Osaka univ.)