Korea Institute of Information Security & Cryptology

ICISC 2019

Call for Participants

The 22nd Annual International Conference on Information Security and Cryptology

December 4(Wed)~6(Fri), 2019, Seoul, Korea

http://www.icisc.org

KOREANA Hotel, Seoul, Korea (http://www.koreanahotel.com)

TOPICS of INTEREST INCLUDE, but are not limited to

-Access Control & Audit
-Authentication and Authorization
-Biometrics
-Block and Stream Ciphers
-Cloud Computing Security
-Copyright Protection
-Cryptanalysis
-Cryptographic Protocol
-Digital Forensics
-Digital Signature
-Distributed Systems Security
-Efficient Implementation
-Electronic Commerce
-Hash Function
-Homomorphic Encryption
-Identity Management
-ID-based Cryptography
-Information Hiding
-Intrusion Detection and Prevention
-Key Management
-Mobile Security
-Privacy Enhancement
-Public Key Cryptography
-Secure Multiparty Computation
-Side Channel Attacks and Countermeasures
-Social Network Security
-Software Security
-Smart Device Security

Improtant Dates

Conference Date : December 4(Wed) ~ 6(Fri), 2019
Submission Deadline : September 16(Mon), 2019 (UCT 22:00)
Notification Due : October 28(Mon), 2019
Proceedings version deadline : November 7 (Thu), 2019
Early Registration : ~~Before Nov.25, 2019~~ **Before Nov.27, 2019**

Committee

General Chair

Hyun Sook Cho (National Security Research Institute, Korea)
Kyung-Hyune Rhee (Pukyoung National University, Korea)

Organizing Chair

Changhoon Lee (Seoul National University of Science and Technology, Korea)

Program Chair

Jae Hong Seo (Hanyang University, Korea)

Programs

ICISC 2019 Program

Wednesday, (2019-12-04)	
8:30 – 9:20	**Registration**
9:20 – 9:30	**Opening Remarks**
9:30 – 10:45	**Session 1: Block Ciphers and Authenticated Encryption** (Session Chair: TBA) A Revised Version of Block Cipher CHAM Dongyoung Roh, Bonwook Koo, Younghoon Jung, Il Woong Jeong, Dong-Geon Lee, Daesung Kwon, and Woo-Hwan Kim (The Affiliated Institute of ETRI) Systematic Construction of Nonlinear Product Attacks on Block Ciphers Nicolas T. Courtois (University College London), Matteo Abbondati (Independent Maths teacher based in London), Hamy Ratoanina (University College London), and Marek Grajek (Independent cryptography and crypto history expert) Authenticated Encryption Based on Lesamnta-LW Hashing Mode Shoichi Hirose (University of Fukui),Hidenori Kuwakado (Kansai University), and Hirotaka Yoshida (National Institute of Advanced Industrial Science and Technology)
10:45 – 11:15	**Coffee Break**
11:15 – 12:15	**Invited Talk 1** (Session Chair: TBA) Practical Applications of Homomorphic Encrypton Miran Kim (University of Texas)
12:15 – 14:00	**Lunch**
14:00 – 15:15	**Session 2: Block Ciphers Implementation** (Session Chair: TBA) All the HIGHT You Need on Cortex-M4 Hwajeong Seo (Hansung University) and Zhe Liu (Nanjing University of Aeronautics and Astronautics) Fast AES implementation using ARMv8 ASIMD without Cryptography Extension Hayato Fujii (University of Campinas), Felix Carvalho, Rodrigues (University of Campinas), and Julio Lopez (University of Campinas) FACE-LIGHT: Fast AES-CTR Mode Encryption for Low-end Microcontrollers Kyungho Kim (Hansung University), Seung Ju Choi (Hansung University), Hyeokdong Kwon (Hansung University), Zhe Liu (Nanjing University of Aeronautics and Astronautics), and Hwajeong Seo (Hansung University)
15:15 – 15:45	**Coffee Break**
15:45 – 17:00	**Session 3: Secure Outsourcing and Cloud Security** (Session Chair: TBA) Sum it Up: Verifiable Additive Homomorphic Secret Sharing Georgia Tsaloli and Aikaterini Mitrokotsa (Chalmers University of Technology) There Is Always an Exception: Controlling Partial Information Leakage in Secure Computation

	Máté Horváth, Levente Buttyán, Gábor Székely and Dóra Neubrandt (CrySyS Lab, BME) An Automated Security Analysis Framework and Implementation for MTD techniques on Cloud Hooman Alavizadeh (Massey University), Hootan Alavizadeh (Imam Reza International University), Dong Seong Kim (The University of Queensland), Julian Jang-Jaccard (Massey University), and Masood Niazi Torshiz (Islamic Azad University)

Thursday, (2019-12-05)	
9:30 – 10:45	**Session 4: Post-Quantum Cryptography 1** (Session Chair: TBA) Security Analysis of Group Action Inverse Problem with Auxiliary Inputs with Application to CSIDH Parameters Taechan Kim (NTT) Secure Key Encapsulation Mechanism with Compact Ciphertext and Public Key from Generalized Srivastava Code Jayashree Dey and Ratna Dutta (Indian Institute of Technology Kharagpur) Improvement of binary and non binary Statistical Decoding Algorithm Pierre-Louis Cayrel (Laboratoire Hubert Curien), Cheikh Thiécoumba Gueye (Université Cheikh Anta Diop), Junaid Ahmad Khan (Dongguk University), Jean Belo Klamti (Université Cheikh Anta Diop), and Edoardo Persichetti (Dakota State University)
10:45 – 11:15	**Coffee Break**
11:15 – 12:15	**Invited Talk 2** (Session Chair: TBA) Information Security in Quantum Time Lily Chen (NIST)
12:15 – 14:00	**Lunch**
14:00 – 15:00	**Invited Talk 3** (Session Chair: TBA) Secure and Verifiable Computation Huaxiong Wang (Nanyang Technological University)
15:00 – 15:20	**Coffee Break**
15:20 – 16:20	**Invited Talk 4** (Session Chair: TBA) Lattice-Based Zero-Knowledge Proofs: Shorter and Faster Constructions and Applications Ron Steinfeld (Monash University)
16:20 – 16:40	**Coffee Break**
16:40 – 17:30	**Session 5: Post-Quantum Cryptography 2** (Session Chair: TBA) LizarMong: Excellent Key Encapsulation Mechanism based on RLWE and RLWR Chi-Gon Jung (Seoul National University), JongHyeok Lee (Kookmin University), Youngjin Ju (Hanyang University), Yong-Been Kwon (Hansung University), Seong-Woo Kim (Seoul National University), and Yunheung Paek (Seoul National University) Efficient Identity-Based Encryption from LWR Jung Hee Cheon (Seoul National University, Republic of Korea), Haejin Cho (LG Electronics, Republic of Korea), Jaewook Jung (LG

	Electronics, Republic of Korea), Joohee Lee (Seoul National University, Republic of Korea), and Keewoo Lee (Seoul National University, Republic of Korea)
18:30 – 20:30	**Banquet**

Friday, (2019-12-06)	
9:30– 10:30	**Session 6: Speeding Up Public Key Cryptography** (Session Chair: TBA) Faster Bootstrapping of FHE over the Integers Jung Hee Cheon (Seoul National University), Kyoohyung Han (Coinplug Inc.), and Duhyeong Kim (Seoul National University) Complete Addition Law for Montgomery Curves Jaeheon Kim (The Affiliated Institute of ETRI), Je Hong Park (The Affiliated Institute of ETRI), Dong-Chan Kim (Kookmin University), and Woo-Hwan Kim (The Affiliated Institute of ETRI)
10:30 – 11:00	**Coffee Break**
11:00 – 11:50	**Session 7: Side-Channel Attack** (Session Chair: TBA) Improved CRT-RSA Secret Key Recovery Method from Sliding Window Leakage Kento Oonishi (The University of Tokyo), Xiaoxuan Huang (The University of Tokyo), and Noboru Kunihiro (University of Tsukuba) Differential random fault attacks on certain CAESAR stream ciphers Kenneth Koon-Ho Wong, Harry Bartlett, Leonie Simpson and Ed Dawson (Queensland University of Technology)
	Farewell

Registration

Conference Registration Fee

	Early Registration (On/Before Nov.25, 2019)	Late Registration (After Nov.25, 2019)
General Participant	$500 (600,000 won)	$600 (700,000 won)
Full-time Student	$300 (350,000 won)	$400 (500,000 won)

한국인등록자 사전등록 방법 (※ 국내 거주 외국인 포함)

- 학회 홈페이지(www.kiisc.or.kr) -> 학술행사 -> 학회행사 -> **사전등록시 성명/소속 영문으로 기재**
- **사전등록 송금처**

- 예금주: 한국정보보호학회
- 계좌번호: (국민은행) 754-01-0008-146

- 사전등록시 등록비는 위의 구좌로 송금하시고 입금자가 대리일 경우 통보바랍니다.
  학생의 경우kiisc@kiisc.or.kr로 학생증 사본 송부바랍니다.

*** 반드시 영문 성함 / 소속으로 등록 바랍니다.**

- 신용카드 결제 시 세금계산서 발급이 불가합니다.(부가가치세법 시행령 제57조)
- **사전등록 마감일: 2019년 11월 27일(수)**
- 계산서 신청 시, 익일 안으로 등록하신 이메일로 청구용계산서가 발행됩니다. 영수용계산서가 필요하신 경우 사전에 학회로 연락바랍니다.

International Participants Registration instruction and Registration Payment Method

▸ Offline registration : Please fill out the REGISTRATION form below and send it to us via fax +82-2-564-9226. Payment can be made with credit cards (Visa or Master Card only) or wire transfer payable in US dollars ($) to ICISC 2019 (Koreans can pay in Korean currency (W))

▸ Online (E-mail) registration : Please fill out the REGISTRATION form below and send it to kiisc@kiisc.or.kr. Payment can be made with credit cards (Visa or Master Card only) or wire transfer payable in US dollars ($) to ICISC 2019 (Koreans can pay in Korean currency (W)).

▸ Early Registration Due : 2019/11/25 (Mon.)
▸ Credit card : Please fill out the Registration form
▸ Wire Transfer

beneficiary' name : KIISC
beneficiary's account number : 754-01-0008-146
beneficiary's bank : Kookmin Bank
the branch name : Yeoksamyeok Branch
SWIFT code : CZNBKRSE
beneficiary' address : Seongji Heights 3-Cha Bldg., Room 909
507, Nonhyeon-ro, Gangnam-gu, Seoul 06132, Korea

Contact

Korea Institute of Information Security &Cryptology (KIISC)
Tel: +82-2-564-9333-4 (ext. 2)
Fax: +82-2-564-9226
Homepage: **http://www.kiisc.or.kr/**
E-mail: **kiisc@kiisc.or.kr**

Hosted by

Korea Institute of Information Security &Cryptology (KIISC), Korea