



ICISC 2025

Call for Participants



The 28th Annual International Conference on Information Security and Cryptology

November 19 ~ November 21, 2025

SKY31 CONVENTION, 31F LOTTE WORLD TOWER, Seoul, Korea

<http://www.icisc.org/>

General Chairs: Young-Ho Park (Sejong Cyber University, Korea), Soo Hoon Hwang (NSR, Korea)

Organizing Committee Chairs:

Jongsung Kim (Kookmin University, Korea), Myungseo Park (Hansung University, Korea), Woo-Hwan Kim (NSR, Korea)

Programming Committee Chairs:

HwaJeong Seo (Hansung University, Korea), Dongjae Lee (Kangwon National University, Korea)

IMPORTANT DATES

Submission deadline	September 19 , September 24, 2025 18:00 KST (GMT + 9 hr)
Acceptance notification	October 29, 2025
Camera-ready submission	November 7, 2025
Author registration deadline	November 7, 2025
Participant registration deadline	November 10, 2025 November 17, 2025
ICISC 2025 Conference	November 19 ~ November 21, 2025

OVERVIEW

Original research papers on all aspects of theory and applications of information security and cryptology are solicited for submission to ICISC 2025, the 28th Annual International Conference on Information Security and Cryptology which is sponsored by NSR(National Security Research Institute) and KIISC (Korean Institute of Information Security and Cryptology), Korea.

TOPICS of INTEREST INCLUDE, but are not limited to:

Cryptography Track

- Authentication and Authorization
- Blockchain Security
- Block and Stream Ciphers
- Copyright Protection
- Cryptographic Protocols
- Cryptanalysis
- Digital Forensics
- Digital Signature
- Distributed Systems Security
- Efficient Cryptography Implementation
- Functional encryption
- Hash Function
- Homomorphic Encryption
- ID-based Cryptography
- Intrusion Detection and Prevention
- Information Hiding
- Key Management
- Post-quantum cryptography
- Privacy Enhancement
- Public Key Cryptography
- Side Channel Attacks and Countermeasures
- Secure Multiparty Computation
- Software Security
- Smart Device Security
- Zero-knowledge proofs

Security Track

- Analysis of network and security protocols
- Anonymity and censorship-resistant technologies
- Applications of cryptographic techniques
- Authentication and authorization
- Automated tools for source code/binary analysis
- Automobile security
- Critical infrastructure security
- Denial-of-service attacks and countermeasures
- Embedded systems security
- Exploit techniques and automation
- Hardware and physical security
- HCI security and privacy
- Malware analysis
- Mobile/wireless/cellular system security
- Network-based attacks
- Network infrastructure security
- Operating system security
- Practical cryptanalysis (hardware, DRM, etc.)
- Security policy
- Techniques for developing secure systems
- Trustworthy computing
- Trusted execution environments
- Unmanned System Security
- Vulnerability research
- Web Security

INSTRUCTIONS for AUTHORS

Submissions must not substantially duplicate work that any of the authors have published elsewhere or submitted in parallel to any other conference or workshop that has proceedings. The paper should start with a title, an abstract and keywords, but must be anonymous. The length of the submission should not exceed 20 pages in Springer's LNCS format, excluding the bibliography and clearly marked appendices. Since committee members are not required to read the appendices, the paper should be intelligible without them. All papers must be in PDF format. It is strongly recommended that submissions be processed using LaTeX2e according to the instruction at <https://www.springer.com/gp/computer-science/lncs/conference-proceedings-guidelines>. Authors of accepted papers must guarantee that their paper will be presented at the conference.

CONFERENCE PROCEEDINGS



The proceedings will be published by Springer-Verlag in the Lecture Notes in Computer Science.

PROGRAMS

Wednesday (2025-11-19)

KST 13:30 – 14:45 UTC 04:30 – 05:45 (Hall: Auditorium)	Session 1: AI-Driven Threat Detection & Federated Learning (Session Chair : <i>Universiti Tunku Abdul Rahman Prof. Wai Kong Lee</i>)
	Role-Aware Multi-modal Federated Learning System for Detecting Phishing Webpages <i>Bo Wang, Imran Khan, Martin White, and Natalia Beloff</i>
	Tabular or Image Input? Transformers for NIDS: A Comparative Study <i>Loreen Mahmoud, Aafia Hussain, and Sugata Gangopadhyay</i>
	AdvCodeGen: Adversarial Code Generation via Large Language Models <i>Eun Jung, Jiacheng Li, Yonghwi Kwon, and Hyounghick Kim</i>
KST 14:45 – 15:00 UTC 05:45 – 06:00	Break Time
KST 15:00 – 15:50 UTC 06:00 – 06:50 (Hall: Auditorium)	[Invited Talk I] (Session Chair : <i>Kangwon National University, Prof. Dongjae Lee</i>) Lattice-based Proof Systems and Application to Homomorphic Encryptions <i>Yongsoo Song</i>
KST 15:50 – 16:05 UTC 06:50 – 07:05	Break Time
KST 16:05 – 17:20 UTC 07:05 – 08:20 (Hall: Auditorium)	Session 2: Generative & Steganographic Security Applications (Session Chair : <i>Korea Institute of Science and Technology Information, Dr. Woojin Seok</i>)
	Generative AI-based Steganographic Techniques for Tactical Communication Message Concealment and Modification <i>So-Yeon Yoon and Hyun Kwon</i>
	Code Region Extraction Improves Scalable IoT Malware Clustering with Respect to Functional Labels <i>Kosuke Nikawa, Chansu Han, Akira Tanaka, Kazuki Iwamoto, Takeshi Takahashi, and</i>

	<i>Jun 'ichi Takeuchi</i>
	PathFault: Automated Exploit Generator for Web Services via HTTP Message Parser Discrepancies <i>Juryeok Kim and Youngjoo Shin</i>

Thursday (2025-11-20)

KST 09:35 – 10:50 UTC 00:00 – 01:50 (Hall: Auditorium)	Session 3 : Post-Quantum Cryptography & Migration (Session Chair : <i>Hanyang University, Prof. Seunghyun Seo</i>)
	Zero-Downtime Post-Quantum TLS 1.3 Migration: A Bridge-Server-Based Approach <i>Minjoo Sim, Subin Jo, Hyuntae Song, Eunseong Kim, and Hwajeong Seo</i>
	On the Feasibility of Deploying Lattice-Based PQC in Arm TrustZone TEEs: A Systematic Vulnerability Assessment <i>Hyunmin Kim</i>
	Post-Quantum Fujisaki-Okamoto Transformation for Anonymous Identity-Based Encryption <i>Yui Tsuchiya, Toi Tomita, and Junji Shikata</i>
KST 09:35 – 10:50 UTC 00:00 – 01:50 (Hall: Conference A)	Session 4 : Side-Channel & Fault Analysis in PQC (Session Chair : <i>Sungshin Women 's University, Prof. Yongha Son</i>)
	Breaking Masked Kyber: ResNet-Based Masked Kyber Share Recovery Method <i>Yaoling Ding, Haotong Xu, Chong Luo, Annyu Liu, Zheyu Zhang, Jing Yu, and An Wang</i>
	Side-Channel Leakage Assessment of SMAUG-T: Exploiting Hamming Weight Patterns in Polynomial-to-Message Conversion <i>Gwang-sik Kim and Young-sik Kim</i>
	Quantum Circuit Implementation and Resource Analysis of AIM2 <i>Gyeongju Song, Kyungbae Jang, Seyoung Yoon, Minwoo Lee, and Hwajeong Seo</i>
KST 10:50 – 11:10 UTC 01:50 – 02:10	Break Time
KST 11:10 – 12:00 UTC 02:10 – 03:00	[Invited Talk II] (Session Chair : <i>Hansung University, Prof. Hwajeong Seo</i>) Accelerating Post-quantum Cryptography and Functional Encryption with Massively Parallel Architecture <i>Wai Kong Lee</i>
KST 12:00 – 13:30 UTC 03:00 – 04:30	Break Time (Lunch Time in Korea)
KST 13:30 – 15:10	Session 5 : Network & Application Security (Session Chair : <i>Lund University, Dr. Anubhab Baksi</i>)

UTC 04:30 – 06:10 (Hall: Auditorium)	Comprehensive Security Analysis of End-to-End Encryption in LINE <i>Takehiro Matsumoto, Atsushi Tanaka, Kyosuke Yamashita, Ryoma Ito, and Takanori Isobe</i>
	Revealing the Chain with pytm-Seq: Approach for Multi-step Attack Detection <i>Geunwoo Baek, Jiwon Kwak, and Seungjoo Kim</i>
	Vector-Input Hashing Modes for Collision-Resistant Pseudorandom Function <i>Shoichi Hirose, Tetsu Iwata, and Hidenori Kuwakado</i>
KST 13:30 – 15:10 UTC 04:30 – 06:10 (Hall: Conference A)	Session 6 : Quantum Cryptanalysis & Theoretical Limits <i>(Session Chair : Electronics and Telecommunications Research Institute, Dr. Yousung Kang)</i>
	Can Quantum Break ZUC? Only with a Million Qubits and a Billion Years to Spare <i>Anik Basu Bhaumik, Suman Dutta, Siyi Wang, Anubhab Baksi, Kyungbae Jang, Amit Saha, Hwajeong Seo, and Anupam Chattopadhyay</i>
	(Best Paper) Homomorphic Transciphering for Secure Migration from LEA-128 to LEA-256 <i>Jaeyeon Lee, Seunghyun Cho, Saehoon Jung, Young-Sik Kim</i>
	Reconsidering Naito Feed-Forward-Free Double-Block-Length Hash Function <i>Zhuoxi Lin and Chun Guo</i>
	Impossibility Results of Card-Based Protocols via Mathematical Optimization <i>Shunnosuke Ikeda and Kazumasa Shinagawa</i>
KST 15:10 – 15:25 UTC 06:10 – 06:25	Break Time
KST 15:25 – 16:40 UTC 06:25 – 07:40 (Hall: Auditorium)	Session 7 : Implementation & Hardware Acceleration <i>(Session Chair : Electronics and Telecommunications Research Institute, Dr. Keonwoo Kim)</i>
	High-Speed 16-Radix Polynomial Multiplication on ARM Cortex-M4 with Recursive Karatsuba Layers <i>Minjoo Sim, Hyunjun Kim, Minwoo Lee, and Hwajeong Seo</i>
	Maximizing ARIA-CTR Performance through Kernel-Level Memory Optimization on the Apple M1 GPU <i>Siwoo Eum, Minho Song, Minjoo Sim, and Hwajeong Seo</i>
	Optimized Frobenius and Cyclotomic Cubing for Enhanced Pairing Computation <i>Leila Ben Abdelghani Bouraoui, Nadia El Mrabet, Loubna Ghammam, and Lina Mortajine</i>
KST 15:25 – 16:40 UTC 06:25 – 07:40 (Hall: Conference A)	Session 8 : Symmetric Cryptanalysis & New Constructions <i>(Session Chair : Chosun University, Prof. Hyunil Kim)</i>
	On the Resistance of Rijndael-256 against Related-Key Boomerang and Rectangle Attacks <i>Namil Kim, Wonwoo Song, Seungjun Baek, Yongjin Jeon, Jongsung Kim, and Ki Hyo Nam</i>

	<p>(Best Paper) On the Weak Differential Resistance of MGFN and the Exploration of Variants <i>Bingqing Li and Ling Sun</i></p>
	<p>New Derivation Rule for Linear Approximations and Its Application to ChaCha <i>Zhengting Li, Lin Ding, Xinhai Wang, Honglei Wang, and Jiang Wan</i></p>
<p>KST 16:40 – 16:55 UTC 07:40 – 07:55</p>	<p>Break Time</p>
<p>KST 16:55 – 17:45 UTC 07:55 – 08:45 (Hall: Auditorium)</p>	<p>[Invited Talk III] (Session Chair : <i>Hansung University, Prof. Hwajeong Seo</i>) Non-Malleable Encryption from QC-MDPC Codes <i>Anubhab Baksi</i></p>
<p>KST 17:45 – 18:00 UTC 08:45 – 09:00</p>	<p>Break Time</p>
<p>KST 18:00 – 20:30 UTC 09:00 – 11:30 (Hall: Conference A)</p>	<p>Banquet</p>

Friday (2025-11-21)	
<p>KST 10:00 – 10:50 UTC 01:00 – 01:50 (Hall: Auditorium)</p>	<p>[Invited Talk IV] (Session Chair : <i>Hansung University, Prof. Hwajeong Seo</i>) Relaxed Vector Commitment for Shorter Signatures <i>Seongkwang Kim</i></p>
<p>KST 10:50 – 11:05 UTC 01:50 – 02:05</p>	<p>Break Time</p>
<p>KST 11:05 – 12:20 UTC 02:05 – 03:20 (Hall: Auditorium)</p>	<p>Session 9 : Advanced Cryptographic Protocols & Signatures (Session Chair : <i>National Security Research Institute, Dr. Nari Lee</i>)</p>
	<p>Strong Designated Verifier Signatures with Non-delegatability from CSIDH <i>Hiroki Minamide, Keisuke Tanaka, and Masayuki Tezuka</i></p>
	<p>An Undeniable Signature Scheme Utilizing Module Lattices <i>Kunal Dey, Mansi Goyal, Aditi Kar Gangopadhyay, and Bhupendra Singh</i></p>
	<p>A Witness Encryption for Quadratic Arithmetic Programs <i>Tao-Hsiang Chang, Yu-Chen Wu, Zi-Yuan Liu, Jen Chieh Hsu, Raylin Tso, and Masahiro Mambo</i></p>
	<p>Farewell</p>

REGISTRATION

| International Participants Payment Method

Registration Deadline : November 10, 2025(UTC+09:00) Participants can registration for the conference until November 10, 2025(UTC+09:00)

Please read carefully the registration guidelines below.

Each paper must have at least one author registered with the payment received by the author registration deadline (Nov.7) to avoid being withdrawn from the conference.

Registration includes:(a) participation in the offline conference (b) access to the online proceedings (c) one copy of the LNCS proceedings (d) one lunch and one banquet (e) a souvenir.

General Participants	550 USD
Student	350 USD

▶ Registration Fees (International)

We use online registration to complete the registration for participants.

Click on the registration page link: <https://kiisc.or.kr/pre-registration>

[Credit card]

- Use a credit card payment system (EXIMBAY)

[Wire Transfer]

- beneficiary' name: KIISC

- beneficiary's account number: 754-01-0008-146

- beneficiary's bank: Kookmin Bank

- the branch name: Yeoksamyek Branch

- SWIFT code: CZNBKRSE

- beneficiary' address: Room 909, Seongji Heights 3-Cha Bldg., 507, Nonhyeon-ro, Gangnam-gu, Seoul, Korea 06132

* This payment method is provided by Eximbay and is billed as www.eximbay.com.

* Note: Please note that the billing descriptor will be listed as EXIMBAY.COM.

[한국인(국내거주인) 등록안내

■ **사전등록 기간 (연장): 2025년 11월 10일(월)까지-2025년 11월 17일(월)까지**

모든 논문은 ****11월 7일(저자 등록 마감일)****까지 최소 한 명 이상의 저자가 반드시 등록을 완료해야 합니다.

▶ Registration Fees (Domestic)

일반	750,000 원
학생(전일제)	450,000 원
군/공무원	450,000 원
시니어(63 세이상) 종신회원	무료

■참석자 제공

오프라인 학술대회 참가, 온라인 프로시딩, LNCS 프로시딩 1 권, 중식 1 회, 만찬 1 회, 기념품 제공

■ 등록방법

학회 홈페이지 접속 www.kiisc.or.kr → 상단 메뉴 「학회행사」 클릭→ 「사전등록 바로가기」 선택→ ICISC 2025 (Domestic) 클릭 후 신용카드 혹은 무통장 입금 선택하여 등록 진행

■ 무통장 입금 시 등록비 결제 안내

(1) 무통장입금 계좌 정보

- 은행명: 국민은행
- 계좌번호: 754-01-0008-146
- 예금주: 한국정보보호학회

(2) 입금 시 유의사항

사전등록 시 등록비는 위의 계좌로 송금하시고 입금자명이 대리인명이나 단체명으로 송금되는 경우, 등록자 본인 확인이 어려울 수 있습니다. 이 경우 등록 시 메모란에 입금자명과 신청자명을 기재하거나, 이메일 또는 전화로 별도로 알려주시기 바랍니다.

(3) (면세)계산서 발행 관련 안내

청구용 계산서는 등록 익일 내에 등록 시 기재하신 이메일로 발행됩니다. 영수용 계산서가 필요한 경우 사전에 학회로 연락 바랍니다.

(단, 신용카드 결제 시 계산서 발급 불가, 부가가치세법 시행령 제 57 조에 의거)

■ 증빙서류 제출 및 등록 자격 안내

(1) 학생 등록자의 경우 kiisc@kiisc.or.kr 로 학생증 사본 제출

학생은 다른 소속이 없는 전일제(학부생/대학원생) 에 한함

(2) 군·공무원 등록자

kiisc@kiisc.or.kr 로 공무원증 사본 제출

주무관청에 소속된 공무원증 소지자만 해당 (※ 국공립 교직원 제외)

(3) 시니어 무료등록

학회 중신회원 중 1963년 12월 31일 이전 출생자에 한함

■ 등록 및 참가확인서 발행 안내

(1) 등록확인서 발행

-발행 시점: 결제 완료 후 즉시 발행 가능

-발행 방법: 한국정보보호학회 홈페이지 상단의 「행사 등록 및 참가확인서 바로가기」클릭→ 등록 시 기재한 성함과 이메일입력→ 등록확인서 출력

-결제 방식별 발행 시점:

신용카드 결제:결제 후 바로 출력 가능

계좌이체: 이체 확인 후 출력 가능

(2) 참가확인서 발행

-발행 시점: 행사 **종료 다음날(익일)**부터 발행 가능 (※ 등록비 미입금 시 발행 불가)

-발행 방법: 한국정보보호학회 홈페이지 상단의 「행사 등록 및 참가확인서 바로가기」클릭→ 등록 시 기재한 성함과 이메일입력→참가확인서 출력

(3) 현장등록의 경우 kiisc@kiisc.or.kr 로 등록 및 참가확인서 발행 요청

|Registration Policy

At least one presenter per accepted paper must register for the conference.

We are unable to offer refunds, cancellations, or substitutions for any registrations for this event.

|Contact Information for Registration

Korea Institute of Information Security & Cryptology Room 909, Seongji Heights 3-Cha Bldg., Nonhyeon-ro 507, Gangnam-gu, Seoul, Korea 06132

Tel : +82-2-564-9333(ext.2) Fax : +82-2-564-9226 Email :kiisc@kiisc.or.kr Business Registration Number: 114-82-04432

행사 문의처: 한국정보보호학회 사무국 02-564-9333 (내선 2),kiisc@kiisc.or.kr

계산서 문의처: 한국정보보호학회 사무국 02-564-9333 (내선 5),kiisc@kiisc.or.kr