

Call for Participants

The 27th Annual International Conference on Information Security and Cryptology

November 20 ~ November 22, 2024, Seoul, Korea

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

General Chairs: Jaecheol Ha (Hoseo University, Korea), Soo Hoon Hwang (NSR, Korea)

Organizing Committee Chairs: Ki-Woong Park (Sejong University, Korea), Hwa-Jeong Seo (Hansung University, Korea), Woo-Hwan Kim (NSR, Korea)

Programming Committee Chairs: Jongsung Kim (Kookmin University, Korea), Jungsoo Park (Kangnam University, Korea), Lee Wai Kong (Universiti Tunku Abdul Rahman, Malaysia)

IMPORTANT DATES

Submission deadline	~~September 6, 2024 18:00 KST (GMT + 9 hr)~~ → September 22, 2024 18:00 KST (GMT + 9 hr)
Acceptance notification	October 30, 2024
Camera-ready submission	November 6, 2024
Author registration deadline	November 8, 2024
Participant registration deadline	November 12, 2024
ICISC 2024 Conference	November 20 ~ November 22, 2024

OVERVIEW

Original research papers on all aspects of theory and applications of information security and cryptology are solicited for submission to ICISC 2024, the 27th Annual International Conference on Information Security and Cryptology which is hosted 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
- Biometrics
- 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

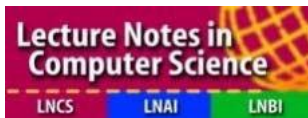
Security Track

- AI Security
- Analysis of Network and Security Protocols
- Anonymity and Censorship-resistant Technologies
- Applications of Cryptographic Techniques
- Automated tools for source code/binary analysis
- Automobile security
- Botnet defense
- 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 (2024-11-20)

KST 13:15 - 14:05 UTC 04:15 - 05:05 (Hall: Auditorium)	Session 1 : Cryptanalysis of Block Ciphers (Session Chair : Bonwook Koo, National Security Research Institute, Korea)
	Exploring the Optimal Differential Characteristics of SM4: Improving Automatic Search by Including Human Insights <i>Bingqing Li and Ling Sun</i>
	Investigation of the Optimal Linear Characteristics of BAKSHEESH <i>Yuxuan Peng, Jinpeng Liu and Ling Sun</i>
	Break Time
KST 14:25 - 15:25 UTC 05:25 - 06:25 (Hall: Auditorium)	[Invited Talk I] (Session Chair : Seunghyun Seo, Hanyang University, Korea) Accordion Mode Development, Donghoon Chang (NIST & Strativia, USA)
KST 15:45 - 17:00 UTC 06:45 - 08:00 (Hall: Auditorium)	Session 2 : Cyber Security I (Session Chair : Woojin Seok, Korea Institute of Science and Technology Information, Korea)
	Simultaneous Multiplication Protocol based on Packed Linear Secret Sharing and its Applications <i>Shohei Mita and Kazuki Yoneyama</i>
	Reinterpreting System Calls for Enhanced IoT Malware Analysis Using Function Call Graphs <i>Wei-Jen Liao, Tao Ban, Shin-Ming Cheng and Takeshi Takahashi</i>
	LUA-IoT: Let's Usably Authenticate the IoT <i>Markus Dahlmanns, Jan Pennekamp, Robin Decker and Klaus Wehrle</i>

Thursday (2024-11-21)

KST 10:00 - 10:50 UTC 01:00 - 01:50 (Hall: Auditorium)	Session 3 : Signature Schemes (Session Chair : Jonghwan Park, Sangmyung University, Korea)
	Designated-Verifier Ring Signatures: Strong Definitions, Generic Constructions and Efficient Instantiations <i>Jiaming Wen, Willy Susilo, Yanhua Zhang, Fuchun Guo and Huanguo Zhang</i>
	Tightly Secure Lattice-based Synchronized Aggregate Signature in Standard Model <i>Hiroaki Anada, Masayuki Fukumitsu and Shingo Hasegawa</i>
KST 10:50 - 11:10 UTC 01:50 - 02:10	Break Time
KST 11:10 - 12:00 UTC 02:10 - 03:00 (Hall: Auditorium)	Session 4 : AI Security (Session Chair : Taekyoung Kwon, Yonsei University, Korea)
	Pre-trained Language Models for Alert Aggregation: Limitations and Opportunities <i>Wenwu Xu, Pengyi Wu, Peng Wang, Guoqiao Zhou and Lidong Zhai</i>
	Does Ordinality in Encoding Matter for XAI? A Case Study on Explainable IDS <i>Harry Chandra Tanuwidjaja, Tao Ban, Takeshi Takahashi, Tsung-Nan Lin, Boyi Lee and Muhamad Erza Aminanto</i>
KST 12:00 - 13:30 UTC 03:00 - 04:30 (Hall: Conference A)	Break Time (Lunch Time in Korea)
KST 13:30 - 14:30 UTC 04:30 - 05:30 (Hall: Auditorium)	[Invited Talk II] (Session Chair : Jongsung Kim, Kookmin University, Korea) Committing Security of Authenticated Encryption, Yu Sasaki (NTT, Japan)
KST 14:30 - 14:50 UTC 05:30 - 05:50	Break Time

KST 14:50 – 16:05 UTC 05:50 – 07:05 (Hall: Auditorium)	Session 5 : Applied Cryptography I (Session Chair : Kwangsu Lee, Sejong University, Korea)
	FineDReaM : A Boolean Query Searchable KP-ABE-Based Fine-Grained Authorized Encrypted-Data Retrieval Mechanism <i>Suryakant Prasad and Y. Sreenivasa Rao</i>
	A Formal Treatment of Envelope Encryption <i>Shoichi Hirose and Kazuhiko Minematsu</i>
	Efficient Privacy-Preserving Counting Method with Homomorphic Encryption <i>Jae-yun Kim, Saerom Park, Jieun Yun and Jung Hee Cheon</i>
KST 14:50 – 16:05 UTC 05:50 – 07:05 (Hall: Conference A)	Session 6 : Applied Cryptography II (Session Chair : Yousung Kang, Electronics and Telecommunications Research Institute, Korea)
	Experimental Analysis of the Optimization-based Factorization Algorithm <i>Junpei Yamaguchi, Tetsuya Izu and Noboru Kunihiro.</i>
	Fast Private Set Intersection from Polynomial Multiplication Triples <i>Kai Chen, Yongqiang Li, Ya Han and Mingsheng Wang</i>
	Enhancing Differential Fuzzing of Cryptographic Libraries with Sustainable Hybrid Fuzzing and Crypto-Specific Mutation <i>Jeewoo Jung and Taekyoung Kwon</i>
KST 16:05 – 16:25 UTC 07:05 – 07:25	Break Time
KST 16:25 – 17:40 UTC 07:25 – 08:40 (Hall: Auditorium)	Session 7 : Quantum Cryptography & Deep Learning based Analysis (Session Chair : Kyung Chul Jeong, National Security Research Institute, Korea)
	RSA Quantum Cryptanalysis: A Thorough Exploration of n-Bit Attacks and Emerging Factoring Techniques <i>Rini Wisnu Wardhani, Dedy Septono Catur Putranto and Howon Kim</i>
	Quantum Circuit for Curve25519 with Fewer Qubits <i>Gyeongju Song and Hwajeong Seo</i>
	CS-Net: A Deep Learning-Based Analysis for the Cryptography and Steganography <i>Duk Young Kim, Kyoungbae Jang, Hyunji Kim, Yujin Oh, Seyoung Yoon and Hwajeong Seo</i>
KST 17:40 – 18:00 UTC 08:40 – 09:00	Break Time
KST 18:00 – 20:30 UTC 09:00 – 11:30 (Hall: Conference A)	Banquet

Friday (2024-11-22)

KST 10:00 – 10:50 UTC 01:00 – 01:50 (Hall: Auditorium)	Session 8 : Side-Channel & Automotive Attack (Session Chair : Myungseo Park, Hansung University, Korea)
	REAF: Replacing Exponential Activation Function to Prevent Side-Channel Analysis <i>Joonsup Kim, Dongjun Park, Gysang Kim, Sujin Park, Daehyeon Bae, Heeseok Kim and Seokhie Hong</i>
	Assessment of Automotive Attack Feasibility Methods in Comparison to Railway and Aviation Methods <i>Johannes von Richthofen, Christoph Krauß, Johann Altgenug, Dominik Spsychalski and Wolfgang Hommel</i>
KST 10:50 – 11:10 UTC 01:50 – 02:10	Break Time
KST 11:10 – 12:25 UTC 02:10 – 03:25 (Hall: Auditorium)	Session 9 : Cyber Security II (Session Chair : Dongjae Lee Kangwon National University, Korea)
	An Information-Sharing System that Guarantees the Authenticity and Privacy of Contributors <i>Mebae Ushida, Takeshi Miyamae, Takeru Fukuoka, Yoshiyuki Sakamaki, Yoshitomo Sakuma, Kota Miyake and Takuya Sakamoto</i>
	Malicious node identification based on behavioral statistical features and social relationships <i>Guangcan Cui, Li-Sheng Huang, Fengjun Zhang, Zuoyuan Niu, Kai Shi and Yunhai Lan</i>
	LiST+: An Improved Lightweight Sharable and Traceable Secure Mobile Health System <i>Suryakant Prasad and Y. Sreenivasa Rao</i>
	Farewell

REGISTRATION

| International Participants Payment Method

Registration Deadline : ~~November 12, 2024 (UTC+09:00)~~ **November 18, 2024 (UTC+09:00)**

Participants can registration for the conference until November 12, 2024 (UTC+09:00)

Please read carefully the registration guidelines below.

Each paper must have at least one author registered (general registration, not student registration), with the payment received by the author registration deadline (Nov. 8) to avoid being withdrawn from the conference. All registrations include one LNCS proceeding, online proceeding.

▶ Registration Fees (International)

General Participants (Authors)	550 USD
Student	350 USD

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: Yeoksamyeok Branch
- SWIFT code: CZNBNKRSE
- 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: 2024년 11월 12일(화) 11월 18일(월)까지 (등록기간 연장)
(논문 발표자는 2024년 11월 8일(금)까지 등록)

▶ Registration Fees (Domestic)

일반	650,000 원
학생(전일제)	400,000 원
군/공무원	400,000 원
시니어(63 세이상) 종신회원	무료

- * 학회 홈페이지(www.kiisc.or.kr)접속 -> 학회행사 -> 사전등록바로가기 -> ICISC 2024 (Domestic) 클릭
- * 무통장입금시 입금계좌 예금주 : 한국정보보호학회 (국민은행) 754-01-0008-146
입금명은 필히 [행사명 첫 글자+ 등록자 성함]으로 기재해 주시기 바랍니다. 예) ICISC 등록 홍길동 - “I 홍길동” 기재
- * 계산서 신청 시, 익일 안으로 등록하신 이메일로 청구용 계산서가 발행됩니다. 영수용 계산서가 필요하신 경우, 사전에 학회로 연락 바랍니다.
- * 신용카드 결제 시 계산서 발급이 불가 합니다. (부가가치세법 시행령 제 57 조)
- * 학생의 경우 kiisc@kiisc.or.kr 로 학생증 사본을 송부 바랍니다. 학생은 다른 소속이 없는 전일제(학부생/대학원생)에 해당합니다.
- * 군·공무원 등록은 주무관청에 소속 중인 공무원증 소지자에 한합니다.(국공립 교직원 제외)
- kiisc@kiisc.or.kr 로 공무원증 사본을 송부해 주시기 바랍니다.

- * 시니어 무료등록은 학회 종신회원으로 1962년 12월 31일 이전 출생자에 한합니다.
- * 등록확인서 및 참가확인서는 한국정보보호학회 홈페이지 상단 "행사등록 및 참가확인서" 바로 가기를 클릭하신 후 등록 시 기재하시 성함과 이메일을 기재하시면 출력 가능합니다.
(단, 참가확인서는 행사종료 후 다음날부터 발급 가능하며 등록비 납부완료자에 한합니다.)

| 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

Korea Institute of Information Security & Cryptology (KIISC)

Tel: +82-2-564-9333-4 (ext. 3) Fax: +82-2-564-9226

Homepage: <http://www.kiisc.or.kr/> E-mail: kiisc@kiisc.or.kr