ICISC 2023

Call for Participants

The 26th Annual International Conference on Information Security and Cryptology

November 29 ~ December 1, 2023, Seoul, Korea

http://www.icisc.org/

General Chair: Yoojae Won (Chungnam National University, Korea)

Organizing Committee Chairs:
Young-Ho Park (Sejong Cyber University, Korea), Junbeom Hur (Korea University, Korea)

Programming Committee Chairs:
HwaJeong Seo (Hansung University, Korea), Suhri Kim (Sungshin Women's University, Korea)

IMPORTANT DATES

Submission deadline	**~~September 15, 2023 18:00 KST (GMT + 9 hr)~~** **→ October 6, 2023 18:00 KST (GMT + 9 hr)**
Acceptance notification	**November 10, 2023**
Camera-ready submission	**November 15, 2023**
Author registration deadline	**November 17, 2023**
Participant registration deadline	**November 21, 2023**
ICISC 2023 Conference	**November 29 ~ December 1, 2023**

OVERVIEW

Original research papers on all aspects of theory and applications of information security and cryptology are solicited for submission to ICISC 2023, the 26th Annual International Conference on Information Security and Cryptology which is sponsored by 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

- 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
- 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 http://www.springer.de/comp/lncs/authors.html. 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 (2023-11-29)	
KST 09:30 - 09:40 UTC 12:30 - 12:40	Opening Remarks
KST 09:40 - 11:00 UTC 12:40 - 02:00	Session 1 : Cryptanalysis & Quantum Cryptanalysis I (Session Chair : Prof. Suhri Kim (Sungshin Women's University))
	Enhancing the Related-Key Security of PIPO through New Key Schedules *Seungjun Baek, Giyoon Kim, Yongjin Jeon and Jongsung Kim*
	Optimized Quantum Implementation of SEED *Yujin Oh, Kyoungbae Jang, Yu-Jin Yang and Hwajeong Seo*
	Depth-Optimized Quantum Implementation of ARIA *Yu-Jin Yang, Kyung-bae Jang, Yu-jin Oh and Hwa-Jeong Seo*
	Finding Shortest Vector using Quantum NV Sieve on Grover *Hyunji Kim, Kyoungbae Jang, Yujin Oh, Woojin Seok, Wonhuck Lee, Kwangil Bae, Ilkwon Sohn and Hwajeong Seo*
KST 11:00 - 11:10 UTC 02:00 - 02:10	Break Time
KST 11:10 - 12:10 UTC 02:10 - 03:10	Session 2 : Side Channel Attack I (Session Chair : Dr. Byoungjin Seok (Seoul National University of Science and Technology))
	Extended Attacks on ECDSA with Noisy Multiple Bit Nonce Leakages *Shunsuke Osaki and Noboru Kunihiro*
	Single Trace Analysis of Comparison Operation based Constant-Time CDT Sampling and Its Countermeasure *Keonhee Choi, Ju-Hwan Kim, Jaeseung Han, Jae-Won Huh and Dong-Guk Han*
	A Lattice Attack on CRYSTALS-Kyber with Correlation Power Analysis *Yen-Ting Kuo and Atsushi Takayasu*
KST 12:10 - 13:30 UTC 03:10 - 04:30	Break Time (Lunch Time in Korea)
KST 13:30 - 14:30 UTC 04:30 - 05:30	Session 3 : Cyber Security I (Session Chair : Prof. Seung-Hyun Seo (Hanyang University))

	A Comparative Analysis of Rust-Based SGX Frameworks: Implications for building SGX applications *Heekyung Shin, Jiwon Ock, Hyeon No and Seongmin Kim*
	BTFuzzer: a profile-based fuzzing framework for Bluetooth protocols *Min Jang, Yuna Hwang, Yonghwi Kwon and Hyoungshick Kim*
	mdTLS: How to make middlebox-aware TLS more efficient? *Taehyun Ahn, Jiwon Kwak and Seungjoo Kim*
KST 14:30 - 14:40 UTC 05:30 - 05:40	Break Time
KST 14:40 - 15:40 UTC 05:40 - 06:40	Session 4 : Cyber Security II & Side Channel Attack II (Session Chair : Prof. Kwangsu Lee (Sejong University))
	PHI: Pseudo-HAL Identification for Scalable Firmware Fuzzing *Seyeon Jeong, Eunbi Hwang, Yeongpil Cho and Taekyoung Kwon*
	Lightweight Anomaly Detection Mechanism based on Machine Learning Using Low-Cost Surveillance Cameras *Yeon-Ji Lee, Na-Eun Park and Il-Gu Lee*
	Side-Channel Analysis on Lattice-Based KEM using Multi-feature Recognition - The Case Study of Kyber *Yuan Ma, Xinyue Yang, An Wang, Congming Wei, Tianyu Chen and Haotong Xu*
KST 15:40 - 15:50 UTC 06:40 - 06:50	Break Time
KST 15:50 - 17:10 UTC 06:50 - 08:10	Session 5 : Applied Cryptography I (Session Chair : Dr. Dongyoung Roh (National Security Research Institute))
	Enhancing Prediction Entropy Estimation of RNG for On-the-Fly Test *Yuan Ma, Weisong Gu, Tianyu Chen, Na Lv, Dongchi Han and Shijie Jia*
	Leakage-Resilient Attribute-based Encryption with Attribute-hiding *Yijian Zhang, Yunhao Ling, Jie Chen and Luping Wang*
	Constant-Deposit Multiparty Lotteries on Bitcoin for Arbitrary Number of Players and Winners *Shun Uchizono, Takeshi Nakai, Yohei Watanabe and Mitsugu Iwamoto*
	Single-Shuffle Card-Based Protocols with Six Cards per Gate *Tomoki Ono, Kazumasa Shinagawa, Takeshi Nakai, Yohei Watanabe and Mitsugu Iwamoto*

Thursday (2023-11-30)	
KST 10:00 - 11:00 UTC 01:00 - 02:00	[Invited Talk I] (Session Chair : Prof. Hwajeong Seo (Hansung University)) Title: Secure Implementation of Post-Quantum Cryptography: Challenges and Opportunities *Prof. Rei Ueno (Tohoku University)*
KST 11:00 - 11:10 UTC 02:00 - 02:10	Break Time
KST 11:10 - 12:10 UTC 02:10 - 03:10	Session 6 : Signature Schemes (Session Chair : Prof. Mun-Kyu Lee (Inha University))

	1-out-of-n Oblivious Signatures: Security Revisited and a Generic Construction with an Efficient Communication Cost *Masayuki Tezuka and Keisuke Tanaka*
	Compact Identity-based Signature and Puncturable Signature from SQISign *Surbhi Shaw and Ratna Dutta*
	High Weight Code-based Signature Scheme from QC-LDPC Codes *Chik How Tan and Theo Fanuela Prabowo*
KST 12:10 - 13:30 UTC 03:10 - 04:30	Break Time (Lunch Time in Korea)
KST 13:30 - 14:30 UTC 04:30 - 05:30	[Invited Talk II] (Session Chair : Prof. Joonwoo Lee (Chungang University, Korea)) Title: CryptAttackTester: Formalizing Attack Analyses *Dr. Tung Chou (Academia Sinica)*
KST 14:30 - 14:40 UTC 05:30 - 05:40	Break Time
KST 14:40 - 16:00 UTC 05:40 - 07:00	Session 7 : Applied Cryptography II & Quantum Cryptanalysis II (Session Chair : Prof. Yongwoo Lee (Inha University, Korea))
	Efficient Result-Hiding Searchable Encryption with Forward and Backward Privacy *Takumi Amada, Mitsugu Iwamoto and Yohei Watanabe*
	Finsler Encryption *Tetsuya Nagano and Hiroaki Anada*
	Experiments and Resource Analysis of Shor's Factorization Using a Quantum Simulator *Junpei Yamaguchi, Masafumi Yamazaki, Akihiro Tabuchi, Takumi Honda, Noboru Kunihiro and Tetsuya Izu*
	Quantum Circuits for High-Degree and Half Multiplication For Post-Quantum Analysis *Rini Wisnu Wardhani, Dedy Septono Catur Putranto and Howon Kim*
KST 16:00 - 16:10 UTC 07:00 - 07:10	Break Time
KST 16:10 - 17:10 UTC 07:10 - 08:10	Session 8 : Korean Post Quantum Cryptography (Session Chair : Prof. Seongmin Kim (Sungshin Women's University))
	Theoretical and Empirical Analysis of FALCON and SOLMAE using their Python Implementation *Kwangjo Kim*
	Security Evaluation on KpqC Round 1 Lattice-based Algorithms Using Lattice Estimator *Suhri Kim, Eunmin Lee, Joohee Lee, Minju Lee and Hyun A Noh*
	On the security of REDOG *Tanja Lange, Alex Pellegrini and Alberto Ravagnani*
KST 17:10 - 18:00 UTC 08:10 - 09:00	Break Time
KST 18:00 - 20:30 UTC 09:00 - 11:30	Banquet (Hotel Koreana Diamond Hall 2F)

Friday (2023-12-01)	
KST 10:00 - 11:00 UTC 01:00 - 02:00	[Invited Talk Ⅲ] (Session Chair : Prof. Hwajeong Seo (Hansung University)) Title: Hash Based Signatures and Ascon-Sign *Dr. Anubhab Baksi (Nanyang Technological University)*
KST 11:00 - 11:10 UTC 02:00 - 02:10	Break Time
KST 11:10 - 12:30 UTC 02:10 - 03:30	Session 9 : Cryptanalysis & Applied Cryptography III (Session Chair : Dr. Taehwan Park (National Security Research Institute))
	Distinguisher and Related-Key Attack on HALFLOOP-96 *Jinpeng Liu and Ling Sun*
	Not optimal but efficient: a distinguisher based on the Kruskal-Wallis test *Yan Yan, Elisabeth Oswald and Arnab Roy*
	Feasibility Analysis and Performance Optimization of the Conflict Test Algorithms for Searching Eviction Sets *Zhenzhen Li, Xue Zihan and Wei Song*
	Revisiting Key Switching Techniques with Applications to Light-Key FHE *Ruida Wang, Zhihao Li, Benqiang Wei, Chunling Chen, Xianhui Lu and Kunpeng Wang*
	Farewell

REGISTRATION

| International Participants Payment Method

Registration Deadline : November 21, 2023 (UTC+09:00)

Participants can registration for the conference until November 21, 2023 (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. 17) to avoid being withdrawn from the conference. All registrations include one LNCS proceeding, online proceeding.

▶ Registration Fees (International)

Offline Attendance	General Participants (Authors)	500 USD
	Student	300 USD
Online Attendance	General Participants	200 USD
	Student	

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 : 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 : 2023 년 11 월 21 일(화)까지
(논문 발표자는 2023 년 11 월 17 일(금)까지 등록)

▶ Registration Fees (Domestic)

Offline Attendance	일반	600,000 원
	학생(전일제)	350,000 원
	군/공무원	350,000 원
Online Attendance	일반 / 학생(전일제) / 군.공무원	200,000 원
시니어(63 세이상) 종신회원	무료	

* 학회 홈페이지(www.kiisc.or.kr)접속 -> 학회행사 -> 사전등록바로가기 -> ICISC 2023 (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)
*** Paper 논문발표자(저자 중 최소 1 인)는 오프라인 참석비용으로 등록해주시기 바랍니다.**
* 학생의 경우 kiisc@kiisc.or.kr 로 학생증 사본 송부 바랍니다. 학생은 다른 소속이 없는 전일제(학부생/대학원생)에 한합니다.
* 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 1961 년 12 월 31 일 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