www.wisa.or.kr

The 24th World Conference on Information Security Applications

WISA 2023

August 23-25, 2023

MAISON GLAD, Jeju Island, Korea, Hybrid (on-off mix) conference

Hosted by Korea Institute of Information Security & Cryptology

Sponsored by Ministry of Science and ICT   국가정보원 NATIONAL INTELLIGENCE SERVICE

Co-Sponsored by KISA 한국인터넷진흥원   ETRI Electronics and Telecommunications Research Institute   NSR National Security Research Institute   ICTK   CM culture makers

HUAWEI   ICTK   네이버시스템   SPACE&BEAN   SSNC 에스에스앤씨

KEY CONTACTS

General Information

Kiwook Sohn
Seoul National University of Science and Technology, Republic of Korea
kiwook@seoultech.ac.kr
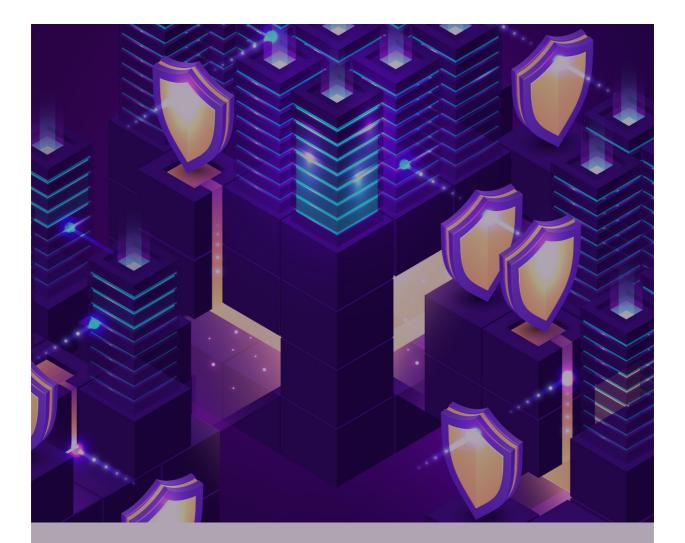
Jong-Hyouk Lee
Sejong University, Republic of Korea
jonghyouk@sejong.ac.kr

Technical Program

Howon Kim
Pusan National University, Republic of Korea
howonkim@pusan.ac.kr

Jonghee Youn
Yeungnam University, Republic of Korea
youn@yu.ac.kr

Registration: KIISC (Korea Institute of Information Security and Cryptology)
Korea Institute of Information Security and Cryptology Seongji Heights 3-Cha Bldg.,
Room 909 507 Nonhyeon-ro(Yeoksam-dong), Gangnam gu, Seoul 06132, Korea
Tel: +82-2-564-9333~4
Fax: +82-2-564-9226
E-mail: kiisc@kiisc.or.kr

The 24th World Conference on Information Security Applications

WISA 2023
CONTENTS

▶ Committee

▶ General Chair
Yoojae Won   Chungnam National University, Republic of Korea

▶ Program Committee Chairs
Howon Kim   Pusan National University, Republic of Korea
Jonghee Youn   Yeungnam University, Republic of Korea

▶ Organizing Committee Chairs
Kiwook Sohn   Seoul National University of Science and Technology, Republic of Korea
Jong-Hyouk Lee   Sejong University, Republic of Korea

▶ Program Committee Members
Marcus Peinado   Microsoft, USA
Swee-Huay Heng   Multimedia University, Malaysia
Seog Chung Seo   Kookmin University, Republic of Korea
Naoto Yanai   Osaka University, Japan
Dongseong Kim   The University of Queensland, Australia
Sang Uk Shin   Pukyong National University, Republic of Korea
Kouichi Sakurai   Kyushu University, Japan
Seonghan Shin   National Institute of Advanced Industrial Science and Technology (AIST), Japan
Jong Kim   POSTECH, Republic of Korea
Masakatsu Nishigaki Shizuoka University, Japan
Meng Yu   Roosevelt University, USA
Jin Hong   University of Western Australia, Australia
Hyun Kwon   Korea Military Academy, Republic of Korea
Qiong Huang   South China Agricultural University, China
Ulrich Rührmair   Ruhr University Bochum, Germany
Junghwan Rhee   University of Central Oklahoma, USA
Junji Shikata   Yokohama National University, Japan
Amril Syalim   University of Indonesia, Indonesia
Dooho Choi   Korea University, Republic of Korea
Yonghwi Kwon   University of Virginia, USA
Hiroaki Kikuchi   Meiji University, Japan
Taeguen Kim   Soonchunhyang University, Republic of Korea
Doowon Kim   University of Tennessee, USA
Eul-Gyu Im   Hanyang University, Republic of Korea
Xiaofeng Chen   Xidian University, China
Eueung Mulyana   Bandung Institute of Technology, Indonesia

Hongjun Choi	DGIST, Republic of Korea
Young-Woo Kwon	Kyungpook National University, Republic of Korea
Joonsang Baek	University of Wollongong, Australia
Jin-Hee Cho	Virginia Tech, USA
Hyungon Moon	UNIST, Republic of Korea
Yeongpil Cho	Hanyang University, Republic of Korea
Hwajeong Seo	Hansung University, Republic of Korea
Changhoon Lee	Seoul National University of Science and Technology, Republic of Korea
Jongsung Kim	Kookmin University, Republic of Korea
YouSung Kang	ETRI, Republic of Korea
Yuseok Jeon	UNIST, Republic of Korea

▶ Organizing Committee Members

Hyun O Kwon	KISA, Republic of Korea
Dong-Hwan Oh	KISA, Republic of Korea
Kibom Kim	NSR, Republic of Korea
Eunyoung Kim	NSR, Republic of Korea
Jeong Nyeo Kim	ETRI, Republic of Korea
Daesung Moon	ETRI, Republic of Korea
Jungsuk Song	KISTI, Republic of Korea
Jun Lee	KISTI, Republic of Korea
Im-Yeong Lee	Soonchunhyang University, Republic of Korea
Jung Taek Seo	Gachon University, Republic of Korea
Haehyun Cho	Soongsil University, Republic of Korea
Dong-Guk Han	Kookmin University, Republic of Korea
Bona Kim	SSNC, Republic of Korea
Misim Jung	Culture Makers, Republic of Korea
Yoonjung Kwon	NAONWORKS, Republic of Korea

The 24th World Conference on Information Security Applications

WISA 2023

▶ Conference Program

DAY 1 August 23 (Wednesday), 2023

Time \ Room	Crystal Hall
13:00 - 13:30	Registration /Opening Remarks
13:30 - 14:10	**Invited Talk: 5G-AKA and EAP-AKA' from Cryptographic Perspectives** - Seonghan Shin (National Institute of Advanced Industrial Science and Technology, Japan) **Session Chair: Howon Kim (Pusan National University)**
14:10 - 14:30	Coffee Break
14:30 - 16:10	**Session 1: Cryptography** **Session Chair: Dooho Choi (Korea University)**
16:10 - 16:30	Coffee Break
16:30 - 18:10	**Session 2: Network & Application Security** **Session Chair: Bonam Kim (Kookmin University)**

DAY 2 August 24 (Thursday), 2023

Time \ Room	Crystal Hall	Jade Hall
09:30 - 10:20	**Keynote 1: Leaking AI: On Side-Channel Vulnerabilities (and more) on EdgeML Devices** - Bhasin Shivam(Nanyang Technological University, Singapore) **Session Chair: Young-Woo Kwon (Kyungpook National University)**	
10:20 - 10:40	Coffee Break	
10:40 - 12:20	**Session 3: Privacy & Management** Session Chair: Yoonho Choi (Pusan National University)	**Session 4: Attacks & Defenses** Session Chair: Daeseon Choi (Soongsil University)
12:20 - 13:40	Lunch Break (Convention Hall, 1F)	
13:40 - 14:30	**Keynote 2: Post-Quantum Cryptography: Now and Onwards** - Bo-Yin Yang(Academia Sinica, Taiwan) **Session Chair: Hwajeong Seo (Hansung University)**	
14:30 - 15:00	Coffee Break	
15:00 - 16:30	**KIISC Board Meeting, Social Networking**	**Poster Session 1 in front of Jade Hall** Session Chair: Jonghee Youn (Yeungnam University)
16:30 - 18:00		**Poster Session 2 in front of Jade Hall** Session Chair: Jonghee Youn (Yeungnam University)
18:00 - 18:30	Break Time	
18:30 - End	Banquet (Convention Hall, 1F)	

DAY 3 August 25 (Friday), 2023

Time \ Room	Crystal Hall	Jade Hall
09:30 - 11:50	**Session 5: Hardware & Software Security** Session Chair: Haehyun Cho (Soongsil University)	**Session 6: Post-Quantum Cryptography & Quantum Cryptanalysis** Session Chair: Jong Hwan Park (Sangmyung University)
11:50 - 13:00	Lunch Break (Crystal Hall, 2F)	

Special Session ◀

▶ IITP 정보보호 기술교류회

시간	주요 내용
개최목적	정보보호 분야 R&D 추진방향 소개와 우수과제 전시·시상식 개최를 통한 연구자 연구 의욕 고취 및 우수성과 공유 추진
개최일시	2023년 8월 22일(화) 13:50~18:00
개최장소	메종글래드 제주 크리스탈홀
참석자	정보보호 분야 기술교류회 참관자 및 우수과제 수상자 등
주관	정보통신기획평가원(IITP)
주요 내용	정보보호 분야 정부 R&D 추진방향 소개, 우수과제 시상 및 연구성과 발표 우수과제 전시 (6개 과제) 등

● 세부일정(안)

시간	주요 내용	비고
13:20~13:50	우수과제 전시	–
13:50~14:10	정보보호 분야 정부 R&D 추진방향 소개	IITP 정현철 PM
14:10~14:40	우수과제 시상식	원장상(4개) 및 격려패(6개)
14:40~15:00	휴식 및 연구자 네트워킹	–
15:00~18:00	우수과제 연구성과 발표(10개 과제)	우수과제 연구책임자

※ 주요 내용은 행사 사정에 따라 변동 가능

CONTENTS

DAY 2 **August 24 (Thursday), 2023**

Session 3: Privacy & Management
Session Chair: Yoonho Choi (Pusan National University)

Systematic Evaluation of Robustness Against Model Inversion Attacks on Split Learning

Hyunsik Na, Yoonju Oh, Wonho Lee and Daeseon Choi (Soongsil University)

Vulnerability Assessment Framework Based on In-the-Wild Exploitability for Prioritizing Patch Application

Seong-Su Yoon, Do-Yeon Kim, Ga-Gyeong Kim and Ieck-Chae Euom (Chonnam National University)

Patchman: Firmware Update Delivery Service Over the Blockchain for IoT Environment

Yustus Eko Oktian, Uk Jo, Simon Oh, Hanho Jeong, Jaehyun Kim, Thi-Thu-Huong Le and Howon Kim (Pusan National University)

Security Risk Indicator for Open Source Software to Measure Software Development Status

Hiroki Kuzuno (Kobe University), Tomohiko Yano (SECOM Co., Ltd.), Kazuki Omo (SIOS Technology, Inc.), Jeroen van der Ham (University of Twente) and Toshihiro Yamauchi (Okayama University)

Session 4: Attacks & Defenses
Session Chair: Daeseon Choi (Soongsil University)

Defending AirType against Inference Attacks using 3D In-Air Keyboard Layouts: Design and Evaluation

Hattan Althebeiti, Ran Gedawy, Ahod Alghuried (University of Central Florida), Daehun Nyang (Ewha Womans University) and David Mohaisen (University of Central Florida)

Robust Training for Deepfake Detection Models Against Disruption-Induced Data Poisoning

Jaewoo Park, Hong Eun Ahn, Leo Hyun Park and Taekyoung Kwon (Yonsei University)

Multi-class Malware Detection via Deep Graph Convolutional Networks using TF-IDF-based Attributed Call Graphs

Irshad Khan and Young-Woo Kwon (Kyungpook National University)

OCR meets the Dark Web: Identifying the Content Type Regarding Illegal and Cybercrime

Donghyun Kim, Seungho Jeon (Gachon University), Jiho Shin (Korean National Police University) and Jung Taek Seo (Gachon University)

DAY 3   **August 25 (Friday), 2023**

Session 5: Hardware & Software Security
Session Chair: Haehyun Cho (Soongsil University)

Protecting Kernel Code Integrity with PMP on RISC-V

Seon Ha and Hyungon Moon (Ulsan National Institute of Science and Technology)

Exploiting Memory Page Management in KSM for Remote Memory Deduplication Attack

Seungyeon Bae, Taehun Kim, Woomin Lee and Youngjoo Shin (Korea University)

Mutation Methods for Structured Input to Enhance Path Coverage of Fuzzers

Yonggon Park, Youngjoo Ko and Jong Kim (Pohang University of Science and Technology)

Improved Differential-Linear Cryptanalysis of Reduced Rounds of ChaCha

Ryo Watanabe, Nasratullah Ghafoori and Atsuko Miyaji (Osaka University)

SP-Fuzz: Fuzzing soft PLC with semi-automated harness synthesis

Seungho Jeon and Jung Taek Seo (Gachon University)

Session 6: Post-Quantum Cryptography & Quantum Cryptanalysis
Session Chair: Jong Hwan Park (Sangmyung University)

Quantum Circuit Designs of Point Doubling Operation for Binary Elliptic Curves

Harashta Tatimma Larasati and Howon Kim (Pusan National University)

PQ-DPoL: An Efficient Post-Quantum Blockchain Consensus Algorithm

Wonwoong Kim, Yeajun Kang, HyunJi Kim, Kyoungbae Jang and Hwajeong Seo (Hansung University)

Efficient Implementation of the Classic McEliece on ARMv8 processors

Minjoo Sim, Hyeokdong Kwon, Siwoo Eum, Gyeongju Song, Minwoo Lee and Hwajeong Seo (Hansung University)

Evaluating KpqC Algorithm Submissions: A Balanced and Clean Benchmarking Approach

Hyeokdong Kwon, Gyeongju Song, Minjoo Sim, Minwoo Lee and Hwajeong Seo (Hansung University)

Depth-Optimized Implementation of ASCON Quantum Circuit

Yujin Oh, Kyungbae Jang (Hansung University), Anubhab Baksi (Nanyang Technological University) and Hwajeong Seo (Hansung University)

CONTENTS

Identity Concealing Steganography-based Data Sharing Mechanism

Jinsu Kim and Namje Park (Jeju National University)

SGX-Enabled Edge Cloud Architecture for Secure Data Augmentation

Jiwon Ock and Seongmin Kim (Sungshin Women's University)

Solid Pod-based Medical Data Sharing System to Ensure Data Sovereignty

Sohui Kim, Minjeong Kim and Il-Gu Lee (Sungshin Women's University)

A Study on Establishing a Secure Remote Work Environment in a VDI Environment Based on Zero Trust

Chang Hoon Kim (Daegu University), Howon Kim (Pusan National University), Sokjoon Lee (Gachon University), Young Rang Kim (Pribit Technology) and Jungsoo Park (Hoseo University)

Analyzing Risk Attitudes in DeFi Crypto Credit Lending through On-chain Data

Simon Oh, Yeongjae Shin (Pusan National University), Uk Jo, Hyoeun Kang (SmartM2M), Kyeongwoo Oh, Jaehyun Kim, Bogeum Kim, Hyejin Sim, Changwoo Choi and Howon Kim (Pusan National University)

Parameter Optimization Techniques for Privacy and Utility Trade-off of Differential Privacy

Jung-Hwa Ryu, Sun-Jin Lee, Hye-Yeon Shim and Il-Gu Lee (Sungshin Womens' University)

A Study on Digital Human Ownership Management Techniques in Metaverse Based on NFT

Changhyun Roh, Changjun Choi, HyunSoo Kim and DongMyung Shin (LSWare Inc.)

Exploring Hybrid Quantum-Classical Approaches for Information Security

Dedy Septono Catur Putranto, Rini Wisnu Wardhani and Howon Kim (Pusan National University)

Analysis of International Trends for the Introduction of Zero Trust

Jeong Hyeop Hong, Sun Woo Kim, Ui Hyun Park and Kyung-ho Son (Kangwon National University)

TrustVoice: Detecting Voice Phishing Apps Using Their Runtime Behaviors

Chanjong Lee and Hyoungshick Kim (Sungkyunkwan University)

The RSA Algorithm's Quantum Cryptanalysis Posture

Rini Wisnu Wardhani, Dedy Septono Catur Putranto and Howon Kim (Pusan National University)

Blockchain-based Zero Trust System for Medical Data Exchange

Yohan Kim, Hanho Jeong, Jaehan Cho, Donggyu Kim, SangBong Oh and Howon Kim (Pusan National University)

Metaverse Copyright Ownership Verification using Redundant Verification for Virtual Performance

Won-Bin Kim, Changhyun Roh, Yongjoon Joe and Dong-Myung Shin (LSware Inc.)

Poster Session 2   **16:30 - 18:00, August 24 (Thursday), 2023**

Session Chair: Jonghee Youn (Yeungnam University)

Physical Layer Security Mechanism for Secure Trigger- based Uplink Multi-User Transmission

So-Hyun Park and Il-Gu Lee (Sungshin Women's University)

Efficient Implementation of Kyber on MSP430 Environment

DongHyun Shin, YoungBeom Kim and Seog Chung Seo (Kookmin University)

Optimization Study of Parallel Implementation for Scrypt: A Memory Hard Function

Seongjun Choi, Dongcheon Kim and Seog Chung Seo (Kookmin University)

High-Performance Kyber Implementation on ARMv7 Neon Technology

YoungBeom Kim (Kookmin University), Jeonghwan Shin, Hojoong Park (KT R&D Center Infra DX Lab), and Seog Chung Seo (Kookmin University)

Defense Against Adversarial Evasion Attacks on Self-Driving Car Using Image Quantization

Seungyeol Lee, Hyeonro Lee and Jaecheol Ha (Hoseo University)

Face Verifiable Anonymization in Video Surveillance

Sungjune Park, Hyunsik Na, Seungmin Kim and Daeseon Choi (Soongsil University)

A Multi-step Framework for Botnet Attack Detection in IoT Environment

Hojun Jin, Seungho Jeon and Jung Taek Seo (Gachon University)

Implementation of Montgomery Reduction and Butterflies for CRYSTALS-Dilithium on RISC-V

Yongryeol Choi, YoungBeom Kim and Seog Chung Seo (Kookmin University)

The Sky's Betrayal: Drone Hijacking on DJI Enhanced WiFi Protocol

Derry Pratama (Pusan National University), Jaegeun Moon (SmartM2M), Agus Mahardika Ari Laksmono, Dongwook Yun, Byeonguk Jeong, Iqbal Muhammad (Pusan National University), Janghyun Ji (SmartM2M) and Howon Kim (Pusan National University)

Efficient Implementation of Multiplication Reduction over NIST Prime P-384 for 8 bit AVR Processor

Mingi Kim, YoungBeom Kim and Seog Chung Seo (Kookmin University)

A Study on Tor Traffic Identification Technology for Blocking Dark Web Access in a LAN Environment

Hongbi Kim, Daeil Jang and Seunggoo Ji (Korea Internet & Security Agency)

Contact PUF: Highly Stable Physical Unclonable Functions Based on Contact Failure Probability in 180 nm, 130 nm, and 28 nm CMOS Processes

Duhyun Jeon (ICTK Holdings), Dongmin Lee and Byong-Deok Choi (Hanyang University)

An Implementation of Lightweight RISC-V Trusted Execution Environment with Memory Encryption and Task Isolation

Woojung Park, Janghyun Ji and Jaegeun Moon (SmartM2M)

Strengthening Secure Payment Systems in 5G-based IoT: A Comprehensive Analysis of Tokenization and PCI DSS Compliance

Hyeon No, Heekyung Shin, Jiwon Ock, Yeeun Kim and Seongmin Kim (Sungshin Women's University)

Tri-band-based Wi-Fi Indoor Localization to Defend against Jamming Attacks

Jin-Min Lee, Na-Yeon Shin, Jung-Hyun Moon and Il-Gu Lee (Sungshin Women's University)

On Secrecy of RSMA-enabled UAV Downlink Communications: Problem and Research Trends

Tri-Hai Nguyen, Heejae Park and Laihyuk Park (Seoul National University of Science and Technology)

Accelerating Key Derivation Function on GPU Architectures

Dong-Cheon Kim and Seog Chung Seo (Kookmin University)

Enhancing Robustness of Self-Driving Car Regression Models through Feature Squeezing

Hyeonro Lee, Seungyeol Lee, Seongwoo Hong and Jaecheol Ha (Hoseo University)

Privacy-Preserving DTx Data with Differential Privacy

Gee-Hee Yun and Kyoung-Jin Kim (Sungshin Women's University)

Side Channel Attack Resistant Binarized Neural Network Accelerator

Junho Lee, Haeyoung Kim, Dongwook Yun and Howon Kim (Pusan National University)

Tabling GHASH in LEA-GCM on GPU and Optimization

Jaeseok Lee, Dongcheon Kim and Seog Chung Seo (Kookmin University)

Research on Identification of Cyber Attacker Groups and Interpretation of Results

Sungtaek Oh and Woong Go (Korea Internet Security Agency)

Evaluation Criteria for Cyberattack Scenarios Used in Training Exercises

Insung Song, Seungho Jeon and Jung Taek Seo (Gachon University)

Malextension: Malicious Extension to Hack your Browser

Jiwon Jang, Ye-Sol Oh (Sungshin Women's University), and Il-Gu Lee (Sungshin Women's University)

▶ International Participants Payment Method

Registration Deadline: August 10, 2023 (UTC+09:00)

Participants can register for the conference until August 10, 2023 (UTC+09:00)

Please read carefully the registration guidelines below.

We use online registration to complete the registration for participants.

Click on the registration page link: https://kiisc.or.kr/payment/pay/173

At least one presenter per accepted paper, poster must register for the conference as an attendance until Aug. 5, 2023 (UTC+09:00)

▶ Registration Fees (International)

Online Attendance	Student	350 USD
	General Participant	
Offline Attendance	Student	350 USD
	Offline Attendance General Participant	500 USD

(Online) Registration includes (a) access to the online conference and (b) the access to the online proceedings.

(Offline) Registration includes (a) access to the online conference and (b) the access to the online proceedings (c) 2 Lunches, 1 Banquet

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

▶ Registration-Related Inquiries

If you have any questions regarding your registrations, please contact the Registration Company via email at kiisc@kiisc.or.kr

▶ Registration Policy

At least one presenter per accepted paper, poster must register for the conference as an author.

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

▶ Registration

▶ 한국인 (국내거주인) 등록안내
Registration Fees (Domestic) : 사전등록 2023년 8월 10일(목)까지

*논문 발표자는 2023년 8월 5일(토)까지 등록

Offline Attendance	학생(전일제)	500,000 원
	군·공무원	500,000 원
	일반	700,000 원
Online Attendance	학생(전일제)/일반	200,000 원
시니어(63세 이상) 종신회원		무료

(오프라인) 온라인 학술대회 참석 링크, 온라인 프로시딩, 점심2회, 만찬 1회 제공
(온라인) 온라인 학술대회 참석 링크, 온라인 프로시딩 제공

▷ 학회 홈페이지(www.kiisc.or.kr)접속 → 학회행사 → 사전등록바로가기 → WISA 2023 (Domestic) 클릭
   (신용카드/계좌이체 결제 가능)
▷ 사전등록 송금처
– 예금주 : 한국정보보호학회
– 계좌번호 : (국민은행) 754-01-0008-146
* 입금명은 필히 [행사명 첫 글자+ 등록자 성함]으로 기재해 주시기 바랍니다.예) WISA 홍길동 – "W홍길동" 기재
* 사전등록 시 등록비는 위의 구좌로 송금하시고, 입금자가 대리일 경우 통보바랍니다.
* 계산서 신청 시, 익일 안으로 등록하신 이메일로 청구용 계산서가 발행됩니다. 영수용 계산서가 필요하신 경우,
   사전에 학회로 연락 바랍니다.
* 등록확인서는 한국정보보호학회 홈페이지 상단 행사 등록 및 참가확인서 바로 가기를 클릭하신 후 등록 시 기재하
   시 성함과 이메일을 기재하시면 출력 가능합니다. (결제 완료 후 발행 가능)
* 참가확인서는 행사 종료 후 익일부터 한국정보보호학회 홈페이지 상단 행사 등록 및 참가확인서 바로 가기를 클릭
   하신 후 등록 시 기재하시 성함과 이메일을 기재하시면 출력 가능합니다. (결제 완료 후 발행 가능)
* 학생은 다른 소속이 없는 전일제(학부생/대학원생)에 한합니다.
* 학생의 경우 kiisc@kiisc.or.kr로 학생증 사본 송부 바랍니다.
* 군·공무원 등록은 주무관청에 소속 중인 공무원증 소지자에 한합니다. (국공립 교직원 제외) kiisc@kiisc.or.kr로
   공무원증 사본 송부해 주시기 바랍니다.
* 시니어 무료등록은 학회 종신회원으로 1961년 12월 31일 이전 출생자에 한합니다.
* PAPER/POSTER 논문 발표자(저자 중 최소 1인) 는 오프라인 참석 비용으로 등록해주시기 바랍니다.

The 24th World Conference on Information Security Applications

WISA 2023

Korea Institute of Information
Security & Cryptology