KIISC

정보보호학회 논문지
“차세대암호” 논문모집

1970년대 말 Diffie, Hellman에 의해 공개키 암호 개념이 제안되고 Rivest, Shamir, Adleman에 의해 RSA가 설계된 이후 지난 40여 년 동안 현대 암호는 크게 대칭 암호와 공개키 암호로 구분되어 발전하여 왔으며, 인증, 전자서명, 키 설정 등 다양한 암호 응용 분야가 연구되었습니다. 최근에는 양자컴퓨터의 가시화에 따른 기존 암호 체계의 잠재적인 취약성에 대응하기 위한 NIST의 양자내성암호(Post-Quantum Cryptography) 공모, 자원이 제약된 환경에서도 안전하게 동작 가능한 암호를 제공하기 위한 NIST의 경량암호(Lightweight Cryptography) 공모 등 표준화 활동과 함께, 데이터를 보호한 상태에서 연산 및 데이터 분석이 가능한 동형암호(Homomorphic Encryption) 및 함수암호(Functional Encryption) 등 다양한 고급 기능을 제공하는 암호들도 활발히 연구되고 있습니다.

한국정보보호학회 논문지에서는 이러한 최근의 암호 연구 동향과 최신 기술 연구 성과를 공유하기 위해 “차세대암호” 특별섹션을 만들었으며, 이를 통해 우리나라의 최근 연구 현황과 성과를 소개하고자 합니다. 관련 연구자들의 많은 관심과 투고를 부탁드립니다.

본 특별섹션으로 투고하시면 일반투고 비용으로 긴급 심사를 통해 신속하게 출간됩니다. 단, 수정·보완 등의 사유로 발간 준비가 지연되면 일반논문으로 처리될 수 있습니다.

1. 일정

- 논문제출 : ~~2022년 10월 7일(금)까지~~ 10월 14일(금)까지 / *제출기한 연장
- 논문발간 : 2022년 12월호 게재
- 담당편집위원 : 이문규 교수 (인하대학교, mklee@inha.ac.kr)

2. 논문 모집분야

- Post-Quantum Cryptography
- Lightweight Cryptography
- Homomorphic Encryption
- Functional Encryption
- White-box Cryptography
- Cryptography for Blockchains
- Next-Generation Cryptographic Protocols
- Cryptographic Applications for Emerging Computing Environments
- Efficient Software Implementation of Cryptographic Algorithms
- Efficient Hardware Implementation of Cryptographic Algorithms

3. 논문 제출 절차: 한국정보보호학회 홈페이지 (http://kiisc.or.kr) “논문투고” 클릭

⇨ KISTI 한글 논문 시스템 로그인

⇨ **논문 투고시 분야: 특별섹션 (차세대암호) 선택**

⇨ 심사진행

4. 논문 제출 문의: [e-mail] kiisc@kiisc.or.kr [Tel] 02-564-9333 (내선:3)

한국정보보호학회 논문지편집위원회