KIISC

정보보호학회 논문지
"Post Quantum Cryptography(차세대 공개키 암호)" 논문모집

양자 컴퓨터의 발전가능성과 더불어 인수분해, 이산대수에 기반한 공개키 암호의 안전성 문제가 대두되고 있다. 이러한 인식으로 미국 NIST는 향후 미국에서 사용할-실질적인 세계표준으로 사용될 것으로 판단됨- 공개키 암호를 공모하고 있다. 이러한 공개키 암호는 향후 양자 컴퓨터가 개발되어도 안전해야하므로 Post Quantum Cryptography(이하 PQC)라 불리고 있다. 현재 3라운드 후보인 PQC 암호들은 격자기반, 코드기반, 다변수 기반 암호들이며 대체 후보(Alternate Candidates)들까지 고려하면 Isogeny 기반 문제도 포함된다. 본 특집 세션에서는 향후 공개키 암호를 이끌어갈 PQC 암호를 다룬다. PQC암호와 관련된 PQC암호의 안전성 분석, 효율적인 SW 및 HW구현, PQC 암호의 부채널 분석 및 대응법 설계, 새로운 PQC 암호의 설계, PQC암호와 관련된 양자 회로 설계 등 PQC완 관련된 모든 연구 내용을 다룰 예정이다.

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 : **2021년 4월 22일(목) 까지**
- 논문발간 : 2021년 6월호 게재
- 담당편집위원 : 홍석희 교수 (고려대학교, shhong@korea.ac.kr)

2. 논문 모집분야

- Security analysis for PQC
- A new design of PQC
- Efficient software implementations on PQC
- Hardware Implementations on PQC
- Quantum logic circuits for PQC
- Side-channel attacks and countermeasures on PQC
- Fault attacks and countermeasures on PQC

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

⇨ KISTI 한글 논문 시스템 로그인

⇨ 논문투고 분야: 특별섹션 (차세대 공개키 암호 / **Post Quantum Cryptography**) 선택

⇨ 심사진행

4. 논문제출 문의 : (e-mail) kiisc@kiisc.or.kr, (Tel) 02-564-9333 / 내선: 3

한국정보보호학회 논문지편집위원회