차세대 암호 및 인증 시스템

□ 양자 컴퓨터 환경에서 현재 사용되고 있는 암호시스템의 안전성이 위협받고 있어 차세대 암호기술의 확보와 다양한 응용처 적용 및 검증 필요

□ 화상회의·원격의료 등 원격서비스가 확대되면서 개인 정보가 온라인 상에서 생성/공유되며 보안 위협이 증대되고 있어 제한된 환경에서도 편리하고 안전한 인증 기술 개발이 요구됨

[분야 및 공모 예시]

- 고성능 PQC 알고리즘 개발 및 NIST PQC 표준 알고리즘 평가 기법
  - ·연산속도 개선, 압축 기법 및 안전한 키 저장기법, 부채널 공격에 강인한 연산기법 등
  - ·NIST 표준 알고리즘의 공격 기법, PQC 알고리즘 안전성 증명, 후보 알고리즘의 보안성 개선 기술 등
- 양자내성 동형암호/다자간 연산 기술 및 블록체인에 적용가능한 영지식증명 기술
  - ·민감정보(성별, 나이 등)를 익명화해도 효율적인 암호기술
  - ·블록체인 장부 상에 기록되는 정보 중 민감정보를 익명화할 수 있는 영지식 증명 기술 등
- 원격 서비스 환경 제약 하에서도 편리하고 안전한 사용자 인증 기술
  - ·비 신뢰 환경에서의 사용자 인증 기술 (제어권이 없는 환경, 위·변조가 가능한 상황 등 고려)
  - ·연속성/편의성을 가지는 사용자 인증 기술 (1회 인증 후 사용자 변경제한, 인증 요청을 반복하는 등의 편의성을 저해하지 않는 기술 등)
  - ·미래 신규 Form Factor 기기에서의 인증 기술 (Wearable 기기 등 Interface가 제한된 환경 고려)

□ 문의처 : e-mail) creative.ftf@samsung.com / Tel) 02-6147-8654

- 이 상 -