"양자내성암호 전환" 특집호 발간에 즈음하여

2023년 7월 국가정보원·과학기술정보통신부는 행정안전부 등 관계부처와 함께 국내 암호체계를 양자내성암호로 전환하기 위한 종합 대책을 담은 마스터플랜을 수립했다고 공표했다.

해당 마스터플랜은 양자내성암호 전환과 관련된 역량확보, 제도절차마련, 전환지원, 기반생태계 조성과 같은 전략을 중심으로 2023년부터 시행되었으며 장기간의 플랜 과정을 거쳐 2035년까지 국내 양자내성암호 전환을 완성하는 것을 목표로 하고 있다. 현 마스터플랜의 발표로 인해 양자내성암호 전환의 당위성은 보다 강화되었으며 산학연이 이제 모두 양자내성암호 전환에 큰 관심을 가지게 되는 계기가 되었다. 현재 미국 NIST에서는 1차적으로 양자내성암호 키교환과 전자서명에 대한 표준화를 완성 및 배포하였으며 한국에서는 올해안으로 KpqC 공모전 결과를 발표할 예정이다. 확정된 양자내성암호 알고리즘은 이제 양자내성암호 전환을 Real-world 상에 적용하기 위한 실용화 준비 단계에 진입하였으며 이로인해 지금까지 고려되지 않았던 다양한 실질적인 양자내성암호 전환 문제에 직면하게 될 것으로 판단된다.

본 특집호에서는 국내·외 양자내성암호 표준화 및 전환 정책 동향을 비롯하여 실제 양자내성암호 전환의 핵심기술인 양자내성암호 소프트웨어 및 하드웨어 구현, 양자내성 X.509, 양자내성 하이브리드 KEM/DSA, 양자내성 블록체인과 같은 실용적인 기술 동향에 대해 확인해 본다. 그리고 양자내성암호 전환의 근본으로 돌아가 실제 양자컴퓨터가 양자내성암호 그리고 AES, SHA-2, SHA-3와 같은 암호군들의 양자보안강도 저하에 미치는 영향도 함께 확인해 보도록 한다. 해당 최신 동향들을 확인해 봄으로써 양자내성암호 전환에 필요한 기술과 정책 그리고 방향성에 대해 확인 가능할 것으로 판단된다. 이를 기반으로 앞으로의 양자내성암호 전환 마스터플랜의 성공적인 달성을 이룩할 수 있도록 산학연 관계자 모두가 힘을 합쳐야 할 것으로 판단된다.

끝으로 바쁘신 중에도 소중한 시간을 내시어 원고를 집필해 주신 집필자분들과 편집에 수고해 주신 학회지 편집 위원회, 그리고 학회 사무국 관계자 여러분께 감사를 드립니다.

2024년 12월

한성대학교 융합보안학과 부교수 서 화 정