"차세대 컴퓨팅과 양자내성암호" 특집호 발간에 즈음하여

현재 컴퓨터의 구조적인 한계를 뛰어넘는 차세대 컴퓨팅 기술로서 양자컴퓨터와 인공지능 반도체에 대한 관심이 그 어느 때보다 뜨겁다. 특히 양자컴퓨터는 기존 컴퓨팅 방식으로는 수백 년이 걸릴 수도 있는 문제를 다항 시간 내에 해결할 수 있는 잠재력을 가지고 있으며, 이는 오늘날 보편적으로 사용되는 RSA 및 ECC 기반의 공개키 암호 시스템의 보안성을 심각하게 위협한다. 따라서 이러한 위협에 대응하기 위해 양자컴퓨터에 안전한 양자내성암호(Post-Quantum Cryptography, PQC)로의 전환은 더 이상 선택이 아닌 필수적인 과제가 되었다.

미국 NIST는 2024년에 양자내성암호 표준으로 ML-KEM, ML-DSA, 그리고 SLH-DSA를 최종 선정하여 발표하였다. 국내에서도 이에 발맞추어 KpqC 공모전을 통해 양자내성암호 후보 알고리즘을 평가하고, 올해 초 총 4종의 우수 알고리즘(NTRU+, SMAUG-T, AIMer, HAETAE)을 최종 선정하였다. 이들 알고리즘은 향후 다양한 보안 서비스에 적용될 것으로 기대되며, 이를 위해서는 각 알고리즘에 대한 구조와 보안성, 구현 효율성에 대한 폭넓은 이해가 선행되어야 한다.

이에 본 특집호에서는 국내 양자내성암호 관련 산학연의 이해를 돕기 위해 KpqC에서 선정된 2종의 KEM(Key Encapsulation Mechanism) 알고리즘(NTRU+, SMAUG-T)과 2종의 DSA(Digital Signature Algorithm) 알고리즘(AIMer, HAETAE)을 중점적으로 살펴본다.

아울러 본 특집호에서는 양자내성암호를 둘러싼 보다 넓은 기술적 배경도 함께 조망한다. 먼저, 양자컴퓨터 및 인공지능 반도체의 최근 기술 발전 동향을 살펴보고, 양자보안성을 검증하기 위한 타원곡선암호(ECC)의 양자회로 구현 동향에 대해서도 기술한다. 나아가, ECC가 실질적으로 적용되고 있는 대표적 사례인 블록체인 플랫폼 상에서의 양자내성암호 적용 연구에 대해서도 소개하며, 암호기술의 실용성과 미래 방향을 함께 고찰하고자 한다.

마지막으로, 양자내성암호의 실제 도입을 위한 핵심 인프라인 공개키 기반 인증서 시스템(PKI)의 전환 문제에 주목하여, 양자내성과 기존 암호를 동시에 지원하는 하이브리드 인증서 구조와 연구 동향을 함께 정리하였다. 이는 향후 보안 인프라의 연속성과 상호운용성을 확보하는 데 필수적인 요소로 작용할 것이다.

끝으로, 바쁘신 일정 속에서도 귀중한 시간을 내어 훌륭한 원고를 집필해 주신 집필자 여러분께 깊은 감사의 인사를 드리며, 본 특집호의 기획과 편집에 애써주신 학회지 편집 위원회와 학회 사무국 관계자 여러분께도 진심으로 감사의 말씀을 전한다. 이 특집호가 양자내성암호에 대한 이해를 넓히고, 국내 암호기술 발전에 의미 있는 기여를 하기를 기대한다.

2025년 6월

한성대학교 융합보안학과 부교수 서 화 정