"양자내성암호와 부채널분석" 특집호 발간에 즈음하여

양자컴퓨터가 현재의 암호체계를 무력화시킬 수 있다는 위협적인 상황이 점점 더 그 가능성을 키워가고 있어서 암호학자들과 보안산업 종사자들이 다각도의 양자리스크 대응을 고민하고 있다. 양자리스크 대응의 중요한 한 축은 양자컴퓨터의 암호해독으로부터 안전한 새로운 암호 알고리즘을 개발하는 것이다. AES, RSA, SHA2와 같은 현재의 암호 알고리즘들이 수 년 내에 당장 무용지물이 되는 것은 아니지만 중장기적인 미래를 위한 준비의 일환으로 미국 NIST에서는 양자컴퓨터의 암호해독 연산에 강인한 양자내성암호를 공개경쟁으로 공모하여 2022년 7월에 4종의 최종 표준화 대상 알고리즘(KEM 1종 및 DSA 3종)을 선정하였다. 이와는 별도로 기반문제가 다른 4종의 KEM 알고리즘을 지정하여 추가적인 분석을 진행하고 있다. 또한, 국내에서는 양자내성암호연구단(KpqC연구단)이 '양자내성암호 국가공모전'을 통해 다양한 난제 기반의 양자내성암호 개발을 독려하고 있다. 양자내성암호는 현재의 비트 기반 디지털 기기에서 효율적으로 동작되어야 하며 동시에 양자컴퓨터 암호해독 연산을 극복할 수 있음이 검증되어야 한다. 따라서, 양자내성암호의 안전성을 검증하기 위해서는 현재의 디지털 기기에서 동작할 때 취약점이 될 수 있는 부채널 분석과 오류주입 공격에 대한 방어능력도 증명해야 하고, 양자컴퓨터(또는 양자컴퓨팅 시뮬레이터)에서 양자 알고리즘으로 분석하는 상황에서도 안전하게 동작하는 방어능력을 증명해야 한다.

본 특집호에서는 먼저, 고성능의 범용 양자컴퓨터가 없는 상황에서 양자자원량(큐비트 수, 양자게이트 수, 수행시간 등)을 계산하여 암호의 양자보안강도를 추정하는 <Q|Crypton> 플랫폼을 소개한다. 암호 알고리즘과 암호해독용 양자 알고리즘을 모두 고려하여 양자컴퓨터 사용 자원량을 비교하는 현실적인 접근법으로 향후 양자내성암호들의 성능 비교를 위해 활용될 수 있을 것으로 보인다. 그리고, 코드 기반 양자내성암호를 대상으로 현재의 디지털 기기에서 부채널 분석 공격의 영향을 살펴본다. 이어서 양자컴퓨터에서 동작되는 양자 알고리즘에 기반해서 양자내성암호의 안전성을 분석하려는 다양한 연구결과를 살펴본다. 격자 기반 양자내성암호에 대한 양자분석 기술 동향을 살펴보고, 특히 대표적인 격자 기반 양자내성암호인 Crystals-Kyber와 Crystals-Dilithium의 안전성 분석 동향은 별도로 소개한다. 또 다른 수학적 난제 배경인 다변수 이차식 기반 전자서명의 안전성 분석 및 표준화 동향을 살펴보고, 코드 기반 암호와 아이소제니 기반 암호의 공격사례도 분석한다. 국내외 양자내성암호 전환 정책 및 상용화 동향을 소개하면서 본 특집호를 마친다.

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

2023년 2월

ETRI 미래암호공학연구실 실장 강유성