"NIST/KPQC 양자내성암호 공모전 동향" 특집호

양자컴퓨터 기술에 대한 발전은 인류에게 있어 기존 난제들에 대한 새로운 최적화 기술을 제공해 준다는 점에서 큰 이점을 가져올 것으로 판단된다. 하지만 양자컴퓨터를 통한 최적화 기술이 암호화 해독 기술과 결합하게 될 경우 현재 널리 사용되고 있는 공개키 암호의 해킹으로 이어질 수 있기에 양자알고리즘을 통한 해킹에 대비하는 것이 요구되고 있다. 미국에서는 NIST를 중심으로 양자내성암호 공모전을 진행 중에 있다. 다년의 연구 결과를 통해 양자내성암호의 보안성을 확인함과 동시에 연산 효율성을 적절히 갖춘 Kyber, Dilithium, FALCON, 그리고 SPHINCS+가 최종 표준안으로 선정되었으며 현재 표준화가 진행 중에 있다. NIST에서는 추가적으로 양자내성 전자서명 알고리즘을 선정하기 위한 공모전을 진행 중에 있다. 국내에서는 KpqC 연구단을 주축으로 한국형 양자내성암호 공모전을 개최하여 진행 중이며 현재 최종 후보군 8종에 대한 검증이 진행 중에 있다. KpqC 공모전에서는 올해 안으로 최종 후보군을 결정하는 것을 목표로 하고 있다.

본 특집호에서는 현재 개발 중에 있는 양자컴퓨팅 플랫폼에 대해 먼저 상세히 확인해 보도록 한다. 이를 통해 양자컴퓨터를 통한 실제 공격의 위협을 대략적으로 가늠해 볼 수 있다. 이러한 기술 개발 척도를 기반으로 양자컴퓨팅 플랫폼을 활용한 대칭키와 해시함수에 대한 해킹 동향에 대해서도 확인해 본다. 현재 양자내성과 관련된 보안 척도를 명확히 정의할 수 없기에 기존 대칭키와 해시함수에 대한 양자 알고리즘을 적용을 통해 양자보안성을 확인하고 있기에 해당 척도를 명확히 하는 것은 중요하다. 그리고 현재 진행 중에 있는 NIST의 추가적인 양자내성암호 전자서명 그리고 국내 KpqC 양자내성암호 공모전의 현황에 대해 확인해 본다. 특히 KpqC 공모전에 제출된 알고리즘들에 대해서 보다 상세히 본 특집호에서 확인해 보도록 한다. 이와 더불어 양자내성암호 선정에 있어 중요한 척도로 작용하고 있는 구현 효율성 관점에서 최신 양자내성암호에 적용된 방법론에 대해 확인해 보도록 한다. 마지막으로 암호 활용의 역기능 중 하나인 랜섬웨어 관점에서 양자내성암호가 미치는 영향에 대해 확인해 보도록 한다.

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

2024년 4월

한성대학교 융합보안학과 부교수 서 화 정