"양자컴퓨터와 정보보호" 특집호 발간에 즈음하여

양자컴퓨터는 양자 역학의 특성을 활용한 차세대 컴퓨터로써 얽힘(entanglement)과 중첩(superposition) 이라는 양자 성질을 가진다. 여기서 얽힘은 큐비트들이 서로 얽혀있는 경우, 어떤 큐비트의 상태가 변화하면 다른 큐비트의 상태에도 영향을 줄 수 있는 성질을 말하며 중첩은 0과 1의 상태를 동시에 확률적으로 가질 수 있는 상태를 말한다. 이러한 양자 역학의 성질을 이용하면 고전컴퓨터에 비해 연산 속도가 획기적으로 고속화 시킬수 있다. 하지만 양자컴퓨터는 기존에 난제로 알려졌던 암호학의 기반 문제들에 대해서도 양자알고리즘을 기반으로 하여 연산 최적화를 수행한다. 따라서 대칭키 암호의 경우 기존보다 두 배 이상의 킷값을 사용해야 하며 공개키 암호의 경우 다른 수학적 난제에 기반한 알고리즘으로의 전환이 요구되고 있다. 물론 양자컴퓨팅의 발전으로 인해 정보보안 분야에서 새롭게 도약하고 있는 분야로는 해킹에 대한 안전성을 높인 양자암호통신과 양자를 통해 난수성을 높인 양자난수발생기가 있다.

본 특집호에서는 전세계 대표적인 IT 기업들이 투자하고 있는 양자컴퓨팅의 현재 발전상황과 이를 활용할 수 있는 양자컴퓨팅 플랫폼에 대해 확인해 보도록 한다. 이러한 양자컴퓨터 상에서 연구되고 있는 대칭키에 대한 해킹인 그루버 알고리즘 및 공개키에 대한 해킹인 쇼어 알고리즘의 동향에 대해 확인해 보도록 한다. 실제 양자컴퓨터의 가장 큰 활용처인 양자인공지능 기술에 대해서도 살펴보도록 한다. 또한 차세대 공개키 알고리즘인 양자내성암호 공모전과 양자내성암호에 대한 실질적인 성능을 객관적으로 평가할 수 있도록 도움을 준 벤치마크 플랫폼에 대해 확인해 보도록 한다. 이러한 양자내성암호를 기반으로 현재 시스템을 안전한 양자내성암호로 전이 방법에 대해서도 살펴보도록 하며 양자내성서명 알고리즘을 통해 안전성을 확보한 블록체인 기술에 대해서도 확인해 보도록 한다. 마지막으로 양자컴퓨팅 기술을 통해 보안성을 높인 양자암호통신과 양자난수발생기에 대해서도 살펴보도록 한다.

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

2023년 4월

한성대학교 융합보안학과 부교수 서 화 정