"최신암호기술" 특집호 발간에 즈음하여

현재 우리 사회는 다양한 변화의 소용돌이에 있다고 해도 과언이 아닙니다. 2019년부터 계속된 COVID-19로 인해 비대면 중심으로 교육, 업무 환경이 개편되고 있으며, 양자컴퓨터의 개발 가속화로 인해 지금까지 사용하던 공개키 암호들의 안전성이 위협받고 있습니다. 블록체인기술은 가상화폐, NFT와 같은 새로운 형태의 자산 보유를 실현 가능하게 하고 있습니다. 뿐만 아니라, 모든 사물이 인터넷에 연결되어 서로 통신하는 IoT 환경과 이를 더욱 가속화할 6G 통신 환경이 도래하고 있습니다. 이러한 다양한 사회적, 기술적 변화에서 개인과 조직의 프라이버시와 데이터를 보호하는 것은 더욱 중요해지고 있으며 이에 따라 정보보호 분야에서 암호의 역할 역시 더욱 커지고 있습니다.

이번 특집호에서는 이러한 추세에 맞추어 암호기술에 대한 최신 연구동향을 담았습니다. 현재 진행중인 IoT 환경과 비대면, 클라우드 컴퓨팅 시대, 그리고 다가올 6G 통신 및 양자컴퓨팅 시대에서 사용자의 데이터를 보호할 수 있는 다양한 암호기술의 연구동향에 대해 다루었습니다. 또한, 부채널분석과 양자컴퓨터를 활용한 암호분석에 대한 최신 동향도 다루었습니다.

첫 번째 원고는 양자컴퓨팅 시대에도 안전한 양자내성 블록체인에 대한 기술적 동향에 대해 살펴보았습니다. 다양한 형태의 양자내성 암호에 대해 알아보고 이를 활용한 양자내성 블록체인으로의 전환을 위한 기술적 동향을 파악할 수 있습니다. 두 번째 원고는 NIST 양자내성암호 공모의 Round 3 Alternative로 각광을 받고 있는 타원곡선 Isogeny 기술에 기반한 양자내성암호의 연구동향 대해 알아보았습니다. Isogeny 기반 양자내성암호의 장점과 향후 연구 분야에 대해 확인할 수 있습니다. 세 번째 원고는 프라이버시를 보호하면서 암호화된 데이터에 연산을 수행할 수 있는 함수 암호의 연구동향에 대해 알아보았습니다. 임의의 연산과 제한된 연산을 지원하는 다양한 형태의 함수 암호에 대한 기술적 동향을 파악할 수 있습니다. 네 번째 원고는 현재 NIST 경량암호 공모에 선정된 최종 후보 10종의 인증암호에 대한 특징을 분석하였습니다. 트위커블 기반, 순열함수 기반, 스트림 암호 기반 암호들의 연산 특징과 안전성에 대한 분석을 전반적으로 수행하였습니다. 다섯 번째 원고는 NIST 양자내성암호 공모의 Round 3 최종 후보에 선정된 격자기반 KEM 알고리즘인 SABER, CRYSTALS-KYBER, NTRU에 대한 부채널분석 연구동향에 대해 제시하였습니다. 현재까지 알려진 다양한 부채널분석 기법과 함께 이들에 대한 대응기법 동향을 함께 분석하였습니다. 여섯 번째 원고는 양자컴퓨터를 활용한 암호분석 기술로서 해시함수의 충돌쌍을 공격하는 최신 동향에 대해서 제시하였습니다.

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

2022년 2월

국민대학교 정보보안암호수학과 서석충