“양자내성암호 알고리즘” 특집호 발간에 즈음하여

최근 미국, 중국, 영국 등에서 양자컴퓨터 관련 기술이 국가적인 차원에서 개발되고 있다. Google, IBM, Microsoft, Intel과 같은 글로벌 기업 또한 양자컴퓨터 개발에 박차를 가하고 있는 상황이다. 이러한 기술 개발은 우리 삶에 여러 영향을 줄 것이다. 예상할 수 있는 주요 영향 중 하나로 현 공개키 암호체계의 변화를 들 수 있다. 1994년에 P. Shor가 소개한 양자 알고리즘은 양자컴퓨팅을 사용하여 다항식 시간 내에 인수분해나 이산대수 문제를 해결할 것으로 알려져 있다. Shor 알고리즘을 구현할 수 있는 양자컴퓨터의 실용화는 곧 현 공개키 암호에 대한 위협으로 직결된다.

이러한 위협에 대한 대응으로 전 세계의 많은 국가는 새로운 암호체계 관련 연구를 확대 지원하기 시작했다. 양자컴퓨팅을 이용한 공격에도 안전할 것으로 기대되는 암호를 ‘양자내성암호(이하 Post-Quantum Cryptography, PQC)’라고 한다. 2017년 미국의 표준화 기구 NIST는 전 세계를 대상으로 PQC 표준화 공모사업을 시작하였다. 이를 필두로 여러 국가에서 PQC 개발 및 표준화를 시작하였고 다수는 현재 진행 중이다.

반면, 국내에서는 연구 저변이 넓지 않고 중장기적인 투자와 지원이 적어, 몇몇 연구자들을 중심으로 산발적이고 단발적인 연구가 진행되고 있었다. 그러나 점차 PQC 개발의 중대성에 대한 인식이 높아져 2021년에 양자내성암호연구단(이하 KpqC 연구단)이 결성되게 되었다. KpqC 연구단은 국가보안기술연구소가 국가정보원의 후원으로 설립한 연구단이다. 당해 연구단은 양자내성암호 국가공모전(이하 KpqC 공모전)을 개최하며 0라운드를 시작하였다. 현재는 1라운드를 진행하고 있으며, 총 16편의 알고리즘이 제안되어 국내외적으로 공개 검증 중에 있다.

이러한 공모전 진행 상황과 국내 PQC 기술력 확보의 중요성에 대한 인식에 기초하여 본 특집호는 KpqC 공모전에 제안된 알고리즘과 이와 관련된 내용을 중심으로 아홉 편의 원고를 다룬다. **「양자내성암호 국가공모전」**은 KpqC 공모전의 추진 배경, 개최 취지, 진행 상황 및 추후 계획 등을 전반적으로 소개한다. **「KpqC 공모전에 제출된 Hash-and-Sign 구조의 격자 기반 서명 기법 분석」**은 KpqC 알고리즘 Peregrine과 SOLMAE를 소개하고 그 설계기법과 특징을 분석한다. **「KpqC 공모전에 제출된 Fiat-Shamir with aborts 구조의 격자 기반 서명 기법 분석」**은 KpqC 알고리즘 HAETAE, GCKSign, NCC-Sign를 소개하고 그 설계기법과 특징을 분석한다. **「KpqC 공모전 1라운드 격자 기반 PKE/KEM 알고리즘 분석」**은 KpqC 알고리즘 NTRU+, SMAUG, TiGER의 기반 문제, 설계 방식, 특징, 안전성 분석 방식 등을 분석하고, 구현성능을 비교·분석한다. **「KpqC에 제출된 코드기반 암호의 소개 및 분석」**은 KpqC 알고리즘 Enhanced pqsigRM, Layered ROLLO-I, PALOMA, REDOG을 소개하고 안전성의 근거와 성능을 분석한다. **「KpqC 공모전 1라운드 암호(그래프/다변수/아이소제니/영지식) 암호 소개」**은 다변수 기반 MQ-Sign, 아이소제니 기반 FIBS, 그래프 기반 IPCC, 영지식 증명을 사용하는 AIMer를 소개하고 각 알고리즘의 특징을 살펴본다. **「KpqC 암호 알고리즘의 효율성**

관점에서의 분석」은 KpqC 알고리즘을 암호 구현 효율성 관점에서 비교·분석하고 추후 표준화를 고려한 운영방안을 제시한다. 또한 NIST에서 선정한 표준 알고리즘과의 성능을 비교·분석한다. **「LWE-like KEM/전자서명에 대한 부채널 대응기법 동향」**은 KpqC 알고리즘의 효율성을 분석하고 LWE 기반 알고리즘에 대한 부채널 동향을 소개한다. 마지막으로 **「양자내성암호 특허동향」**은 양자내성암호 알고리즘 및 알고리즘 구현과 관련된 특허출원 동향을 소개한다.

끝으로 바쁘신 중에도 시간을 내어 원고를 작성해 주신 집필자분들과 편집에 수고해 주신 학회지 편집위원회, 그리고 학회 사무국 관계자 여러분에게 깊은 감사를 드립니다.

2023년 6월

국가보안기술연구소 책임연구원 지 성 택