부호 기반 양자 내성 암호 NIST 표준화 동향

최승주 * 권혁동 * 서화정 *†
* 한성대학교 대학원 IT융합과

요 약

● 양자 컴퓨터 시대에 대비한 양자 내성 암호 연구가 진행 중

● 양자 내성 암호 기반 중 부호 기반에 대한 고찰

양자 컴퓨터

● 큐비트를 이용한 병렬적인 연산 처리 가능

● 확률로 존재하는 연산 방법 사용

● 기존 컴퓨터를 사용하면 몇 백 년이 걸릴 연산을 몇 분 안에 연산이 가능

● 소인수 분해 기반의 암호들의 연산을 깰 수 있음

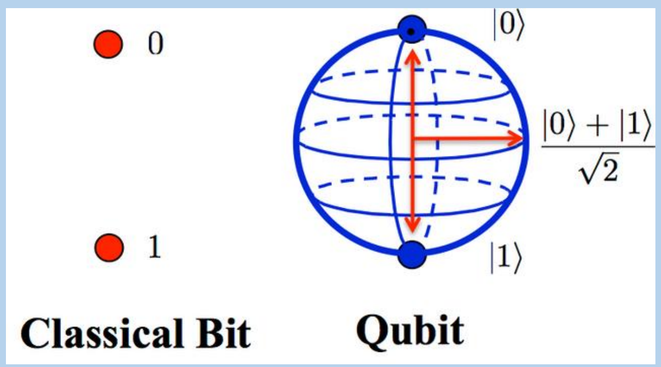

Fig 1. 양자 컴퓨터의 큐비트

부호 기반 암호

● 메시지에 의도적으로 에러 비트를 첨부하여 전송

● 신드롬 복호화 과정을 통해 NP-Complete 어려움의 난이도 확보, 양자 컴퓨터의 연산에도 안전

NIST 양자 내성 암호

● 2016년 NIST 양자 내성 암호 표준 공모전 개최

● Round 1, NIST에서 요구한 내성 암호 특성을 충족하는 64개의 양자 내성 암호 후보 선출

● Round 2, 제출된 양자 내성 암호 후보들에 대한 최적화 요구

● 총 26개의 공개키 암호 및 서명 알고리즘 선정

● 2022/2024 양자 내성 암호 표준화 완성으로 예상

● 양자 컴퓨터 시대에 대비한 양자 내성 암호에 대한 많은 관심과 신속한 연구가 필요

기반	공개키 암호/ 키 생성	서명
부호	Bike Classic McEliece HQC LEDAcrypt NTS-KEM ROLLO RQC	
격자	CRYSTALS-KHYBER Frondose LAC Newcome NTRU NTRU Prime Round 5 SABER Three Bears	CRYSTALS-DILITHIUM FALCON qTESLA
다변수 다항식		GeMSS LUOV MQDSS Rainbow
아이소제니	SIKE	
해시		SPHINCS+
제로 지식 증명		Picnic

Fig 2. NIST 양자 내성 암호 Round 2