양자 암호화 동향

(2021.10.28., 양자정보연구지원센터)

□ NIST 양자 암호화 표준

○ 배경

- 1994년 Peter Shor가 양자 컴퓨터를 이용해 인수 분해와 이산 로그 문제를 해결할 방법을 고안
- 이제는 현실이 된 양자 컴퓨터가 고전적인 암호 체계에 위협이 되어 양자 암호화의 필요성이 대두

○ 암호화 표준 구축 노력

- 미국 NIST(National Institute of Standards and Technology)는 2016년부터 시작되었던 양자 암호화 표준을 결정하기 위한 연구를 2021년 말 마무리할 것으로 밝힘
- 69개의 제출물 중 현재 7개의 알고리즘까지 좁혀진 상태
- NIST의 표준에 앞서 일부 회사들은 양자키 배포(QKD)를 포함한 몇몇 양자 암호화 체계를 실험 중

□ 양자 암호화 경쟁

○ 중국에서 양자키 배포가 적용된 거리 4,600km에 달하는 통합 양자 네트워크를 구축

○ 유럽연합 행정부(EC)는 유럽 연합 전역의 주요 기반시설을 양자 암호화가 적용된 보안 네트워크(Euro Quantum Communication Infrastructure, EuroQCI)로 연결하려고 함

- 양자 암호화 보안 네트워크를 위한 기업 연합체가 결성되었고, 양자키 배포를 지원하는 지상파 세그먼트를 설계
- 2024년까지 시범운영하고 2027년까지 초기 운영서비스를 시작하는 것이 목표

□ Arqit 양자 암호화 위성

ㅇ 양자 암호화 컨소시엄

- 양자 암호화 기업 Arkit이 영국, 미국, 일본, 캐나다, 이탈리아, 벨기에 및 오스트리아를 대표로 하는 양자 암호화 컨소시엄 구성
- 2023년 영국에서 양자 암호화 위성 발사 목표

ㅇ Arqit의 양자 암호화 기술

- FQS(Federated Quantum System)라는 양자 암호화 기술 사용
- 현재 많이 테스트 중인 양자키 배포(QKD) 방식은 광자가 가지는 민감성으로 인한 에러 발생 비율이 높아 장거리 통신에 부적합하며 전용 하드웨어 장비가 필요로 함
- FQS 방식의 경우 특별한 하드웨어가 필요 없는 양자 클라우드 형태로 폐쇄적인 플랫폼을 통해 동맹국 간의 상호 운용이 가능한 형태

ㅇ BT, Sumitomo Corporation, Northrop Grumman, Leonardo, QinetiQ Space NV, qtlabs 및 Honeywell가 협력

ㅇ 이탈리아, 벨기에, 오스트리아 및 아일랜드를 제외한 EU(유럽연합)은 EuroQCI라는 유럽 양자 통신 네트워크 개발 계획에 참여하고 있으므로 Arqit FQS에 참여할지 불분명

(원문)

1. https://www.theverge.com/22523067/nist-challenge-quantum-safe-cryptography-computer-lattice
2. https://www.nature.com/articles/s41586-020-2401-y
3. https://www.computerweekly.com/news/252501687/European-led-consortium-investigates-quantum-cryptography
4. https://www.zdnet.com/article/quantum-key-distribution-could-seal-the-5g-rift-with-china-say-engineers/
5. https://arqit.uk/
6. https://spacenews.com/governments-ally-for-federated-quantum-encryption-satellite-network/
7. https://www.electronicsweekly.com/news/business/quantum-encryption-via-satellite-2021-06/
8. https://www.kisa.or.kr/
9. https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci