양자통신 소·부·장 기술검증 및 양자통신검증센터

박상길†, 김인규*, 남기동, 주정진*

한국전자통신연구원(ETRI) 입체통신연구소 ICT시험연구센터

*한국전자통신연구원(ETRI) 인공지능컴퓨팅연구소 양자기술연구본부

wideideal@etri.re.kr

Technology Verification of Small-Scale, Components and Devices in Quantum Communication and the Quantum Communication Verification Center

Sangkil Park, Ingyoo Kim, Kidong Nam, Jungjin Ju

ETRI

요 약

본 논문은 전국망 단위로 구축된 개방형 양자테스트베드와 이를 이용한 양자통신, 양자암호통신의 기술검증 및 관련 기관의 기술력 향상을 지원하는 ETRI의 양자통신 소·부·장 기술검증 및 양자통신검증센터의 임무를 기술한다. 양자통신 소·부·장(소재·부품·장비) 기술검증 및 양자통신검증센터는 양자기술의 상용화와 산업화를 위해 핵심 부품과 장비의 성능, 안정성, 보안성을 평가하는 인프라로, 국내외 기술 경쟁력 강화와 공급망 안정화에 기여하고 있습니다.

Ⅰ. 서 론

양자 키 분배장비(QKD)는 송신자와 수신자(예: Alice와 Bob) 사이에 양자역학의 원리를 이용해 절대적으로 안전한 대칭키(비밀키)를 생성하고 분배합니다. 이렇게 분배된 대칭키는 ARIA-256등과 같은 고성능 대칭키 암호 알고리즘에 적용되어 실제 통신 데이터의 암복호화에 사용됩니다. QKD 로 생성된 키는 정보이론적으로 완전한 비밀성을 보장하기에 공격자가 무한한 계산능력을 가지고 있다 하더라도 양자역학적 특성(복제 불가능성, 측정시 산태 변화 등) 때문에 키를 탈취(MITM : Man in the Middle attack)할 수 없다는 의미이다. QKD에 의해 분배된 키는 OTP(One-Time Pad) 방식으로 사용되며 메시지 자체도 안전하게 관리된다.

양자통신은 송수신자 사이에 양자물리학적 특성에 기반한 양자 얽힘현상을 전달하는 양자 네트워크기술로서 양자 얽힘 특성을 이용하여 양자 노드 간에 양자 상태를 직접 교환할 수 있는 기술을 의미한다.

Ⅱ. 본론

양자암호(Qunatum Cryptography)와 양자 키 분배(QKD) 기술이 개발됨에 따라, 적은 수의 광자를 이용한 양자통신이 시작되었습니다.

본 논문에서는 양자통신과 양자암호통신에 대한 ETRI의 기술지원 분야와 관련된 세부내용을 제시하고 있다.

양자통신은 단순히 실현 가능성을 증명하는 단계를 넘어 캠퍼스 간, 도시 간, 국가 간, 나아가 지상과 우주를 연결하는 형태로 발전하고 있습니다. 이미 여러 국가에서 상용망 서비스가 시작되고 있습니다. 양자컴퓨팅 기술과 더불어 양자 정보를 처리하고 교환할 수 있는 양자인터넷, 양자정보를 저장하는 양자 메모리 및 네트워크 노드 사이에서 원거리 통신을 가능하게 하는 양자중계기(Quantum Repeater) 등이 연구개발되고 있습니다.

양자통신과 양자인터넷에 사용되는 소재·부품·장비로서 양자 메모리(Quantum Memory), 양자난수 발생기(QRNG), 단일광자 검출기(SDP), 결맞음 광 검출기(Coherenet Photodetector), 양자광원(Quantum Source), 양자간섭계(Quantum Interferometer)등이 새로운 시장을 형성해가고 있습니다.

양자통신 기술에 적용되는 양자물리학적 기술들은 광자를 기반으로 하며, 한국전자통신연구원(ETRI)에서는 수십 년간 진행해 온 광통신 소자 연구 인프라와 양자 통신 및 양자네트워크 연구경험을 바탕으로 초기 상용품 시험에 필요한 양자통신 실험 설비를 구축하고 성능 측정, 기술 컨설팅 등 양자기술 개발을 위한 기술지원으로헛허 양자통신 소·부·장 기술검증 OpenLAB을 통해 기술검증을 지원한다.

- ○ 성능평가 : 양자간섭계, 양자광원, 편광조절기 등 양자통신 부품과 단일 광자 검출기(SPD)등 장비 및 관련 핵심부품의 양자특성을 측정
- ○ 양자통신 기술개발 컨설팅

양자암호통신기술은 양자기술 중 가장 빠르게 상용화가 진행된 분야로, 0과 1이 중첩되는 양자역학 원리를 이용하여 도청, 감청 및 해킹이 원천적으로 불가능하므로 미래 양자컴퓨터가 상용화되어도 가장 안전한 통신 환경을 제공합니다. 보안인증제도는 국정원이 운영하는 제도로, 국가기관과 공공기관이 정보보호시스템과 네트워크 장비를 도입하여 운영하기 위한 안정성을 확인하는 제도입니다. ETRI는 양자통신검증센터를 통하여 다음과 같은 기술검증 및 컨설팅을 지원합니다..

- ○ 기능 검증 : 국내 표준인 '양자키 분배망 도입·운영 지침'기반의 양자키분배장비(QKD), 양자키관리장비(QKMS), 양자통신암호화장비(QENC)에 대한 기능검증
- ○ 보안성 검증 : 국가정보원의 보안기능확인서 제도 중 양자암호통신장비 제품군 3종(QKD, QKMS, QENC)에 대해 '국가용 보안요구사항'을 만족여부를 검증 및 컨설팅 서비스 제공
- ○ 상호호환성 검증 : 다양한 제조사의 장비가 표준을 준수하며 이종의 장비가 서로 연동하기 위한 프로토콜 준수여부를 개방형 양자테스트

베드를 이용하여 검증

Ⅲ. 결론

본 논문에서는 개방형 양자테스트베드와 이를 기반으로 구축되는 양자암호통신, 양자통신 기술에 대해 표준기반의 기술 신뢰성 확보와 보안성 검증을 통해 국내 양자산업의 기술력 향상과 로벌 경쟁력 강화에 핵심 역할을 수행하고 있으며, 정부·연구기관·민간의 협력 체계가 더욱 강화될 전망입니다.

ACKNOWLEDGMENT

본 사업은 과학기술정보통신부와 한국지능정보사회진흥원(NIA)의 “양자기술 시험검증 및 컨설팅 지원”사업에 속하며 양자기술의 산업화를 촉진하고 시장선점 및 상용기술 개발을 지원하기 위해 테스트베드 구축과 양자기술 시험·검증 등을 지원하기 위한 목적의 일환으로 수행함.

약 어 정 리

QKD : Quantum Key Distribution

QKDN : Quantum Key Distribution Network

PQC : Post Quantum Cryptography

QRNG : Quantum Random Number Generator

SPD : Single Phton Detector

참 고 문 헌

[1] S. -K. Park, Y. Lee, Y. Jeong, J. J. Ju, K. -D. Nam and S. Park, "A Functional Verification Study of Quantum Key Distribute Networks and Services with a Trusted Node applied in KOREN," 2022 13th ICTC, pp. 1663-1666

[2] 김인규, 주정진, “양자통신 테스트베드 동향”, Electronics and Telecommunications Trends. Vol. 39, No. 5, Oct 2024, pp. 86-97