양자키분배를 위한 양자네트워크 기술 동향 연구

석우진, 이원혁
한국과학기술정보연구원
wjseok@kisti.re.kr, livezone@kisti.re.kr

A Study on Quantum Network Technologies for Quantum Key Distribution

Woojin Seok, Woohyuck Lee
Korea Institute of Science and Technology Information

요 약

본 논문에서는, 양자키분배(QKD)를 위하여 사용되는 네트워크 기술들을 조사하고 분석하고자 한다. 양자키분배 기술은 양자컴퓨터의 등장으로 발생한 양자위협에 대한 대응기술로써 대칭 암호키를 안전하게 전달하는 기술이다. 단일광자를 전달하는 방식 및 양자얽힘 현상을 활용하는 양자네트워크 방식들이 사용될 수 있다. 양자키분배를 네트워킹 문제를 해결하기 위한 이러한 양자네트워크 기술들을 분석하고자 한다.

Ⅰ. 서 론

2020년에 보고된 미국 에너지부의 양자인터넷 청사진 전략에서는 양자물리현상을 기반한 양자네트워킹 기술의 향후 적용대상 분야를, 양자암호통신과 분산양자컴퓨터, 2가지로 구분하였다[1]. 양자암호통신(“Secure Quantum Communication”)은 양자적 특성을 활용하여 안전하게 암호키를 전달하는 방식으로써 양자컴퓨터의 출현으로 인한 양자위협에 대응하기 위한 기술이다. 이러한 양자암호통신에서 대칭 암호키를 안전하게 전달하는 기술로써 양자키분배(QKD) 기술이 사용된다. 이를 실현하기 위해서는, 단일광자를 전달하는 기술이 우세하며 하드웨어 장비로 구현되어 실제 적용하는 수준이다. 하지만 궁극적으로는 양자얽힘 현상을 이용한 양자중계기 기술 실현을 지향하고 있다. 양자얽힘 교환을 통하여 양자정보를 전달하는 기술은 또한 분산양자컴퓨터(“Upscaling Quantum Computing”)의 핵심기술로도 사용될 것이다. 본 논문에서는 양자키분배 네트워크를 위하여, 단일광자 기술을 사용하여 정보를 전달하거나, 양자얽힘 현상을 이용하여 정보를 전달하는 기술들의 동향을 분석하고자 한다.

Ⅱ. 양자키분배를 위한 네트워킹 기술

양자컴퓨터의 출현으로 정보통신의 기반이 되는 암호통신 자체가 위협을 받게 되었다. 이를 양자위협이라고 하며, 이에 대한 대응기술로써, 양자물리현상을 정보통신에 적용한 양자암호통신 기술이 발전하게 되었고, 양자키분배(QKD)기술은 양자키를 안전하게 전송하는 양자암호통신 기술 중 하나이다. 이러한 양자키분배를 위하여 사용되는 네트워킹 기술을 양자적 특성을 기반으로 단일광자 전달 방식과 양자얽힘교환(entanglement swapping)으로 분류할 수 있겠다.

Fig.1. Normal(좌) and and Single Photon(우) Light Source

단일광자 전달 방식은 Fig.1 처럼 광원이 다중 광자를 방출하게 되면 도청자는 그 중 일부 광자를 몰래 빼내어 신호를 도청하는 공격(Photon Number Splitting Attack)이 가능하지만, 단일광자를 사용하면 도감청을 원천적으로 차단하는 기술이다. 단일광자 기술을 실현하기 위해서 각 노드간 단일광자 송·수신을 연결하는 네트워크 인프라로써, 기존의 LASER 방식에 의한 광통신망이 아닌 전용의 광케이블 인프라 구축이 필요하다. 양자얽힘 현상을 사용하는 네트워킹 기술은 단일광자 전달 방식보다 기술 구현의 난이도가 높은 것으로 인식된다. 송수신간의 양자얽힘과 중간노드를 통한 양자얽힘 스와핑 기술로써, 미국 LBNL 연구소를 중심으로 QUANT-NET 이름으로 진행된 사례가 있다[2].

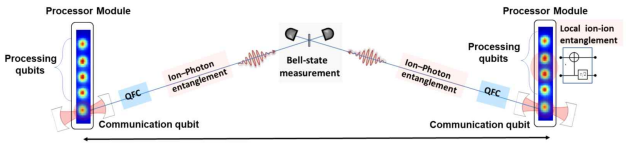

Fig.2. Entabglement Swapping

Ⅲ. 양자키분배 거리 확장 문제점 및 연구동향

단일광자기술은 실제 장비로 구현되어 적용되는 기술이다. Fig.3과 같이 실제 대전/오창에 설치되어 양자키분배를 구현한 사례이다. 두 개의 원거리 사이트에 각각 QKD 전송장비가 설치되며 이를 전용의 광통신 선로로 연결된다.

Fig.3. QKD network between Daejon and Ochang

하지만 문제는 70-80키로미터를 벗어나서 더 먼거리를 전송하기 위해서는 중간노드 역할의 장비가 필요하다. 하지만 양자 특성상 양자 정보는 저장이 되기 어려워서 네트워크 스위치나 라우터 같은 장비가 개발되어 있지 않다. 단일 홉 거리를 벗어나는 범위의 네트워킹을 위하여 2가지 정도의 기술적 제안이 있다. 첫 번째는, 위성QKD 기술을 사용하는 것이다. 단일광자 전송의 특성상 70-80킬로미터를 벗어나는 광역 전송을 위하여 위성을 사용한다. QKD 장비를 탑재한 위성을 중심으로 원거리 사이트들이 QKD 전송을 실시하는 것이다. 대표적인 국가사례로 중국은, 현재까지 두 개의 위성을 사용하여 양자네트워크를 구성하고 있으며, 중국내 다수의 도시간의 피어-투-피어 양자네트워크를 구성하였다. 두 개위성과 기존 광선로기반 통신을 혼용하여 전국망 수준의 QKD 네트워크를 구축하고 있다고 보고되고 있다. 싱가폴의 경우도, 위성을 사용하여 거리의 한계 문제를 해결하고자 한다. 싱가폴의 경우, 국가의 특성상 스타-토폴로지 방식의 단일홉으로 싱가폴 국가를 양자 네트워크로 연결이 가능하나, 국제간 양자네트워킹을 위해서 위성을 사용하여 거리의 한계 문제를 해결하려고 한다. 특히 싱가폴의 경우, 자국기업에서 제작한 위성QKD 기술을 사용하고자 하며, 산학연 연계한 기술협력 체제가 우수하게 구축되어 있다. 일본의 경우도, 중기적인 계획으로 위성을 활용한 QKD 통신을 포함하고 있다. 두 번째는, 신뢰노드(Trusted Node)를 포함하여 QKD 네트워크를 연장하는 것이다. 이는 완벽한 QKD 네트워크라고 할 수는 없지만, 양자위협에 대응하는 차원으로 QKD 네트워크 구축하여, 강력한 보안망 수준을

구축하는 차원에서 설득력이 있다.

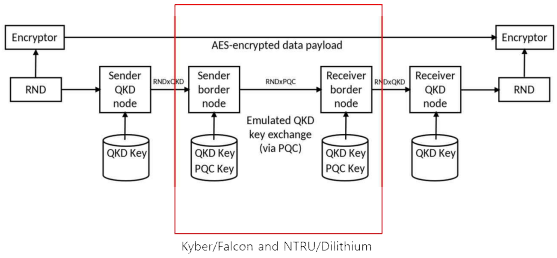

Fig.4. Using PQC to Interconnect QKD Networks

유럽의 독일, 폴란드, 스페인의 경우, 각국별 QKD 네트워크가 존재하고 이를 상호 연결하기 위한 연구를 하고 있다. 이를 통하여, 각각의 단일홉 기반 QKD 네트워크 거리 한계를 극복하고자 한다. 중간노드인 독일 사이트에서는 PQC 암호를 사용하여 보안/암호 관점에서 충분히 높은 수준의 암호로 인캡슐레이션 하는 방식을 사용하며 QKD 양자키를 전달하는 신뢰노드 방식의 하이브리드 방식으로 구현하였다. 이는 양자위협의 대응이라는 차원에서 충분히 높은 수준의 PQC 암호를 사용하여 양자네트워크를 구성하는 것이라 할 수 있겠다. PQC 암호방식으로는 Kyber/Falcon 및 NTRU/Dilithium 알고리즘을 사용하였으며, 이는 미국 NIST에서 제공하는 PQC 암호표준안을 수용하는 것이다. 비록 PQC 암호체계를 혼용하여 QKD 네트워크 연장에 사용하는 것이 완벽하게 종단간 양자적 특성을 기반한 보안망이라고 할 수는 없으나, 기술적으로 충분히 우수한 수준의 보안망 구축이라는 의미 부여는 가능한 것으로 판단된다. 일본도 유럽과 유사한 방식을 사용하지만, 하나의 중간노드에서 양자키를 전환하는 방식으로 거리를 연장하는 방식을 취하고 있다[3]. 유럽 방식처럼 완전한 QKD 네트워크 라고 할 수는 없지만, 암호 네트워크 관점에서 단일노드 안에서 기밀성을 유지한 채로 키를 전달한다는 점에서 충분히 높은 수준의 보안망 구성의 의미는 있다고 하겠다.

IV 양자키분배 회선 전용 문제점 및 연구동향

양자키분배 네트워크에서는 인프라는 Fig 5에서 보듯이 일반 네트워크 회선과 양자채널 회선을 요구하며, 이때 사용되는 양자채널 회선은 전용의 광케이블이 사용되어야하며, 이는 광케이블을 전용사용으로 인한 경제적 비효율성 문제를 포함한다. 그래서 QDK 양자암호통신은 국방, 정부기관 등 공공의 특수 목적이 아닌 상업적으로 접근하기가 어려운 인프라 구축 기술이라 할 수 있다. 현재 대부분의 구현된 QKD 기술들은 단일광자 검출기를 통해서 구현된 QKD 네트워크들이 주를 이루며 기술적으로는 DV QKD(Discrete Variable Quantum Key Distribute)에 해당하며, 이는 광자의 이산적 특성을 사용한다. 반면에, CV QKD(Continuous Variable Quantum Key Distribute)는 빛의 연속적인 진폭·위상 변화를 사용하여 양자 키를 분배하는 기술로서, 빛의 연속적인 물리량(광장의 진폭과 위상)을 이용하며, 연속적인 확률 분포(Continuous Variable)를 가진다. 기존 통신 인프라와 호환성이 좋아 차세대 양자보안 통신망 구축에서 중요한 역할을 할 수 있는 방식이다. 즉, 전용 광섬유만을 요구하지 않고, 일반적으로 사용하는 도심·메트로망의 WDM(파장분할 다중화) 광케이블 위에 다른 채널과 함께 공존할 수 있다. 이러한 CV QKD 기술을 사용하면 광케이블을 전용으로 사용하는 비용문제 해결이 가능할 것이다. 미국 노스웨스턴 대학교는 미국 연구망 인프라(Starlight)에서 양자 얽힘을 이용한 정보전달을 성공적으로 시연하였다 [4]. 이는 인터넷 트래픽이 이미 흐르고 있는 광섬유 케이블 위에서 양자 상태를 텔레포트함으로써, 기존 통신망과 공존하는 양자 통신 기술의 실현 가능성을 보여준 중요한 연구이다. 미국 연구망 인프라(Starlight) 연구 시설을 포함한 Chicago Quantum eXchange (CQC)의 연구 인프라를 활용하여, 기존의 인터넷 트래픽이 흐르는 광섬유 위에서 양자 텔레포테이션을 가능하게 함으로써, QKD 네트워크 역시 광케이블을 전용으로 사용하는 비용 문제를 해결할 수 있는 연구로 평가할 수 있다.

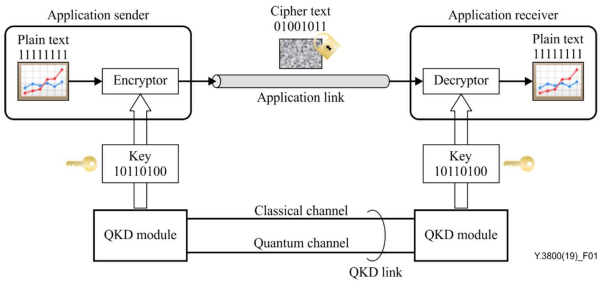

Fig.5. QKD Network Standard (ITU)

V 토의 및 결론

양자통신에 기술적 한계 중 하나로 제시되고 있는 거리적 한계는, 양자통신에 사용되는 BSM(Bell State Measurement) 기술이 아직 전반적으로 확산되지 않은 상태에서 단일광자 방식의 QKD 네트워크가 1홉 수준으로 한정되어 있기 때문이다. 이러한 거리적 한계를 극복하기 위하여 양자중계기 기술이 지속적으로 연구되고 있다. 특히, 일본에서는 도시바를 포함한 산업계가 기술 구현을 선도하고 있다. 양자중계기의 중요요소로써, “bell pair generating” 요소와 “quantum memory” 부분에서 아직 완성도가 미비한 것으로 보고되고 있으나, 개발의 정도가 중기단계 이상의 수준으로 평가된다. 또한 QKD 네트워크의 거리 문제를 해결하기 위하여 현실적인 대안으로써 위성 QKD 기술이 거론되고 있는 상황에서, 싱가폴 역시 산업계가 위성QKD를 실제 구현하여 선도하고 있으며, 싱가폴 SpecQtral 기업이 대표적이다. 기술적으로, 양자키분배를 위한 양자네트워크 기술에서 거리의 한계를 극복하기 위하여 위성QKD를 사용하는 중기적 방안과 양자중계기를 개발하는 장기적 방안으로 요약할 수 있다. 또한, 광케이블 전용 문제를 해결하기 위하여 전용 광케이블이 아닌 사용중인 광케이블을 활용하는 기술들의 기술 성숙도가 초기를 벗어나는 수준으로 평가된다. 이러한 기술들을 상호 연계하여 국가규모의 양자키분배 네트워크 형성이 가능할 것으로 판단된다.

ACKNOWLEDGMENT

이 논문은 2025년도 한국과학기술정보연구원(KISTI)의 기본사업으로 수행된 연구입니다. (국가연구 인프라 기반 양자암호통신망 기술개발, K-25-L05-M02-C02-S01)

참 고 문 헌

[1] “From Long-distance Entanglement to Building a Nationwide Quantum Internet”, Report of Doe, Quantum Internet Blueprint Workshop, Feb.5-6, 2020

[2] “QUANT-NET: A testbed for quantum networking research over deployed fiber”, Inder Monga et al., QuNet '23, NY USA, September 10 - 14, 2023

[3] “Interoperable key relay between heterogeneous QKDNs”, Mayuko Koezuka et al., Qcrypt 2023

[4] “Quantum teleportation coexisting with classical communications in optical fiber”, Jordan M. Thomas et al., Journal of Optica, Vol. 11, Issue 12, pp. 1700-1707, 2024