인터도메인 양자암호통신망 연동을 위한 Trusted Bridge 양자키관리 시스템 개발

심규석, 이원혁
한국과학기술정보연구원
{kusuk007, livezone}@kisti.re.kr

Development of a Trusted Bridge Quantum Key Management System for Inter-Domain Quantum Key Distribution Network Interconnection

Kyu-Seok Shim, Wonhyuk Lee
Korea Institute of Science and Technology Information

요 약

최근 양자암호통신 분야의 세계적인 투자와 장비의 발전으로 다양한 벤더사에서 QKD(Quantum Key Distribution) 장비를 제작하고, 기능을 추가하고 있다. QKD는 같은 벤더사간의 키를 분배하는 방식으로 다른 벤더사의 QKD와 같이 사용할 수 없기 때문에 각 벤더사마다 도메인이 정해진다. 따라서 양자암호 통신망 도메인은 QKD 벤더사의 종속되며, 서로 다른 도메인의 양자암호 통신망을 연결하는 것은 많은 어려움이 있다. ETSI, ITU-T 등 다양한 표준들이 발표되며 도메인간의 연결을 위한 방법론이 제시되어 있지만, 현실적인 어려움은 해결하지 못하였다. 본 논문은 서로 다른 도메인의 양자암호 통신망 (QKD Network)를 연동하기 위해 Trusted Bridge 양자키관리 시스템을 제안한다. 제안된 시스템은 서로 다른 양자암호통신망(QKDNi)을 연결하여 양자암호통신 망 확장성을 높이고, 비용 절감을 가능하게 한다. 또한 도메인 간 안전한 키 전달을 위해 별도의 키 관리 구조를 구축하여 QKD 기반 암호화 기법을 활용하여 전송 구간의 보안을 강화하였으며 ETSI GS QKD 020 표준을 적용하여 상호운용성을 확보하였다. 제안하는 시스템을 통해 향후 다양한 양자암호통신 환경에서 서로 다른 도메인 간 연동을 위한 핵심 기술로 활용될 수 있을 것으로 기대된다.

Ⅰ. 서 론

최근 양자암호통신 분야의 많은 투자와 장비의 발전으로 다양한 벤더사에서 양자암호장비를 제작하면서 QKD 장비는 다양해지고 있다. QKD는 양자역학적 원리를 이용한 대칭키를 분배하는 장비로 프로토콜 및 키를 분배하는 방식 등의 원인으로 동일한 장비에서 키를 분배하고 있다. 따라서 다른 종류의 QKD 장비간의 키를 분배할 수 없기 때문에 같은 종류의 QKD 장비마다 도메인이 정해진다. 따라서 양자암호 통신망 도메인은 QKD 장비에 종속되며, 서로 다른 QKD 장비로 하나의 도메인을 구성하는 것은 많은 어려움이 있다[1].

이를 해결하기 위해 ETSI, ITU-T 등 다양한 표준기관에서 인터도메인 연결을 위한 표준을 발표하였으며, 서로 다른 양자암호 통신망 도메인간의 연결을 위한 방법론을 제안하였지만, 현실적인 어려움은 해결하지 못하였다. ETSI GS QKD 020 표준은 서로 다른 양자키관리 시스템에게 키를 전달할 수 있는 메시지 포맷, 정보 등에 대해 정의하였고, ITU-T Y.3810 문서에서는 다양한 형태의 인터도메인 연동 구조를 제안하였다[4].

Y.3810 문서에서 제안한 구조 중 Interworking Functions(IWFs)구조는 서로 다른 도메인과 별도의 제 3지역에서 키를 전달하는 방식이다. 제 3지역은 물리적 보안경계를 통해 키를 안전하게 전달하는 구조를 가진다. 해당 구조는 EuroQCI 등 통합적인 양자암호통신망을 구성하는 네트워크에서 사용하고 있다. 그러나, 양자키 전달을 위해 별도의 구역을 마련하고 물리적 보안경계로 사용자의 출입등을 관리해야하는 어려움이 있다.

다른 구조로는 Gateway Functions(GWFs)으로 각 도메인 사이에 QKD를 설치하여 해당 구간을 양자 대칭키로 암호화하여 키를 전송하는 방법이다. 그러나 연결되는 구간의 양자키관리 시스템은 서로 다른 QKD와 연결이 가능해야하는 시스템적인 한계가 존재한다.

본 논문에서 제안하는 Trusted Bridge 양자키관리 시스템은 두 도메인 사이에 QKD 장비와 양자키관리 시스템을 설치하여 두가지 구조의 문제를 해결한다. IWFs의 구조에서 제 3지역을 설정하고 물리적 보안경계를 관리해야하는 단점을 해결하고, GWFs의 구조에서 서로 다른 QKD와 연동해야하는 양자키관리 시스템의 한계를 해결한다. 본 시스템을 통해 향후 다양한 양자암호통신 환경에서 인터도메인을 연결해야하는 상황의 확장성을 높이기 위한 핵심 기술로 활용될 것으로 기대된다.

Ⅱ. 본론

본 논문에서는 인터도메인 양자암호통신망 연동을 위한 ITU-T 표준 구조의 한계를 극복하고, 양자키관리 시스템 간의 인터페이스에는 ETSI GS QKD 020 표준을 사용하여 상호운용성을 확보하며 안전한 양자키관리 시스템 구조를 제안한다[5].

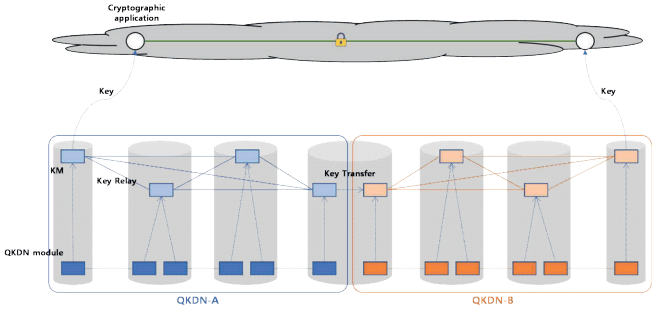

그림 1 ITU-T Configuration for QKDNi with IWFs

ITU-T 표준에서 제안한 구조 중 그림1은 IWFs 구조를 간략하게 표현

하였다. 인터도메인 QKDN을 연결하기 위해 IWFs 구조는 제 3지역을 설정하여 양자키관리 시스템간에 키를 전송한다. 또한 해당 구역에서 키관리 시스템간의 양자 안전 암호화가 이루어지지 않기 때문에 물리적 보안 경계로 설정하여 관리자가 직접 해당 구역을 관리해야 한다. 따라서 인터도메인을 연결하기 위한 구간이 있을 시 물리적 공간 자원과 인력 자원이 소비된다.

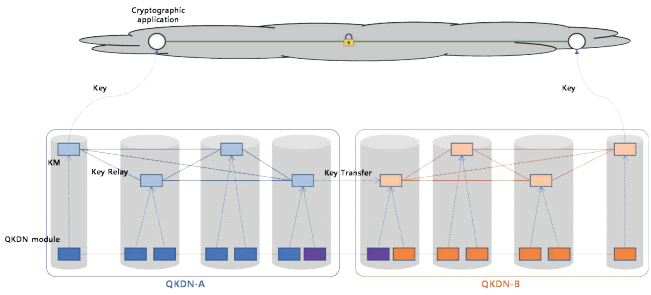

그림 2 ITU-T Configuration for QKDNi with GWFs

그림2는 ITU-T 표준에서 제안한 GWFs 구조를 간략하게 표현하였다. GWFs 구조는 IWFs 구조와 다르게 별도 구역을 설정할 필요가 없기 때문에 IWFs의 단점을 해결할 수 있다. 다만 각 도메인의 키관리 시스템이 이기종 양자키분배장치 연동 기능이 필수적인 요소이다. 양자키관리 시스템과 양자키분배장치간의 명확한 표준이 설정되지 않은 시점이고, 이미 상용화된 제품은 해당 기능을 다시 추가해야하는 시스템적인 한계가 존재한다.

ITU-T 표준의 GWFs구조와 IWFs구조의 공통적인 한계는 각 도메인간, 각 벤더사간의 정보 교환을 하기 어렵다. 즉, QKDN-A와 QKDN-B가 다른 통신사업자라면 각 통신사업자의 정보를 직접적으로 교환해야한다. 또한 각 벤더사간의 정보 또한 직접적으로 교환해야한다. 이러한 정보 교환은 통신 사업자간의 보안 문제와 각 벤더사간의 재산권 문제가 발생할 수 있다. 또한 통신사업자, 벤더사간에 필요한 정보가 다를 수 있기 때문에 정보 교환의 문제도 해결해야한다.

따라서 본 논문에서 제안하는 Trusted Bridge 양자키관리 시스템은 두 구조의 단점을 모두 해결한다. 그림 3은 Trusted Bridge 양자키관리 시스템을 통한 인터도메인 양자암호통신망 연동 구조를 간략하게 표현한다.

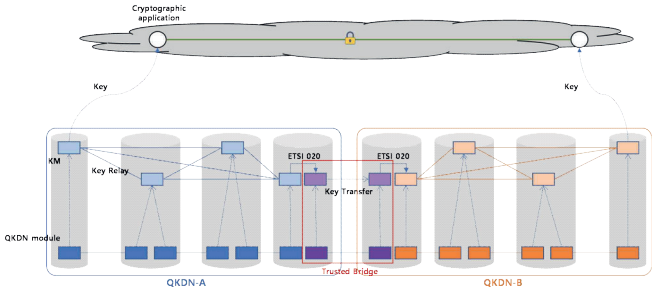

그림 3 Configuration for QKDNi with Trusted Bridge

제안하는 Trusted Bridge 양자키관리 시스템은 그림과 같이 연동하는 구간에 설치되는 QKD 시스템이다. Trusted Bridge 구조는 각 도메인 연결 구간에 양자키관리 시스템 쌍과 QKD 시스템 쌍을 브릿지 형태로 구성한다. 각 도메인과 연결되는 양자키관리 시스템과 Trusted Bridge는 ETSI 020 표준 인터페이스를 이용하여 키를 전달하며, 해당 구간은 이미 물리적보안경계로 관리되고 있기 때문에 안전한 구간으로 가정한다. 따라서 연동된 각 도메인의 양자키관리 시스템은 ETSI 020 표준 인터페이스만 적용하면 본 시스템을 통해 인터도메인 양자암호통신망 확장이 가능하다.

위의 구조로 인터도메인을 연동하게 되면 IWFs 구조의 별도 구역이 불필요하다. 또한, GWFs 구조의 키관리 시스템 기능 중 필수로 이기종 QKD 연동 기능이 없어도 표준으로 정의된 이기종 키관리 시스템 연동 기능만 지원하면 인터도메인 양자암호통신망을 연동할 수 있다.

향후 본 시스템을 KREONET(Korea Research Environment Open NETwork)의 양자암호통신망에 적용하여 다양한 QKD 장비와 연동할 수 있는 확장성 높은 양자암호통신망을 구성할 계획이다[2,3]. 또한 각 도메인의 토폴로지 정보를 상대 도메인에서 알 수 없으므로 각 도메인의 Q-SDN-Controller에게 목적지를 입력하여 경로를 내려받는 구조도 적용할 예정이다.

Ⅲ. 결론

본 논문에서는 인터도메인 양자암호통신망 연동을 위한 Trusted Bridge 양자키관리 시스템을 제안했다. 제안하는 시스템은 기존의 인터도메인 양자암호통신망 연동 구조의 단점을 해결하였다. 또한 각 도메인을 연결하는 구간은 QKD키로 보안하여 양자안전성을 가지며, 양자암호통신망을 구성하는 양자키관리 시스템은 이기종 양자키관리 시스템 연동 표준만 적용하면 어떤 환경에서도 해당 시스템을 적용할 수 있는 확장성을 가진다.

향후 제안하는 시스템을 KREONET 양자암호통신망에 적용하여 다양한 QKD 장비로 구성된 양자암호통신망을 구성할 계획이며 Q-SDN-Controller간의 연동을 통한 효율적인 양자키 전달 방안을 연구할 예정이다.

ACKNOWLEDGMENT

이 논문은 2025년도 한국과학기술정보연구원(KISTI)의 기본사업으로 수행된 연구입니다. (과제번호: K25L5M2C2)

참 고 문 헌

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum Cryptography,” Rev. Mod. Phys., Vol.74, No.1, 2002, p.145

[2] 심규석, 김용환, 이찬균, 이원혁. “KREONET 양자암호통신 환경에서 양자키 관리 시스템을 위한 양자키 저장 관리 모듈 설계 및 검증”, 2022년 한국통신학회 동계학술대회

[3] Shim, Kyu-Seok, Yong-Hwan Kim, and Wonhyuk Lee. "A design of secure communication architecture applying quantum cryptography." Journal of Information Science Theory and Practice 10.spc (2022): 123-134.

[4] ITU-T Y.3800-series . Quantum key distribution networks -Applications of machine learning, July 2021.

[5] ETSI GS QKD 020 2023. Protocol and data format of REST-based Interoperable Key Management System API. Group Specification Draft v0.2.1. European Telecommunications Standards Institute (ETSI), Industry Specification Groups (ISG).