양자암호 전달 네트워크 기능구조

이지은 KT 융합기술원 인프라연구소 책임연구원
상의정 KT 융합기술원 인프라연구소 전임연구원
박춘걸 KT 융합기술원 인프라연구소 팀장

1. 머리말

2013년 6월 10일, 미국국가안보국(NSA)의 전 직원 에드워드 스노든은 가디언과 워싱턴 포스트를 통해, 미국 국가안보국과 영국 등의 정보기관이 전 세계의 개인 통화기록과 인터넷 사용 정보 등의 개인정보를 도청했다는 사실을 폭로했다. 이에 많은 나라에서 사이버 보안에 대한 심각성을 깨닫고, 자국의 기밀을 보호하기 위한 기술을 확보하고자 노력하고 있다.

현재 유망한 데이터 보호 기술 중 하나인 양자암호통신은 양자물리법칙에 기반을 두어 양자 키분배(QKD, Quantum Key Distribution) 장치로부터 비밀키를 제공받아 암호통신을 하는 기술이다. QKD는 단일 광자 큐빗(Single Photon Qubit)에 데이터를 실어 보내는데, 데이터가 도청될 경우 양자상태가 소멸하여 해킹 사실을 즉시 알 수 있다는 장점이 있다.

최근 양자암호통신에 대한 관심이 높아짐에 따라 ITU-T, ETSI 등 국제 표준기구에서는 QKD 장치뿐만 아니라 프로토콜, 네트워킹 기술 등 다양한 분야에 대한 표준화를 추진 중이다. 이에 국내에서도 양자암호통신 연구가 활발히 이루어지며 국내 고유표준 제정의 필요성도 높아졌다. 본고에서는 2019년 양자암호통신 관련 국내 고유표준으로 제정된 '양자암호 전달 네트워크의 기능구조'에 대해 소개하고자 한다.

2. 표준 개발 목적

이 표준은 QKD 기술과 전달(Transport) 네트워크 기술을 결합하여 종단 간 양자암호 기반 통신서비스를 제공할 수 있는 양자암호 전달 네트워크의 기능구조를 정의한다. 이를 통해 통신사업자, 장비 제조사, 솔루션 공급자 등 양자암호통신 산업 생태계를 활성화시키고 기술개발 및 관련 산업을 장려하고자 한다. 표준에는 <표 1>과 같은 고려사항들을 바탕으로 기능구조, 기능요소, 참조점, 서비스 절차, 보안 고려사항 등이 포함된다.

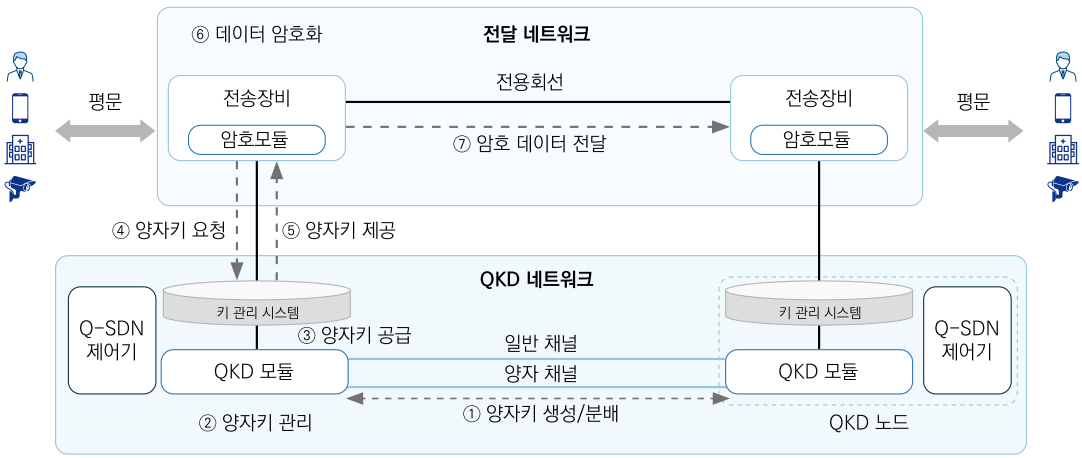
〈표 1〉 양자암호 전달 네트워크 고려사항

고려사항	내용
보안성(Security)	QKD 네트워크는 기존의 데이터 네트워크와 보안적으로 분리된 환경에서 운영되어야 한다. 특히, 양자키를 생성하는 QKD 모듈은 기존 데이터 네트워크에서의 어떠한 직접적 접근도 허용하지 않아야 한다.
효율성(Efficiency)	양자암호 전달 네트워크의 기능요소들은 기존 데이터 전달 네트워크의 전달효율을 최대한 보장할 수 있도록 구성되어야 한다.
투명성(Transparency)	QKD 네트워크는 기존의 데이터 네트워크가 종단 간 양자암호통신을 위하여 필요한 양자키를 쉽게 획득할 수 있도록 개방화된 인터페이스(Open Interface)를 제공해야 한다.
상호운용성(Interoperability)	양자암호통신 산업의 활성화를 위해서 양자암호 전달 네트워크를 구성하는 하드웨어 또는 소프트웨어를 포함하는 다양한 장치들은 상호운용성을 보장할 수 있어야 한다.
강건성(Robustness)	안정적인 양자암호통신 서비스를 제공하기 위해 양자암호 전달네트워크에서의 장애와 실패에 대한 탐지 및 회복에 필요한 관리 및 제어에 대한 요구사항을 고려해야 한다.
정책제어(Policy Control)	양자암호통신에 대한 Flow별 QoS 보장 및 과금 정책에 대한 제어/관리 기능이 제공되어야 한다.
확장성(Scalability)	기존 데이터 네트워크의 다양한 전달 메커니즘을 보장할 수 있도록 양자암호 전달 네트워크가 설계되어야 한다.

3. 표준의 개요

3.1 양자암호 전달 네트워크의 일반적 구조

양자암호 전달 네트워크에서 QKD 모듈[2]은 대국의 장비와 연결된 양자 채널[2]과 일반 채널을 통해 대칭형 양자 암호키(이하 양자키)를 생성 및 분배하고, 생성된 키 스트림(Stream)을 키 관리 시스템에 공급한다. 키 관리 시스템[1]은 QKD 모듈이 공급한 키 스트림을 수신하여 적절한 크기로 분할, 저장하여 양자키 제공을 준비한다. 전송장비의 암호 모듈(Encryption Module)은 전송장비로 들어오는 데이터 암호화를 위해 QKD 노드[3]의 키 관리 시스템에 종단 간 양자암호통신 서비스를 위한 양자키를 요청한다. 이후 키 관리 시스템은 Q-SDN 제어기[3]에게 암호 모듈이 요청한 조건에 적합한 양자키 자원 및 경로를 요청하여 구성하고 대칭형 양자키를 암호모듈에 제공한다. 전송장비의 암호모듈은 제공받은 키를 이용하여 데이터를 암호화하고 데이터 채널을 통해 대국으로 전달한다.



[그림 1] 양자암호 전달 네트워크

대국에서는 수신한 암호화 데이터를 사전에 설정된 대칭형 양자키로 복호화하여 전송장비로 전달한다.

3.2 전달 네트워크(Transport Network)와의 관계

양자암호 전달 네트워크는 QKD 네트워크와 기존의 전달 네트워크로 구성되며 종단 간 사용자에게 양자암호 기반 전용회선 서비스를 제공한다. 또한 전달 네트워크는 QKD 네트워크를 운영하기 위해 필요한 양자 채널과 일반 채널, 데이터 채널을 제공한다.

단일 광자 수준의 매우 약한 신호를 전달하는 양자 채널은 잡음에 민감하다. 이 때문에 전달 네트워크 관점에서 양자 채널의 특성을 고려한 양자암호 전달네트워크 구조를 설계하는 것이 필요하다. [그림 2]는 이러한 2가지 양자채널 운영구조를 제시한다.

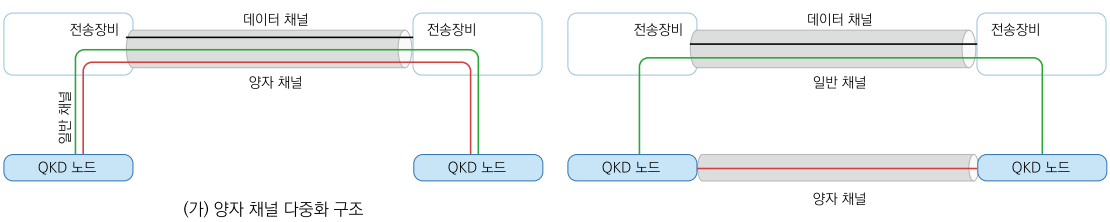
[그림 2] (가)의 양자 채널 다중화 구조는 양자 채널, 일반 채널, 데이터 채널을 모두 동일한 링크에 할당하여 서비스를 제공한다. 이와 같은 구조는 기존의 전달 네트워크를 이용해서 양자서비스를 제공하므로 추가 광케이블 투자 없이 양자서비스를 제공할 수 있는 이점이 있다. 그러나 데이터 채널의 강한 신호(약 1천만 배)로 인해 양자 채널에 잡음이 발생할 수 있어 데이터 채널과 양자 채널 간의 이격에 대한 고려가 필요하다. [그림 2] (나)의 양자 채널 전용 구조는 양자 채널을 위한 전용 링크를 추가적으로 할당하여 양자암호 서비스를 제공하는 구조이다. 데이터 채널의 강한 신호로 인한 양자 채널 잡음을 고려할 필요가 없는 장점이 있다.

3.3 양자암호 전달 네트워크 참조모델의 기능요소와 참조점

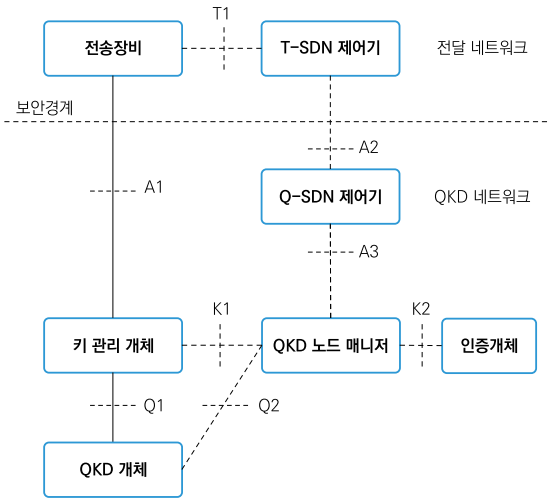
양자암호 전달 네트워크는 QKD 네트워크와 전달 네트워크로 구성된다. QKD 네트워크는 두 개 이상의 QKD 노드로 이루어지며 각각의 QKD 노드는 양자키의 관리, 생성, 전달을 수행한다. Q-SDN 제어기는 QKD 네트워크의 전체적인 자원 관리와 감시, 제어를 담당한다. 이와 더불어 양자 채널, 일반 채널을 포함하는 QKD 네트워크를 전달 네트워크에 구축, 운용하기 위한 기존 데이터 망 자원 할당 요청을 T-SDN 제어기와의 인터페이스를 통해 전달한다. T-SDN 제어기는 Q-SDN 제어기의 요청에 따라 전달 네트워크에 양자암호 전달 네트워크를 위한 자원을 할당한다. 양자암호 전달 네트워크 참조모델의 기능 요소와 참조점은 [그림 3]과 같다.

3.4 양자암호 전달 네트워크 구축모델

양자암호 전달 네트워크는 QKD 개체와 키 관리 개체가 분리된 구조와 통합된 구조, 두 가지 모델로 구축된다. QKD 개체와 키 관리 개체가 분리된 구조는 QKD 개체와 키 관리 개체가 독



[그림 2] 양자 채널 운영구조



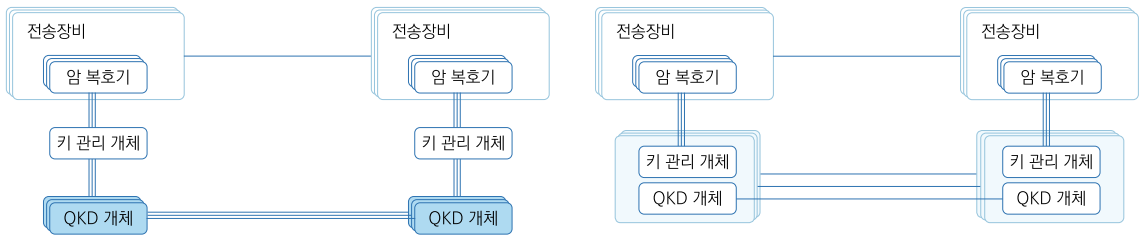
[기능 요소]

> 전송장비: 기존 데이터 망의 전송장치
> T-SDN 제어기: 기존 데이터 망의 네트워크 제어기
> Q-SDN 제어기: QKD 네트워크 제어기
> QKD 노드 매니저: QKD 네트워크 내 관리자
> 인증개체: 어플리케이션 인증
> 키관리개체: 양자암호키 관리
> QKD개체: 양자암호키 생성

[참조점]

> T1: 전달 네트워크 제어 인터페이스
> A1: 전송장비 암호화 모듈과 키관리 개체간 인터페이스. 키 요청/할당
> A2: QKD용 전달 네트워크 구성, QKD망 정보 전달을 위한 인터페이스
> A3: 노드별 자원/장애 정보 수집, 진단/제어 요청 인터페이스
> K1: 자원정보 수집, Key 라우팅 요청/제어 인터페이스
> K2: 양자키 제공에 대한 인증 처리 인터페이스
> Q1: 연속된 양자키 스트림 제공 인터페이스
> Q2: QKD 개체에 대한 정보 수집, 진단/제어 인터페이스

[그림 3] 양자암호 전달 네트워크 참조모델의 기능 요소 및 참조점



[QKD개체-키관리개체 분리 구축 모델] [QKD개체-키관리개체 통합 구축 모델]

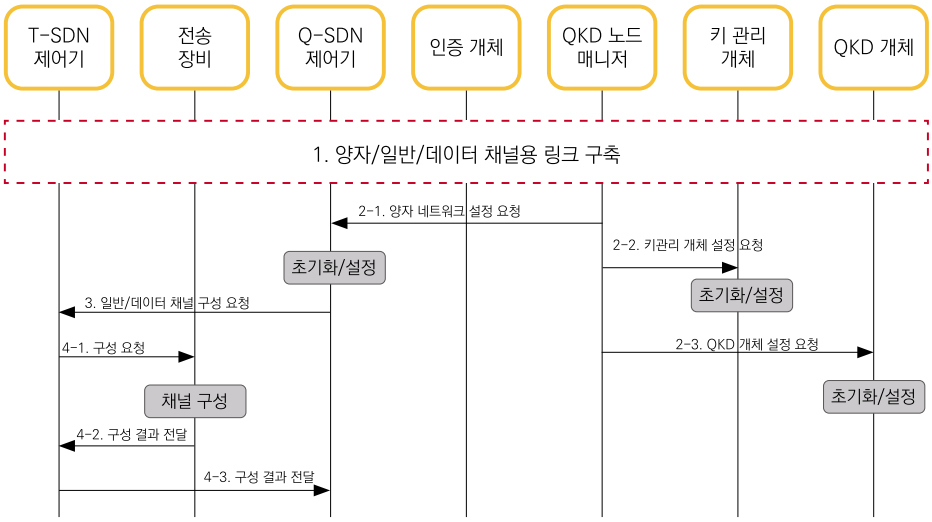
[그림 4] 양자암호 전달 네트워크 구축모델

립적으로 존재한다. 그래서 장비 제조사에 상관없이 개방형, 표준화된 인터페이스를 통해 다기종 QKD를 수용할 수 있다. QKD 개체와 키 관리 개체가 통합된 구조는 하나의 특정 QKD 장비와 키 관리 개체가 통합되어 있는 폐쇄적 구조로 기종 QKD 네트워크를 구성하기 어려우며 N:N 네트워크 또한 수용이 불가능하다.

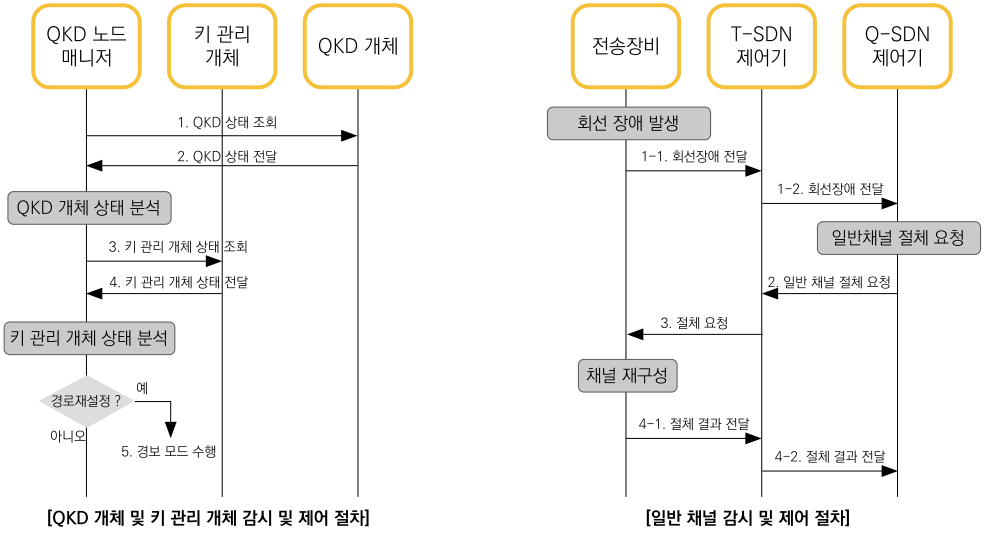
3.5 양자암호 전달 네트워크 서비스 절차

양자암호 전달 네트워크 운영하려면 네트워크의 구축, 관리, 제어 등을 포함하는 서비스 절차가 필요하다. [그림 5]는 양자암호 전달 네트워크의 구축 절차를 나타낸다. 양자암호 전달 네트워크를 구성하는 통신채널은 양자 채널, 일반 채널, 데이터 채널이 있으며, 최초 구축 시 QKD 모듈의 초기화 및 설정, 양자/일반/데이터 채널에 대한 구성이 필요하다. [그림 5]는 일반/데이터 채널로 전달 네트워크를 활용하는 경우로 가정한다.

QKD 개체나 키 관리 개체에 문제가 발생하면 QKD 노드 매니저[3]는 [그림 6]과 같이 QKD 개체나 키 관리 개체의 상태를 조회한다. QKD 노드 매니저는 전달받은 QKD 링크 정보를 바탕으로 경로 재설정이 필요한 경우, Q-SDN 제어기로 경로 재설정 요청 및 경보를 발생할 수 있다. 일반채널에 장애가 있을 경우에는 일반 회선 절체가 필요하며, Q-SDN제어기는 T-SDN 제어기로의 연동을 통해 절체를 요청할 수 있다.



[그림 5] 양자암호 전달 네트워크 구축 절차



[그림 6] 양자암호 전달 네트워크 감시 및 제어 절차

4. 표준 활용 방안

이 표준은 양자암호 전달 네트워크의 참조모델과 기능 요소, 구축 모델을 통해 양자암호 서비스를 제공하기 위해 고려해야 할 필수 요소를 제공한다. 따라서 기존 인프라 및 서비스를 절대보안이 가능한 양자암호통신 인프라로 전환하고자 하는 기획자 및 통신사업자뿐만 아니라 QKD 장비 및 암호모듈 제조사, 암호키관리/암호네트워킹 등 솔루션 사업자에게 참조모델로 활용될 것으로 기대한다. 특히 이 표준은 특정 장비 또는 사업자에 종속적이지 않고 개방형 인터페이스를 통해 상호 운용성을 보장할 수 있는 구조를 제공함으로써 개방형 산업생태계 활성화에 기여할 것이다.

5. 맺음말

양자 컴퓨터의 발달로 기존의 암호화 체계가 위협을 받아 이에 대응하는 기술로서 양자암호통신 인프라가 떠올랐다. 그러나 고가의 장비, 전송 거리 제약, 낮은 암호키 생성 속도 같은 단점을 극복하기 위한 요소기술 개발이 필요하다. 또한 요소기술들을 시스템화하고 시스템 간 상호 운용성, 보안성 확보를 위한 표준화 기술개발도 지속돼야 한다.

이를 위해 최근 우리나라에서도 국가 차원의 양자암호통신 기술개발 R&D 및 실증인프라 구축을 위한 투자뿐만 아니라 민간에서의 상용화를 위한 연구개발도 이어지고 있다. 이 표준은 상용 양자암호통신 인프라 구축을 위해 필요한 구조, 기능요소, 서비스절차, 운영 등에 필요한 요소를 제시하는 국내 고유표준으로, 향후 지속적인 표준개발 및 확장을 통해 우리나라를 양자암호통신 선도국으로 성장시키는 데 밑거름이 될 것이다.

참고문헌

[1] ETSI GS QKD 004 V1.1.1, Application Interface, 2010.12.

[2] ETSI GS QKD 012 V1.1.1, Device and Communication Channel Parameters for QKD Deployment, 2019.02.

[3] ITU-T Y.3800, Overview on networks supporting quantum key distribution, 2019.10.

주요 용어 풀이

- QKD(Quantum Key Distribution): 양자 정보 이론에 기초한 정보 이론적 보안과 함께 대칭 암호화 키를 생성 및 분배하는 절차 또는 방법
- 양자암호 전달 네트워크: QKD 네트워크와 전달 네트워크(Transport Network)를 결합한 종단 간 사용자에게 양자암호 키 기반 암호통신 서비스를 제공하는 네트워크