양자통신 표준화의 현황과 과제

김정윤 양자통신(PG225) 의장, 한국전자통신연구원 네트워크연구본부 책임연구원

1. 머리말

지난 2018년 7월 ITU-T SG13 회의에서 KT와 LG유플러스, ETRI 등 한국 통신사업자와 국내 양자암호통신 선도 7개 기업 및 기관이 공동으로 제안한 양자암호키 분배망 기술에 대한 표준초안이 승인되어 신규 표준항목 개발이 시작되었다[1]. ITU-T SG13에서 시작된 양자암호키 분배망표준 개발은 전통적으로 통신망 기술 개발을 전담해 온 SG13 그룹으로서는 양자암호키 통신을 위한 통신망 구조 및 기능, 양자암호키 통신망의 전송장비 간 인터페이스, 서비스 절차 등의 상세 내용을 국제 표준으로 제정하는 계기가 되었다는 의의가 있다.

한국은 양자암호키 분배망의 표준 개발에 주도적으로 참여하고, 상용 통신망에서 양자암호키 통신을 구축하는 방법과 해킹 시도에 대응하는 시나리오를 도출하였으며, 관련 기술의 상용화 발판을 마련했다는 측면에서 큰 의미가 있다.

더욱이 양자암호키 분배망 표준화는 다가오는 양자인터넷 시대를 준비하기 위한 첫걸음으로서, 한국이 양자 기술의 주도권을 잡을 절호의 기회로 여겨진다[2].

본 고는 다 음과 같이 구성되었다. 먼저 2장에서는 유럽전기통신표준협회(ETSI), ITU-T, 인터넷 연구태스크포스(IRTF)가 완료 또는 추진하고 있는 표준문서를 중심으로 양자통신 표준화 현황을 살펴본다. 3장은 본 고에서 소개하는 양자통신 표준화 현황을 통하여 소규모로 적용하던 양자통신 기술이 어떤 방식으로 양자인터넷으로 발전할 수 있는지 전망해본다.

2. 양자통신 표준화 현황

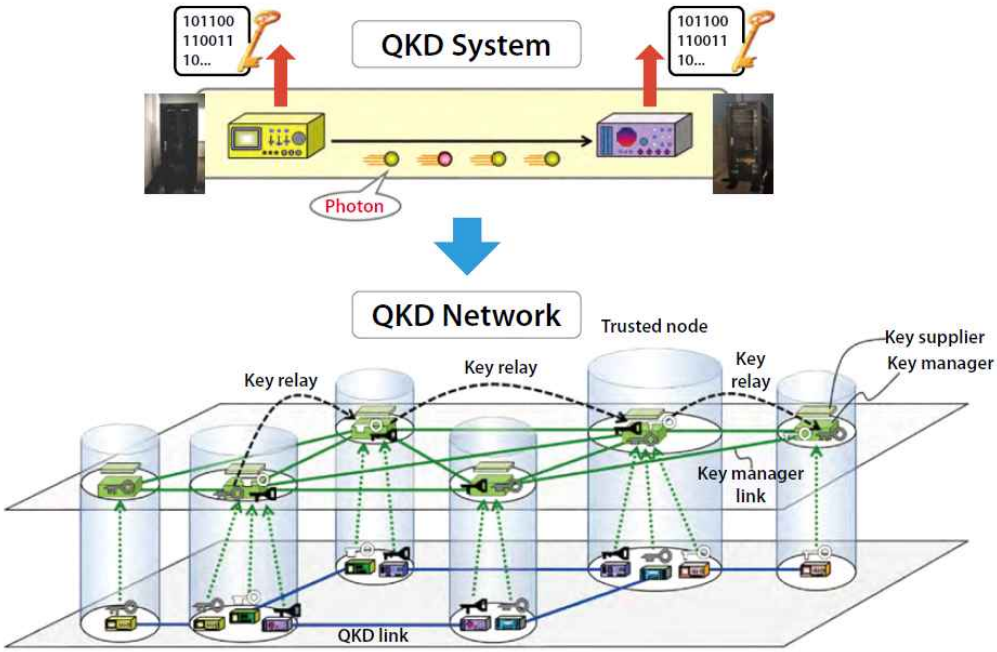
양자통신은 양자(quantum)들이 가지고 있는 중첩성을 이용한 통신이다. 기존 통신이 주로 전자기파(빛)를 이용하여 파장 또는 진폭의 차이에 의한 정보를 입력하는 방식이라면, 양자 통신은 양자 또는 빛의 편광성 또는 간섭 현상을 이용하여 정보를 하나하나 구분하여 입력하는 방식이다.

전자기파를 이용한 기존 통신은 누구나 정보를 이용할 수 있는 공개 채널이다. 반면, 양자통신은 양자 또는 빛의 편광성과 간섭성을 이용하며 주고받는 사람이 한정되어 있다. 이것을 양자 채널이라고 한다.

양자통신은 양자 채널과 공개 채널, 두 개 채널을 모두 이용한다. 먼저 양자통신을 시작하기 위해 송신자는 편광판 두 개와 하나의 비트를 나타내는 편광 상태를 서로 미리 정한다. 그리고 메시지를 담은 임의의 비트를 양자 채널을 통해 편광시켜서 보낸다. 이때 편광에 따라 광자 신

호는 수신자의 편광 필터로 전달된다. 이렇게 하여 난수가 만들어진다. 이같이 암호통신에서 암호키의 안전성을 확실하게 보장해 줄 수 있는 기술이 바로 양자암호키 분배 (QKD, Quantum Key Distribution) 기술이다[3].

송신자가 보낸 광자 신호는 물리적으로 편광에 의한 난수가 발생하고, 한쪽이 정보를 알려주면서 이때 같은 필터를 사용했는지 검증한다. 같은 필터를 사용한 비트에 대해서만 보관하고 서로 다른 필터를 사용한 비트는 제거한다. 이와 같은 과정을 거치면 위의 송신자와 수신자는 공개 채널을 통해 결정한 비트 값을 공유하고, 이것을 암호로 활용한다. 이런 이유로 양자통신은 구체적으로 양자암호 통신이라 불리며, 통신망 관점에서는 양자암호키 분배망(QKDN, QKD network)이라고 한다. [그림 1]은 양자암호키 분배 시스템과 분배망의 개념을 나타낸다[1].



[그림 1] 양자암호키 분배 시스템과 분배망의 개념

본 장에서는 ETSI, ITU-T 그리고 IRTF가 완료 및 진행 중인 표준문서를 살펴보고, 양자통신의 표준화 현황을 조망한다.

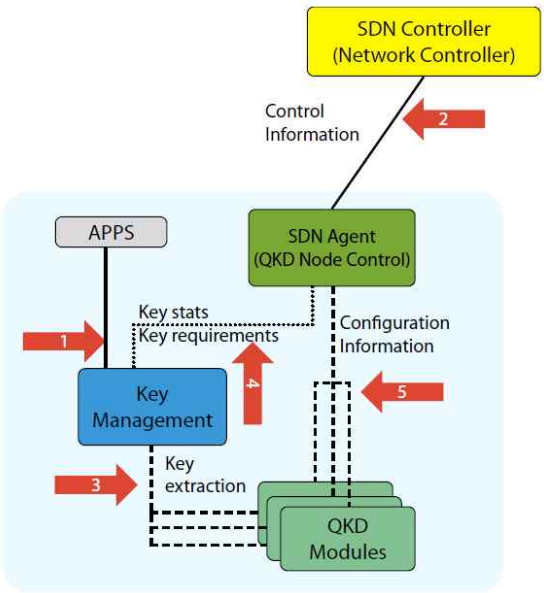
2.1 ETSI 표준화 현황: 양자암호키 분배시스템으로 시작

양자통신의 표준화는 2008년 10월 출범한 ETSI QKD 그룹에서 양자암호키 분배시스템 표준을 개발하면서 시작하였다. ETSI QKD 그룹은 2022년까지 QKD에 대한 11개의 표준을 완료하고 4개 문서를 진행하고 있다. 완료한 표준은 <표 1>에서 표준번호에 완료된 시기를 표시하였고, 주로 QKD 링크 수준 문제에 중점을 두고 있다. 또한 QKD 광학 구성 요소, 모듈, 내부 및 애플리케이션 인터페이스, 실용적인 보안 등을 포함한다. ETSI는 최근 QKDN 구조 및 공통 기준에 기반한 QKD 보안 인증 사양에 대한 연구를 시작하였다.

<표 1> ETSI 양자암호키 분배 표준문서

표준번호	표준명	내용
ETSI GS QKD 002 V1.1.1 (2010-06)	Use Cases	양자암호키분배의 사용사례
ETSI GR QKD 003 V2.1.1 (2018-03)	Components and Internal Interfaces	양자암호키분배의 구성요소와 내부 인터페이스
ETSI GS QKD 004 V2.1.1 (2020-08)	Application Interface : 1	양자암호키분배 애플리케이션의 인터페이스
ETSI GS QKD 005 V1.1.1 (2010-12)	Security Proofs	양자암호키분배의 보안 증명
ETSI GR QKD 007 V1.1.1 (2018-12)	Vocabulary	양자암호키분배 용어정의
ETSI GS QKD 008 V1.1.1 (2010-12)	QKD Module Security Specification	양자암호키분배 모듈의 보안 규격
ETSI GS QKD 011 V1.1.1 (2016-05)	Component characterization: characterizing optical components for QKD systems	부품 특성: 양자암호키 분배시스템용 광학 부품 특성
ETSI GS QKD 012 V1.1.1 (2019-02)	Device and Communication Channel Parameters for QKD Deployment	양자암호키분배 배포를 위한 장치와 통신채널 파라미터
DGS/QKD-0013 (GS QKD 013)	Transmitter module characterisation	양자암호키분배 전송 모듈의 특성
ETSI GS QKD 014 V1.1.1 (2019-02)	Protocol and data format of REST-based key delivery API : 3	REST 기반 암호 전달 응용프로그램 인터페이스의 프로토콜과 데이터 포맷
ETSI GS QKD 015 V2.1.1 (2022-04)	Control Interface for Software Defined Networks : 2 4 5	소프트웨어 정의 통신망의 제어 인터페이스
DGR/QKD-017 (GR QKD 017)	Network architectures	양자암호키 분배망 구조
ETSI GS QKD 018 V1.1.1 (2022-04)	Orchestration Interface for Software Defined Networks	소프트웨어 정의 통신망의 오케스트레이션 인터페이스
DGR/QKD-019 (GR QKD 019)	Design of QKD interfaces with Authentication	인증을 통한 양자암호키분배 인터페이스의 설계
DGS/QKD-020 (GS QKD 020)	Interoperable KMS API	상호운용이 가능한 암호키관리시스템의 응용프로그램 인터페이스

ETSI 양자암호키 분배 시스템에 정의된 인터페이스와 대응하는 관련 표준은 [그림 2]와 <표 1>과 같이 설명된다[4]. 여기서 (1)은 암호키를 요청하는 애플리케이션 인터페이스, (2)는 SDN 제어기와 QKD 노드의 인터페이스, (3)은 KMS와 QKD 모듈의 인테페이스, (4)는 SDN 에이전트와 KMS의 인터페이스, 그리고 (5)는 SDN 에이전트와 QKD 모듈의 인테페이스를 나타낸다[5, 6, 7].



[그림 2] ETSI 양자암호키 분배 인터페이스와 관련 표준의 관계

2.2 ITU-T 표준화 현황: 양자암호키 분배망의 확장

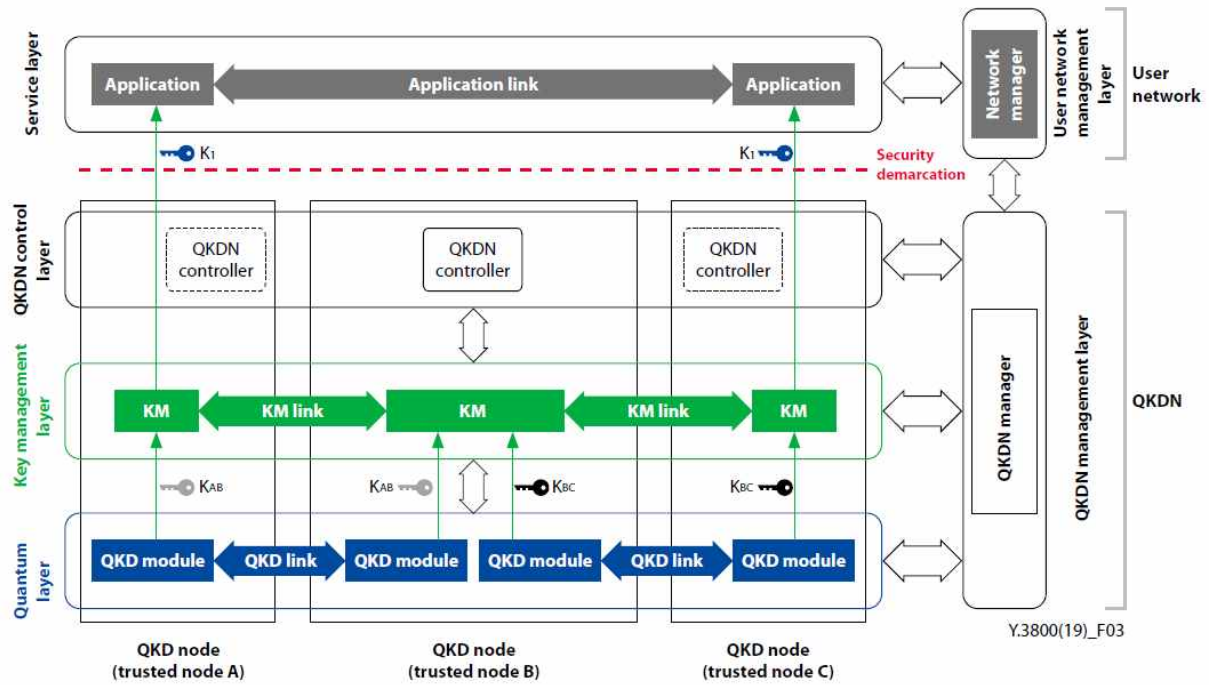
ITU-T SG13에서 제정한 양자암호키 분배망 표준화 현황은 다음과 같다. 먼저 ITU-T Y.3800[8] 표준은 QKD를 지원하는 통신망에 대한 개요를 제공하고, 이러한 개념적 구조 및 관련 기본 기능에 대한 세부 정보를 설명한다. 이 표준은 표준화된 기술 측면에서 QKDN 구현을 위한 설계, 배포, 운영 및 유지 관리를 지원하는 것을 목표로 한다.

QKDN의 주요 목표는 통신 보안을 높이는 것이다. 이를 위한 주요한 접근 방식은 QKD 링크를 통해 직접 연결되지 않은 경우에도 지정된 QKD 노드 간에 암호키를 공유하고, QKD 노드를 통해 사용자 네트워크의 암호화 애플리케이션에 암호키를 제공하는 것이다. 암호키를 공유하기 위해 암호키를 대상 QKD 노드로 전달하고, 이 노드는 저장한 암호키를 중계하여 암호화 애플리케이션에 제공하는 방식을 사용한다. 이러한 전체 작업을 암호키 관리라고 한다. QKD 노드는 인증되지 않은 당사자의 침입 및 공격으로부터 보호된다는 점에서 신뢰노드라고 하며, 이것은 QKDN의 필수 가정이다.

[그림 3]은 QKDN과 사용자 망의 개념적 구조를 설명한다. 각 QKD 노드는 QKD 모듈과 암호키 관리자(KM, Key Manager)를 포함한다. 한쌍의 QKD 모듈은 각각 송신 및 수신 QKD 노드에 위치하고, QKD 링크를 통해 연결된다. KM은 KM 링크로 연결되고 암호키 중계 기능을 포함한 암호키 관리 기능을 제공한다. QKD 모듈, QKD 링크, KM 및 KM 링크는 QKDN 제어기(controller)가 제어한다. QKDN 제어기는 암호키 중계 경로를 제어할 수 있다. KM은 사용자에 해당하는 암호화 애플리케이션에 암호키를 제공하며, 사용자 망은 송수신 암호화 애플리케이션을 포함한다. KM은 암호키 공급 기능도 포함한다. QKDN 관리자(manager)는 일반적으로 QKDN을 전체적으로 모니터링하고 관리한다.

일반적인 시나리오에서 사용자 망의 암호화 애플리케이션은 필요한 암호키를 KM에 요청한다. 이 요청에 의하여 KM은 지정된 형식으로 암호키를 안전하게 제공한다. 애플리케이션 링크의 데이터 전송은 암호화 애플리케이션에서 제공하는 암호키로 암호화된다. 암호화 애플리케이션

에 암호키가 제공되면 애플리케이션은 자체 책임 하에 암호키를 사용하고, QKDN은 암호키 관리 정책에 따라 암호키를 삭제하거나 보존해야 한다. 따라서 사용자 망과 QKDN의 경계에 보안이 설정되어야 한다.



[그림 3] 양자암호키 분배망과 및 사용자 망의 개념적 구조

기본적으로 단일 QKDN의 기능적 요구사항 및 구조는 QKDN의 기능적 요구사항을 설명한 표준 ITU-T Y.3801[9]과 QKDN의 기능적 아키텍처 및 운영 절차를 정의한 표준 ITU-T Y.3802[10]를 기반으로 정의된다.

표준 ITU-T Y.3801은 양자 계층, 암호키 관리 계층, QKDN 제어 계층 및 QKDN 관리 계층에 대한 기능적 요구 사항을 정의한다. 이 권고의 범위는 네트워크 측면에서 암호키의 보안과 직접 관련된 기능적 요구 사항을 정의한다.

표준 ITU-T Y.3802는 QKDN의 기능 구조 모델을 정의한다. 이 모델을 실현하기 위해 QKDN의 세부 기능 요소와 참조점, 구조 구성 및 기본 운영 절차를 정의한다. QKDN의 계층은 양자 계층, 키 관리 계층, 양자암호키 분배망 제어 계층, 양자암호키 망관리 계층, 서비스 계층 및 사용자 망관리 계층으로 구성된다. QKDN의 기능은 QKD 모듈, 키 관리자, QKDN 제어기, QKDN 관리자, QKD 링크 및 KM 링크, 암호화 애플리케이션, 사용자 망 관리자 및 사용자 망의 애플리케이션 링크을 포함한다.

QKDN을 효율적이고 안전하게 운영하려면 암호키 관리가 최우선 과제이다. 이를 기반으로 의미 있는 QKD 운영 및 서비스를 실현할 수 있기 때문이다. 암호키 관리는 기본적으로 안전하게 QKD 모듈에 의해 생성된 암호키의 저장, QKD노드 간 암호키의 중계, 그리고 사용자 요청에 의한 암호화 애플리케이션에 대한 암호키 제공 등을 포함한다.

양자암호키 분배망의 암호키 관리를 정의하는 ITU-T Y.3803[11] 표준은 QKDN의 상호 운용성

을 실현하고 보안을 보장하며 QKD의 애플리케이션을 확대하는데 필수적인 표준이다.
Y.3804[12] 표준은 QKDN를 통해 안전하게 안정적으로 효율적인 통신서비스를 제공하고 QKDN과 사용자 망의 관리를 전체적으로 지원하기 위해 QKDN의 제어와 관리에 대한 기능과 절차를 정의한다. 본 표준의 구체적인 기능은 제어 및 관리 특정 기능 (예: 라우팅 제어를 위한 경로 계산, 세션 제어를 위한 액세스 트래픽 조정/스위칭/분할을 포함한 세션 제어, QoS 및 과금 정책 제어 등), 제어 및 관리 기능 구성 요소와 다른 계층의 구성 요소간 제어 및 관리 참조점, 다계층 제어 및 관리 오케스트레이션 기능, 사용자 네트워크 관리 시스템 같은 외부 관리 시스템과의 연동을 포함한다.
Y.3805[13] 표준은 QKDN 제어를 위해 SDN 기술을 적용하기 위한 요구사항, 기능 구조, 참조점, 계층적 SDN 제어 기능, SDN 기반 제어 절차를 정의한다. SDN 제어는 논리적으로 중앙집중적이고 프로그래머블하며 계층적인 제어 기능을 제공하여, 신속한 서비스를 제공하는 특징이 있다.

2.3 IRTF 표준화 현황: 양자인터넷으로 진화

IRTF 양자인터넷(Quantum Internet, QI) 그룹은 단순하게 물리적으로 분산되어 있는 양자 프로세서(Quantum Processor)들 간을 연결하는 네트워크로 양자인터넷을 정의하였다[14]. 현재까지 양자인터넷은 다양한 물리 연구소 및 양자역학 이론 연구기관의 노력으로 개발되고 많은 발전을 이루었다. 이러한 연구 결과를 토대로 다음 단계로 가기 위해 필요한 노력은 네트워크 엔지니어링 측면의 접근이다. 즉, 양자인터넷은 순수한 양자 프로세서 간 연결을 위한 통신망 구조뿐만 아니라 통신망의 제어 및 관리를 위해 현재 인터넷과의 공존 및 통합이 필요하며, 양자인터넷의 구조를 설계할 때 현재 인터넷의 설계 철학을 기반으로 발전해야 한다.
IRTF QI 그룹의 목표는 양자인터넷의 완성을 위해서 현재 인터넷의 설계 철학을 기반으로 네트워크 엔지니어링 측면에서 주요 핵심 기술을 다음과 같이 정리하였다[4].

- 라우팅: 양자 메모리의 신뢰성이나 파동이 일정하게 지속되는 시간의 제약과 같은 양자의 고유한 특성으로 인해 양자인터넷에서 최적의 경로를 계산하는 것은 매우 도전적이며, 이러한한계를 극복하기 위한 라우팅 알고리즘 등 방안을 연구하고 네트워크 엔지니어링 설계에 반영하여야 한다.
- 자원 할당: 모든 네트워크는 한정된 자원으로 인하여 자원 활용의 제약을 받는다. 양자 인터넷 또한 예외일 수 없으며, 특히 양자 메모리의 신뢰성 등과 같은 양자 특성으로 인하여 추가적인 자원 제약을 받게 되므로 이러한 한계를 해결할 수 있는 연구가 필요하다.
- 연결 설정: 양자인터넷은 현재 인터넷의 패킷 형태 메시지 전달과는 달리 얽힘 상태를 메시지로 전달해야 하기 때문에 네트워크 연결 상태(semantics)의 변화를 네트워크 엔지니어링 설계에 반영하여야 한다.

- 상호운용성: 현재 양자통신의 하드웨어 및 프로토콜은 개별적으로 개발되고 있기 때문에 상호운용성 제공을 위한 표준개발이 필요하며, 이를 위해 유즈케이스, 요구사항, 구조 및 프로토콜 측면의 표준 개발이 필요하다.
- 보안: 양자인터넷 자체의 보안을 어떻게 보장할 것인가에 대한 연구도 네트워크 엔지니어링 설계 단계에서 고려되어야 한다.
- API 설계: 현재 인터넷에서는 비트(bit) 개념을 기반으로 소켓(Socket) API를 인터넷 응용을 위해 제공하고 있으나 큐비트(Qbit) 기반의 양자인터넷에서는 고유한 양자 특성을 반영하는 응용 API를 어떻게 제공할 것인가에 대한 연구가 네트워크엔지니어링 설계 과정에 반영되어야 한다.

현재 QI 연구그룹에서 개발하고 있는 표준문서는 <표 3>과 같다.

<표 3> IRTF 양자인터넷 표준문서

표준번호	표준명	내용
draft-irtf-qirg-principles-11	Architectural Principles for a Quantum Internet	양자인터넷을 위한 구조 관점의 원리
draft-irtf-qirg-quantum-internet use-cases-14	Application Scenarios for the Quantum Internet	양자인터넷을 위한 애플리케이션 시나리오

특히 양자인터넷을 위한 애플리케이션 시나리오[15]는 응용서비스의 용도에 따라서 양자 암호 분배와 양자 확약 등의 양자 암호 응용서비스, 분산 센서 등의 양자 센싱 응용서비스, 원격/분산 양자 컴퓨팅 같은 양자 컴퓨팅 응용서비스로 구분할 수 있다.

- 양자 암호 응용서비스: 양자 암호 분배 같은 보안 통신 설정, 복잡한 문제를 신속하게 해석하는 비잔틴 협상, 복제가 불가능한 양자 화폐 등이 있다.
- 양자 센싱/계측 응용서비스: 양자 특성을 이용하여 양자 센서의 민감도를 향상하는 것으로서 초정밀 네트워크 클럭 동기화, 고민감 센싱, 양자 이미징를 이용한 자기뇌파검사 등이 포함된다.
- 양자 컴퓨팅 응용서비스: 원격에 있는 소용량의 양자 컴퓨터 무리를 연결하는 분산 양자 컴퓨팅은 원격지에 있는 양자 컴퓨터에 계산 업무를 위임하면서 동시에 개인정보를 보호하는 보안 양자 컴퓨팅 등이 있다.

3. 맺음말

현재 양자암호키 통신에서 광케이블을 이용한 양자 전송 거리는 100km의 벽을 넘지 못하고 있다. 또한 양자키 생성 속도도 100 Kbps 수준에 머물고 있는 실정이다. 따라서 양자암호 통

신이 양자 통신망으로 발전하기 위해서는 양자 중계기, 양자 메모리 등 양자암호키 분배망을 구성하는 핵심 장비의 기능과 성능이 담보되어야 한다.
한편 지금까지의 양자암호키 통신은 송신자와 수신자가 동일한 도메인에서 통신하는 것을 가정하였다. 양자암호키 통신 장비는 동일한 업체에서 생산한 장비여서 상호운용성에 문제가 없기 때문에 통신이 실패할 수 있다는 가정을 허용하지 않았다. 그러나 장거리에 위치한 송신자와 수신자는 원격 통신이 가능해야 하고 이를 위해 대규모의 양자 통신망을 구축해야 한다.
또한 양자 통신망은 지정학적 위치에 따라서 독립된 사업자에 의해서 운영될 수 있다. 복수의 양자 통신망 사업자 사이의 연동을 보장하는 방법의 표준화가 완료될 때, 양자통신망은 양자인터넷으로 발전할 수 있을 것이다.

※ 본 연구는 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임. (No. 2020-0-00890, QKD 프로토콜간 상호 운용성 확보를 위한 신뢰노드 코어 및 인터페이스 개발사업, 2020.4.1 ~ 2024.12.31)

[주요 용어 풀이]

- 양자 암호키 분배, Quantum Key Distribution, QKD: 양자 통신을 위해 비밀키를 분배·관리하는 기술. 보안이 필요한 송수신자 사이에 양자 암호 키 분배(QKD) 기술을 사용하여 암호화에 필요한 비밀키를 안전하게 공유할 수 있다. 양자 키 분배를 위해 얽힘 상태 광자 쌍을 이용하거나, 단일 광자를 이용하는 방법이 있다.

[참고문헌]

[1] 이규명, "ITU-T 양자암호 네트워크 표준화 현황", 정보와 통신, 2022.5
[2] 김정윤, "양자암호 연동 표준화 현황", 정보와 통신, 2022.5
[3] ETSI QKD ISG, https://www.etsi.org/technologies/quantum-key-distribution
[4] Vicente Martin, ETSI 017 NwkArch Network Architectures on ETSI ISG QKD and Possible Extensions Towards QIN, ETSIITU QKD JOINT MEETING, 10 JUNE 2020
[5] ETSI GS QKD 004(V2.1.1), "Quantum Key Distribution (QKD); Application Interface"
[6] ETSI GS QKD 014(V1.1.1), "Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API"
[7] ETSI GS QKD 015(V2.1.1), "Quantum Key Distribution (QKD); Control Interface for Software Defined Networks"
[8] Recommendation ITU-T Y.3800, "Overview on networks supporting quantum key distribution," October 2019.
[9] Recommendation ITU-T Y.3801, "Functional requirements for quantum key distribution networks," April 2020.
[10] Recommendation ITU-T Y.3802, "Quantum key distribution networks - Functional architecture," December 2020.

[11] Recommendation ITU-T Y.3803, "Quantum key distribution networks . Key management," December 2020.
[12] Recommendation ITU-T Y.3804, "Quantum key distribution networks - Control and management," September 2020.
[13] Recommendation ITU-T Y.3805, "Quantum Key Distribution Networks - Software Defined Networking Control," December 2021.
[14] IETF/IRTF QIRG, https://datatracker.ietf.org/group/qirg/about/
[15] draft-irtf-qirg-quantum-internet-use-cases-14, Application Scenarios for the Quantum Internet

※ 출처: TTA 저널 제205호