정 보 보 호 학 회 지
제 32 권 제4호, 2022. 8

양자암호통신 글로벌 표준화 현황

윤 춘 석*

요 약

차세대 보안 기술인 양자암호통신은 ETSI, ITU-T, JTC1 SC27 등 여러 국제 표준화 기구들이 적극적으로 표준을 개발하고 있다. 표준화 기구별 집중하고 있는 이슈들은 조금씩 다르지만, 많은 나라들이 경쟁적으로 기술 개발 및 표준화에 열을 올리고 있다. 본고에서는 국제 표준화 기구별 개발중인 양자암호통신 기술 관련 표준들의 특징과 현황을 소개한다.

Ⅰ. 서 론

양자암호통신은 물리학에서 말하는 양자 역학적 성질을 활용한 암호통신이다. 수학적 어려움에 기반한 기존 암호통신체계와는 다르게 물리적 성질에 의해 그 안전성을 보장받기에 안전한 차세대 보안 통신 기술로 연구되고 있다.

현재 세계 여러 나라들은 양자암호통신 시범망 구축을 통한 상용화 준비에 박차를 가하고 있으며, 그와 동시에 표준화된 기술 정립을 위한 다양한 국제 표준들도 개발되고 있다.

양자암호통신 장비를 어떻게 만들지에 대한 표준을 만들고 있는 ETSI, 장비의 보안성 검증을 위한 방법 표준을 만들고 있는 JTC1 SC27, 양자암호통신 네트워크 구축을 위한 표준을 개발하고 있는 ITU-T 등 각각의 국제 표준화 단체들은 각각의 전문분야에 맞는 국제 표준들을 개발하고 있다.

본고에서는 이런 표준화 단체들의 양자암호통신 국제표준 개발을 위한 노력들을 살펴보고, 그 특징들을 소개하고, 해당 분야에 관심이 있는 산학연 전문가들에게 최신 정보를 제공하고자 한다.

Ⅱ. 표준화 단체별 현황 분석

본 장에서는 각 표준화 단체별 개발중인 양자암호통신 표준화 특징 및 현황을 살펴보고자 한다.

2.1. ETSI ISG QKD

유럽전기통신표준협회(ETSI)는 2008년부터 양자암호통신과 관련된 그룹(ISG QKD)를 만들어 운영하고 있다. 이는 세계 최초로 양자암호통신과 관련된 국제 표준을 만들기 위한 시도였으며 현재까지도 활발하게 국제 표준을 개발하고 있다.

현재까지 개발된 표준 문서들은 아래와 같다.

표 1에서 보여주는 완성된 표준들은 양자암호통신 장비의 어플리케이션 인터페이스, 보안성 증명, 모듈 사양, 구성요소 특성, 표준 인터페이스, 채널 매개변수 등 양자암호통신 장비를 구성하는 요소나 장비의 기본 안전성을 보장하기 위한 내용들이 주를 이루고 있다.

또한, 이러한 ETSI의 노력은 뒤에서 소개할 ITU-T나 JTC1 SC27과 서로 밀접한 교류속에 그 주제와 범위를 확장해 가고 있다. 공식 사이트에서도 소개하고 있는 것처럼, 최근에는 장비의 특성에서 벗어나 양자암호통신 네트워크를 위한 네트워크 구조, 소프트웨어 정의 네트워크를 위한 제어 인터페이스 등을 추가하기 시작했고, 양자암호통신 시스템을 위한 보호 프로파일, 단방향 시스템의 트로이 목마 공격으로부터의 보호 등에 대한 표준들도 개발하는 중이다.

ETSI ISG QKD는 세계최로 양자암호통신 기술을 국제 표준화했다는 상징성을 가지는 그룹으로 전세계의 양자암호통신 표준화 작업에 발맞추어 안전하고 효율적인 양자암호통신 시스템 환경을 정립하는데 큰 도움이

본 연구는 과학기술정보통신부와 한국지능정보사회지능원(NIA)가 주관하는 양자암호통신 시범인프라 구축/운영 사업의 일환으로 수행되었습니다.
* 주식회사 케이티 (선임연구원, chuck.yoon@kt.com)

〔표 1〕 ETSI ISG QKD개발 표준 문서 목록

표준 번호	표준 제목
018 V1.1.1	Orchestration Interface for Software Defined Networks
015 V2.1.1	Control Interface for Software Defined Networks
015 V1.1.1	Control Interface for Software Defined Networks
004 V2.1.1	Application Interface
012 V1.1.1	Device and Communication Channel Parameters for QKD Deployment
014 V1.1.1	Protocol and data format of REST-based key delivery API
007 V1.1.1	Vocabulary
003 V2.1.1	Components and Internal Interfaces
011 V1.1.1	Component characterization: characterizing optical components for QKD systems
005 V1.1.1	Security Proofs
008 V1.1.1	QKD Module Security Specification
004 V1.1.1	Application Interface
002 V1.1.1	Use Cases

되고 있다.

2.2. ITU-T (SG11, SG13, SG17)

국제전기통신연합 전기통신표준화부문(ITU-T)는 2018년부터 양자암호통신 네트워크와 관련된 표준들을 개발하고 있다. 양자암호통신을 단대단 통신 기술에서 네트워크화 시키는데 중점을 두고 표준을 개발하고 있으며, 양자암호통신 기술 전문가들과 네트워크 전문가들의 협력으로 국제 표준화 기구들 중에서 가장 많은 양의 국제 표준을 개발하고 있다.

ITU-T 에서는 3개의 연구반(SG)이 표준을 개발하고 있다. SG13은 가장 먼저 양자암호통신 네트워크 구조 표준을 개발하고 관련 후속표준들을 개발하고 있으며, SG17은 양자암호통신 네트워크 보안 기술 표준들을 개발하고 있다. 또한, 최근 SG11에서는 양자암호통신 네트워크 레이어들을 연결하는 각각의 인터페이스에 대한 프로토콜들을 개발하고 있다.

현재까지 개발된 표준 문서들은 아래와 같다.

〔표 2〕 ITU-T SG13 개발 표준 문서 목록

표준 번호	표준 제목
Y.3800	Overview on networks supporting quantum key distribution
Y.3801	Functional requirements for quantum key distribution networks
Y.3802	Quantum key distribution networks - Functional architecture
Y.3803	Quantum key distribution networks - Key management
Y.3804	Quantum key distribution networks - Control and management
Y.3805	Quantum key distribution networks - Software defined networking control
Y.3806	Quantum key distribution networks - Requirements for quality of service assurance
Y.3807	Quantum key distribution networks - Quality of service parameters
Y.3808	Framework for integration of quantum key distribution network and secure storage network
Y.3809	A role-based model in quantum key distribution networks deployment
Y.3810	Quantum key distribution network interworking framework
Y.3811	Quantum key distribution networks - Functional architecture for quality of service assurance
Y.3812	Quantum key distribution networks - Requirements for machine learning based quality of service assurance

표 2는 SG13의 Q.6와 Q.16에서 완성된 양자암호통신 네트워크 표준 목록이다. 양자암호통신 네트워크 기본 구조와 기능, 키관리, 네트워크 제어 및 관리, 서비스 품질 보증 요구사항, 이기종 네트워크간 연동 구조 등 대규모 양자암호통신 네트워크를 구축하기 위해 필요한 세부 사항들을 다루고 있다.

또한, 서비스 품질 파라미터들을 측정하기 위한 방법, 이기종 네트워크간 연동 구조의 상세 기능, 소프트웨어 정의 네트워킹 제어를 통한 네트워크 연동, 머신러닝기반 연동 기능구조, 미래 양자 인터넷 기술 보고서 등을 개발 중이다.

이를 통해 대규모 양자암호통신 네트워크를 구축하고 이기종 장비간 연동 및 다양한 사업자/국가 간 양자암호통신 네트워크 연동을 위한 기반 기술을 정립할 수

있게 되었다.

표 3은 SG17의 Q.15에서 완성된 양자암호통신 네트워크 보안 표준 목록이다. 이렇게 개발된 SG17의 표준들은 크게 두 분야로 구분해서 볼 수 있다.

첫 번째로, 양자암호 기술 자체의 보안성을 확보하기 위한 표준으로 양자 난수 생성기 구조를 정의한 표준과 키 조합을 통한 암호키 공급을 위한 구조 표준이다.

난수 생성기는 보안기술이 적용되는 곳에서는 없어서는 안될 중요한 기술로, 양자 효과를 활용한 양자 잡음원과 관련된 표준은 X.1702가 처음이다.

암호키 조합 기술은 서로다른 방식으로 생성된 암호키들을 조합하고 필요한 응용서비스들에 충분한 양의 암호키를 공급하기 위해 필요한 구조를 정의하고 있다. 이는 양자암호통신 네트워크의 확장성을 보장하고 기존 보안 인프라와의 유연한 연동을 보장한다.

두 번째는, 양자암호통신 네트워크의 보안성을 확보하기 위한 표준들로 보안 구조 표준, 키 관리 보안 요구사항 표준, 그리고 기존 보안스토리지 네트워크와의 연동을 위한 표준들이다.

이 표준들은 SG13에서 개발한 양자암호통신 네트워크 구조에 대한 보안 요구사항, 프레임워크 등을 정의하는 표준이다.

또한, SG17에서는 SG13에서 정의한 네트워크 구조 등을 기반으로 안전성을 확보하기 위해 필요한 기술들을 연구하고 있으며, 네트워크 구조/운용 표준을 기반한 보안 표준들을 지속해서 개발하고 있다.

표 4는 SG11의 Q.2에서 개발중인 표준 목록이다.

〔표 3〕 ITU-T SG17 개발 표준 문서 목록

표준 번호	표준 제목
X.1702	Quantum noise random number generator architecture
X.1714	Key combination and confidential key supply for quantum key distribution networks
X.1710	Security framework for quantum key distribution networks
X.1712	Security requirements and measures for quantum key distribution networks - key management
X.1715	Security requirements and measures for integration of quantum key distribution network and secure storage network

〔표 4〕 ITU-T SG11 개발 표준 문서 목록

표준 번호	표준 제목
Q.QKDN_profr	Quantum key distribution networks - Protocol framework
Q.QKDN_Ak	Protocols for Ak interface for QKDN
Q.QKDN_Ck	Protocols for Ck interface for QKDN
Q.QKDN_Kq-1	Protocols for Kq-1 interface for QKDN
Q.QKDN_Kx	Protocols for Kx interface for QKDN

SG13에서 완성된 네트워크 구조 표준을 토대로 각각의 계층별 인터페이스에서 사용될 프로토콜들을 상세하게 정의하고 있다. 2021년 처음 개발을 시작하여 아직 표준을 완성하기 위해 개발중인 단계이다.

2.3. ISO/IEC JTC1 SC27 WG3

기존의 암호장비들이 받고 있는 KCMVP나 CC 인증 같은 보안장비 인증 절차들은 물리적 법칙에 기반한 양자암호통신 장비에는 적용할 수 없는 문제를 가지고 있다.

이에 새로운 표준과 절차의 필요성을 바탕으로 ISO/IEC JTC1/SC27/WG3에서 양자암호통신 보안 인증 절차를 만들기 위한 기반 표준을 개발하고 있다.

현재 개발되고 있는 이 2개의 표준은 요구사항을 정의하는 표준과, 테스트/평가방법을 정의하는 표준으로 개발되고 있다.

첫 번째 표준에서는 양자암호통신 기술의 안전성을 보장하기 위해서 필요한 기준을 세우고, 상세한 장비의 구조와 필수적인 요구사항들의 명확한 한계를 정의한다.

〔표 5〕 JTC1 SC27 WG3 개발 표준 문서 목록

표준 번호	표준 제목
23837-1	Security requirements, test and evaluation methods for quantum key distribution – Part 1: Requirements
23837-2	Security requirements, test and evaluation methods for quantum key distribution – Part 2: Evaluation and testing methods

두 번째 표준에서는 첫 번째 표준의 기준을 만족하는지 평가할 수 있는 방법을 구체적으로 제시한다.

이 두 개의 표준들은 현재 DIS(Draft International Standard)단계로, 국가회원에게 투표를 위한 회람이 곧 시작될 예정이며, 2023년 최종 완성을 목표로 계속 개발을 진행중에 있다.

Ⅲ. 결 론

본고에서는 양자암호통신 기술의 국제표준화 기구별 현황에 대해 분석하였다. 특히 장비를 구성하는 요소와 보안성을 확보하기 위한 표준을 시작으로 네트워크를 위한 구조등도 개발하기 시작한 ETSI, 양자암호통신을 대규모 네트워크화 하고 그 안전성을 확보하기 위한 표준들을 개발하고 있는 ITU-T, 양자암호통신 기술의 보안성을 확보하고 보안 인증절차의 기반이 되는 표준을 개발하는 JTC1 SC27을 중심으로 현재 개발되고 있는 표준 목록과 특징들을 살펴 보았다.

양자암호통신 기술은 기술개발과 관련 국제표준이 동시에 이루어 지고 있다. 양자역학을 전공한 물리학자부터 장비를 개발하는 전문가와 네트워크 전문가, 그리고 보안 전문가까지 다양한 분야의 사람들이 모여 차세대 보안 통신 기술을 개발하고 표준을 만들고 상용화하기 위해 노력하고 있다. 앞으로도 다양한 국제 표준들과 기술들이 개발될 것으로 기대된다.

국내 기술의 발전과 글로벌 국가 경쟁력 확보를 위해서 관심있는 국내의 전문가/기업/연구소등의 적극적인 참여와 기술/표준 개발등이 필요하다. 정부와 민간의 적극적인 지원을 통해 대한민국이 양자암호통신 기술의 글로벌 리더가 되기를 기대해본다.

참 고 문 헌

[1] www.etsi.org/technologies/quantum-key-distribution
[2] www.itu.int/en/ITU-T/studygroups/2022-2024/11/Pages/default.aspx
[3] www.itu.int/en/ITU-T/studygroups/2022-2024/13/Pages/default.aspx
[4] www.itu.int/en/ITU-T/studygroups/2022-2024/17/Pages/default.aspx
[5] www.iso.org/standard/77097.html

〈저 자 소 개〉

윤 춘 석 (Chun Seok Yoon)

2011년 2월 : 경북대학교 컴퓨터공학과 졸업
2014년 2월 : 고려대학교 정보보호대학원 석사
2017년 2월 : 고려대학교 응용물리학과 박사 수료
2018년 5월~현재 : 주식회사 케이티 선임연구원

<관심분야> 양자암호통신, 양자인증/서명 프로토콜, 양자암호 알고리즘, 양자암호통신 국제표준