

양자암호 기술 보안 표준화 동향

권대성 국가보안기술연구소 책임연구원
장진각 국가보안기술연구소 책임연구원



1. 머리말

구글, 인텔, 마이크로소프트 등 글로벌 기업들이 주목하는 양자컴퓨팅 기술이 최근 매우 빠르게 발전하고 있다. 양자컴퓨터와 같은 신개념 컴퓨팅 기술은 전자 인증, 서명 등에 사용되는 현재의 공개키 암호체계가 매우 쉽게 해독될 수 있게 만든다는 것이 알려져 있다. 하지만, 한 번 설치되어 사용되기 시작한 공개키 암호체계를 새로운 암호체계로 바꾸는 과정은 매우 오랜 시간을 필요로 한다. 따라서 양자컴퓨팅에 취약한 공개키 암호기술에 대한 보안 대응책 마련은 장기간에 걸친 보안성 확보 측면에서 매우 시급하게 다루어야 할 중요한 문제이다.

양자컴퓨터에 안전한 암호체계 대안으로 현재 PQ(Post-Quantum) 암호와 양자암호가 연구되고 있다. PQ 암호는 양자컴퓨터가 해결하기 어려운 것으로 예상되는 수학적문제로 만든 공개키 암호이다. 현재 NIST에서 새로운 PQ 암호 공모사업이 진행 중이며, 안전한 PQ 암호가 선정되면 표준화 과정을 통해 널리 사용될 수 있을 것이다. 반면, 양자암호는 어떠한 새로운 컴퓨팅 개념이 나오더라도, 양자물리에 오류

가 없다면 안전한 물리 암호이다. 양자암호는 통상 양자키분배(QKD, Quantum Key Distribution)를 의미하며, 쪼갤 수 없는 양자인 광자(photon)를 정보전달 매개체로 한 키분배 프로토콜을 통해 암호화용 비밀키(암호키)를 실시간 분배한다.

QKD는 다양한 디바이스에 저가격에 구현되기 어렵다는 단점을 가지고 있지만, PQ를 비롯한 현대 암호와 달리 컴퓨팅 및 지능의 발전에도 안전성을 장기간 유지할 수 있고, 2000년대 초반부터 세계 각국에서 시험망을 운영하는 등 시스템기술이 성숙되어 있다는 장점을 가지고 있다. 이러한 장점을 살려 최근에는 QKD를 실 사용환경에 적용하기 위한 표준화가 구체화 되고 있으며, ETSI, ISO, ITU-T 등 여러 국제 표준화 기구에서 QKD 기술보고서, 기술규격 등을 발표하고 있다.

QKD의 주요 용도가 암호키를 다루기 때문에 보안관점의 기술 표준화가 필수적이며, 최근 ISO/IEC JTC1의 정보보안 위원회(SC27)에서 QKD의 보안관점 표준화를 진행하려고 하고 있으나, 기존 보안전문가들과의 공감대 형성을 필요로 하고 있다.

본고에서는 국내외 표준화기구의 QKD 기술 표준

화 동향을 보안관점으로 기술하고, QKD의 조기 실용화를 위한 국가보안기술연구소의 보안관련 표준화 활동에 대하여 기술하고자 한다.

2. 양자키분배 기술 표준화 동향

2.1 표준화 대상

QKD 기술은 단일광자를 이용하는 첫 번째 양자기술이면서도, 암호시스템의 암호키를 다루는 암호기술, 통신망에 구축되어 정보전송에 사용하는 통신기술이기도 하다. QKD 기술의 특성을 무엇으로 생각하느냐에 따라 기술 표준화의 방향도 다양할 수 있다.

기술의 구현 측면에서는 QKD의 기본 골격인 프로토콜 기술, 프로토콜 구현을 위해 양자광원을 사용하여 양자정보를 전달하는 광학기술, 기존정보통신망을 사용하여 유효한 양자정보를 골라낸 후 암호키를 만들어내는 통신 및 암호기술, 위의 과정을 시스템화하는 시스템 기술, 만들어진 QKD 시스템을 활용한 네트워크 기술 및 키관리 기술 등 다양한 기술이 필요하며, 각각은 모두 중요한 표준화 대상이다.

기술의 활용 측면에서 QKD는 지점 대 지점(point-to-point) 암호통신 및 이를 지원하는 기술이다. QKD는 원래 일회용암호(one-time pad)를 대체하는 기술로 제시되어 정보이론적 안전성 증명이 이루어진 기술이다. 즉, 이것 자체로 완전한 암호통신을 하는 것이 이론적으로 가능하다. 하지만 현재 개발된 QKD 시스템은 인증 문제, 속도 문제가 있어 일회용암호로 사용되는 것 보다는 현대암호시스템의 암호키로 사용하고, 실제 암호통신은 양자컴퓨터와 무관한 안전성의 현대 비밀키암호를 사용하는 것이 더 적합하다. 일회용암호로 사용되거나 암호키로 사용되거나 관계없이, QKD는 암호의 핵심인 암호키를 생성하는 용도로 사용된다.

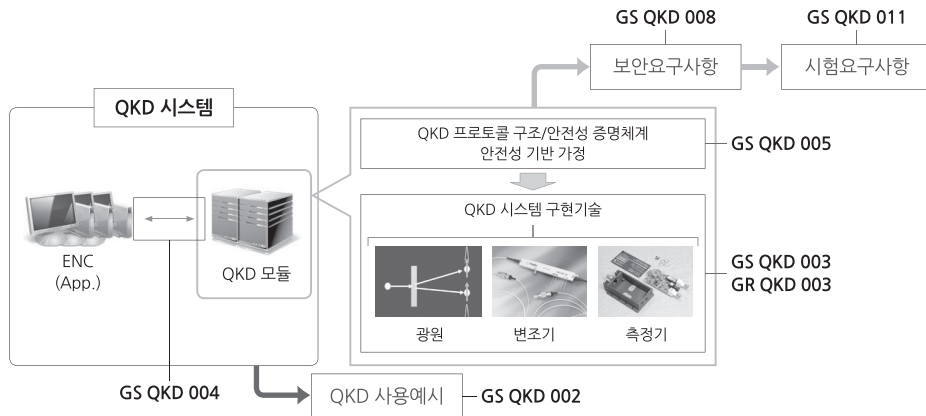
암호용도로 사용되는 장치들은 ISO/IEC 19790 표준을 기반으로 하는 CMVP(Cryptographic Module Validation Program) 혹은 ISO/IEC 15408 표준을 기반으로 IT 제품 및 시스템의 보안성 평가 목적의 CC(Common Criteria) 두 가지의 인증제도 관점의 기술 표준화 준비가 필요하다.

이후 장에서는 QKD 기술 표준화를 추진하는 단체들이 QKD 활용성을 기준으로 구현 기술을 어떻게 표준화하는지 살펴보도록 하겠다.

2.2 유럽전기통신표준화협회(ETSI)

유럽지역 표준화기구인 ETSI는 2008년부터 QKD ISG(Industry Specification Group)을 통해 QKD 기술의 표준화를 추진하고 있다. ISG가 만드는 그룹규격(GS, Group Specification)은 산업화를 위해 필요한 규격을 선제적으로 만드는 것으로 산업체가 주도하고 있으나, 유럽시장에 대한 강제력을 가지고 있지는 않다. QKD 분야에는 현재까지 총 6종의 그룹규격문서와 1종의 그룹보고서가 발표되었고, 비공개 검토중인 4건의 추가 규격이 준비 중이다.

ETSI의 QKD 표준은 ISO/IEC 19790 표준의 절차를 활용하려고 한다. ETSI는 QKD 시스템을 구성하는 경우 필요한 표준들을 QKD 장치 입장에서 구성하고 있다. 즉, QKD 시스템 컴포넌트인 광학계 구현 및 양자광원/측정기/변조기의 규격요소 정의(GS/GR QKD 003), 이 컴포넌트들을 통해 만들어지는 프로토콜 구조, QKD 안전성 증명체계 등의 안전성 증명 기술(GS QKD 005), QKD 모듈이 암호장치와 연동되는 키관리 인터페이스(GS QKD 004) 표준이 있다. ISO/IEC 19790 문서의 QKD 모듈 버전인 QKD 모듈 보안규격(GS QKD 008)과 QKD 시스템 구현에 사용되는 광학부품들의 특성 및 측정시험 규격(GS QKD 011)을 정의한다. 그리고 QKD



[그림 1] ETSI의 QKD 기술 표준화 현황

시스템이 사용되는 다양한 시나리오 예시(GS QKD 002)가 문서로 정의되어 있다.

한편, ETSI는 ETSI/IQC Quantum Safe Workshop(2017년)에서 QKD 기술의 표준화에 10년이 소요될 것으로 예측하고 있으며, 이 기간 동안 QKD 기술과 공개키 암호기술인 Quantum Safe 기술 표준화를 통해 양자 컴퓨팅 기술의 급격한 발전에도 암호기술의 혼란을 최소화 하는 방향으로 기술 표준화를 수행할 계획임을 발표한 바 있다.

2.3 ISO/IEC JTC1/SC27

국제표준화기구 ISO/IEC JTC1(합동위원회1)은 정보통신기술 세계표준을 담당한다. 현재 5개의 워킹그룹, 22개의 소위원회가 활동하고 있다. 32개 정회원국(P member) 및 66개 준회원국(O member)으로 운영되며, 한국은 정회원국으로 참여하고 있다.

27소위원회(SC27)는 IT 보안기술 표준을 다루고 있고, 운영그룹 포함 8개의 워킹그룹이 표준화를 담당하고 있다. 이 중 WG3(Working Group 3)에 2017년 11월 중국이 QKD 기술 표준화를 제안하였다. 스페인이 간사국인 WG3은 보안평가, 시험 및 규격을 담당하는 그룹이다.

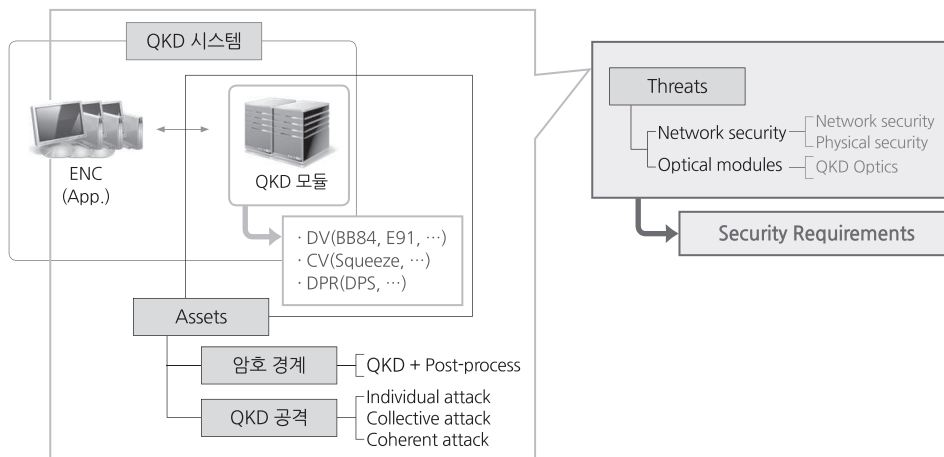
중국이 제안한 프로젝트는 ETSI와는 다르게 CC

관점의 기술 표준 제안을 준비하고 있다. SP(Study Period) 단계에 있는 본 프로젝트는 ISO/IEC 15408 표준을 활용하여 QKD 모듈에 대한 보호자산과 위협요소를 구분하는 과정에 있다.

현재까지 다양한 QKD 기술에 대한 소개와 함께 QKD의 보호자산별 주요 위협을 정리하고 있다. 주요 위협은 QKD 장치에 대한 네트워크 보안위협과 광학모듈에 대한 위협으로 구분하고 있다. 전자는 현대 암호제품에 대한 보안 위협이 QKD 장치에도 동일하게 적용될 수 있음을 설명하고, 후자는 기존 암호제품과는 별개인 QKD를 구현하는 광 모듈에 대한 보안위협을 새로 정의하고 구별해야 함을 설명한다. 이를 통해 새로운 기술인 QKD에 대한 평가기준을 제시하고자 하는 상태이다.

중국이 WG3에 제안한 QKD 프로젝트는 ISO/IEC 정례회의에서 의견 수렴과정을 거치고 있으며, 암호 알고리즘 표준화를 담당하고 있는 WG2(Working Group 2) 전문가들의 의견도 받고 있다.

기존 보안기술과의 상이성으로 인하여, 표준 전문가들과 공감대 형성에 어려움을 겪고 있으며 기술 필요성, 문서의 적절성 등에 대한 다양한 의견이 제시되고 있어 이 프로젝트의 진행 경과를 주목할 필요가 있다.



[그림 2] ISO/IEC JTC1/SC27/WG3에 제안된 중국의 QKD 표준 범위

중국이 제안한 QKD 프로젝트는 현재 제안 단계인 SP(Study Period) 단계에 있고, 2019년 2월 WD(Working Draft) 단계로 넘어가는 투표가 예정되어 있다.

2.4 ITU-T SG13

UN 산하 국제기구인 국제전기통신연합(ITU)은 1865년 설립되어, 1947년부터 UN의 전문기관이 되었다. 유선통신, 전파, 방송, 위성 주파수 등의 국제 표준, 조정 역할을 담당하고 전기통신표준화분야(ITU-T)는 전기통신기술, 운용 등을 다루며 산하 SG13(13연구반)은 미래 네트워크를 담당하는 연구반이다. 최근 KT는 QKD 지원 네트워크에 대한 표준을 SG13에 제안하였고, 표준화 착수요청이 승인되어 표준화 절차에 돌입하게 되었다.

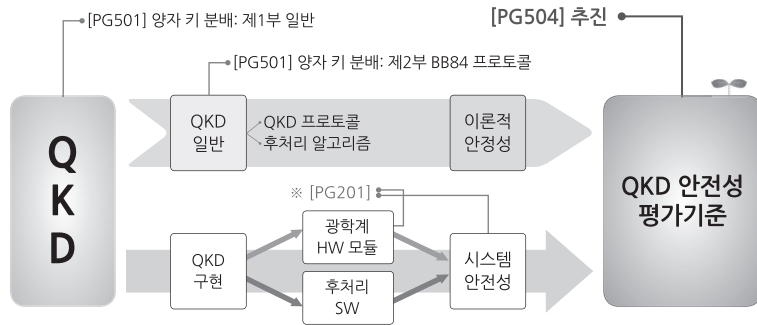
QKD를 지원하기 위한 네트워크 토폴로지로서 지점 대 지점, 지점 대 다지점(point-to-multi point), 신뢰 중계기(trust-node)/양자중계기를 사용하는 연결 구성(concatenated configuration)을 제안하고, 양자레이어를 포함하는 네트워크 레이어를 제안하였다.

2.5 TTA 정보보호기술위원회(TC5)

TTA는 국내 정보통신기술 표준을 담당하며, QKD 표준화는 통신망 기술위원회(TC2)와 정보보호 기술위원회(TC5)에서 진행하고 있다. TC2에서는 통신망 인프라에서 제공되는 주요 전기통신 응용 및 서비스 기술표준을 수행하여 통신관점의 QKD 표준화가 진행되고 있다. 반면 TC5에서는 국내 정보보호 표준, 국제표준화 추진 및 대응을 위한 정보보호기반, 개인정보, 사이버보안, 평가인증 등의 프로젝트를 수행하고 있으며 보안관점의 QKD 표준화가 진행 중이다.

TC2의 QKD 표준화는 퀀텀정보통신 연구조합에서 추진 중이며, ETSI의 기술규격을 인용표준으로 제정하고 있다. 본 표준들은 통신관점의 표준으로 이미 TTA 저널에서 소개한 바 있어, 본고에서는 TC5의 QKD 표준화 현황을 정리하고자 한다.

TC5의 QKD 표준화는 국가보안기술연구소에서 추진 중이다. QKD가 암호시스템의 암호키 생성모듈로 사용되고, 현대암호시스템과 QKD 모듈이 하나의 암호경계 안에서 구현되는 것을 모델로 한다. 그리고 CMVP 방식의 안전성 확인을 목표로 한다.



[그림 3] TTA의 QKD 표준화 현황

현대암호시스템에서 암호모듈 검증을 위해 적용되는 CMVP 제도는 블록암호, 해쉬함수, 공개키암호 등의 핵심 암호알고리즘을 보호함수로 선정하고 (CAVP¹⁾), 이 보호함수를 구현하는 시스템이 안전성 누수 없이 구현하는지 확인하는(CMVP) 방식이다. 암호 알고리즘을 보호함수로 선정하는 것은 TC5 중 501 프로젝트 그룹(PG501)의 역할이고, 이 알고리즘이 구현된 시스템의 보안성평가는 504 프로젝트 그룹(PG504)의 역할이다.

QKD를 CMVP 방식으로 안전성 실증을 하기 위해서는 먼저 암호 알고리즘에 해당하는 QKD 프로토콜이 보호함수로 선정되어 있고, 이를 암호시스템에서 안전하게 구현하도록 만들어야 한다. 이를 위해서 PG501에서는 QKD 프로토콜 일반론 및 디코이가 적용된 BB84 프로토콜의 표준화가 진행되어 2018년 12월 표준 제정이 예정되어 있다. 이 표준화된 프로토콜을 구현한 암호시스템에 대한 보안성을 위해 QKD 보안요구사항에 대한 표준화 작업이 PG504에 제안되어 2019년도에 진행될 예정이다.

QKD를 현대암호시스템과 함께 사용하기 위해서는 QKD 자체의 안전성, 현대암호시스템과 QKD의 연동 특성이 QKD 모듈에 대한 현대암호시스템 안전성 분석기술 적용과 함께 고려되어야 한다. QKD

보안요구사항은 ISO/IEC 19790 표준에 QKD 프로토콜이 구현되어질 때 검토되어야할 안전성증명, QKD 적용으로 인해 도입이 필요한 인증체계, QKD를 위해 필요하거나 QKD가 생성하는 보안매개변수의 관리방법, 부채널 공격(양자 전용 추가) 등이 기존 표준문서에 덧붙여(wrapping) 검토되며, 기존 암호시스템에 없는 QKD 기술 안전성 확인을 위한 광학계 및 후처리 구현시험이 함께 포함되도록 정리되고 있다.


또한, 보안요구사항에 대한 안전성 평가 시험의 기준이 될 시험요구사항에 대한 표준까지 정립이 되면 국내 QKD 기술에 대한 보안 관점의 표준화 체계가 구축될 것이다. 현재 세계 어느 표준화기구에서도 보안성을 기준으로 표준이 정립되지 못하고 있어 TC5의 표준화 체계가 완성되는 것만으로도 QKD 기술 표준화의 새로운 이정표가 될 수 있을 것이다.

3. 맺음말

QKD 기술은 양자기술이 실용화되는 첫 분야로 기술 표준화에 대한 수요가 확대되고 있는 신기술 분야이다. 그동안 통신 관점의 표준화가 시도되고 있으나, 암호기능의 보안 관점 표준화는 전세계적으

1) Cryptographic Algorithm Validation Program, 알고리즘 표준화

로도 개념정립 단계로, 이에 대한 체계적 표준화 준비가 매우 필요하다.

국내 QKD 기술표준화는 ETSI, ISO/IEC와 달리 QKD 프로토콜 표준화부터 진행되고 있다. QKD 기술 전문가 중심인 ETSI, ISO/IEC의 QKD 표준화 과정과는 다르게, 국내 QKD 기술 표준화는 암호 전문가와 QKD 전문가 모두의 참여를 통해 만들어가고 있다. 기술 구현의 대상인 QKD 프로토콜의 표준화, 프로토콜의 구현물인 QKD 적용 암호시스템의 보안요구사항 표준화, 이를 시험하기 위한 시험요구사항 표준화 추진을 통하여 QKD 기술의 시스템 안전성 확보를 위한 체계적인 접근방법을 제공하게 될 것이다. 

※ 본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 정보통신방송연구개발사업의 일환으로 수행하였음[1711073835, 양자암호통신망 구축을 통한 신뢰성 검증기술 및 QKD고도화를 위한 핵심요소기술 개발]

[참고문헌]

- [1] ISO/IEC 19790 Information technology – Security techniques – Security requirements for cryptographic modules.
- [2] ISO/IEC 15408 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.
- [3] ETSI Quantum Key Distribution and documents there in, <https://www.etsi.org/technologies-clusters/technologies/quantum-key-distribution>.
- [4] 유용석 외, 양자암호통신 국제 표준화 동향, TTA저널 표준/시험인증기술동향, 2016. 07/08.
- [5] 5th ETSI/IQC Quantum-Safe Workshop 2017, <https://www.etsi.org/news-events/events/1173-etsi-iqc-quantum-safe-workshop-2017>.
- [6] ISO/IEC JTC1/SC27/WG3 N1583 2nd Call for Contributions for an ISO/IEC JTC 1/SC 27/WG 3 Study Period on Security requirements, test and evaluation methods for quantum key distribution.
- [7] ITU-T SG13-TD166/WP3, Draft Recommendation ITU-T Y QKD_FR 'Framework for Networks to supporting Quantum Key Distribution'.
- [8] TTA, '양자 키 분배: 일반' (표준번호 부여 예정)
- [9] TTA, '양자 키 분배: BB84 프로토콜' (표준번호 부여 예정)
- [10] TTA, '양자 키 분배: 보안 요구사항' (과제 제안)

[주요 용어 풀이]

- PQ 암호(Post-Quantum Cryptography): 양자컴퓨터 개발 후에도 안전한 (공개키)암호기술
- QKD(Quantum Key Distribution): 양자 통신을 위해 비밀 키를 분배 관리하는 기술