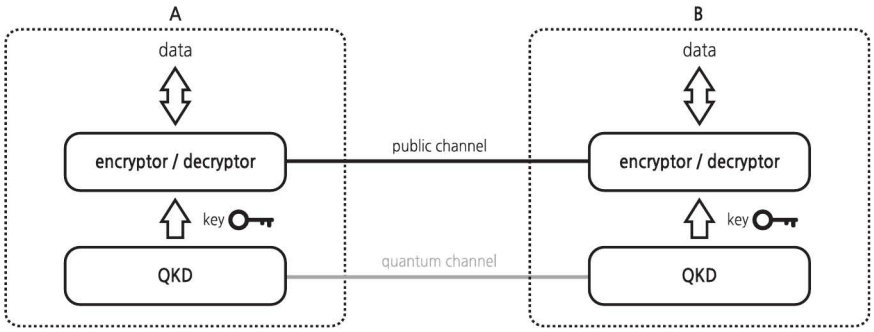
양자암호통신 국제 표준화 동향

유용석 홍익대학교 조교수
김아정 세종대학교 교수
이준구 KAIST 교수
곽승환 SK Telecom 랩장

1. 머리말

양자(quantum)의 상태에 정보를 실어서 전송하고 수신하는 양자암호통신 기술이 최근 주목을 받고 있다. 양자는 쪼개지거나 복제할 수 없기 때문에 양자의 상태에 기록된 정보는 근본적으로 도청이 불가능하다. 이 때문에 양자암호통신 기술은 계산 복잡도 기반의 기존 암호 기술의 한계를 극복할 수 있는 대안으로 활발히 연구되고 있다.

양자암호통신 기술 중에서 상용화에 가장 근접한 기술로 양자암호키분배(Quantum Key Distribution, 이하 QKD) 기술이 있다. QKD는 양자암호통신 기술을 이용하여 비밀키를 분배하고 관리하는 기술이다. [그림 1]에 보이는 것과 같이 높은 수준의 보안 통신이 필요한 양단 A와 B에 설치된 QKD 시스템은 quantum channe을 통하여 A와 B에 동일한 비밀키를 제공한다. QKD 시스템을 통해 양단에 분배되는 비밀키는 절대적인 보안성이 확보된다. 따라서 이 비밀키를 사용하여 암호화한 데이터는 일반 통신선로를 통해 전송하더라도 도감청의 위험으로부터 안전하다. 이처럼 기존의 광통신망에 QKD 시스템을 추가하면 비교적 간단히 절대적인 보안성을 확보할 수 있다. 따라서 보안이 중요시되는 공공 네트워크, 군 통신망, 금융망 등에 QKD가



[그림 1] 양자암호키분배(QKD)의 개념도

<표 1> ETSI QKD ISG의 주요 회원 단체

Applied Communication Sciences, Austrian Institute of Technology, Cadzow Communications Consulting Ltd (UK), BMWi - Federal Ministry of Economics and Technology, DCMS Department for culture, Media and Sport Organization, Facultad de Informatica, Universidad Politecnica de Madrid, Hewlett-Packard, Huawei Technologies (UK) Co. Ltd, ID Quantique, Institut Mines Telecom, Istituto Nazionale di Ricerca Metrologica, Mitsubishi Electric RCE, National Institute of Information and Communications Technology, NTT Corporation, Qunion, SK Telecom, SWISSCOM, TELEFONICA, THALES, TOSHIBA RESEARCH EUROPE LTD, Tubitak Uekae, Universida Politecnica de Madrid, University of Waterloo

<표 2> ETSI QKD ISG의 의장단 현황

직 책	소 속	이 름
Chairman	TOSHIBA RESEARCH EUROPE LTD	Andrew Shields
Vice Chairman	University of Waterloo	Norbert Lutkenhaus
Vice Chairman	Tubitak Uekae	Atilla Hasekioglu
Vice Chairman	Huawei Tech.(UK) Co., Ltd	Momtchil Peev

도입될 것으로 예상되고 있다.

QKD의 구현을 위해 일반적으로 사용되는 양자는 광자(photon)이며, 광자 기반의 QKD 기술은 기존 광통신 기술이 고도화된 기술로도 이해할 수 있다. 가장 큰 차이점은 정보 전달을 위해서 사용되는 광자의 숫자이다. 기존의 광통신 기술에서는 한 bit의 정보가 수많은 광자에 상태에 의해서 전송이 되지만, QKD 시스템에서는 하나 혹은 단 몇 개의 광자의 상태에 정보가 기록하고 추출되어야 한다. 따라서 QKD 구현을 위해서는 단일 광자 송수신기, 초고감도 광 신호처리 기술, 광자의 손실 혹은 도청을 극복하는 양자암호 프로토콜, 키 관리 및 암호화 프로토콜 등의 최첨단 기술들이 종합적으로 사용된다.

이러한 QKD 기술의 국제 표준화는 유럽 표준화기구인 ETSI(European Telecommunications Standards Institute)를 중심으로 활발히 진행되고 있다. 유럽의 EC FP6-project Secure Communication based on Quantum Cryptography의 결과, 양자암호통신의 핵심기술 중 하나인 QKD의 표준화 필요성에 대한 합의가 이루어졌고, ETSI 산하에 QKD를 담당하는 ETSI QKD Industry Specification Group(ISG)이 2008년 10월 9일 설립되었다. ISG는 빠르게 변하는 시장의 요구에 대응하기 위한 제도로서 ETSI 산하의 다른 프로젝트 그룹에 비해 ISG는 생성과 표준화 진행이 상대적으로 빠른 장점이 있다. ISG에서는 Group Specification(GS)를 제정하는데, GS는 강제력은 없지만 유럽 시장 진출에 중요한 요소가 된다. ETSI QKD ISG는 신기술인 QKD에 대한 개념과 이론적 배경을 정리하는 것부터 실제 QKD 시스템에 대한 표준 제정까지 QKD 관련 폭넓은 분야를 담당하고 있다.

본고에서는 ETSI QKD ISG를 중심으로 QKD 국제표준화 동향과 대응 방안에 대해 논의한다.

2. ETSI의 QKD 표준화 동향

2.1 ETSI QKD ISG의 조직 구성

QKD 표준을 담당하고 있는 ETSI QKD ISG는 현재 23개의 회원 단체를 가지며, 주요 단체는 〈표 1〉과 같다. 국내 참여단체로는 SK Telecom과 퀀텀정보통신연구조합(Qunion)이 있다. ETSI QKD ISG의 의장은 Toshiba의 자회사인 TOSHIBA RESEARCH EUROPE LTD 소속의 Andrew Shields이다. 의장과 부의장 3명을 포함한 의장단 현황은 〈표 2〉와 같다.

<표 3> 완료된 ETSI Group Specification QKD

번 호	제 목	제정년월	내 용
QKD 002	Use Cases	2010. 9	양자암호키 분배 응용 사례
QKD 003	Components and Internal Interfaces	2010. 12	QKD 장비의 부품과 부품 간 인터페이스에 대한 표준
QKD 004	Application Interface	2010. 12	QKD 장비와 외부 장비와의 연동 인터페이스에 대한 표준
QKD 005	Security Proofs	2010. 12	QKD 시스템의 보안성에 대한 개념과 구체적 기준 제시
QKD 008	QKD Module Security Specification	2010. 12	QKD 장비의 보안 요구사항
QKD 011	Component characterization: characterizing optical components for QKD systems	2016. 5	QKD 장비의 광부품에 대한 표준

<표 4> ETSI QKD ISG에서 진행 중인 Work Item

관련표준	제 목	상 태	내 용
QKD 003	QKD Components and Internal Interfaces	Adoption	2010년 version 1이 제정된 이후 진보된 기술 반영 위해 개정
QKD 007	QKD Ontology	Early Draft	QKD 관련 용어와 개념을 정리
QKD 010	IS Trojan	Start of Work	QKD system에 대한 Trojan Horse 공격과 방어 방법
QKD 012	QKD Deploy Parameters	Start of Work	QKD system의 설치 및 운용환경에 대한 표준

2.2 완료된 표준

ETSI QKD ISG는 연 2회의 정기회의를 개최하며, 2016년 6월의 20차 정기회의까지 6개의 ETSI Group Specification 표준 문서를 제정했다. 현재까지 제정된 표준 문서는 〈표 3〉과 같다.

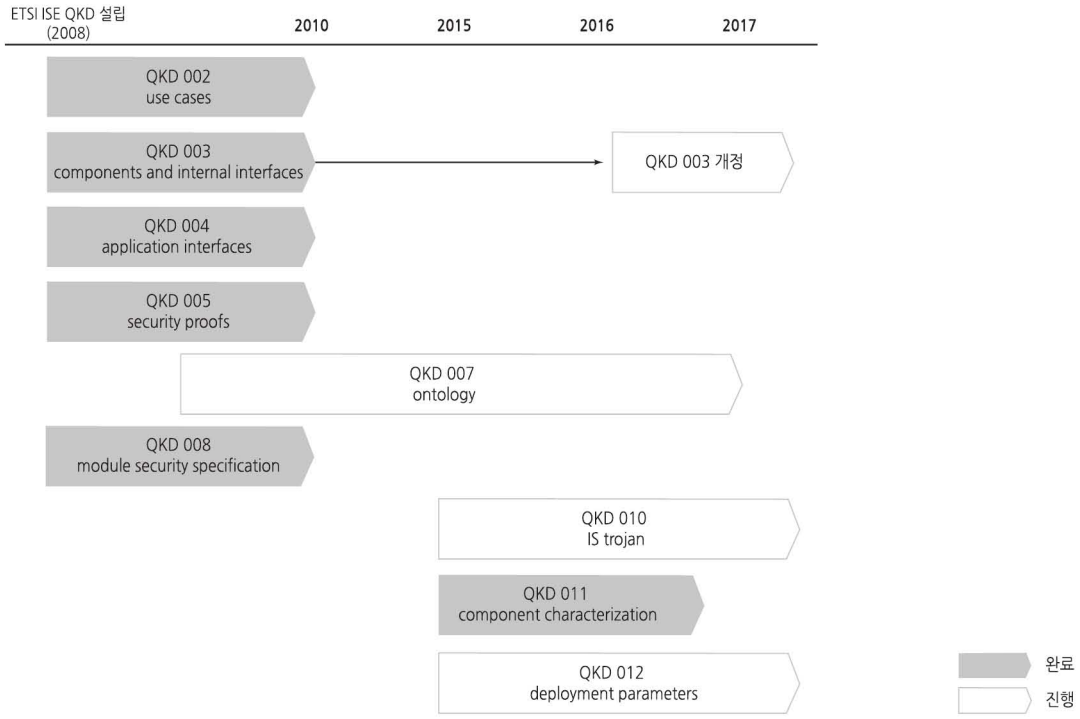
2.3 진행 중인 표준

ETSI QKD ISG의 항목별 표준화 활동은 WI(Work Item) 단위로 이루어진다. 각 WI는 Adoption, Start of Work, Early Draft, Stable Draft, Final Draft for Approval, Approval, Publication의 단계에 따라서 표준화가 진행된다.

현재 4건의 WI가 진행 중이며 그 세부 내용은 〈표 4〉와 같다. 한 WI은 QKD 003의 개정이며 다른 3건은 새로운 표준의 제정 작업이다.

2010년에 QKD 003 Components and Internal Interfaces 표준 문서의 version 1이 발간된 이후 기술적 발전을 표준에 반영하기 위해서 개정 작업이 시작되었다. QKD 003 표준의 개정은 2015년 11월에 발의되어 2016년 2월에 WI로 adoption되었다. 해당 표준은 QKD 시스템의 구성 부품들과 그 사이의 인터페이스에 대한 표준을 다루는 문서로 single photon source, single photon detector, modulation 방법 등에 대한 표준을 포함한다. 개정 작업의 라포처는 영국 National Physical Laboratory 소속의 Christopher Chunnilall이며 지난 2016년 6월 정기회의에서는 기존의 표준 문서에 어떤 내용을 추가할 것인지에 대한 논의가 이루어졌다.

새로운 표준 QKD 007 Ontology는 여러 QKD 표준 문서들에 흩어져있는 QKD에 대한 용어와 개념을 정리하여 일치시킬 필요에 따라 시작되었다. 2009년에 시작된 이 WI의 라포처는 영국 TOSHIBA RESEARCH EUROPE LTD 소속의 Ward Martin으로 Early Draft를 개선하여 다음 단계인 Stable Draft를 생성하는 작업을 담당하고 있다.



[그림 2] ETSI QKD 표준화 현황

QKD 010 IS Trojan은 QKD system에 대한 Trojan Horse 공격 가능성을 분석하고 이에 대한 방어 방법을 제시하는 표준 문서가 될 것이다. QKD 007과 같이 Ward Martin이 Rapporteur를 담당하고 있으며, 2013년 11월에 발의되어 2016년에 출판을 목표로 하였으나, 일정이 지연되어 아직 Start of Work 상태이다.

QKD 012 Deploy Parameters는 QKD system의 설치 및 운용환경에 대한 표준으로 프랑스 Institut Mines-Telecom 소속의 Romain Alleaume이 Rapporteur를 담당하고 있다. 2014년 1월에 발의된 이 WI는 아직까지 작업이 시작된 이후 큰 진전이 없는 상태이다.

2.4 ETSI QKD 표준화 현황

2008년 설립된 이후 ETSI QKD ISG에서 완료 혹은 진행 중인 QKD 표준을 시간에 따라 도시하면 [그림 2]와 같다. 그림에 보이는 것처럼 ETSI QKD ISG 설립 초기에 2년간 5건의 표준을 제정하였으며, 그 이후에는 1건의 표준이 제정되었고 다른 WI들은 예정보다 지연되고 있는 상황이다.

3. 맺음말

본고에서는 ETSI를 중심으로 QKD 기술의 국제표준화 동향에 대해서 논의하였다. 유럽을 중심으로 진행된 QKD 국제표준은 2008년에서 2010년까지 5건의 표준이 제정되었고, 그 이후에 1건이 추가로 제정되며 현재 4건의 WI이 진행 중이다.

따라서 ETSI GS QKD 표준을 준용하는 QKD 부품과 시스템을 개발하고자 한다면, 완료된 QKD 표준 문서를 기준으로 개발하면서 2010년 이전에 제정

된 QKD 002, 003, 004, 005, 008의 개정 가능성을 예의 주시해야 할 것이다. QKD 003 Components and Internal Interfaces의 경우 개정 작업이 시작되긴 하였으나, 기존의 표준 문서에 새로운 기술을 추가로 설명하는 형태로 진행되어 전체적인 내용 면에서 큰 변화는 없을 것으로 예상된다.

다른 한편, QKD 관련 최신 연구 결과를 국제 표준으로 반영하며 유럽 시장을 선점하고자 하는 산업체는 ETSI QKD ISG에 참가하는 국내 단체들을 통하여 ETSI QKD 표준에 적극적으로 참여하며 시장을 선점할 수 있는 기회를 모색해야 할 것이다.

또한, 양자암호통신 기술의 발전과 상용화를 촉진하기 위해서는 QKD 기술의 국내 표준을 제정하여 국내 기술역량을 결집할 필요가 있다. 이를 위해서 유럽에서 진행되고 있는 QKD 표준화 사례는 좋은 참고 자료가 될 것이다.

※본 연구는 미래창조과학부 및 정보통신기술진흥센터의 정보통신·방송 연구개발사업의 일환으로 수행하였음. [R-20150903-002203, 양자암호통신 분야 QKD 기술 표준개발]

[참고문헌]

[1] TTA 정보통신용어사전(양자정보통신)

[2] ETSI Committee Technical Working Procedures

[3] ETSI GS QKD 002 Use Cases, http://www.etsi.org/deliver/etsi_gs/qkd/001_099/002/01.01.01_60/gs_qkd002v010101p.pdf

[4] ETSI GS QKD 003 Components and Internal Interfaces, http://www.etsi.org/deliver/etsi_gs/QKD/001_099/003/01.01.01_60/gs_QKD003v010101p.pdf

[5] ETSI GS QKD 004 Application Interface, http://www.etsi.org/deliver/etsi_gs/QKD/001_099/004/01.01.01_60/gs_QKD004v010101p.pdf

[6] ETSI GS QKD 005 Security Proofs, http://www.etsi.org/deliver/etsi_gs/QKD/001_099/005/01.01.01_60/gs_QKD005v010101p.pdf

[7] ETSI GS QKD 008 QKD Module Security Specification, http://www.etsi.org/deliver/etsi_gs/QKD/001_099/008/01.01.01_60/gs_QKD008v010101p.pdf

[8] ETSI GS QKD 011 Component characterization, http://www.etsi.org/deliver/etsi_gs/QKD/001_099/011/01.01.01_60/gs_QKD011v010101p.pdf

[주요 용어 풀이]

- 양자정보통신: Quantum Information Communication, 양자정보통신은 양자암호통신이나 양자 컴퓨팅 등 양자 관련 정보통신기술(ICT)을 총칭한다.
- 양자암호통신 혹은 양자암호키분배: QKD, Quantum Key Distribution, 양자암호통신 기술은 양자의 상태에 정보를 실어서 전송하고 수신하는 기술을 말한다. 양자는 쪼개지거나 복제할 수 없기 때문에, 양자의 상태에 기록된 정보는 근본적으로 도청이 불가능하다. 이런 양자암호통신 기술을 활용하여 비밀키를 분배하고 관리하는 기술이 양자암호키분배 기술이다. 양자암호통신을 통해 분배된 비밀키를 사용하여 데이터를 암호화 하면 전송되는 데이터에 대한 도감청을 근본적으로 막을 수 있다.