정 보 보 호 학 회 지
제 30 권 제4호, 2020. 8

양자키 분배 네트워크를 위한 보안 요구 사항과 양자 난수 생성기 표준화 동향

심 동 희*

요 약

본 논문에서는 국제전기통신연합(ITU)의 정보통신기술 표준을 담당하고 있는 ITU-T에서 보안 분야 표준을 제정하고 있는 SG17에서의 양자암호통신 표준화 동향을 소개하고자 한다. 양자암호통신은 더 이상 쪼갤 수 없는 물리량의 최소 단위인 양자(Quantum)의 특성을 이용해 도청 불가능한 암호키(Key)를 생성, 송신자와 수신자 양쪽에 나눠주는 기술인 양자 키 분배 기술을 기반으로 하며, 이 양자 키 분배 기술을 통신망에 적용하여 보안 서비스를 제공하기 위한 보안 요구 사항과 관련된 상호호환성을 보장하기 위한 표준화가 ITU-T SG17에서 진행중에 있으며, 본고에서 관련 표준화 현황을 살펴보았다.

Ⅰ. 서 론

최근 양자컴퓨터 기술의 발전으로 기존 암호 체계에 위협을 가할 것으로 염려되고 있어, 양자컴퓨팅 기술의 공격에도 안전한 양자암호 기술에 대한 관심이 뜨겁다. 특히 양자컴퓨팅을 이용한 기존 암호체계의 공격에도 안전한 양자 키 분배 기술에 대한 표준화도 본격적으로 논의가 시작되어 [3] 관련 표준화 동향을 살펴보는 것도 의의가 크다고 하겠다. 아울러, 모든 사물이 무선으로 연결되는 5G 네트워크에서 보안은 아주 중요한 요소이다. 각종 센서와 수만 가지의 디바이스를 통신망에 연결하여 편리한 생활을 누릴 수 있지만, 해킹이나 도청이 발생하면 사회에 미칠 파장은 매우 크다고 할 수 있다. 최근 이러한 복잡해지고 다양해진 보안 이슈에 대응하고 해킹을 원천봉쇄하기 위해 양자암호통신 기술에 대한 관심이 증가하고 있으며, 또한 양자컴퓨팅 기술의 발전으로 기존 암호 체계에도 위협을 가할 것으로 염려되고 있어 양자물리학에 기반하여 양자컴퓨팅 기술의 공격에도 안전한 양자암호 기술이 각광 받을 전망으로 양자암호 보안 기술을 표준화하고 있는 ITU-T SG17에서의 양자암호 표준화 동향을 살펴보고자 한다.

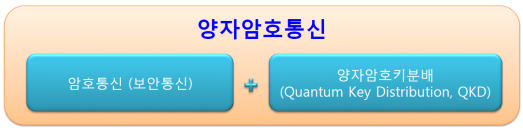
Ⅱ. 양자암호통신 기술 개요

암호통신은 장치 간 또는 프로그램 간에 암호화된 데이터를 전송하는 것으로, 송신부에서는 암호키를 이용해 암호화된 데이터를 전송하고 수신부는 동일한 암호키를 이용해 암호화된 데이터를 복호화한다. 암호통신에서는 송신부와 수신부에서 동시에 사용하는 암호용 대칭 키의 분배(공급) 및 관리가 매우 중요한데, 이 때 양자키 암호 분배 기술이 활용될 수 있다. 양자키 분배 기술은 양자역학 원리를 이용해 도청불가한 암호키를 안전하게 송수신부에 분배(공급)하여 -암호키를 주기적으로 교체하여 안전성 향상하는 것을 목적으로 한다.

다시 말하면, 양자암호통신은 더 이상 쪼갤 수 없는 물리량의 최소 단위인 양자(Quantum)의 특성을 이용해 도청 불가능한 암호키(Key)를 생성, 송신자와 수신자 양쪽에 나눠주는 통신기술이다. 여기에서 암호키란 송신자와 수신자만이 암호화된 정보를 열어볼 수 있도록 하는 금고 열쇠와 같다. 만약 누군가 암호키를 탈취하거나 복제하면 정보가 누출될 뿐만 아니라, 송신자와 수신자 모두 그 사실을 모를 수도 있어 위험하다. 암호통신에서 가장 중요한 것은 암호키의 안전성인데, 그 키의 안정성을 양자역학 기반, 이론적으로 확실하게 보장해 줄 수 있는 기술이 바로 '양자암호키분배' 기술이라고 할 수 있다.

* SK텔레콤 T3K센터, 5GX기술그룹, 5GX표준화팀 (팀장, donghee.shim@sk.com)

일반 암호키의 경우에는 정해진 정보를 암호화해서 보내지만, 양자암호통신은 양자역학의 특성상 수신자가 정보를 받는 순간에서야 그 정보가 결정된다. 해커가 중간에 암호키 정보를 가로채도 무의미한 정보가 된다. 또 외부에서 송신자와 수신자 사이의 통신망에 침투하면 정보 자체가 변하기 때문에 해킹 시도 여부도 바로 파악할 수 있다. 양자암호통신을 이용하면 암호키를 안전하게 생성하고 상대방에게 전달할 수 있다. 예를 들어, 기존 통신을 A와 B가 공을 주고 받는 행위로 비유한다면, 제3자인 C가 공을 가로챈 다음 똑같은 모양으로 복제해 B에게 전달하는 경우를 상상할 수 있는데, 이럴 경우 탈취 여부를 알기 힘들 것이다. 공 대신 비눗방울이라고 가정한다면, 누군가 중간에서 살짝만 건드려도 비눗방울이 터지거나 모양이 변형될 것이다. 양자암호통신은 비눗방울을 주고 받는 것과 같아, 복제 자체가 불가능하고 탈취 시도 흔적이 남게 된다. 그렇기 때문에 양자암호통신은 암호키가 탈취, 복제되는 것을 원천적으로 차단하는 것이다. 정리하자면, 정보보안 기술 중 하나인 암호통신에 양자현상을 이용해 암호키(비밀열쇠)를 분배(공급)하는 기술이 양자키 분배 기술이다.



〔그림 1〕 양자암호통신

Ⅲ. ITU-T SG17 양자암호 표준화 개요

ITU-T SG17 에서의 양자암호 표준화는 2018년 8월 회의에서 시작되었다. SK텔레콤 및 ID Quantique에서 제안한 2개의 신규 표준화 과제 (Work Item)를 통해 ITU-T SG17에서 본격적으로 논의가 시작되었으며, 해당 2개의 신규 과제는 '양자키 분배 기술 네트워크를 위한 보안 고려 사항' (Security considerations for quantum key distribution network) 및 '양자 노이즈 난수 생성기 구조'(Quantum noise random number generator architecture)' 등으로 통신망에서 양자 보안 기술을 직접 적용하여 활용할 수 있는 핵심 기술인 양자키 분배 기술과 양자 노이즈 난수 생성기에 대한 핵심 표준이라고 할 수 있다.

이후 2019년 1월 SG17 회의에서 3개의 추가 신규 표준화 과제가 승인되었는데 해당 표준 과제들은 '양자키 분배 네트워크를 위한 키 결합과 보안 키 공급' (Key combination and confidential key supply for quantum key distribution networks), '양자키 분배 네트워크를 위한 보안 프레임워크' (Security framework for quantum key distribution networks) 및 '양자키 분배 네트워크를 위한 보안 요구 사항 - 키 관리' (Security requirements for quantum key distribution networks - key management) 등이다.

2019년 9월 SG17 회의에서는 양자키분배 네트워크를 구성하기 위해 필요한 신뢰 노드 (Trusted Node) 관련 신규 표준화 과제가 추가로 제안되었다. 해당 표준화 과제의 명칭은 '양자키 분배 네트워크를 위한 보안 요구 사항 - 신뢰 노드' (Security requirements for Quantum Key Distribution Networks-Trusted node)이다.

다음 소단원에서 각 표준 과제들의 내용을 각각 간략하게 살펴보도록 하겠다.

〔표 1〕 양자암호기반 보안 관련 ITU-T SG17 표준화 과제

표준화 과제	과제명
TR.sec-qkd	Security considerations for quantum key distribution network
X.sec-QKDN-ov	Security framework for quantum key distribution networks
X.sec-QKDN-km	Security requirements for quantum key distribution networks - key management)
X.cf-QKDN	Key combination and confidential key supply for quantum key distribution networks
X.sec-QKDN-tn	Security requirements for Quantum Key Distribution Networks-Trusted node
X.qrng-a	Quantum noise random number generator architecture

Ⅳ. 양자키 분배 기술 표준화

이 소단원에서는 ITU-T SG17 에서의 양자키 분배

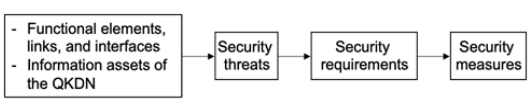
기술 표준화 과제 각각에 대해 살펴보도록 한다.

4.1. 양자키 분배 네트워크를 위한 보안 요구 사항

양자키 분배 네트워크를 위한 보안 요구 사항은 크게 4개의 표준으로 나뉘어서 표준화가 진행 중이다. 양자키 분배 네트워크를 위한 보안 요구 사항에 대한 표준화가 필요한지에 대한 갭분석, 타 표준 기구에서의 표준화 현황, 필요한 표준화 영역 등을 우선 논의하고 고려사항을 정의하기 위한 과제로 양자키 분배 기술 네트워크를 위한 보안 고려 사항' (Security considerations for quantum key distribution network) 과제가 승인되어 2018년 8월부터 표준화가 진행되어 올해 3월 (2020년 3월) SG17회의에서 최종 승인되었다. 해당 리포트에서 표준화 대상과 영역을 정의하였고 요구 사항을 구체적으로 정의하기 위한 '양자키 분배 네트워크를 위한 보안 프레임워크' (Security framework for quantum key distribution networks) 과제를 별도 과제로 진행해 오고 있는데 해당 표준은 SG17에서 양자키 분배 네트워크 보안 요구사항을 정의하기 위한 체계와 프레임워크 그리고 상위 요구 사항을 정의하는 표준이다. 해당 표준은 올해 (2020년) 8월 회의에서 최종 승인을 목표로 하고 있다. 그림 2에 양자키 분배 네트워크를 위한 보안 프레임워크 도출 절차를 도시하였다. 해당 표준에서는 양자키 분배 네트워크를 구성하는 요소(functional element), 각 요소간의 링크(link)와 인터페이스(interface) 및 양자키 분배 네트워크 내의 정보 자산(information asset) 등을 우선 정의한 후, 이 요소들에 대한 보안 위협(security threat) 분석을 통해 이에 대비가 필요한 영역을 보안 요구사항(security requirements)를 도출하였다.

그림 3은 양자키 분배 네트워크를 구성하는 구성요소와 각 요소들의 관계, 그리고 각 요소와 연관된 정보 자산을 정리한 내용으로 이 내용을 기반으로 보안 요구사항을 도출하는 것이 해당 표준의 목표이다.

'양자키 분배 네트워크를 위한 보안 프레임워크'



〔그림 2〕 양자키 분배 네트워크를 위한 보안 프레임워크 도출 절차

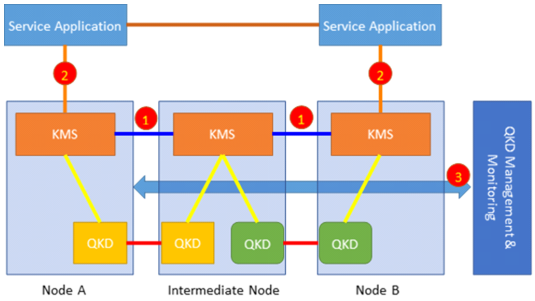
Element	Information assets	Key data	Meta-data	Control and management information
	QKD link			x
	KM link	x	x	x
	Control link		x	x
	Management link		x	x
	KM-App link	x	x	
	QKDNM-NM link			x
QKD node (trusted node)	QKD module	x	x	x
	KM	x	x	x
	QKDN controller		x	x
	QKDN manager		x	x
	QKD-KM link	x	x	

〔그림 3〕 양자키 분배 네트워크를 구성하는 요소와 각 요소들간의 관계 및 정보 자산 정의

(Security framework for quantum key distribution networks) 표준의 내용에 기반하여 양자키 분배 네트워크에서 양자암호 키를 관리하기 위한 요구사항을 정의하는 '양자암호 키 관리를 위한 보안 요구 사항'(Security requirements for quantum key distribution networks - key management)에 대한 표준화가 진행 중에 있으며, 아울러 양자키분배 네트워크를 구성하기 위해 필요한 신뢰 노드 (Trusted Node) 관련 신규 표준화 과제도 별도로 진행 중에 있다. 해당 표준화 과제의 명칭은 '양자키 분배 네트워크를 위한 보안 요구 사항 - 신뢰 노드' (Security requirements for Quantum Key Distribution Networks-Trusted node)이다.

양자암호 키 관리를 위한 보안 요구 사항'은 양자키 분배 네트워크를 여러 QKD 노드를 연결하여 구성할 경우 키를 어떻게 관리하고 전달하여 사용할지를 정의하는 규격이라고 할 수 있다.

양자암호통신을 위한 간략화된 계층 구조를 그림 4에 간략히 도식화하였다. 맨 아래 계층인 QKD 계층은 실제 광학 장비를 통해 양자를 생성하고 송신 그리고 수신하는 물리적 계층으로서 양자를 송수신하고 제대로 송수신되었는지를 검증하는 다양한 프로토콜 들이 이미 상용화되어 있어 즉시 적용이 가능하다. 그 위 KMS는 Key Management System(키 관리 시스템)의 약자로 (해당 용어는 정의하기에 따라 달라질 수 있으나 본 논문에서는 설명을 위해 이렇게 표시하기로 한다) 일반적인 QKD 시스템은 그동안은 point to point 시스템으로서 다시 말해 1:1 통신에 국한되어 사용되어 왔었으나 실제 통신망에 적용하기 위해서는 거대한 통신망에 여



〔그림 4〕 양자암호통신을 위한 간략화된 계층 구조

러 노드에 QKD를 적용하기 위해서는 여러개의 relay node가 필요하게 된다. 이는 물리적 양자 신호 처리를 위해서는 광통신 케이브과 그와 관련된 소자들이 필요한데 아직 거리제한이 있어 1:1 통신으로는 거대한 통신망의 암호화 장비들을 연결할 수 없기 때문이다. 결국 양자암호통신을 위해서는 QKD 노드가 여러 개 중간에 들어가서 연결을 하여 최초 송신자가 생성한 키를 최종 수신자가 전달받기 위해서 신뢰할 수 있는 중간 노드를 필요한 수만큼 연결해야 하며 이 때 키를 전달하고 또 관리하기 위한 기능이 필요한데 이 기능이 KMS(키 관리 시스템)이라고 할 수 있다. 이 위에 실제 이 암호키를 전달받아 암호화 하고 복호화 하는 암호화 장비들이 연결되는데 이것이 Service Application으로 표시되어 있다. 이것은 간략화된 모델로 실제 표준화가 완성될 경우 보다 상세한 기능들이 들어가서 복잡해 질 수 있으나 개념적으로는 크게 3개의 논리적 계층으로 양자암호통신을 구성할 수 있다고 보면 될 것이다.

4.2. 양자키 분배 네트워크를 위한 키 결합과 보안 키 공급

양자키 분배 기술은 기존의 암호화 장비를 활용하되 수학적 계산 기반의 암호화 키를 생성하는 키 생성 방법이 아닌 양자키 분배를 활용하여 암호화 키를 생성하는 것으로 기존 암호화 장비를 그대로 활용 가능하다. 이 때 양자키 분배 기술로 암호화 키를 생성할 수 없는 경우에는 여전히 기존의 수학적 계산 기반의 암호화 키를 생성하는 방법으로 암호화 키를 암호화 장비에 제공해야 하는데 이 때는 기존의 비대칭 암호 체계를 활용하여 제공할 수 있다.

이 외에도 기존 혹은 퀀텀 컴퓨팅에도 안전한 암호화 알고리즘으로 생성된 키와 양자키 분배 기술로 생성된 키를 결합하여 암호화 키의 보안 정도를 더 높이는 경우도 생각할 수 있다.

아울러 양자키 분배 기술로 생성된 암호화 키를 기존 암호화 장비에 사용하고자 할 경우 이런 장비를 인증하는 방법이 아직 존재하지 않아 기존 인증 절차를 따를 수 밖에 없는데 이런 경우도 표준에 정의하여 양자키 분배 기술 자체를 인증하는 인증 체계가 갖추어지기 전에 기존 인증 체계를 그대로 활용할 수 있을 것이다.

이러한 경우들을 정의하여 기존 암호화 장비에 양자키 분배 기술로 생성된 암호키를 활용하는 방법을 실제 암호화 장비에 활용하고자 하는 것이 '양자키 분배 네트워크를 위한 키 결합과 보안 키 공급' (Key combination and confidential key supply for quantum key distribution networks)이라는 표준의 목적이다.

4.3. 양자난수생성기

암호화 알고리즘에서 난수생성기는 필수불가결하게 활용되는 핵심 기능인데 기존의 난수 생성기는 수학적 함수 기반으로 얻은 유사난수를 사용하기 때문에 난수성이 완전히 보장되지 않는 측면이 존재한다. 양자안수생성기는 무작위 특성을 보이는 양자 샷 노이즈(Quantum Shot Noise)를 이용하여 예측이 불가능하고 패턴이 없는 순수 난수 (True Random Number)를 지속적으로 만들어주는 양자기술 기반의 난수 생성기로 이를 인증 및 다양한 암호화 알고리즘에 적용하거나 암호키로도 활용할 수 있다.

이러한 양자기술 기반의 난수 생성기의 구조와 원리를 표준에 정의하고자 하는 것이 '양자 노이즈 난수 생성기 구조'(Quantum noise random number generator architecture)' 표준의 목적이다. 해당 표준은 SG17에서 2019년 8월 최종 승인되어 X.1702라는 표준으로 발간이 완료되었다.

Ⅴ. 결 론

양자암호기술은 생태계 형성 초기단계로 이제 그 기술의 상용화가 막 시작되어 실제 쓰이는 단계로 진입했다. 실험실에서 머물던 기술이 실제 암호화 장비에 적용되어 사용되는 시기에 다다른 것인데 이를 보다 많은

장비업체들 그리고 서비스업체들이 채용하고 서로 상호 보완성을 보장하기 위해 표준화가 필요하다. 이러한 표준화가 앞에서 설명한 바와 같이 ITU-T SG17에서 시작되어 그 표준화 작업이 한창 진행 중에 있다. 이러한 표준화 활동을 통해 양자암호통신 업계가 보다 성숙해지고 보다 다양한 서비스들이 도출될 것으로 기대하고 있다.

참 고 문 헌

[1] ITU-T 홈페이지, http://www.itu.int

[2] ITU-T SG17 홈페이지, http://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx

[3] ITU-T Technical Report, “Security considerations for quantum key distribution network”, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14825

〈저 자 소 개〉

심 동 희 (Dong-Hi SIM)

1999년 2월 ~ 2007년 5월 : LG전자 차세대통신연구소, 책임연구원

2007년 6월~2009년 6월 : SK텔레콤 기술전략팀, 매니저

2009년 7월 ~ 2012년 6월: European Telecommunication Standards Institute, Technical Officer

2012년 7월~2018년 6월 : SK경영경제연구소 미래연구실, 수석연구원

2018년 7월~현재 : SK텔레콤 T3K센터, 5GX기술그룹, 5GX표준화팀, 팀장

<관심분야> 전자공학, 통신공학, 정보보호, 기술표준화