

양자 암호 보안 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 통신망에 적용하여 보안 서비스를 제공하는 암호통신방법으로, 이를 위한 보안 요구 사항과 관련된 상호호환성을 보장하기 위한 표준화가 ITU-T SG17에서 진행 중에 있으며, 본 고에서 관련 최신 표준화 현황을 살펴보았다.

I. 서 론

양자암호통신은 ‘양자(Quantum, 더 이상 쪼갤 수 없는 물리량의 최소 단위)’의 특성(불확정성, 비가역성, 복제 불가능성)을 이용해 송신자와 수신자만이 해독할 수 있는 일회성 암호키(Key)를 만들어 도청을 막는 통신 기술이다. 현존하는 보안기술 가운데 가장 안전한 통신 암호화 방식으로 평가받고 있다.

특히, 5G 시대에는 통신망을 통해 자율주행에 필요한 데이터, 의료에 필요한 바이오/생체 정보 등을 주고받게 된다. 이러한 데이터는 실생활의 안전과 관련되고, 개인정보를 담고 있어 철저한 보안이 필요하다. 최근에는 슈퍼컴퓨터보다 데이터 처리 속도가 현저히 빠른 양자 컴퓨터가 등장하면서 기존 암호체계의 사전 예측 가능성이 커지고 있어 보안의 중요성도 높아지고 있다.

현재 통신망은 신호의 끊김과 이어짐으로 디지털 신호인 ‘0’과 ‘1’을 구분해 데이터를 주고받는다. 보안을 위해 암호키를 사용하지만, 반대로 암호키만 알면 정보에 접근할 수 있다는 문제가 있다. 즉, 두 사람이 공을 주고받다가 제3자가 몰래 공을 가로챈 후 복제본을 전달해도 탈취 여부를 알기 어렵다.

반면, 양자는 ‘0’이나 ‘1’이라는 특성이 결정돼 있지 않다. 정보를 보내는 곳과 받는 곳에 각각 양자암호키 분배기를 설치하고 매번 다른 암호키를 이용해 ‘0’과 ‘1’을 결정한다. 양자암호키는 한 번만 열어볼

수 있기 때문에 중간에 누군가 가로채더라도 이를 바로 확인해 대처할 수 있어 해킹이 불가능하다. 즉, 비눗방울을 주고받는 것처럼 제3자가 비눗방울을 건들기만 해도 형태가 변형돼 해킹이나 복제 자체가 불가능하다.

특히 양자컴퓨팅을 이용한 기존 암호체계의 공격에도 안전한 양자 키 분배 기술에 대한 표준화도 본격적으로 논의가 시작되어 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 원천 봉쇄하기 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 전망이다.

본 고에서, 양자암호 보안 기술을 표준화하고 있는 ITU-T SG17에서의 양자암호 표준화 동향을 살펴보고자 한다.

* SK 텔레콤 5GX표준화팀 (팀장, donghee.shim@sk.com)

II. 양자암호통신

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, 이때 양자키 암호 분배 기술이 활용될 수 있다. 양자키 분배 기술은 양자역학 원리를 이용해 도청불가능한 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.

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 가로챌 다음 똑같은 모양으로 복제해 B에게 전달하는 경우를 상상할 수 있는데, 이런 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.

III. ITU-T SG17 양자암호 표준화 연력 및 전담 실무반 설립

ITU-T SG17 에서의 양자암호 표준화는 2018년 8월 회의에서 시작되었다. SK텔레콤 및 ID Quantique 에서 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.

앞에서 설명한 대로, 양자키 분배 네트워크를 위한 보안 요구 사항은 크게 4개의 표준으로 나뉘어서 표준화가 진행되어 왔으나, 이 중에서 양자키 분배 네트워크를 위한 보안 요구 사항에 대한 표준화가 필요한지에 대한 검토, 타 표준 기구에서의 표준화 현황, 필

요한 표준화 영역 등을 우선 논의하기 위한 기술 보고서 표준화 과제인 ‘양자키 분배 기술 네트워크를 위한 보안 고려 사항 (Security considerations for quantum key distribution network)’은 2018년 8월부터 표준화가 시작되어 2020년 SG17회의에서 최종 승인되었다. 해당 리포트에서는 표준화 대상과 영역을 정의한 바 있고, 이와 연계하여 요구 사항을 구체적으로 정의하기 위한 ‘양자키 분배 네트워크를 위한 보안 프레임워크’ (Security framework for quantum key distribution networks) 과제를 별도 과제로 진행하였는데 해당 표준은 SG17에서 양자키 분배 네트워크 보안 요구사항을 정의하기 위한 체계와 프레임워크 그리고 상위 요구 사항을 정의하는 표준으로 해당 표준은 2020년 8월 회의에서 예비 승인된 후 이후 11월에 최종 승인되었다.

특히 양자키 분배 네트워크를 위한 키 결합과 보안 키 공급’ (Key combination and confidential key supply for quantum key distribution networks) 표준은 양자키가 전달되는 네트워크를 구성하는 요소와 통신환경·보안 요구사항과 함께, 동 분배기술로 생성된 암호키를 기존 암호키와 결합하여 제공하는 방법을 정의하고 있다. 이를 통해 기존 네트워크와 양자암호통신 네트워크 간에 상호연동이 가능해져, 구축 비용이 절감되고 도입이 보다 빨라질 수 있다.

현재 진행 중인 표준 과제들의 내용은 다음 소단원에서 각각 간략하게 살펴보도록 하겠다.

특히 지난 SG17회의 (2021년 4월) 회의에서는 SG17 산하에 양자암호를 포함한 미래보안기술 연구를 위한 실무반인 Question 15이 설립되었다. 해당 실

[표 1] 양자암호기반 보안 관련 ITU-T SG17 표준화 과제 중 승인이 완료된 표준

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.cf-QKDN	Key combination and confidential key supply for quantum key distribution networks
X.qrng-a	Quantum noise random number generator architecture

무반 (Question 15) 설립에 한국이 주도한 바 있어, 더 큰 의의가 있다고 하겠다.

IV. 양자키 분배 기술 표준화

이 소단원에서는 ITU-T SG17에서 현재 표준화가 진행 중인 양자키 분배 기술 표준화 과제 각각에 대해 살펴보도록 한다.

[표 2] 양자암호기반 보안 관련 ITU-T SG17 표준화 과제 중 현재 표준화가 진행 중인 표준

표준화 과제	과제명
X.sec-QKDN-km	Security requirements for quantum key distribution networks - key management)
X.sec-QKDN-tn	Security requirements for Quantum Key Distribution Networks-Trusted node
X.sec-QKDN_intrq	Security requirements for integration of QKDN and secure network infrastructures
TR.hybsec-qkd	Overview of hybrid security approaches applicable to QKD networks
X.sec-QKDN-AA	Authentication and authorization in QKDN using quantum safe cryptography
X.sec_QKDN-CM	Security requirements for quantum key distribution networks - control and management

4.1. 양자키 분배 네트워크를 위한 키 관리 및 신뢰 노드 보안 요구 사항

‘양자키 분배 네트워크를 위한 보안 프레임워크’ (Security framework for quantum key distribution networks) 표준의 내용에 기반하여 양자키 분배 네트워크에서 양자암호 키를 관리하기 위한 요구사항을 정

의하는 ‘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 설명하면 다음과 같다. 맨 아래 계층인 QKD 계층은 실제 광학 장비를 통해 양자를 생성하고 송신 그리고 수신하는 물리적 계층으로서 양자를 송수신하고 제대로 송수신되었는지를 검증하는 다양한 프로토콜들이 이미 상용화되어 있어 즉시 적용이 가능하다. 그 위에 KMS가 위치하게 되며 KMS는 Key Management System의 약자이다. (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 왔으나 실제 통신망에 적용하기 위해서는 거대한 통신망에 여러 노드에 QKD를 적용하기 위해서는 여러개의 relay node가 필요하게 된다. 이는 물리적 양자 신호 처리를 위해서는 광통신 케이블과 그와 관련된 소자들이 필요한데 아직 거리제한이 있어 1:1 통신으로는 거대한 통신망의 암호화 장비들을 연결할 수 없기 때문이다. 결국 양자암호통신을 위해서는 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 암호화하고 복호화 하는 암호화 장비들이 연결되는데 이것이 Service Application이다. 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. 이러한 키 관리를 위한 표준화가 ‘양자암호 키 관리를 위한 보안 요구 사항’이라는 표준화 과제에서 수행되고 있으며, 해당 표준은 차기 회의인 2021년 8월 회의에서 승인(Consent)을 목표로 하고 있다.

4.2. 양자키 분배 네트워크를 위한 하이브리드 보안 방법과 보안 인프라와의 결합

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 양자키 분배 기술로 생성된 키를 기존 암호화 프로토콜에 적용할 수 있어야 하는데, 이러한 경우들을 정의하여 기존 암호화 장비에 양자키 분배 기술로 생성된 암호키를 활용하는 방법을 실제 암호화 장비에 활용하고자 하는 것이 ‘양자키 분배 네트워크를 위한 하이브리드 보안 방법 개요’(Overview of hybrid security approaches applicable to QKD networks)라는 기술 리포트의 목적이다. 이 보고서는 양자암호 통신과 다양한 보안기술 간 호환성을 제고하기 위한 방법 등을 다루는 기술 리포트로 2021년 4월 회의에 표준화 과제로 채택되었다.

아울러 양자 키 분배 네트워크와 기존의 공인 인증서 인프라와의 연동을 위한 표준화 과제도 진행 중인데, 해당 과제는 2020년 8월에 채택된 바 있다. 해당 표준의 명칭은 ‘양자 키 분배 네트워크와 암호 인프라와의 연동을 위한 보안 요구 사항’ (Security requirements for integration of QKDN and secure network infrastructures)이다.

4.3. 양자 키 분배 네트워크를 위한 인증, 허가 및 제어를 위한 보안 요구 사항

양자 키 분배 네트워크를 구성하는 구성 요소 간의 인증을 어떻게 수행할 것인지를 다루는 표준화 과제가 2021년 4월 회의에서 채택되었다. 해당 표준화 과제는 ‘양자 키 분배 네트워크에서 인증 및 허가’(Authentication and authorization in QKDN using quantum safe cryptography)이다. 이와 별도로 양자 키 분배 네트워크를 제어하고 관리하기 위한 네트워크 구성 요소와 양자 키 분배 네트워크 사이의 인터페이스에 대한 보안 요구 사항을 다루기 위한 표준화 과제가 2021년 4월 회의에서 함께 승인되었는데, 해당 표준화 과제의 명칭은 ‘양자 키 분배 네트워크의 제어와 관리를 위한 보안 요구 사항’(Security requirements for quantum key distribution networks - control and management)이다.

V. 결 론

양자암호기술은 본격적으로 생태계가 형성되어 가고 있으며, 그 기술의 상용화가 빠르게 진행되어 유럽, 미국의 다수 사업자와 한국의 SK 텔레콤 등이 실제 통신망에 적용하고 있다. 보다 많은 장비업체들 그리고 서비스업체들이 기술을 적용하고 상호보완성을 보장하기 위해 표준화가 함께 진행되고 있으며, 이러한 표준화가 앞에서 설명한 바와 같이 ITU-T SG17에서 한창 진행 중에 있다. 이러한 표준화 활동을 통해 양자암호통신 업계가 보다 성숙해 지고 보다 다양한 서비스들이 도출될 것으로 기대된다.

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 SG17 Q15 Work Program https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17&q=15

〈저자 소개〉



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, 5GX Intelligence Co., 5GX표준화팀, 팀장

<관심분야> 5G, 통신공학, 정보보호, 기술표준화