정 보 보 호 학 회 지
제 33 권 제4호, 2023. 8

ITU-T SG17 양자암호 표준화 동향

심 동 희*

요 약

본 논문에서는 국제전기통신연합(ITU)의 정보통신기술 표준을 담당하고 있는 ITU-T에서 보안 분야 표준을 제정하고 있는 SG17에서의 양자암호 표준화 최신 동향을 살펴보았다. ITU-T SG17에서 양자암호 관련 표준화는 실무반인 Q15에서 담당하고 있다. 양자암호통신은 더 이상 쪼갤 수 없는 물리량의 최소 단위인 양자(Quantum)의 특성을 다양한 통신 서비스에 적용하여 가장 높은 수준의 보안 서비스를 제공하는 것을 목적으로 하고 있고, 이를 위해 표준화가 필요한 영역에서의 보안 요구 사항과 그와 관련된 상호호환성을 보장하기 위한 다양한 영역의 표준화를 ITU-T SG17 Q15에서 진행 중에 있는데, 해당 실무반의 표준화 연혁과 현재 진행 중인 다양한 표준화 과제의 최신 표준화 현황을 살펴보았다.

Ⅰ. 서 론

양자암호통신은 '양자(Quantum, 더 이상 쪼갤 수 없는 물리량의 최소 단위)' 역학의 원리를 활용하여 도청에 대한 위험을 제거하여 안전한 통신을 수행하는 기술로 현존하는 보안기술 가운데 가장 안전한 통신 암호화 방식으로 평가받고 있다. 양자의 독톡한 특성(불확정성, 비가역성, 복제 불가능성 등)을 이용해 송신자와 수신자만이 해독할 수 있는 일회성 암호키를 공유하여 도청이 근본적으로 불가능한 통신 기술이다.

특히, 슈퍼컴퓨터보다 데이터 처리 속도가 현저히 빠른 양자 컴퓨터가 등장하고 기존 암호체계를 와해할 수 있음이 알려지면서 이에 대한 대비가 필수로 인식되고 있고, 이를 위한 보안 기술의 중요성도 높아지고 있다. 이 보안 기술이 양자키 분배 (Quantum Key Distribution) 기술로 양자키 분배 기술은 양자의 특성을 이용하여 송수신단 사이 동일한 키를 나누어 가지는 보안 프로토콜이라고 할 수 있다. 양자는 일반적으로 현재 사용하고 있는 컴퓨터의 연산 방식과 다르게 정보를 저장하는 최소단위인 큐빗(Qubit)이 '0'이나 '1'이라는 특성이 결정돼 있지 않고, 측정하는 순간 그 특성이 결정되는 톡특한 성질을 가진다. 이러한 양자의 특성을 이용하는 양자키 분배 기술은 중간에 누군가 양자정보를 가로채는 시도를 할 경우 이를 바로 확인할 수 있어 원칙적으로 해킹이 불가능하다. 최근 더욱 더 복잡해지고 다양해진 보안 이슈에 대응하고 해킹을 원천봉쇄하기 위해 양자암호통신 기술에 대한 관심이 증가하고 있으며, 또한 양자컴퓨팅 기술의 발전으로 기존 암호 체계에도 위협이 되고 있어, 양자역학의 원리에 기반하여, 양자컴퓨팅 기술의 공격에도 안전한 양자키 분배 기술이 각광 받고 있다.

이러한 양자키 분배 기술을 통신망에 적용하기 위해 필요한 요소와 상호호환성을 보장하기 위한 요구사항들을 다양한 표준화 기구에서 표준화하고 있으며 특히 ITU-T에서 보안 영역 전반에 대한 표준화를 담당하고 있는 SG17의 Q15에서 양자 키 분배 및 양자 난수생성기 보안 영역의 표준화를 진행해 오고 있다.

본 고에서는, 양자암호 보안 기술을 표준화하고 있는 ITU-T SG17의 실무반인 Q15에서의 양자암호 표준화 동향을 살펴보고자 한다.

Ⅱ. 양자키 분배 기술

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 도청불가한 암호키를 안전하게 송수신부에 분배(공급)하고 암호키를

* SK텔레콤 혁신사업 (팀장, donghee.shim@sk.com)

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 나눠가지는 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 있는 것이다. 예를 들어, 기존 통신을 A와 B가 공을 주고받는 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 주고받는 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 Q15 양자암호 표준화 연혁

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. 양자 노이즈 난수 생성기 구조 권고안은 X.1702로 제정, 발간되었다.

이후 양자키 분배 관련 보안 요구 사항들에 대한 다양한 표준화 과제가 SG17 회의에서 제안되어 승인되어 표준화가 진행되었는데 그 대표적인 과제들이 '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. 각각 X.1714, X,1710 및 X.1712로 권고안이 채택되었다.

특히 양자키분배 네트워크를 구성하기 위해 필요한 신뢰 노드 (Trusted Node) 관련 신규 표준화 과제가 추가로 제안 및 승인되어 표준화가 진행 중에 있는데, 현재 기술 수준으로 양자키 분배 기술을 네트워크로 구성하기 위해 필수적인 기술인 신뢰 노드에 대한 보안 요구 사항을 제정한다는 데 큰 의의가 있다. 해당 표준화 과제의 명칭은 '양자키 분배 네트워크를 위한 보안 요구 사항 - 신뢰 노드' (Security requirements for Quantum Key Distribution Networks-Trusted node)이다.

아울러 양자 컴퓨팅에 의한 공격에 대해 안전한 양자 내성 보안체계로의 전환을 위해 양자 키 분배 (Quantum Key Distribution - QKD) 기술을 암호키 교환에 활용하는 다양한 하이브리드 접근 방식 들을 분석하기 위한 표준화 과제도 승인되어 표준화를 진행하였는데, 이것은 표준화 기구에서 개발되었거나 아직 개발 중인 다양한 키 교환 방법을 분석하여 양자키 분배 기술을 다양한 네트워크 계층에서 활용할 수 있도록 하는 중요한 표준화 과제이다. 해당 표준화 과제의 이름은 '양자 키 분배 기술을 이용하는 키 교환 방법을 위한 하이브리드 방법들에 대한 개요' (Overview of hybrid approaches for key exchange

with quantum key distribution)로 이미 표준화가 완료되었다.

비교적 최근인 2023년 3월 회의에서는 양자키 분배 기술에서 동일한 양자키를 송수신단에서 공유하기 위한 양자키 분배 프로토콜에 대한 표준화를 시작하기 위한 표준화 과제가 제안되어 승인되었는데 해당 과제의 명칭은 '양자키 분배 네트워크의 양자키 분배 프로토콜 프레임워크' (Framework of quantum key distribution (QKD) protocols in QKD network) 이다. 더 나아가 양자키 분배 기술과 양자 내성 암호를 결합하여 양자 내성 통신을 구성하는 다양한 방법을 분석하고자 새로운 기술보고서가 제안되어 새로운 과제로 표준화가 시작되었는데 해당 과제의 명칭은 '양자 내성 통신을 위한 하이브리드 키 관리 개요' (Overview of key management of hybrid approaches for quantum-safe communications)이다.

특히 SG17 산하에 양자암호를 포함한 미래보안기술 연구를 위한 실무반인 Question 15이 2021년 4월 회의에서 설립된 바 있고, 해당 실무반 (Question 15) 설립을 한국이 주도한 바 있어, 더 큰 의의가 있다고 하겠다.

〔표 1〕 양자암호기반 보안 관련 ITU-T SG17 표준화 과제 중 승인이 완료된 표준

표준화 과제	과제명
XSTR.SEC-QKD	Security considerations for quantum key distribution network
X.1710	Security framework for quantum key distribution networks
X.1714	Key combination and confidential key supply for quantum key distribution networks
X.1702	Quantum noise random number generator architecture
X.1712	Security requirements and measures for QKD networks - key management
XSTR-HYB-QKD	Overview of hybrid approaches for key exchange with quantum key distribution
X.1715	Security requirements and measures for integration of QKDN and secure network infrastructures

표 1은 표준화가 완료되어 제정된 표준의 리스트를 정리한 표이다.

이 중에서 주요한 표준에 대해 각각 살펴보면 다음과 같다.

3.1. 양자키 분배 네트워크를 위한 보안 요구 사항 (X.1710)

양자키 분배 네트워크를 위한 보안 요구 사항 관련 표준화는 그 표준화를 본격적으로 시작 전에 양자키 분배 네트워크를 위한 보안 요구 사항에 대한 표준화가 필요한지에 대한 갭분석, 타 표준 기구에서의 표준화 현황, 필요한 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'로 시작된 바 있다. 해당 과제는 2018년 8월부터 표준화가 시작되어 2020년 SG17회의에서 최종 승인되었다. 해당 보고서에서는 표준화 대상과 영역을 분석하여 정리한 바 있고, 이후 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.

3.2. 양자키 분배 네트워크를 위한 키 관리 보안 요구 사항 (X.1712)

'양자암호 키 관리를 위한 보안 요구 사항'(Security requirements for quantum key distribution networks - key management) 권고안의 주요 내용은 '양자키 분배 네트워크를 위한 보안 프레임워크' (Security framework for quantum key distribution networks) 권고안의 내용에 기반하여 양자키 분배 네트워크에서

양자암호 키를 관리하기 위한 요구사항을 정의한 것이다.

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

양자암호통신을 위한 양자네트워크의 구성은 맨 아래 계층인 QKD 계층, QKD 계층에서 생성한 키를 인접한 노드로 전달하여 최상위 계층인 응용 계층으로 전달되도록 하는 키 관리 계층, 그리고 송수신에서 공유된 키를 실제 사용하는 응용계층으로 간략히 요약할 수 있다. 맨 아래 계층인 QKD 계층은 실제 광학 장비를 통해 양자를 생성하고 송신 그리고 수신하는 물리적 계층으로서 양자를 송수신하고 제대로 송수신되었는지를 검증하는 다양한 프로토콜 들이 작동하는 계층이다. 그 위 키 관리 계층 (Key Management Layer - Key Management System(키 관리 시스템)이라고 불리기도 한다))은 QKD계층에서 생성된 양자키를 목적지로 전달하기 위한 일련의 키 전달 및 관리 기능을 하는 계층이다. 과거 최초 설계된 양자 키 분배 기술은 점대점(point to point)으로 송수신단이 동일한 키를 나누어 가지는 기술로 시작하였는데, (다시 말해 1:1 통신에 국한되어 사용되어 왔었으나) 실제 통신망에 적용하기 위해서는 통신망을 구성하는 여러 노드에 양자키 분배 기술이 적용되어야 하므로 이를 위해서는 여러개의 전달 노드가 필요하며, 이는 양자암호통신을 위해서는 양자키 분배 기술 적용 노드를 연결하여야 하며 이 때 키를 전달하고 또 관리하기 위한 기능이 필요한데 이 기능이 키 관리 계층에 구현된다고 할 수 있다. 이 위에 실제 이 암호키를 전달받아 암호화 하고 복호화 하는 암호화 장비들이 연결되는데 이것이 소위 응용 계층이라고 할 수 있다. 이것은 간략화된 모델로 이런 모델을 기반으로 키를 관리하기 위한 기능들과 이에 대한 보안 요구 사항을 표준화한 것이 ‘양자암호 키 관리를 위한 보안 요구 사항’이라는 권고안이다.

3.3. 양자키 분배 네트워크를 위한 키 결합과 보안 키 공급 권고안 (X.1714)

양자키 분배 네트워크를 위한 키 결합과 보안 키 공급’ (Key combination and confidential key supply for quantum key distribution networks) 권고안(X.1714)은 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.

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 암호체계를 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 해당 권고안의 목적이다.

3.4. 양자키 분배 기술을 활용하는 하이브리드 키 교환 방법 (Overview of hybrid approaches for key exchange with Quantum Key Distribution)

해당 기술보고서에는 양자 키 분배(QKD) 네트워크에서 생성하는 대칭 키를 활용하여 다른 방식으로 생성된 암호키와의 다양한 방식의 결합을 통한 하이브리드 접근 방식의 호환성에 대해서 살펴보았고, 다양한 네트워크 계층의 보안 통신 프로토콜과 함께 QKD를 함께 사용할 수 있도록 하는 표준들을 함께 분석하였으며, 이러한 표준들에서 추가적으로 개발이 필요한 영역들을 함께 살펴보았다. 본 기술 보고서에는 국제기구 또는 지역 표준화 기구에서 표준화되었거나 표준화가 진행 중에 있는 양자 내성 암호 프로토콜에서 양자 키 분배를 하이브리드로 활용 할 수 있는 방법을

분석한 것으로, 이 기술 보고서에서 다루는 하이브리드 방법은 키 교환과 관련된 것이다. 키 교환을 위한 하이브리드 접근 방식은 적어도 두 가지 이상의 다른 키 교환 방법을 결합하여 키 교환 기능을 수행하는 것을 지칭하며, 이 기술 보고서는 양자 키 분배 프로토콜을 하이브리드 키 교환의 맥락에 맞게 수용하는 다양한 방법을 분석하였다.

아울러 양자 키 분배 네트워크와 기존의 공인 인증서 인프라와의 연동을 위한 표준화도 완료되었는데, 해당 권고안은 X.1715로 제정되었다. 해당 표준의 명칭은 '양자 키 분배 네트워크와 암호 인프라와의 연동을 위한 보안 요구 사항과 방안' (Security requirements and measures for integration of QKDN and secure network infrastructures)이다.

Ⅳ. 양자키 분배 기술 표준화

이 소단원에서는 ITU-T SG17에서 현재 표준화가 진행 중인 양자키 분배 기술 표준화 과제 각각에 대해 살펴보도록 한다. 표 2는 현재 ITU-T SG17에서 양자암호 보안 영역 표준화를 담당하고 있는 실무반인 Q15에서 진행 중인 표준화 과제를 요약한 표이다. 본 절에서는 주요 과제의 내용을 간략히 살펴보도록 한다.

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

표준화 과제	과제명
X.sec-qkd-profr	Framework of quantum key distribution (QKD) protocols in QKD network
X.sec-QKDN-tn	Security requirements for Quantum Key Distribution Networks-Trusted node
TR.hyb-qsafe	Overview of key management of hybrid approaches for quantum-safe communications
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
X.sec-QKDNi	Security requirements for Quantum Key Distribution Network interworking (QKDNi)

4.1. 양자키 분배 네트워크를 위한 신뢰 노드 보안 요구 사항

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.

양자 키 분배 기술은 송수신단 사이 잠재적인 도청자에게 알려지지 않는 공통의 무작위 이진 키를 공유할 수 있도록 하고 정보 이론적 보안(ITS)을 양자 역학의 법칙에 기반하여 제공할 수 있는 최고 수준의 보안 기술이나 송수신단 링크 거리에 제한이 있다. 하여, 실제로는 신뢰할 수 있는 노드를 송수신단 사이에 다수 두어 양자키 분배 기술을 원거리간에도 사용할 수 있도록 하는데 이러한 신뢰노드는 양자키 분배 네트워크가 키 분배 거리를 확장하고 양자키 분배 기술 기반 응용 프로그램을 보완하는 데 널리 채택되고 있다. 신뢰 노드의 보안은 일반적으로 그 양자키 분배 네트워크 구성에서 도청자의 접근이 불가능하다고 가정되지만, 이러한 가정을 만족하기 위해 실제 환경에서 다양한 보안 요구 사항을 필요로 한다. 그러나 양자키 분배 네트워크의 핵심인 신뢰 노드와 그와 관련된 보안 요구 사항은 아직 명확히 다루어지지 않았었고, 하여 해당 권고안에서 양자키 분배 네트워크의 신뢰 노드에 대한 보안 요구 사항을 정의하고자 하고 있다. 이 권고안은 신뢰 노드의 보안 위협을 분석하고 보안 요구 사항을 정의하며, 이러한 요구 사항을 충족하는 방안을 표준화하는 것을 목적으로 한다.

4.2. 양자 내성 통신을 위한 하이브리드 키 관리 개요

양자키 분배 기술과 양자 내성 암호를 결합하여 양자 내성 통신을 구성하는 다양한 방법을 분석하고자 새로운 기술보고서가 제안되어 새로운 과제로 표준화가 시작되었는데 해당 과제의 명칭은 ‘양자 내성 통신을 위한 하이브리드 키 관리 개요’ (Overview of key management of hybrid approaches for quantum-safe communications)이다.

양자키 분배 기술은 정보 이론적 보안을 키 교환에 대해 보장할 수 있지만, 특수한 장치와 네트워크 인프라를 필요로 한다. 이에 반해 양자 내성 (PQC) 알고리즘은 양자 컴퓨터 공격에 대해 안전하도록 개발되었지만, 여전히 복잡한 수학적 계산에 근거한 보안에 기반하고 있으며, 이는 미래에 새로운 알고리즘에 의해 보안이 깨질 수 있다는 것을 의미한다. 또한, 양자 내성 암호를 사용하는 상용 시스템은 아직 널리 사용되고 있지 않고 있는 상태이다. 미국에서 양자 내성 암호를 표준화 하고 있는 NIST는 양자 내성 암호 알고리즘의 표준화 작업을 수년간 진행해왔지만 아직 완료되지 않았으며, 최종 알고리즘이 보안 프로토콜에 적용되고 실제 네트워크에서 사용되기까지 더 많은 시간이 소요될 것으로 보인다. NIST에서 최종적으로 선택한 알고리즘이 실제 통신 네트워크에서 사용되기 위해서는 다른 표준화 기구에서 추가적인 표준화 작업이 필요하다. 따라서 양자 내성 암호가 보편적으로 사용되기 전에 양자키 분배 기술과 함께 적절하게 사용하는 것이 논의되고 있으며, 양자 내성 암호를 연구하는 양자 내성 암호 커뮤니티에서도 기존 암호와의 하이브리드 접근 방식이 논의되고 권장되고 있는 실정이다.

양자 키 분배 기술과 양자 내성 암호를 하이브리드 방식으로 결합하여 양자 내성 통신을 구현하기 위해서는 서비스 제공자들이 적용할 수 있는 다양한 옵션을 갖는 것이 중요하다. 이러한 다양한 옵션들을 분석하고 실제 적용된 사례들을 함께 고려하여 양자키 분배 기술과 양자 내성 암호를 함께 적용하는 키 관리 방법을 종합적으로 검토하는 것이 본 보고서의 목적이라고 하겠다.

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. 이 권고안에 대한 표준화는 양자키 분배 네트워크에서의 인증과 허가에 대해 연구하는 것을 목표로 한다. 또한 양자키 분배 네트워크 내에서 아이디와 공개 키 인증서 사용에 대해서도 살펴볼 예정이다. 이는 인증과 허가에 있어서 필수적인 요소들이라고 할 수 있다.

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.

4.4. 양자키 분배 네트워크의 양자키 분배 프로토콜 프레임워크

양자키 분배 기술에서 동일한 양자키를 송수신단에서 공유하기 위한 양자키 분배 프로토콜에 대한 표준화를 시작하기 위한 표준화 과제가 제안되어 승인되었는데 해당 과제의 명칭은 ‘양자키 분배 네트워크의 양자키 분배 프로토콜 프레임워크’ (Framework of quantum key distribution (QKD) protocols in QKD network) 이다. 해당 과제는 2023년 3월 회의에서 표준화 과제로 승인되었다.

ITU-T FG-QIT4N에서는 현재 ITU-T에서 표준화하고 있는 영역 외 양자암호 및 양자기술에 대한 표준화 가능성을 연구하였는데, 특히 FG-QIT4N의 결과물 중의 하나인 D2.3에서는 양자 키 분배 네트워크프로토콜 중에서도 퀀텀 계층에 대한 기술 보고서를 통해 표준화 관점에서 양자키 분배 프로토콜에 대한 개요를 이미 정리한 바 있다. 이 보고서에서는 양자키 분배 프로토콜 표준화의 미비점을 분석하고, SG 17에서 양자

키 분배 프로토콜 프레임워크 표준화 작업을 제안한 바 있는데, 이 제안을 기반으로 신규 표준화 과제를 제안한 것이 바로 '양자 키 분배 네트워크의 양자키 분배 프로토콜 프레임워크'이다. 해당 표준화 과제는 양자키 분배 프로토콜의 프레임워크를 정의하고, 양자키 분배 프로토콜을 구현하는 양자키 분배 모듈의 인증을 촉진하는 데 도움이 될 수 있을 것이다.

4.5. 양자 키 분배 네트워크 연동을 위한 보안 요구 사항

이 권고안 표준화는 다수의 양자키 분배 네트워크를 연동할 경우의 보안 요구 사항을 명시하는 것을 목적으로 한다. 특히, 이 권고안은 양자키 분배 네트워크 연동에 있어 보안 위협과 연동 시 인증 및 허가와 관련된 보안 요구 사항을 표준화할 예정이다.

Ⅴ. 결 론

양자암호기술은 다른 양자 기술에 비해 기술 성숙도가 높아 이미 통신네트워크 및 여러 산업 현장 등에서 사용되고 있는 기술로, 한국 뿐 아니라, 일본, 중국, 미국, 그리고 유럽의 여러 국가에서 다양한 실제 적용 사례들이 보고된 바 있다. 이에 본격적으로 생태계가 형성되어 가고 있고 다수의 양자키 분배 기술 장비업체와 사업자들이 상호호환성을 보장하기 위한 표준화가 진행되고 있으며, ITU-T SG17에서는 보안 영역과 관련된 표준화가 한창 진행 중에 있다. 본 고에서는 ITU-T SG17에서 양자암호 관련 표준화를 수행하고 있는 실무반인 Q15에서의 양자암호 보안 영역의 표준화 연혁과 현재 진행 중인 표준화 과제들의 최신 동향을 살펴 보았다.

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

〈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 혁신사업, 팀장
<관심분야> 5G, 통신공학, 정보보호, 양자암호, 기술표준화