# ITU-T SG15 양자키 분배 표준화 동향

윤빈영 한국전자통신연구원 책임연구원(byyun@etri.re.kr)

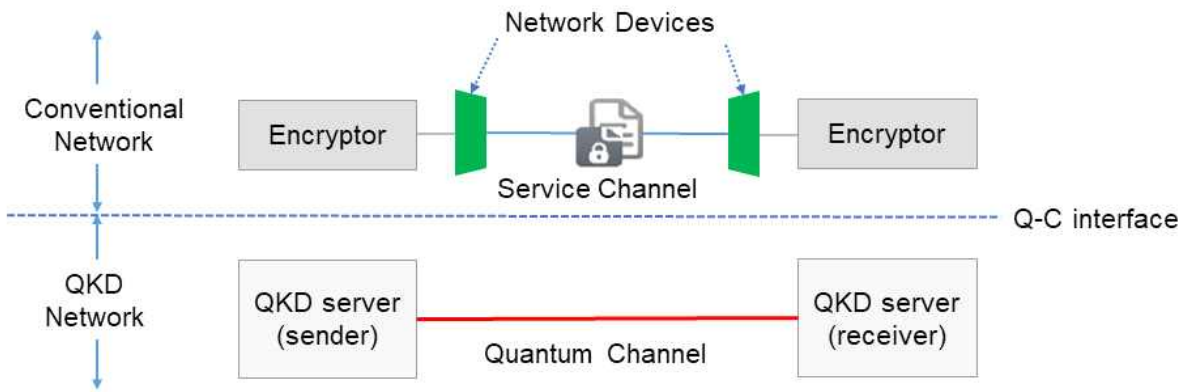
## 1. 머리말

한국의 통신사업자들에 의하여 주도적으로 제안된 양자키 분배(QKD, Quantum Key Distribution) 네트워크에 대한 표준화가 2018년 9월 ITU-T SG13 회의에서 착수되었다. 이후 SG13은 SG15를 포함하여 ITU-T 내부 SG(Study Group)들에게 관련 표준 착수를 통보하는 liaison을 송부하였다. 2018년 10월 개최된 SG15 총회에서는 관련 liaison 문서(Y.QKDN_FR, 'Framework for Networks to supporting Quantum Key Distribution')가 Q12/15에서 검토되었다.

## 2. Liaison 내용 요약

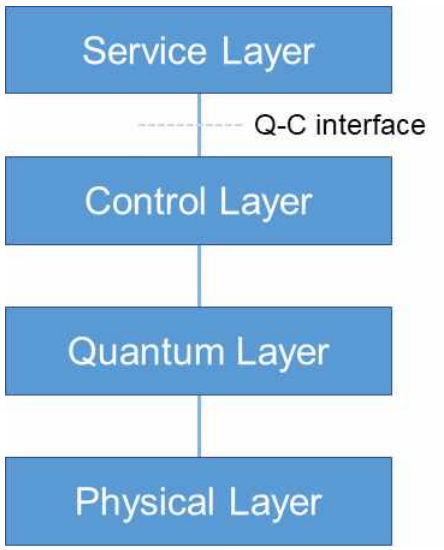
양자키 분배 기술은 양자키 알고리즘으로 사용될 수 있는 비밀키를 분배하는 기술로써 도청을 예방할 수 있는 완벽한 기술로 평가되고 있다. 양자키 분배와 암호화 데이터 전달 네트워크 구조는 [그림 1]과 같이 QKD 네트워크(QKD 서버)와 암호화된 데이터를 전달하는 네트워크(네트워크디바이스, Encryptor)로 구성된다.

송신측 QKD 서버(Sender)는 양자 채널(Quantum channel)을 통해서 양자키(Quantum Key)를 수신측 QKD 서버(Recever)로 전달한다. 양자 채널은 광케이블, 자유공간, 위성전파가 사용될 수 있으며, 포톤(quantum states of light) 형태의 양자키를 전달한다. 현재 광케이블을 사용하는 양자 채널의 경우, 광증폭소자와 같은 디바이스를 사용할 수 없는 제약 때문에 장거리 전송에 제약을 갖는다. 양자키로 암호화된 데이터는 디바이스 사이의 서비스 채널을 통해서 전달된다.




[그림 1] Integrated implementation structure of conventional network and QKD network

양자키 분배를 위한 네트워크 데이터 모델은 [그림 2]와 같이 서비스계층, 제어계층, 퀀텀계층, 물리계층으로 구분된다. 물리계층은 광, 자유공간, 위성전파를 통해서 양자키 전달을 지원하는 계층이며, 양자계층은 양자키를 전달하는 계층이며, 제어계층은 QKD 절차를 제어하는 오케스트레이션 기술을 제공하며, 서비스계층은 양자키에 의하여 생성된 암호화된 데이터를 전달하는 계층이다.




[그림 2] General layered model of the integrated networks

**3. 논의 결과**

SG15는 광기술 기반의 데이터전송 표준을 리딩하는 그룹으로 제안된 QKD 기술이 광전송기술과 어떠한 연관성을 가지고 있는지 논의되었다. SG13에서 보내온 liaison 문서(Y.QKDN_FR)는 양자키 분배 중심의 표준을 기술하고 있으므로 광전송 기술과의 연계성 부족으로 많은 논의가 진행되지 못했다. 즉, 양자키는 기존의 전송 기술에서 사용하는 전통적인 광신호 전달 방법이 아니기 때문에 SG15의 표준 업무와 직접적인 연관성이 없다는 의견이 있었다. 그러므로 기존 liaison 내용만으로는 SG15가 QKD 표준 착수가 어려움이 있으므로 좀 더 구체적인 정보를 SG13에 요청하기로 하였다.

현재 SG15에서 표준화하고 있는 전송 시스템은 데이터 전송을 위한 시스템으로 양자키 전송을 위해서 사용되기 어렵다. 따라서 양자키를 전달하기 위한 물리적인 특성(예를 들어, optical characteristcs 등)에 대한 추가적인 정보 제공이 요구된다. 그러므로 QKD와 관련된 계층 모델(layered model)에 대해서 좀 더 구체적인 정보 제공을 요청한다. 참고로 SG15는 G.800 권고안에 따라서 정보를 전달할 때 전송되는 데이터 포맷과 관련된 경우에만 계층(layer)이라는 용어를 사용하고 있다.