

## 양자암호 네트워크 제어 및 관리 표준 기술

## 최태상

한국전자통신연구원

## 요약

양자정보통신 기술은 양자의 물리학적 성질을 이용하여 정보를 생성, 전송, 저장, 가공하는 정보통신 기술로서, 크게 양자통신, 양자센서/이미징 및 양자컴퓨팅으로 분류된다. 관련 기술 표준화를 위해 먼저 ETSI(유럽전기통신표준기구) 산하 ISG-QKD 위원회에서 QKD 네트워크가 아닌 양자암호 분배 장비 관점의 표준화 활동을 개시하였으며 QKD를 네트워크로 확장하기 위해 ITU-T SG13/SG17/SG11에서는 단계적으로 시장의 필요성이 높은 양자암호 분배 네트워크, 양자암호 보안과 관련 프로토콜에 대한 국제 표준화 활동을 활발히 진행 중에 있다. 또한 ITU-T가 후원하는 QIT4N(Quantum Information Technology for Network) FG(Focus Group)이 양자센서/이미징 및 양자컴퓨팅 관련 표준화 사전 단계의 활동을 추진 중에 있다. 본 고에서는 이들 주요 단체의 표준화 활동 중 특히 국내 ETRI 및 KT가 주도한 QKDN 제어 및 관리 표준화 동향, 개발 중인 표준 기반 QKDN 제어 및 관리 기술 및 기술 적용 Use Case/사례, 마지막으로 본 기술 분야의 향후 개발 방향 및 challenge에 대해서 소개한다.

## I. 서론

양자정보통신 기술은 양자의 물리학적 성질을 이용하여 정보를 생성, 전송, 저장, 가공하는 정보통신 기술로서, 크게 양자통신, 양자센서/이미징 및 양자컴퓨팅으로 분류된다. 이 중 양자통신은 양자암호 분배 (Quantum Key Distribution, QKD), 양자전송, 및 양자 네트워크로, 양자센서/이미징은 양자 측정, 양자센싱, 및 양자 이미징으로, 양자컴퓨팅은 양자 시뮬레이터, 물리양자비트, 논리양자비트, 양자소프트웨어로 각각 세 분류된다. 이 중 ITU-T SG13, SG17 및 SG11에서는 단기적으로 시장의 필요성이 높은 양자암호 분배 네트워크, 양자암호 보안과 관련 프로토콜에 대한 국제 표준화 활동을 활발히 진행 중에 있다. 또한 양자정보통신 기술의 중장기적인 발전 관점에서 ITU-T

가 후원하는 QIT4N(Quantum Information Technology for Network) FG(Focus Group)이 양자센서/이미징 및 양자컴퓨팅 관련 표준화 사전 단계의 활동을 2019년 12월 9일 중국 진안에서 개최된 키크오프 회의를 시작으로 추진 중에 있다.

QKDN 표준화 작업의 개요는 아래 <그림 1>에서 보는 바와 같이 SG13 WP3 Q.16, WP1 Q.6, SG17 Q.15, SG11 Q.2, 및 FG QIT4N에서 다양한 표준 개발이 진행 중에 있다. 2018년 9월에 제정된 첫번째 QKDN 표준인 Y.3800(Overview on networks supporting quantum key distribution)을 필두로 2020년에 Y.3801 - Y.3804 표준이 제정되었으며 2021년 현재 17건의 추가 표준화 작업이 일부는 제정 완료되었거나 개발이 활발히 이루어지고 있다. 신뢰 네트워킹을 담당하고 있는 SG13 Q16에서 Y.3801(formerly Y.QKDN-req), Y.3802(formerly Y.QKDN-arch), Y.3803 (formerly Y.QKDN-KM), Y.3804 (formerly Y.QKDN-CM)은 2020년 10월에 모두 제정 완료되었으며, 추가적으로 Y.3805 (formerly Y.QKDN-SDNC) 권고안이 2021년 12월에, Y.3808 (formerly Y.QKDN\_frint)이 2022년 2월에 제정 완료되었으며 와 Y.3809(formerly Y.QKDN\_BM)이 2021년 12월에 승인된 후 현재 AAP Review 과정에 있다.

서비스품질(QoS)를 담당하고 있는 SG13 Q6에서 Y.3806 (formerly Y.QKDN-qos-req)를 2021년 9월에 제정하였으며, Y.3807(formerly Y.QKDN-qos-pa)를 2021년 12월에 승인하

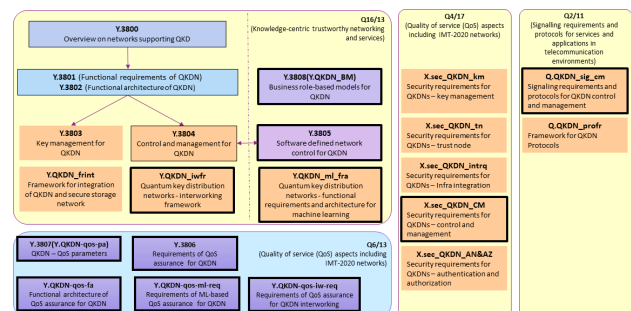


그림 1. OKDN 관련 표준 문서 관계도

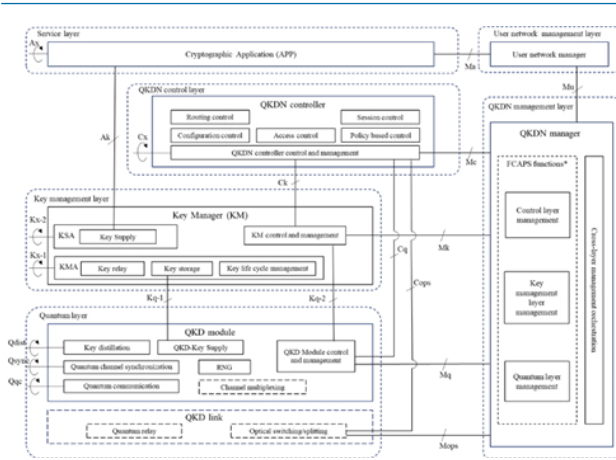


그림 2. QKD 기능 구조

였으며, Y.QKD-qos-fa, Y.QKD-qos-ml-req 권고안 표준화 작업이 진행 중이다. 특히, 2021년 하반기 부터는 상기 제정 완료된 QKD 기본 표준의 후속 작업으로 복수개의 QKD의 범위로 확장된 QKD interworking 및 machine learning을 QKD에 적용하기 위한 표준화 작업이 개시되었다.

〈그림 2〉는 상기에서 언급된 표준 권고안 개발 과정 및 결과를 참여 국, 기관, 이해관계를 중심으로 정리하였다.

〈그림 2〉는 Y.3802에 정의된 QKD 기능 구조로 물리계층인 QKD 모듈과 링크(link)로 구성된 양자 계층(Quantum Layer), 양자암호 키 수명 주기를 관리하는 키 관리 계층(Key Management Layer), QKD를 제어하기 위한 제어 계층(Control Layer), QKD 관리를 위한 관리 계층(Management Layer)로 구성되며 이들 간의 인터페이스 및 세부 기능 요소들이 정의되어 있다. 이들 요소 기능과 인터페이스를 표준화 함으로써 다양한 이기종의 장비들 간의 상호 운용성을 보장할 수 있게 된다. 기능 구조 문서는 중국 Quantum Ctek이, 양자암호 키 관리 문서는 일본 NICT가, 그리고 제어 및 관리와 서비스품질 보증(QoS Assurance) 문서는 한국의 ETRI와 KT가 주 에디터로 표준화 작업을 주도하였다. 주요 참여 기관 외에 Huawei, SK Telecom, Toshiba, 그리고 영국, 미국, 캐나다 정부 등 다양한 기관들이 기고와 논의에 적극적으로 참여를 하였다. 표준 개발 회의는 정기적인 SG 레벨 회의와 RGM(Rapporteur Group Meeting) 외에 거의 1개월 단위로 가상회의(e-meeting) 혹은 임시 대면 회의를 통해 표준화 작업이 진행중에 있다.

양자암호 분배 네트워크 표준화 활동은 SG13 이전에 ETSI(유럽전기통신표준기구) 산하 ISG-QKD 위원회에서 QKD 네트워크가 아닌 양자암호 분배 장비 관점의 표준화 활동을 진행해 왔으나 네트워크 관점의 표준화 활동은 ITU-T SG13이 주도를 하고 있는 상황이다. SG15에서도 광 전송 네트워크 기술과

QKD를 접목하는 표준화 작업을 진행 중이며, SG17 및 ISO/IEC JTC1/SC27에서도 양자 암호학(Quantum Cryptography) 및 QKD 보안 요구사항과 구조 관련 표준화 작업이 진행중으로 SG13과 협력 관계를 유지하고 있다. 표준화 활동을 주도하고 있는 양자암호 통신 네트워크 관련 통신사업자, 벤더, 연구소 및 학계는 기술 개발을 통한 결과물의 기능 검증 및 상호운용성 시험 추진을 위한 다양한 시험망(Testbed) 구축을 위해 노력 중에 있다.

본 표준화 활동의 핵심 의미는 비 표준 All-in-one 블랙박스 시스템 방식으로 전세계 10개 이내 제조사(한국 전무)의 솔루션만 존재하는 현재 양자암호 시스템을 국내의 경쟁력이 확보된 정보통신 기술로 개방형 양자암호 네트워크 국제표준으로 확장하여 국내 관련 산업체 및 통신사업자가 경쟁력을 가질 수 있는 체제로 유도하고자 하는데 있다. 특히 본 표준화 활동을 통하여 ETRI 및 국내 QKD 제조사의 솔루션과 QKD 암호 응용, 제어 및 관리 솔루션의 상호운용성 확보를 통한 국제경쟁력을 제고할 수 있는 중요한 기회로 판단된다.

본 고에서는 상기 다양한 QKD 표준 기술 및 활동 중 국내 ETRI 및 KT가 주도한 QKD 제어 및 관리 표준화 동향, 개발 중인 표준 기반 QKD 제어 및 관리 기술 및 기술 적용 Use Case/사례, 마지막으로 본 기술 분야의 향후 개발 방향 및 challenge에 대해서 소개한다.

## II. QKD 제어 및 관리 기술 표준 동향

본 절에서는 QKD 제어 및 관리를 위해 ITU-T SG13의 Q.16 & Q.6에서 개발을 완료하였거나 현재 진행 중인 표준에 대한 동향을 정리하였다.

### 1. Y.3804 – Quantum key distribution networks – Control and management

QKD 제어 및 관리 최초의 표준은 2020년 9월 제정된 Y.3804 (Control and management for quantum key distribution networks) 이다. 본 표준의 주요 내용은 QKD 서비스의 품질 및 신뢰성을 보장하기 위해 필요한 제어 및 관리 기능을 정의하고 있다. 본 표준은 ETRI와 특히 QKD 사업자인 KT의 주도로 2019년 3월에 초안이 시작된 이후 QKD 표준화에 참여하고 있는 주요 기관들(중국의 Quantum CTEK & Huawei, 일본의 NICT, Toshiba, & NEC, 한국의 SKT, 스위스의 CAS Quantum networks, 캐나다, 미국, 영국)이 참여하여 최종 합의안이 도출되었다. 특히, 본 권고안은 ITU-T 국제표준

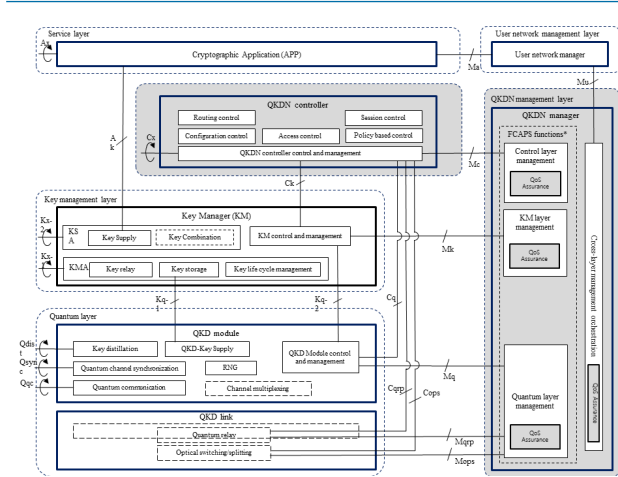


그림 3. QKDN 제어 및 관리 구조도

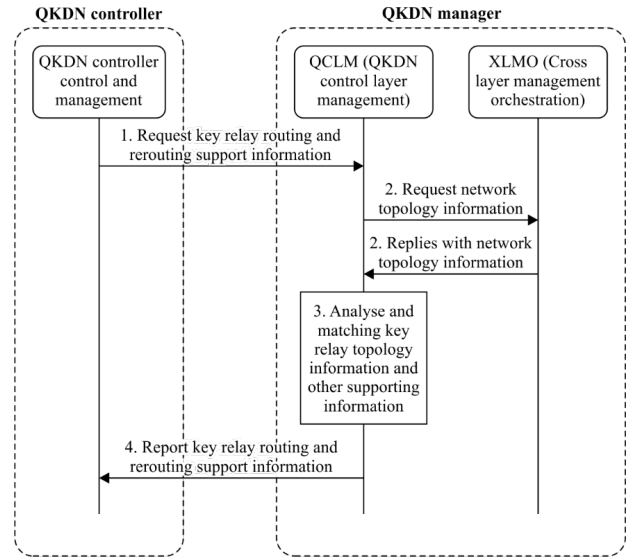
으로 승인 발간하게 된 최초의 QKDN 제어 및 관리 표준이라는 점에서 큰 의미가 있다.

〈그림 3〉은 QKDN 기능 구조 상에서 제어 및 관리 기능과의 관계를 도식하고 있다. 진하게 처리된 박스가 제어 및 관리 기능 범위를 나타낸다.

본 표준의 주요 내용은 QKDN 제어 및 관리를 위한 기능적 요소 및 관련 기능, 참조점 및 절차를 지정한다. 보다 구체적인 기능은 다음과 같다.

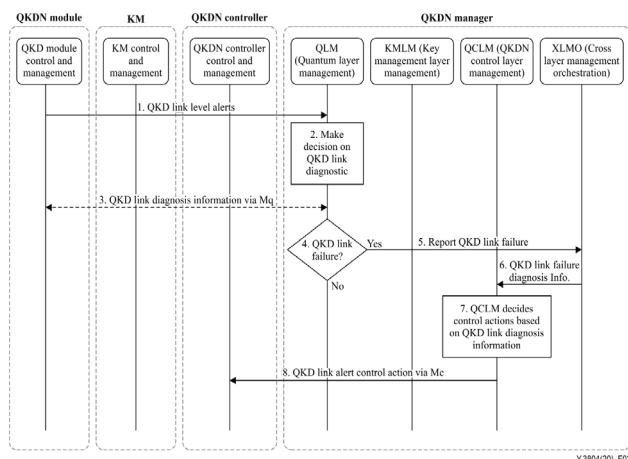
- 제어 및 관리 특정 기능 (예: 라우팅 제어를 위한 경로 계산, 세션 제어를 위한 액세스 트래픽 조정/스위칭/분할을 포함한 세션 제어, QoS 및 과금 정책 제어, 각 계층에 대한 FCAPS(Fault, Configuration, Accounting, Performance, and Security) 관리)
- 제어 및 관리 기능 구성 요소와 다른 계층의 구성 요소간 제어 및 관리 참조점
- 다 계층의 제어 및 관리 오케스트레이션 기능. QKDN 관리 계층에는 다중 계층 (양자, 키 관리 및 QKDN 제어 계층) 및 교차 계층 관리 및 오케스트레이션을 담당하는 여러 기능
- 외부 관리 시스템, 특히 사용자 네트워크 관리 시스템과의 연동 기능, 관리 능력 노출 기능 등

QKDN 각 계층에는 계층에 구체적인 제어 및 관리 기능이 있다. 이를 위해 각 계층별 제어 및 관리 기능은 QKDN manager의 각 계층 관리 기능과 해당 계층 기능 간에 관리 에이전트 기능을 제공한다. 또한 계층 간 관리 조율이 필요한 경우를 위해서 다중 계층 관리 오케스트레이션 기능을 제공한다. 제어 및 관리 계층과 QKDN의 각 계층의 제어 및 관리 기능 요소와의 통신을 위해서 표준 인터페이스인 참조점이 정의되어 있는데 Cx, Ck, Cq, Cops 및 Cqrp는 QKDN 제어를 위해, Mq, Mqrp, Mops, Mk, Mc 및



Y.3804(20) F09

그림 4. QKDN Key relay re-routing 제어 절차



Y.3804(20) F02

그림 5. QKDN 링크 장애 관리 절차

Mu는 QKDN 관리를 위해 표준 인터페이스로 정의되어 있다.

또한 본 표준은 Key relay routing 제어, QKDN 장애 관리를 포함하는 다양한 QKDN 제어 및 관리 절차를 정의하고 있는데 그 중 대표적인 절차인 Key relay re-routing 제어 및 QKDN 장애관리 절차를 다음에 예시한다. 〈그림 4〉는 key relay re-routing 제어 절차를 도식하였다. QKDN controller가 key relay re-routing을 결정할 때 필요한 추가 정보를 QKDN manager에게 요청하면 QKDN manager는 보유하고 있는 네트워크 토폴로지 정보등을 활용하여 re-routing에 필요한 토폴로지 및 관련 제어 정보를 QKDN controller에게 제공하여 re-routing을 제어할 수 있도록 지원한다.

〈그림 5〉는 QKDN 링크에 장애가 발생했을 경우 QKDN



manager가 어떻게 대처를 하는지에 대한 장애 관리 절차를 도시하였다.

QKDN 링크에 장애가 발생하면 QKDN manager는 장애 경고 메시지를 전달받고 장애에 대한 진단을 한 후 필요한 제어 명령어를 생성하여 QKDN controller를 통해서 장애 해결을 위한 제어 액션을 수행하는 절차를 보여준다. 이 외에 다양한 제어 및 관리 절차가 세부적으로 명시되어 있다.

## 2. Y.3805 - Quantum key distribution networks - Software Defined Networking control

Y.3805 표준은 QKDN 제어를 위해 SDN 기술을 적용하고 있으며 요구사항, 기능 구조, 참조점, 계층적 SDN 제어 기능, 및 SDN 기반 제어 절차를 정의하고 있다. SDN 기술의 특성상 기존의 제어 방식 대비 몇 가지 장점을 가지고 있는데 대표적으로 SDN 제어는 논리적으로 중앙집중적, 프로그래머블 및 계층적 제어 기능을 제공한다. 또한 제어 응용에 인터페이스를 직접 제공함으로써 신속한 서비스를 제공할 수 있다. <그림 6>은 QKDN 환경에서 계층적 SDN 제어를 제공하기 위한 개념을 도시하였다. 제어를 할 QKDN의 규모가 클 경우 여러 개의 작은 sub-QKDN으로 나누고 각 sub-QKDN은 별도의 SDN controller를 통해 독립적으로 제어가 되며 전체 QKDN의 제어는 상위 계층의 controller를 통해서 상호 필요 정보를 교환하면서 이루어진다. 계층의 깊이는 관리 대상이 되는 QKDN의 규모에 비례한다.

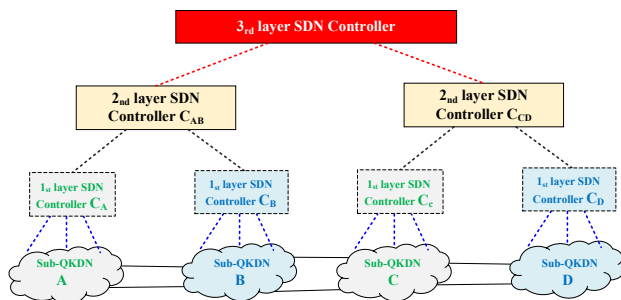


그림 6. QKDN의 계층적 SDN 제어 개념도

다음은 본 표준의 주요 특징으로 설명된 계층적 제어 대표 절차로 <그림 7>은 계층적 key relay routing 제어 절차를 설명한다. Key relay의 요청이 KM 계층에서 전달되면 첫번째 계층의 SDN controller가 key relay 경로가 자체 sub-QKDN 내부에서 결정되는지 여부를 판단한 후 범위를 벗어날 경우 상위 SDN controller에게 요청을 하고 필요한 계층까지 전달된 후 경로를 결정하게 되며 결정된 경로의 설정도 역순으로 하부 SDN

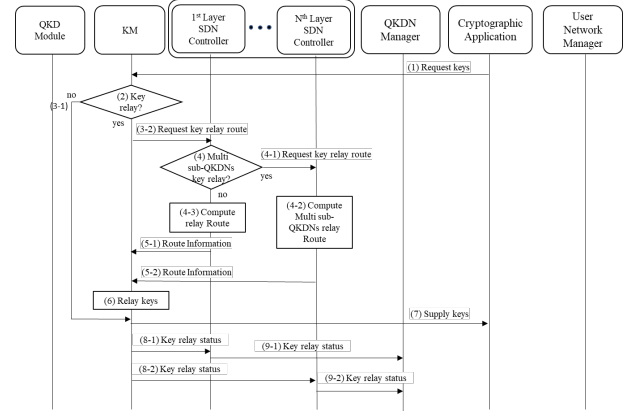


그림 7. SDN기반 계층적 key-relay 제어 절차

controller를 통해서 이루어진다.

본 표준에서는 이외에도 다양한 SDN 기반의 제어 절차에 대해서 정의를 하고 있는데 특히 Y.3804에서 정의된 QKDN 제어 절차는 중복되게 반복하지 않고 SDN과 연계된 절차만을 정의하고 있다.

## 3. Y.3806 - Quantum key distribution networks - Requirements for QoS assurance

ITU-T 표준 Y.3806은 QKDN의 서비스 품질보장 요구사항을 정의하는데 본 표준의 주요내용은 QKDN Controller와 Manager에 내제된 QoS 보장 기능이 지원해야 하는 요구사항을 정의한다. 특히 상위 요구사항은 QKDN QoS 보장에 필요한 Service Level Agreement (SLA), QoS 협상, QoS class, QKDN 구간 네트워크 (QAN QBN)의 QoS 보장 및 종단간 QoS 보장에 필요한 상위 개념의 요구사항을 정의하며, 세부 기능 요구사항은 QKDN QoS planning, QoS monitoring, QoS optimization, QoS provisioning, and QoS protection/recovery 영역으로 나누어 각 영역별 세부 QoS 보장에 필요한 기능 요구사항을 정의하고 있다. 본 표준은 국내 대표 QKDN 서비스 사업자의 관리 시스템의 핵심 표준으로 결정되었으며 정부 주도의 뉴딜 사업의 일환으로 개발 중인 QKDN 관리 시스템에 적용이 단계적으로 이루어질 것으로 예상된다. 본 표준은 ETRI와 KT의 주도로 초안이 시작된 이후 QKDN 표준화에 참여하고 있는 주요 기관들 (중국의 Quantum CTEK & Huawei, 일본의 NICT, Toshiba, & NEC, 한국의 SKT, 스위스의 CAS Quantum networks, 캐나다, 미국, 영국)이 요구사항으로 인한 상호 이해관계를 관철하기 위한 치열한 공방 끝에 2021년 9월에 최종 표준으로 승인되었다.

#### 4. Y.3808 - Quantum key distribution networks - Performance parameters

표준초안 Y.3808 (formerly Y.QKDN\_qos\_pa)은 Y.3806과 같은 시기에 시작되어 QKDN QoS 보장을 위한 서비스 및 네트워크 QoS의 관계 및 품질 지표를 정의하는 것을 목표로 개발을 시작하였으나 개발 과정에서 QKDN의 범위에 국한된 품질 지표를 정의하는 형태로 범위를 축소하여 2022 2월 최종 제정되었다. 본 표준은 QKDN 사업자인 KT 주도로 ETRI가 지원하고 UK, 중국, 일본의 여러 기관에서 참여하고 의견을 조율하여 첨예한 논쟁 끝에 승인을 득함.

〈그림 8〉은 QKDN QoS 보장에 가장 중요한 KSA key 전달 절차를 설명한다. 모두 5 단계의 step으로 구성되며 이 중 QKDN QoS parameter에 직접적인 영향을 주는 step에 step 3은 제외된다. 즉, cryptographic application과 QKDN간의 직접적인 관계가 있는 step에 대해서만 QoS parameter를 정의를 하는 것을 본 표준에서는 원칙으로 하고 있다. 〈그림 9〉는 본 표준에

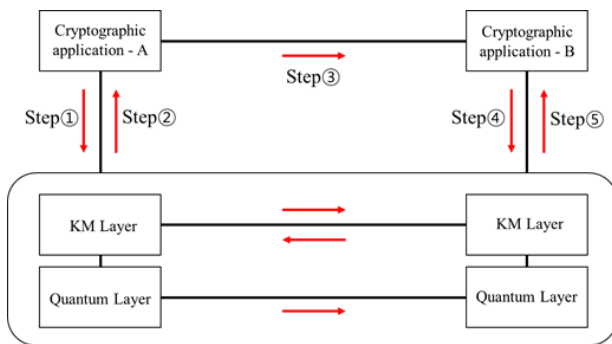


그림 8. KSA key 전달 절차

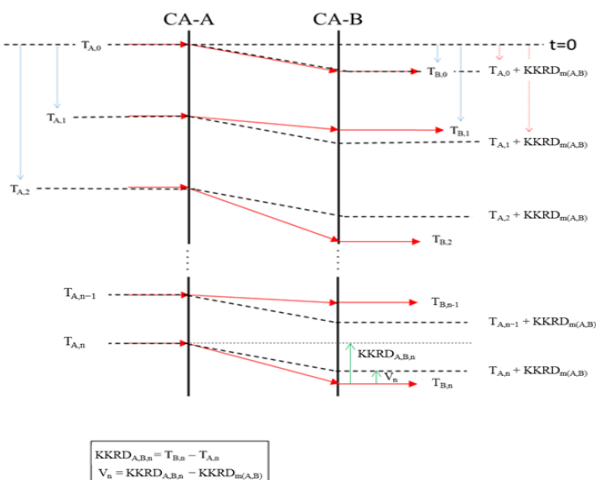


그림 9. KSA key response delay variation 품질 지표

서 정의하고 있는 다양한 QoS parameter 중 대표적으로 KSA key response delay variation 품질 지표를 도식화하였다.

상기 표준들은 현재 시점에 표준 개발이 완료되어 제정이 된 표준들이다. 다음은 현재 개발이 진행 중인 QKDN 제어 및 관리 관련 표준들에 대해서 정리하였다.

#### 5. Y.QKDN\_qos\_fa - Quantum key distribution networks - Functional architecture for QoS assurance

표준초안 Y.QKDN\_qos\_fa는 QKDN의 서비스 품질보장 구조를 정의하며, QKDN의 서비스 품질 보장 개론, 양자암호분배망의 서비스 품질 보장을 위한 기능 구조, 기능 구조의 참조점, 서비스 품질 보장을 위한 절차를 포함한다. 본 표준안의 내용은 거의 개발 완료단계에 와 있으며 2022년 7월 회의에서 승인을 요청할 예정이다. 본 표준안은 ETRI가 주도하고 있으며 KT, 중국 Rayton Networks Technology 사가 공동으로 참여 중이다. 〈그림 10〉은 QKDN의 서비스 품질보장 구조도로 세부 기

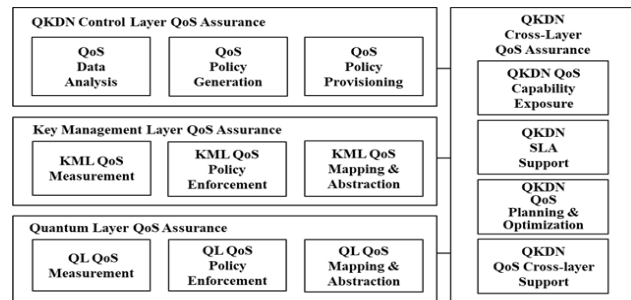


그림 10. QKDN QoS 보장 기능 구조도

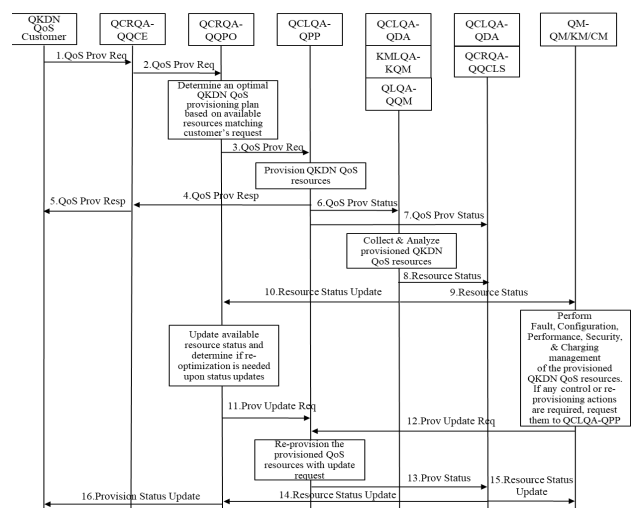


그림 11. QKDN 서비스 생명주기 QoS 보장 절차

능을 보여준다. QKDN의 Quantum, Key management, 및 control 계층별로 각각 QoS 보장을 위한 기능들을 정의하였으며 이들 계층간의 상관관계를 가진 복합적인 경우를 위한 계층간 QoS 보장 기능도 정의되어 있다. 본 표준에서는 이들 개별 기능에 대한 세부 내용과 기능들간의 인터페이스 및 QKDN QoS 보장을 위한 절차도 포함한다.

〈그림 11〉은 QKDN 서비스 생성, 모니터링, 장애 및 성능 관리, 자원 최적화 등을 포함하는 전체 생명 주기 동안 QoS 보장 절차의 한 예를 보여준다.

## 6. Y.QKDN\_qos\_ml\_req - Quantum key distribution networks - Requirements of machine learning based QoS assurance

표준초안 Y.QKDN-qos-ml-req는 QKDN 서비스 품질보장을 위한 기계학습의 기능 요구사항을 정의함. 특히 QKDN 기계학습의 기능 모델은 데이터 수집 기능, 분석 기능, 지능화 기능, 서비스 품질 관리 및 제어 기능으로 구성됨. 제안한 기능 모델은 구성 기능을 통해 데이터 수집, 정보 분석, 서비스 품질 예측, 서비스 품질 결정, 서비스 품질 보장 등의 절차를 수행함. 본 표준은 ETRI가 주도하여 개발 중에 있으며 KT와 중국 측에서 적극적으로 기고에 참여하고 있음. 본 표준은 2022년 하반기를 승인 목표로 작업 중임.

## 7. Y.QKDN\_ml\_fra - Quantum key distribution networks - Functional requirements and architecture for machine learning

표준초안 Y.QKDN\_ml\_fra는 중국과 공동으로 개발을 진행 중인 QKDN에 머신러닝 기능을 적용하기 위한 기능 요구사항 및 구조를 정의하는 표준으로 QKDN에 AI 기술을 접목하는 기반 표준이다. QKDN의 효율적이고 안전한 운영을 위해 다양한 형태의 ML 기능이 요구되고 있다. 예를 들면 QKDN 자원 활용의 최적화, 장애 원인 분석 및 예측, Quantum channel 성능 최적화 등이 대표적이다. 본 표준 개발은 2021년 7월에 승인된 Y.Suppl\_QKDN\_mla 문서에서 정의된 다양한 유즈케이스를 실현하기 위한 기능 요구사항 및 구조를 정의하기 위해 2021년 7월 회의에서 시작된 개발 초기 단계이며 ML 기능을 QKDN 구조에 어떻게 접목할 것인가에 대한 논의가 집중적으로 다루어지고있다. 본 표준안은 국내 주도의 IPR 확보를 위해서도 중요한 표준으로 관련 표준 특허 확보를 위한 전략적인 노력이 필요할 것으로 판단된다.

〈그림 12〉는 현재 논의 중인 ML-enabled QKDN 구조 3가지 방안으로 향후 논의를 거쳐 합의된 구조를 도출할 예정이다.

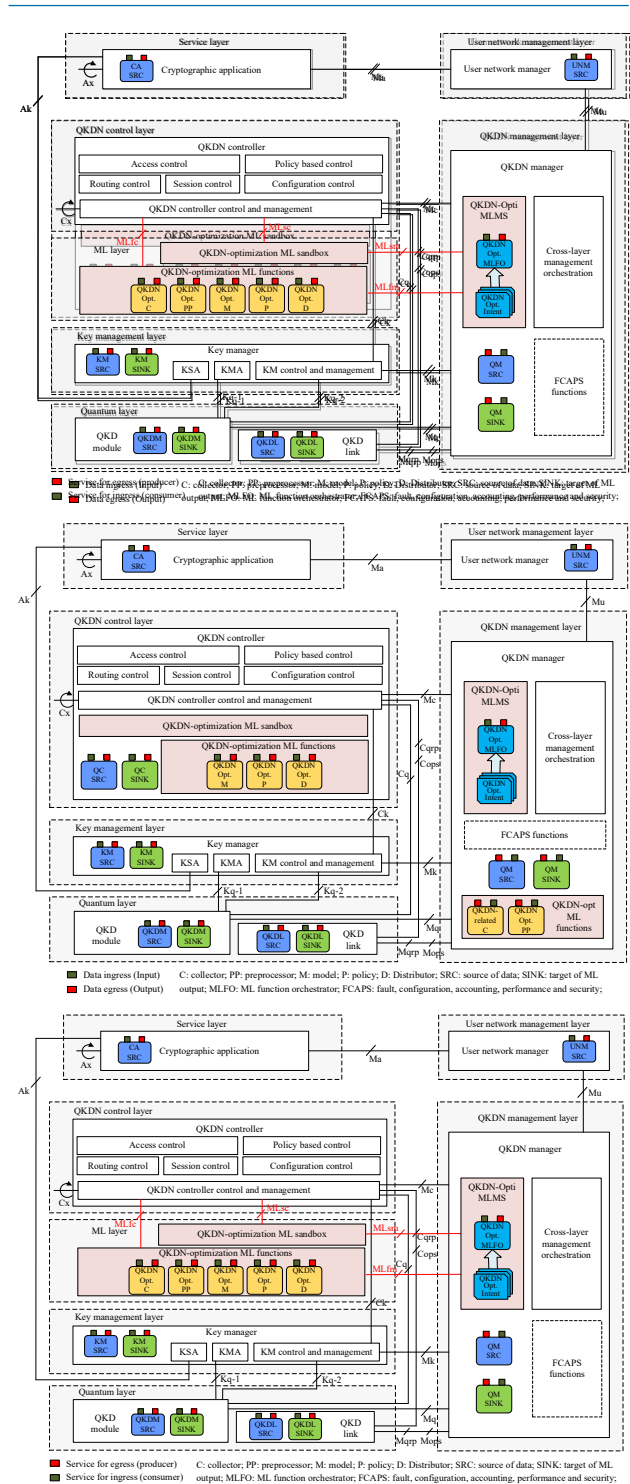


그림 12. ML기능의 위치에 따른 ML 기반 QKDN 구조

## III. QKDN 제어 및 관리 기술 적용 사례

상기에서 설명된 다양한 QKDN 제어 및 관리와 관련된 표준

들을 실제 서비스에 적용하기 위한 노력이 QKDN 표준을 주도하는 주요 기관들인 통신사업자, 벤더, 연구소 및 학계 중심으로 기술 개발을 통한 결과물의 기능 검증 및 상호운용성 시험 추진을 위한 다양한 시험망(Testbed) 구축을 위해 노력 중에 있다. 국내에서도 2020~21년 디지털 뉴딜정책의 일환으로 추진된 “양

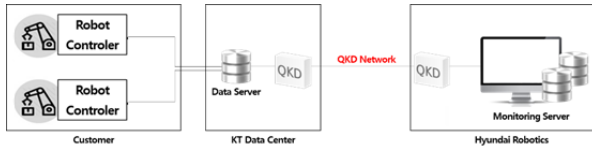


그림 13. QKDN for Smart Factory Use Case



그림 14. QKDN for Social Safety Use Case

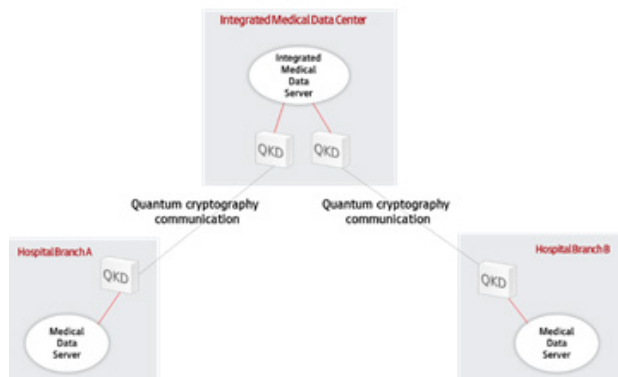


그림 15. QKDN for Medical Centre Use Case

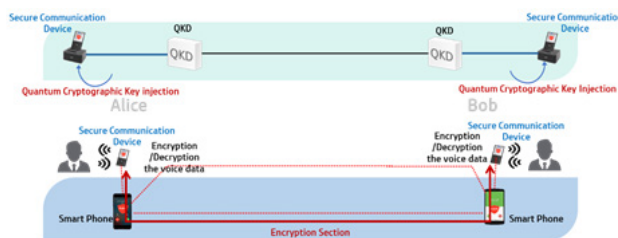


그림 16. QKDN for Secure mVoIP Use Case

자암호통신 시범인프라 구축/운영”과제를 KT 컨소시엄에서 추진하면서 일차적으로 Y.3804의 내용을 중심으로 QKDN 서비스 관리 시스템을 개발하고 이를 시범사업에 적용하였으며 대표적인 양자암호통신 응용서비스 유즈 케이스의 표준화도 연계하여 추진 중에 있다.

대표적인 적용 유스케이스로 다음의 네 가지를 예로 들어보도록 한다. 첫번째가 드론을 활용한 사회 안전망 서비스, 두번째는 의료정보 보호를 위한 데이터 센터 보안 서비스, 세번째는 안전한 mVoIP 서비스, 마지막으로 스마트 팩토리 데이터 보안을 위한 서비스이다. 2021년 연말까지 뉴딜시범사업 1, 2단계를 완료하였으며 이 과정에 상기의 4가지 유스케이스를 적용하였으며, 표준화를 위해서 상기 유스케이스를 ITU-T Focus Group QIT4N (Quantum Information Technology for Networks)에서 개발한 Deliverables에 포함되어 있으며, 2022년 각 담당 Study Group에서 해당 Deliverables들의 표준화를 진행할 예정이다. <그림 13>~<그림 16>은 각 유스케이스의 개념을 도식화 하였다.

## IV. QKDN 제어 및 관리 기술 Challenges

본고에서는 현재까지 진행된 QKDN 표준화 동향을 살펴보고 이 중 국내 연구소 및 통신사업자들이 주도하고 있는 분야인 QKDN 제어 및 관리 기술 표준에 대해서 상세히 기술하였다. QKDN 기술은 아직 개발 및 서비스 초기 단계에 있으며 단기, 중기, 장기적으로 해결해야 될 다양한 도전에 직면해 있다. 이를 위해 ITU-T FG-QIT4N에서는 <그림 17>에서와 같이 간략하게 QKDN의 도전을 정리하였다.

대표적인 표준화 challenge는 다음과 같다.

- QKDN 상호운영 기능 지원 표준화
- QKDN 프로토콜 표준화

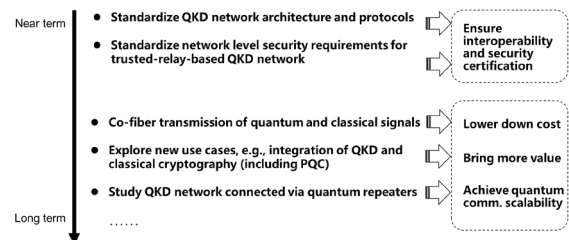


그림 17. Near to long term QKDN challenges



- 시간/주기 동기화 관련 요구사항/프로토콜 표준화
- Multi-protocol 통신 표준화
- AI/ML 기반 QKDN 표준화
- QKDN User Network 통합을 위한 표준화
- QKDN Scalability 표준화

이 중 QKDN 제어 및 관리와 연관된 항목들이 많이 존재하며 이에 대한 추가 표준 개발이 필요하다고 판단된다. 상기에서 기술하였듯이 AI/ML 기반 QKDN 제어 및 관리 표준화 작업은 이미 시작이 되었으며 QKDN Interoperability 표준 작업도 2021년 12월부터 활발히 진행 중에 있다. 연구소 및 통신사업자를 중심으로 국내 대표 참여 기관들도 이 도전을 잘 인지하고있으며 개발에 적극적으로 활동을 전개할 것으로 예상된다.

## V. 결론

본고에서는 현재까지 진행된 QKDN 표준화 동향을 살펴보고 이 중 국내 연구소 및 통신사업자들이 주도하고 있는 분야인 QKDN 제어 및 관리 기술 표준에 대해서 상세히 기술하였다. 또한 개발된 표준을 중심으로 다양한 시범 사업에 적용을 위한 노력을 경주하고 있는 사례들을 정리하였으며 마지막으로 현재 기술 및 표준 개발 초기에 있는 QKDN 이 당면한 다양한 도전에 대해서도 살펴보았다. 본고에서 언급하였듯이 QKDN 표준의 시발점이 된 Y.3800의 제안에서부터 QKDN 요구사항, 구조, 제어 및 관리 표준까지 국내 통신사업자 및 연구소를 중심으로 적극적으로 리딩을 하고 있으나 Quantum Information Technology의 중요성을 고려해 볼 때 보다 체계적이고 장기적인 리더십 확보를 위해서는 관산학연이 더욱 긴밀하게 연대하여 대응할 필요가 있을 것으로 판단된다.

## Acknowledgement

본 논문은 2022 년도 정부 (과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No. 2020-0-00557, 양자정보통신 표준기술 개발사업, 2020.4.1 ~ 2022.12.31)

## 참 고 문 헌

- [1] ITU-T Y.3800
- [2] ITU-T Y.3801
- [3] ITU-T Y.3802
- [4] ITU-T Y.3803
- [5] ITU-T Y.3804
- [6] ITU-T Y.3805
- [7] ITU-T Y.3806
- [8] ITU-T Y.3807
- [9] ITU-T Y.3808
- [10] ITU-T Y.3809
- [11] ITU-T Y.QKDN\_qos\_req
- [12] ITU-T Y.QKDN\_qos\_fa
- [13] ITU-T Y.QKDN\_qos\_ml\_req
- [14] ITU-T Y.QKDN\_ml\_fra

## 약 력



최 대 상

1988년 계명대학교 공학사  
 1991년 미주리-캔사스 주립대학교 공학석사  
 1995년 미주리-캔사스 주립대학교 공학박사  
 1996년~현재 한국전자통신연구원 네트워크연구본부 책임연구원  
 관심분야: Future Networks (5G/6G/V2X, etc) 관리, QoS 관리, 트래픽 측정/분석, 트래픽 엔지니어링, 양자암호네트워크 제어 및 관리