https://doi.org/10.7840/kics.2022.47.8.1068

# 안정적인 양자암호통신망 서비스 제공을 위한 양자키 확장 구조 및 서비스키 관리 방안

김 용 환•, 심 규 석*, 이 찬 균*, 이 원 혁°

# An Quantum Key Expansion Structure and Service Key Management Scheme For Providing Reliable Quantum Key Distribution Network Service

Yong-hwan Kim•, Kyu-Seok Shim*, Chankyun Lee*, Wonhyuk Lee°

요 약

최근 화두가 되고 있는 양자컴퓨팅 기술의 발전에 따라 기존의 통신 보안체계는 새로운 위협에 직면하고 있으며, 이에 따라 새로운 통신보안체계에 대한 이슈로 양자암호통신 기술이 부상하고 있으며, 양자암호통신은 양자키 분배, 데이터 암복호화, 데이터 전송기술로 구성되어 있다. 이 중 핵심이 되는 양자키 분배 기술은 양자의 불확정성의 원리를 활용하여 임의의 두 노드 사이에 대칭키를 기밀성을 보장하도록 생성 분배한다. 이에 따라, 최근 QKD 기반의 양자암호통신망 구축 및 서비스 응용 사례들이 등장하고 있다. 하지만 현재의 QKD 기반의 양자암호통신망 관리 및 서비스키 제공은 기본적인 기능 구현에 초점을 두고 있기 때문에 실질적인 양자암호통신 응용 보안 서비스를 제공하기 위해서는 다양한 응용 서비스 요구사항을 고려한 양자키 관리 및 장애 대응 방안 등의 추가적인 연구가 필요하다. 이에 따라, 본 논문에서는 양자키 부족 현상을 해결하고 양자암호통신망에서 발생할 수 있는 장애에 대응하여 안정적인 양자암호통신망 서비스 환경을 마련하기 위한 양자키 확장 구조와 양자키 관리 정책에 대하여 제안한다. 또한 한정적인 양자키 자원을 활용하여 다양한 양자암호통신 서비스들의 요구사항에 따라 서비스키를 안정적이고 원활하게 제공하기 위한 서비스키 관리 방안에 대하여 제안하고자 한다.

**Key Words :** QKD, Resource Management, Security, Stability, Network

ABSTRACT

With the development of quantum computing technology, the existing communication security system faces new threats. Accordingly, quantum cryptography communication technology is emerging as an issue for a new communication security system. quantum cryptography communication consists of quantum key distribution, data encryption/decryption, and data transmission technology. Among these, QKD technology uses the principle of quantum uncertainty to generate and distribute a symmetric key between any two nodes to ensure confidentiality. Recently, QKD-based quantum cryptography network construction and service application cases are emerging. However, since the current QKD-based quantum cryptography network management and service

※ 본 연구는 2022년도 한국과학기술정보연구원(KISTI) 주요사업 과제로 수행한 것입니다.
• First Author : Korea Institute of Science and Technology Information, yh.kim086@kisti.re.kr, 정회원
° Corresponding Author : Korea Institute of Science and Technology Information, livezone@kisti.re.kr, 정회원
* Korea Institute of Science and Technology Information, kusuk007@kisti.re.kr, 정회원; chankyunlee@kisti.re.kr, 정회원
논문번호 : 202205-099-B-RE, Received May 10, 2022; Revised May 29, 2022; Accepted May 29, 2022

key provision are focused on the implementation of basic functions, in order to provide practical quantum cryptography application security services, further research regarding quantum key management and failure response measures is needed. Accordingly, in this paper, we propose a quantum key extension structure and quantum key management policy to solve the quantum key shortage and provide a stable quantum cryptography network service environment in response to possible failures in the quantum cryptography network. In addition, we propose a service key management method to provide a service key stably and smoothly according to the requirements of various quantum cryptography communication services by using limited quantum key resources.transmission performance between containers that are dynamically created according to the user requirement.

## Ⅰ. 서 론

최근 화두가 되고 있는 양자컴퓨팅 기술의 발전에 따라 기존의 통신 보안체계는 새로운 위협에 직면하고 있으며, 이에 따라 양자컴퓨팅 환경에 대응 가능한 새로운 통신 보안체계에 대한 연구가 주목 받고 있다. 특히, 기존의 통신 보안체계인 RSA(Rivest Shamir Adleman[1]) 공개키 암호화 방식이 양자컴퓨팅을 통하여 빠르게 풀어낼 수 있다는 것이 증명된 이후 이러한 새로운 보안 체계에 대한 연구가 가속화되고 있는 실정이다[2,3]. 대표적으로, 새로운 통신보안체계에 대한 이슈로 양자암호통신 기술이 부상하고 있으며, 양자암호통신은 임의의 두 노드 사이에 양자역학적 원리를 활용하여 기밀성을 보장하는 대칭키를 생성 분배하는 양자키 분배(QKD, Quantum Key Distribution[4,5]) 기술, 분배된 비밀키에 기반 한 데이터 암호화 및 복호화 기술, 암호화된 데이터를 안전하게 전송하기 위한 데이터 전송 기술을 통칭하여 일컫는다.

이 중 양자키 분배 기술은 양자 불확정성의 원리를 기반으로 암호화 프로토콜을 구현하는 안전한 통신 방법을 제공하는 방안으로써 두각을 나타내고 있으며[6-8], 이러한 양자키 분배 기술은 복제 불가능성 원리와 측정 후 붕괴성질로 인해 단일광자를 정확하게 측정할 기회를 한 번으로 제한하여 수신자에게 도달하는 정보를 이용하여 공격자의 유무를 판단할 수 있는 방안을 제공한다[9].

하지만, 기본적으로 양자키 분배 기술은 물리적인 거리상의 제약을 지닌 단대단(Point to Point) 키 분배에 국한된 기술이다. 그렇기 때문에, 중장거리 구간의 양자키 분배 혹은 네트워크상에 존재하는 임의의 다수의 노드들 사이의 양자키 분배를 위해서는 신뢰 노드(Trusted node) 기반 네트워크 단위의 양자키 전달 메커니즘이 요구된다[10,11]. 즉, 양자키 분배 기술이 지닌 거리상의 제약을 해소하고 보다 다양한 환경에서 양자키를 활용한 응용 서비스를 제공하기 위해서는 QKD 네트워크에 대응하는 양자키 관리(Key Management, KM) 계층 망 구성 및 관련 프로토콜 개발을 통한 양자키 전달이 필요하다. 그리고 이 때, 양자키 관리 계층에서 네트워크 단위의 양자키 분배를 위하여 각 도메인마다 양자키 관리 시스템(QKMS, Quantum Key Management System)이 필수적으로 구축되어야 한다. 또한 각각의 도메인 내의 QKMS는 양자키 전달을 위한 경로 선정 등을 위하여 중앙 집중형태의 통합제어기(Q-SDN Controller)에 의하여 관리 및 제어될 필요가 있다. 그리고 이와 관련하여, 유럽전기통신표준협회(ETSI)[12], 국제전기통신연합 전기통신표준화부문(ITU-T)[13], 한국정보통신기술협회(TTA)[14] 등의 국내외 표준화 그룹에서는 QKD 네트워크 계층, 양자키 관리 계층, 서비스 계층으로 구성되는 양자암호통신망 구조 및 절차, 보안 요구사항 등에 대하여 활발하게 정의하고 있다.

한편, 이러한 단대단 양자키 분배를 위한 QKD 기술 및 장비는 상용화 수준으로 발전중이며, 국내의 경우 과학기술정보통신부 주관의 양자암호통신 인프라 시범구축 사업 등을 통하여 양자암호통신망 서비스의 개발 및 실험을 추진한 바 있다[15]. 하지만 아직까지 양자암호통신망 서비스를 안정적으로 제공하기에는 양자키 생성률 및 안정성 측면에서 충분한 수준으로 성숙되지 않았으며 이와 관련된 양자키 관리 정책 또한 미진한 상황이다. 물론, 점진적으로 위의 이슈들이 개선되겠지만 향후 동시에 많은 수의 다양한 양자암호통신망 서비스들을 끊김없이 안정적으로 제공하기 위해서는 서비스 보안 요구사항 수준에 따른 양자키 제공 정책 및 양자키 부족 등의 여러 장애 요인에 따른 대응 방안이 요구된다.

이에 따라, 본 논문에서는 한정적인 양자키 자원을 활용하여 상이한 보안 수준을 지닌 다양한 양자암호통신 서비스들의 요구사항을 충족하며 서비스키를 안

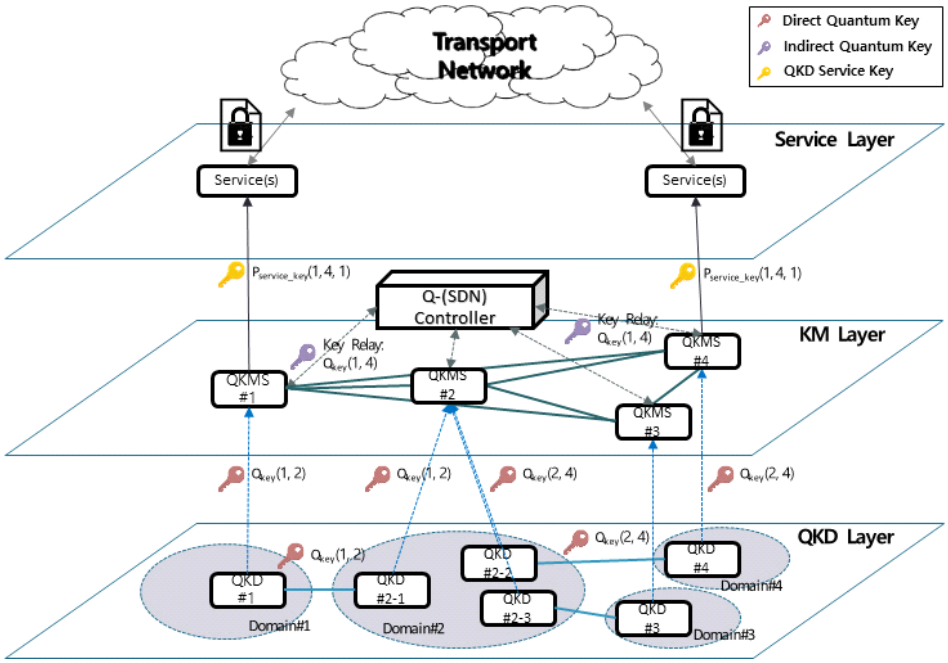


그림 1. 양자암호통신망 계층 구조 및 양자키 흐름
Fig. 1. Quantum cryptography network structure and quantum key flow

정적이고 원활하게 제공하기 위한 파생키 기반 양자키 확장 구조와 서비스키 관리 방안에 대하여 제안하고자 한다. 이를 위하여 보안 수준, 양자키 교체 주기, 요구 양자키 수 등 서비스 요구사항에 따른 2 단계 형태의 양자키 관리 구조를 제안하고 부 양자키 저장소 내의 양자키의 수를 항상 일정 수준 이상으로 유지할 수 있도록 확장함으로써 양자키 부족 현상을 해결하고 QKD 기반 양자암호통신망에서 발생할 수 있는 장애에 대응할 수 있는 방안을 제시하고자 한다. 또한 양자키 확장 구조를 서비스키 관리 방안과 연계하여 다양한 요구사항에 따라 동시에 다수의 서비스들을 지원할 수 있도록 전반적인 양자키 관리 방안을 고안하였다. 이를 통하여 안정적인 양자암호통신망 서비스 환경을 마련하는데 기여하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서 양자키 분배 기술 표준화 문서를 기반으로 한 양자암호통신 네트워크 계층 구조에서의 양자키 관리 구조와 양자키 전달 구조에 대하여 제시한다. 3장에서는 안정적인 양자암호통신망 서비스 환경을 제공하기 위한 QKD 기반 양자키 확장 구조와 서비스키 관리 방안을 제안하고, 4장에서 이에 기반 한 양자키 관리 시스템과 통합 제어기를 구현하여 양자암호통신망이 정상적으로 구동함을 보인다. 그리고 5장에서 본 논문의 결론을 맺는다.

## Ⅱ. 시스템 구조

### 2.1 양자암호통신망 구조

최근 양자컴퓨팅 기술이 부상함에 따라 ETSI, ITU-T, TTA 등 다양한 국내외 표준화 그룹에서 양자암호키 분배와 관련하여 양자암호통신망 전반에 걸친 표준화 작업이 활발하게 진행 중에 있다. 본 논문에서는 이러한 국내외 양자암호통신망 표준화 문서[16-19]에 따라 그림 1과 같이 QKD 네트워크 계층, 양자키 관리 계층, 서비스 계층으로 구성된 양자암호통신망 참조 모델을 따른다.

QKD 네트워크 계층에서는 QKD 장비, 그리고 이를 연결하는 양자 채널과 일반 채널로 구성되며, 두 링크로 연결된 임의의 두 QKD 장비 간에 양자역학적 특성을 활용하여 양자키를 생성 및 분배하는 역할을 수행한다. 양자키 관리 계층에서는 임의의 도메인마다 양자키 관리 시스템을 두고 해당 도메인내의 QKD 장비로부터 생성 및 분배된 양자키를 수집 및 관리한다. 또한 QKD 채널로 직접 연결되지 않은 도메인과의 양자키를 생성하기 위하여 QKMS간 양자키를 전달하는 역할을 수행하는 한편, 서비스 계층의 다양한 양자암호통신 서비스들에게 양자키를 제공하기 위한 양자키 생성, 삭제 등을 생애주기 관리를 포함하는 양자키 관리 역할을 수행한다. 또한 각각의 도메인 내의 QKMS

표 1. 양자키 관리 주요 매개 변수
Table 1. Main parameters for quantum key management

| Notation | Description |
|---|---|
| $Q^{p_{key}}(s,t)$ | QKMS 주 양자키 저장소 |
| $Q^{s}_{key}(s,t)$ | QKMS 부 양자키 저장소 |
| $q^{p}_{key}(s,t)$ | $Q^{p_{key}}(s,t)$에 저장된 양자키 |
| $q^{s}_{key}(s,t)$ | $Q^{s}_{key}(s,t)$에 저장된 양자키 |
| $N^{p_{key}}(s,t)$ | $Q^{p_{key}}(s,t)$의 현재 총 양자키 수 |
| $N^{s}_{key}(s,t)$ | $Q^{s}_{key}(s,t)$의 현재 총 양자키 수 |
| $th^{p}_{key}(s,t)$ | $Q^{p_{key}}(s,t)$의 최소 양자키 보유량 임계치 |
| $th^{s}_{key}(s,t)$ | $Q^{s}_{key}(s,t)$의 최소 양자키 보유량 임계치 |
| $P_{service\_key}(s,t,n)$ | QKMS $s$와 QKMS $t$ 사이의 $n$번째 서비스 세션에 대한 양자키 저장소 |
| $p_{service\_key}(s,t,n)$ | $P_{service_key}(s,t,n)$에 저장된 서비스키 |

들은 중앙 집중형 방식의 통합제어기에 의하여 관리 및 제어된다. 그리고 서비스 계층에서는 다양한 양자암호통신 서비스들이 양자키 관리 계층의 QKMS에 암호화키를 요청하여 공급받은 양자키를 기반으로 암호화 서비스를 제공하는 역할을 수행한다. 그림 1은 이러한 국내외 양자암호통신망 표준에 따른 양자암호통신망의 전체적인 구조 및 키 전달 흐름을 보여준다.

### 2.2 양자키 관리 구조

본 논문에서는 다양한 양자암호통신망 서비스의 안정적인 지원을 위하여 양자키 관리 네트워크상에서 각 도메인을 담당하는 QKMS#$s$는 네트워크상의 서로 다른 임의의 모든 QKMS#$t$마다 별도의 양자키 저장소(Quantum Key Pool, $Q_{key}(s,t)$)를 사전(Proactive Method)에 생성하여 관리함을 가정한다. 그리고 이 때, 각각의 도메인을 담당하는 QKMS#$s$는 서로 다른 임의의 모든 QKMS#$t$마다 주 양자키 저장소(Primary Quantum Key Pool, $Q^{p_{key}}(s,t)$)와 부 양자키 저장소(Secondary Quantum Key Pool, $Q^{s}_{key}(s,t)$)를 사전에 생성하여 관리함을 가정하며, 해당 저장소 내의 양자키를 각각 $q^{p}_{key}(s,t)$. $q^{s}_{key}(s,t)$라 정의한다.

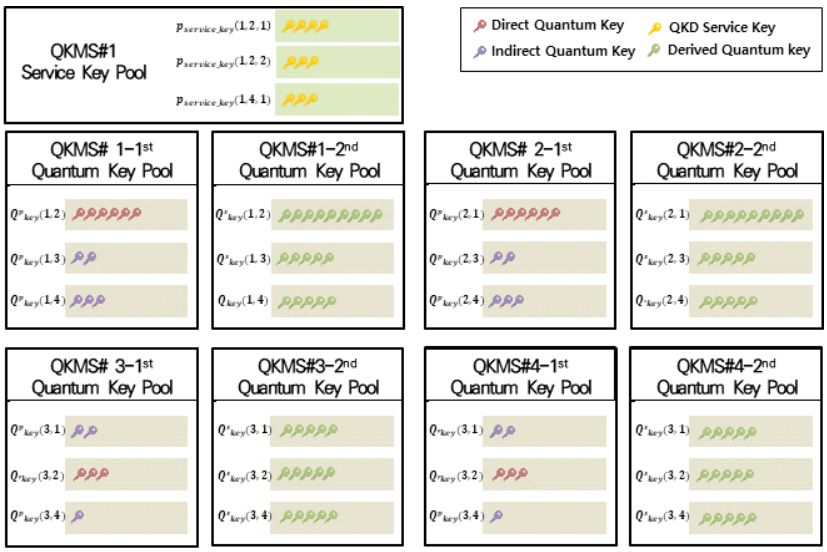


그림 2. 양자키 관리 구조 예
Fig. 2. Example for quantum key management structure

여기서 주 양자키는 QKD를 통하여 분배된 양자키를 의미하며, 부 양자키는 주 양자키의 부족 및 보안 수준에 따른 서비스키 제공을 위하여 양자난수생성기(QRNG, Quantum Random Number Generator[20])로부터 생성되어 주 양자키로 암복호화하여 분배된 양자키를 말한다. 그리고, 각각의 주 양자키 저장소 $Q^{p_{key}}(s,t)$와 부 양자키 저장소 $Q^{s}_{key}(s,t)$의 현재 총 양자키 수를 $N^{p_{key}}(s,t)$, $N^{s}_{key}(s,t)$으로 정의한다. 이 때, 각각의 양자키 관리 네트워크 도메인간의 보유 양자키의 수는 동일함을 가정한다. 가령, QKMS#1의 $p_{key}(1,3)$의 양자키의 수와 QKMS#3의 $p_{key}(3,1)$의 양자키의 수는 같다. 그리고 각 저장소마다 요구하는 최소 양자키의 수에 대한 임계값은 각각 $th^{p}_{key}(s,t)$, $th^{s}_{key}(s,t)$로 사전에 정의되어 있음을 가정한다.

또한, 임의의 종단간 서비스 제공을 위하여 서비스별로 별도의 서비스키 저장소를 관리한다. 임의의 QKMS#$s$와 QKMS#$t$ 사이의 $n$번째 서비스 세션에 대한 요청이 발생(Reactive Method)하면 상응하는 QKD 서비스키 저장소(QKD Service Key Pool, $P_{service\_key}(s,t,n)$)를 생성하고 상응하는 양자키 저장소 $Q_{key}(s,t)$의 양자키 $q_{key}(s,t)$를 활용하여 서비스키를 생성 및 관리한다. 그리고 이 때, 정상적인 경우 네트워크 관리자가 지정한 양자암호통신 서비스 요구 보안 수준에 따라 주 양자키 $q^{p}_{key}(s,t)$와 부 양자키 $q^{s}_{key}(s,t)$ 중 선택하여 서비스키 $p_{service_key}(s,t,n)$를 제공한다. 양자키 부족 현상이 발생하는 경우, 정도에 따라 대응 방법이 상이할 필요가 있으며 이에 대한 상세 내용은 3장에서 다룬다. 표 1은 본 논문에서 제안하는 양자키 확장 구조 및 서비스키 관리 방안을 위하여 사용되는 주요 매개 변수에 대하여 설명한다.

한편, 주 양자키 저장소 $Q^{p_{key}}(s,t)$는 QKMS#$s$와 QKMS#$t$의 상응하는 양자키 관리 네트워크 도메인간 인접 여부에 따라 직접 방식 양자키 저장소와 간접 방식 양자키 저장소로 구분된다. 직접 방식 양자키 저장소는 임의의 두 QKD 노드 간 물리적인 QKD 장비 연결을 통하여 생성하여 QKD 계층에서 각 도메인에 상응하는 양자키 관리 계층으로 전달되는 직접 방식 양자키(Direct Quantum Key)를 저장 및 관리한다. 간접 방식 양자키 저장소는 물리적인 QKD 장비 연결 없이 양자키 관리 계층에서 양자키 전달을 통하여 생성한 간접 방식 양자키(Indirect Quantum Key)를 저장 및 관리한다. 본 논문에서는 양자키 전달 방식으로 ITU-T 표준[18]의 OTP(One Time Password) 기반 XOR(Exclusive OR) 연산 방식을 준용하여 세부 절차를 제안하였다. 이와 관련된 양자키 전달 방식에 대한 설명은 다음절에서 제시한다. 그림 2는 이러한 양자암호통신망 키 관리를 위한 저장소 예를 보여준다. 가령, 그림 1과 같이 4개의 양자키 관리 도메인이 존재할 경우, 각 도메인마다 서로 다른 도메인에 대한 주 양자키 저장소와 부 양자키 저장소를 지니며, 임의의 두 도메인간의 서로 상응하는 양자키는 동일하다.

### 2.3 양자키 전달 구조

현재 QKD 기술은 물리적인 거리상의 제약을 지닌 단대단 양자키 분배에 국한된 기술이기 때문에 중장거리 양자키 교환을 위해서는 신뢰 노드를 통한 양자키 전달이 필요하며, 이를 위해서는 QKD 네트워크에 대응하는 양자키 관리 계층 망 구성을 통한 양자키 전달이 필요하다. 또한 양자키를 전달하기 위해서는 출발지 QKMS부터 목적지 QKMS까지의 라우팅 경로가 필요하며 이를 위해 중앙 집중형 방식의 통합제어기인 Q-SDN Controller에서 QKD 계층과 양자키 관리 계층의 네트워크 토폴로지 정보를 사전에 알고 있음을 가정한다. 그리고 Q-SDN Controller는 해당 정보를 기반으로 양자키 전달을 위한 라우팅 경로를 생성하여 관련된 QKMS들에게 알려야 한다. 본 논문에서는 최적 경로 계산에 대한 상세 방안에 대하여 다루지는 않으며 일반적으로 최소 홉 수, 보유 양자키 수량으로 가중치를 계상할 수 있음을 가정한다.

본 논문에서 제안하는 양자키 관리 계층에서의 양자키 전달 구조는 그림 3에서 보인다. 양자암호통신망

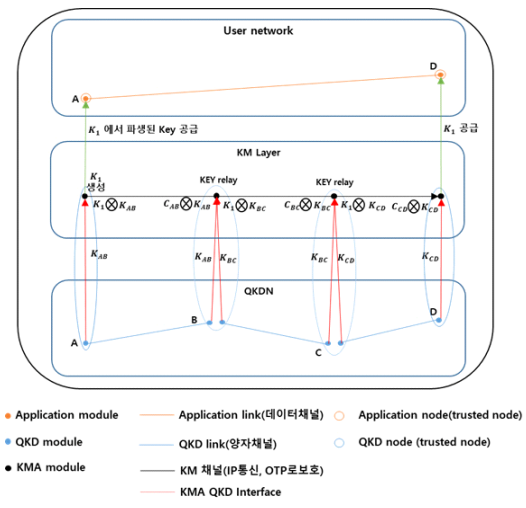


그림 3. 양자키 전달 구조
Fig. 3. Quantum key relay structure

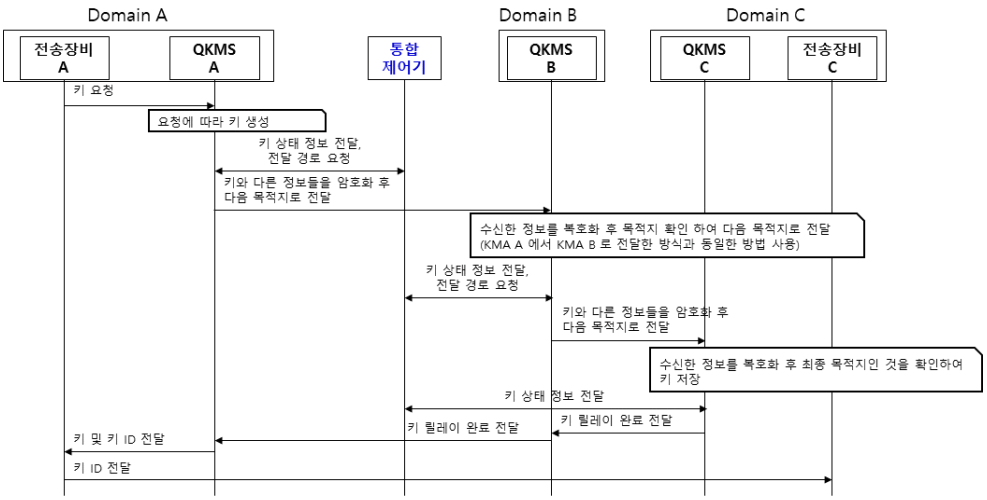


그림 4. 양자키 전달 절차
Fig. 4. Quantum key relay procedure

에서의 양자키 전달에 관한 전반적인 구조는 ITU-T 표준[18]의 OTP 기반 XOR 연산 방식을 준용하였다. 이러한 양자키 관리 계층에서의 양자키 전달을 위해서는 양자키 전달 주체(각 출발지 QKMS와 목적지 QKMS) 간에 전달할 양자키 생성(QKD 자원 부족으로 별도의 난수 생성기 이용 필요), 양자키 전달 주체의 양자키 정보 및 저장소 관리, 양자키 전달 주체 간 양자키 전송을 위한 라우팅 설정 및 물리적인 전송 인터페이스, 암복호화 방안 등에 대한 복합적인 고려가 필요하다.

가령, 그림 1의 양자암호통신망 계층 구조를 가정하였을 때 의 간접 방식 양자키를 생성하기 위하여 QKMS#1에서 QRNG등의 무작위성을 보장하는 랜덤 비트 생성 방식을 통하여 양자키 를 생성하고, 이를 QKMS#11와 QKMS#4의 최적 경로 상의 양자키 , 와 각각 XOR 연산 기반 암·복호화를 통하여 QKMS#4까지 전달한다. 즉, 간접 방식 양자키 생성을 위하여 해당 경로 상의 양자키가 소모된다.

한편, 그림 4는 양자키 전달에 관한 기본 절차를 보여주며 세부 내용은 다음과 같다. 이 때, 양자암호통신 서비스는 물리계층 보안을 담당하는 전송장비로 가정하였다.

1) QKD 전송장비 A가 전송장비 C와 통신하기 위해 QKMS A로 암호화키 요청

2) 전송장비 A의 요청에 따라 출발지 QKMS A에서 난수생성기를 이용하여 목적지 C에 대한 키 스트림 생성

3) QKMS A는 통합제어기에 전송장비 C와 연결된 QKMS까지의 경로 정보 요청

4) 통합제어기에서 경로 생성 후, 해당 도메인 쌍에 해당되는 출발지 QKMS(A), 경유지 QKMS(B), 목적지 QKMS(C)에 전달 정보 전달

5) 출발지 QKMS A에서 경유지 QKMS B로 키 전달: 생성한 키 스트림을 A와 B 간 양자키 스트림으로 XOR 연산 암호화 전송

6) 경유지 QKMS B는 수신한 정보에서 암호화에 사용된 A와 B 간 양자키 식별자 사용해 양자키를 가져와 복호화를 수행하고 목적지 QKMS C 확인

7) 경유지 QKMS B에서 목적지 QKMS C로 키 전달: 수신한 키 스트림을 B와 C 간 양자키 스트림으로 XOR 연산 암호화 전송

8) 목적지 QKMS C는 수신한 정보에서 암호화에 사용된 B와 C 간 양자키 식별자 사용해 양자키 복호화 및 QKD 전송장비 A와 C 간 암호화키 획득

## Ⅲ. 양자키 확장 구조에서의 서비스키 관리 방안

### 3.1 양자암호통신망 부 양자키 관리 방안

본 절에서는 QKD 계층 및 양자키 관리 계층에서 발생할 수 있는 양자키 부족 현상을 해결하기 위하여 파생키 기반의 양자키 확장 방안과 관련 부 양자키 관리 정책에 대하여 제안한다. 양자키 부족 현상은 주로 QKD 계층 장애로 인한 양자키 생성 중단과 임의의 구간의 양자암호통신망 서비스에 의한 양자키 소비량이 해당 구간의 양자키 생성률보다 높아질 때 발생한다.

부 양자키 저장소 $Q^s_{key}(s,t)$의 $q^s_{key}(s,t)$는 양자키 부족 현상을 해결하고 이와 관련된 장애에 대응하기 위한 목적으로 생성된다. QKMS가 최초로 실행되면, 일정시간동안 주 양자키 저장소 $Q^p_{key}(s,t)$에 충분한 양의 $q^p_{key}(s,t)$가 쌓이도록 저장한다. 이 때, 최소한 모든 주 양자키 저장소 $Q^p_{key}(s,t)$는 최소 양자키 보유량 임계값 $th^p_{key}(s,t)$ 이상이 되어야 한다. 그 이후에는 QKMS의 모든 부 양자키 저장소 $Q^s_{key}(s,t)$마다 주 양자키 $q^p_{key}(s,t)$를 활용한 양자키 전달 과정을 통하여 네트워크 운영자가 지정한 초기 임계값 $th^s_{key}(s,t)$까지 부 양자키 $q^s_{key}(s,t)$들을 생성한다.

이 후, QKMS 운영 단계에서는 그림 5의 부 양자키 관리 순서도에 따라 기존의 양자키 $q^p_{key}(s,t)$. $q^s_{key}(s,t)$를 소모하여 각각의 부 양자키 $q^s_{key}(s,t)$를 파생키 기반 확장 형태로 생성 및 관리한다. 이 때, 주요 매개변수인 $th^s_{key}(s,t)$와 $N^s_{key}(s,t)$가 변경되면 그림 5의 절차를 재수행하여 각각의 부 양자키 저장소 $Q^s_{key}(s,t)$가 주어진 최소 양자키 보유량 임계값 $th^s_{key}(s,t)$ 이상의 양자키 보유량을 상시 유지하도록 한다.

만약 임계값 $th^s_{key}(s,t)$ 미만으로 $N^s_{key}(s,t)$가 작아지면 QKMS#$s$와 QKMS#$t$ 사이의 경로상의 모든 구간 <QKMS#a, QKMS#b>마다 $Q^p_{key}(a,b)$가 $N^{pkey}(s,t)$ +1보다 큰 지 확인한다. 만약 조건이 만족하는 경로가 있다면, 해당 구간의 주 양자키 $q^p_{key}(a,b)$를 소모하고, 아니라면 최적 경로상의 부 양자키 $q^s_{key}(a,b)$를 소모하여 각 구간마다 동일 크기의 파생키를 생성한다. 이 때, 하나의 양자키를 활용하여 파생키 확장 방법을 통하여 수십에서 수백 배 이상의 파생키 확장 생성이 가능하며 이의 보안수준 및 확장 정도는 파생 방안에 따라 상이하다. 가령, HMAC 메시지 인증 코드 기반 파생 방식인 HKDF[21]의 경우에 8000 바이트 크기로 파생키를 생성 가능하다. 이 후, QKMS#$s$는 확장된 파생키를 활용하여 OTP 기반 XOR 연산 형태로 전달 가능한 최대한의 신규 부 양자키 집합 $Q'^s_{key}(s,t)$을 무작위성을 보장하는 랜덤 비트 생성 방식을 통하여 생성한다. 신규 부 양자키 집합 $Q'^s_{key}(s,t)$은 해당 경로상의 구간에 따라 순차적으로 파생키의 OTP 기반 XOR 연산을 통하여 암복호화 과정을 반복하여 QKMS#$t$까지 전달된다. 이후 생성하고 소모된 양자키 정보를 각각의 양자키 저장소에 업데이트 한 후 다시 $N^s_{key}(s,t)$가 임계값 $th^s_{key}(s,t)$ 보다 큰 조건을 만족할 때까지 전체 과정이 반복된다.

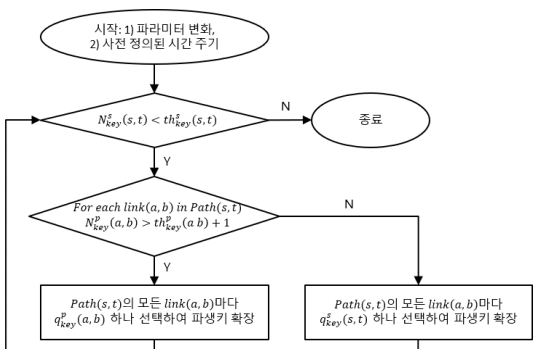


그림 5. 부 양자키 관리 순서도
Fig. 5. Flow chart of secondary quantum key management

또한 양자암호통신망 서비스 요청이 발생하여 암호화 서비스키를 제공함에 있어서도 파생키 기반 양자키 확장을 수행할 수 있다. 해당 $Q_{key}(s,t)$에서 양자키를 선택하여 HKDF 등의 방식으로 파생키를 생성하여 서비스에서 요구하는 암호화키를 제공한다. 더욱이 이 때, 서비스마다 요구하는 암호화키의 사이즈를 상이할 수 있기 때문에 $Q_{key}(s,t)$에 저장되는 양자키의 사이즈는 동일하게 생성하지만 $P_{service_key}(s,t,n)$에는 서비스 요청에 부합하는 키 사이즈의 파생키를 생성하여 제공하도록 한다. 그리고 이 때, 파생키 형태로 생성되는 양자키와 서비스키의 식별자는 각 QKMS에서 생성된 암호화키와 해당 QKMS 쌍의 식별자를 활용하여 동일한 규칙으로 범용 고유 식별자(UUID, universally unique identifier) 형태로 생성함으로써 별도의 과정을 거치지 않고도 해당하는 QKMS 쌍이 동일한 식별자를 가지도록 할 수 있다.

한편, 파생키 기반의 양자키 확장 방안은 양자키 부족 현상 해결과 별개로 QKD 계층과 양자키 관리 계층 및 서비스 계층의 관리자가 상이할 경우 보안 측면에서도 유용하다. 만약 QKD 계층의 운영자가 QKD 계층에서 획득한 양자키를 바탕으로 한 양자키 관리 계층 및 서비스 계층에서의 데이터의 복호화 시도를 원칙적으로 방지할 수 있기 때문이다.

### 3.2 양자암호통신망 서비스키 관리 방안

본 절에서는 안정적인 양자암호통신망 서비스 환경을 제공하기 위한 QKD 기반 양자키 확장 구조에서의 서비스키 관리 방안에 대하여 제시한다.

임의의 QKMS#$s$와 QKMS#$t$ 사이의 $n$번째 서비스 세션에 대한 요청이 발생하면 상응하는 QKD 서비스키 저장소 $P_{service_key}(s,t,n)$를 생성하고 상응하는 양자키 저장소의 양자키를 활용하여 서비스키를 생성 및 관리한다. 그리고 이 때, 충분한 양자키가 공급되는 환경에서는 네트워크 관리자가 지정한 양자암호통신 서비스 요구 보안 수준에 따라 상응하는 주 양자키 $q^{p}_{key}(s,t)$와 부 양자키 $q^{s}_{key}(s,t)$ 중 선택하여 서비스키 $p_{service_key}(s,t,n)$를 제공한다.

하지만 양자키 부족 현상이 발생하는 경우, 상응하는 양자키 저장소가 주 양자키 저장소 $Q^{p_{key}}(s,t)$ 경우와 부 양자키 저장소 $Q^{s}_{key}(s,t)$ 경우에 따라 대응 방법이 상이할 필요가 있다. 한편, 기존 서비스 세션에서 추가적인 서비스키를 요청하는 경우 신규 서비스 세션 요청에 따른 서비스키 저장소 $P_{service\_key}(s,t,n)$ 생성 과정을 제외하고는 서비스키 생성 과정은 동일함을 가정한다.

그림 6은 상세한 양자암호통신 서비스키 관리 순서도를 보인다. 임의의 양자암호통신망 서비스에서 신규 서비스키 요청이 발생하고 해당 서비스의 보안 수준이 주 양자키 $q^{p}_{key}(s,t)$에 대응할 때, 상응하는 주 양자키 저장소 $Q^{p_{key}}(s,t)$의 $N^{p_{key}}(s,t)$가 $th^{p_{s,t}}$보다 클 경우에 주 양자키 $q^{p}_{key}(s,t)$를 활용하여 신규 서비스키 $p_{service_key}(s,t,n)$가 생성되어 서비스키 저장소 $P_{service_key}(s,t,n)$에 저장된다. 그리고 이후 필요에 따라 순차적으로 제공된다. 만약 상응하는 주 양자키 저장소 $Q^{p_{key}}(s,t)$의 $N^{p_{key}}(s,t)$가 $th^{p_{s,t}}$보다 작을 경우, 주 양자키 저장소에서 해당 서비스키를 제공하는데 제약사항이 발생하였다고 판단하며, 이에 따라 부 양자키 저장소 $Q^{s}_{key}(s,t)$에서 서비스키 $p_{service_key}(s,t,n)$를 생성하여 해당 서비스키 저장소 $P_{service_key}(s,t,n)$에 저장한다.

만약 서비스의 보안 수준이 부 양자키 $q^{s}_{key}(s,t)$에 대응하는 신규 서비스키 요청이 발생할 경우, 부 양자키 $q^{s}_{key}(s,t)$를 활용하여 신규 서비스키 $p_{service_key}(s,t,n)$가 생성되어 서비스키 저장소 $P_{service_key}(s,t,n)$에 저장된다. 이후 생성하고 소모된 양자키 정보를 각각의 양자키 저장소에 업데이트 한 후 종료되고 이에 따라, 양자키 확장 기반 부 양자키 관리 절차가 자동적으로 다시 수행된다.

그리고 이 때, 부 양자키 저장소 $Q^{s}_{key}(s,t)$는 $N^{s}_{key}(s,t)$는 항상 $th^{s}_{s,t}$보다 크게 유지하기 위하여 해당 저장소의 양자키를 소모한 경우 임계값과 비교하

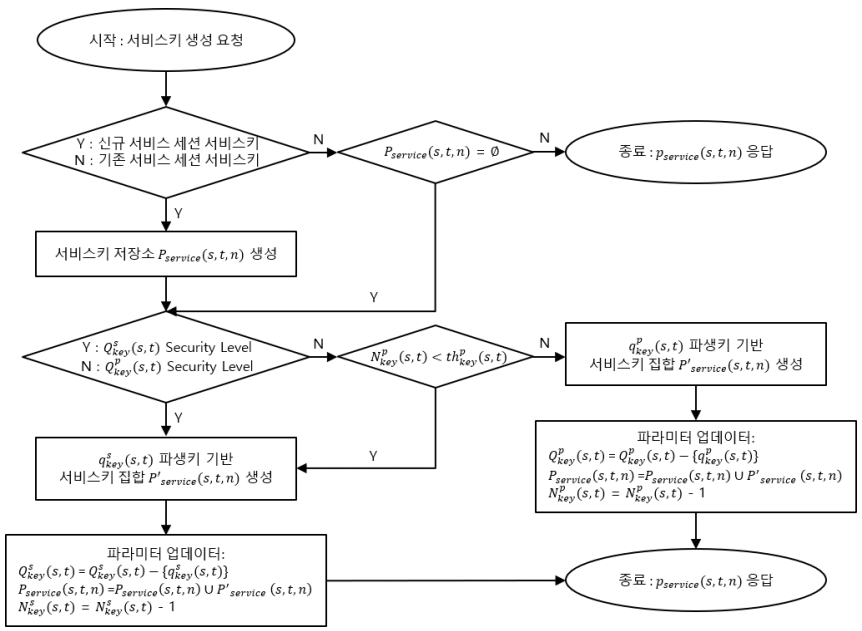


그림 6. 양자암호통신 서비스키 관리 순서도
Fig. 6. Flow chart of quantum service key management

여 양자키의 양이 부족한 경우에 QRNG로 양자키를 생성하여 양자키 전달 정책에 따라 추가 생성함을 가정한다.

동일 도메인에서의 서비스키 요청에 대해서는 상응하는 도메인의 QKMS에서 자체적인 방식을 통한 랜덤비트 생성을 통하여 해당 서비스키들을 생성하여 서비스 저장소 $P_{service_key}(s,s,n)$에 저장하고 이를 순차적으로 꺼내 응답한다. 즉, 동일 도메인 구간에서의 양자암호통신 서비스의 경우, 불필요한 데이터 공간을 최소화하기 위하여 양자키 저장소를 두지 않고 서비스 요구에 따라 서비스키 저장소만 생성하여 서비스키를 제공하고 해당 서비스가 종료되면 해당 서비스 저장소 또한 삭제한다.

## Ⅳ. 성능 분석

본 장에서는 3장에서 제안한 부 양자키 관리 방안 및 서비스키 관리 방안에 따른 양자키 관리 시스템과 통합제어기를 구현하여 양자암호통신망이 정상적으로 구동함을 보인다. 이를 위하여 QKMS는 양자암호통신구성요소 관리를 위한 QKD 제어관리 모듈, QKMS 관리 모듈과 QKMS의 주요 기능을 수행하는 양자키 관리 모듈, 양자키 공급 모듈, 양자키 전달 모듈을 구현하였다. 제안 방안이 포함된 주요 기능 수행 모듈에 대한 세부 내용은 다음과 같다.

양자키 관리 모듈(KMA, Key Management Agent) : 사우스바운드 API를 구현하며, QKD 장비로부터 양자키를 수신하여 저장, 동기화, 삭제 등 관리하는 기능과 양자키의 상태 및 생애 주기를 관리하는 기능 등을 제공

양자키 공급 모듈(KSA, Key Supply Agent) : 노스바운드 API를 구현하며, QKD 응용서비스/네트워크 장비(NE, Network Equipment)에 양자키를 서비스 보안 요구사항에 맞게 할당하고 관리하는 기능 제공

양자키 전달 모듈(KRA, Key Relay Agent) : 이스트-웨스트 API를 구현하며, 중·장거리 및 다대다 QKD를 제공하기 위한 토폴로지 설정 기능, 경로 설정 테이블 설정 기능, 신뢰노드 기반 QKMS 간 양자키 전달 기능을 제공

한편, 양자암호통신망 통합제어기 적용을 위하여 양자암호통신망의 계층 별, 계층 간 토폴로지를 시스템이 인식할 수 있는 형태로 구성 및 관리하기 위한 양자암호통신망 토폴로지 구성·관리 모듈, 제안 방안에 대한 정책을 포함하여 양자암호통신망 구성요소의 정책을 설정 관리하는 제어관리 모듈, 중앙집중형 방식으로 출발지 QKMS로부터 목적지 QKMS까지 양자키 전달 경로를 계산하여 QKMS에게 적용하는 양자키 전달 제어 모듈을 구현하였다.

그림 7은 제안 방안의 기능 검증을 위한 네트워크 구성도를 보인다. 기본적으로 양자키 전달을 위하여 3개의 도메인을 구성하고, 각각의 도메인을 관리하기 위하여 QKMS1, QKMS2, QKMS3를 배치하였다. 그리고 중앙에 통합제어기를 두고 전체 양자암호통신망을 통합 관리하도록 하였다. 이 때, 각 QKMS와 통합제어기는 각각 별도의 서버에 배치하였으며 이의 네트워크는 사설 IP대역 B 클래스를 활용하여 구성(172.16.0.0 ~ 172.31.255.255)하였다.

또한 도메인 1과 도메인 2 사이와 도메인 2와 도메인 3 사이에 QKD 장비(QKDE, QKD Equipment)를 두고 양자키를 생성 및 분배하도록 하였다. 이 때, QKD는 고가의 장비이기 때문에 QRNG 기반의 시뮬레이터를 구현하여 연관된 임의의 2개의 QKD 사이의 양자키를 생성하여 해당 도메인내의 QKMS의 KMA와 연계하여 양자키를 공급하도록 구성하였다.

NE 또한 ETSI 014 표준에 따라 QKMS에 KSA와 연계한 시뮬레이터를 구현하여 적용하였다. 그리고 QKD 장비와 NE 시뮬레이터는 해당하는 도메인을 담당하는 QKMS 서버내에 VM 형태로 구성하였다. 본 장에서는 해당 구성도에서 양자암호통신망에서 QKMS1과 QKMS3쌍 간의 양자키 부족 현상이 발생할 때, 부 양자키 관리 방안 및 양자키 전달 절차에 따라 QKMS1과 QKMS3쌍 간의 양자키가 생성됨을 보인다.

QKMS1의 부 양자키 저장소 $Q^s_{key}(1,3)$내에 보유 양자키량 $N^s_{key}(1,3)$이 양자키 주어진 최소 양자키 보유량 임계값 $th^s_{key}(1,3)$ 이하로 떨어진 경우, QKMS1에서 QKMS3와의 양자키 부족현상이 발생하였음을

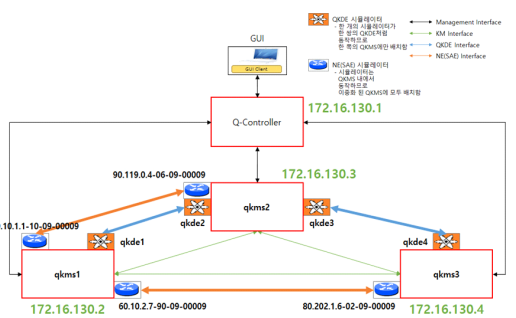


그림 7. 기능 검증용 네트워크 구성도
Fig. 7. Network diagram for functional verification

감지한다. 이후에, QKMS1에서는 그림 8(a)와 같이 난수생성기(RNG, Random Number Generator)로 암호키 리스트를 생성하고, 생성한 암호키들을 키 생성 프로파일에 따라 형식을 조정하여 저장한다. 이 때, QKMS에서 구현의 편의성을 위하여 QRNG 대신 RNG를 활용하여 난수를 생성하였다. RNG는 QRNG에 비하여 충분한 임의성을 보장하지는 못하지만 제안 방안을 검증하기 위한 난수 생성 목적은 달성할 수 있다.

위의 과정을 통하여 생성된 암호화키 리스트의 전달을 위하여 QKMS1은 2장 3절의 양자키 전달 구조에 따라 그림 9와 같이 통합제어기에 전달 경로를 요청하여 수신하고, 이에 따라 해당키를 QKMS2로 OTP 암호화하여 전달한다. 이 때, $Q^{s}_{key}(1,2)$에서 양자키를 획득하여 XOR 형태로 OTP 암호화를 수행한다. 그리고 이를 수신한 QKMS2는 이를 다시 $Q^{s}_{key}(2,1)$에서 동기화된 양자키를 획득하여 복호화한다. 그리고 QKMS2는 통합제이기로부터 전달 경로를 확인하여 QKMS3로 $Q^{s}_{key}(2,3)$에서 획득한 양자키를 활용하여 OTP 암호화하여 전달한다. 그리고 마지막으로 이를

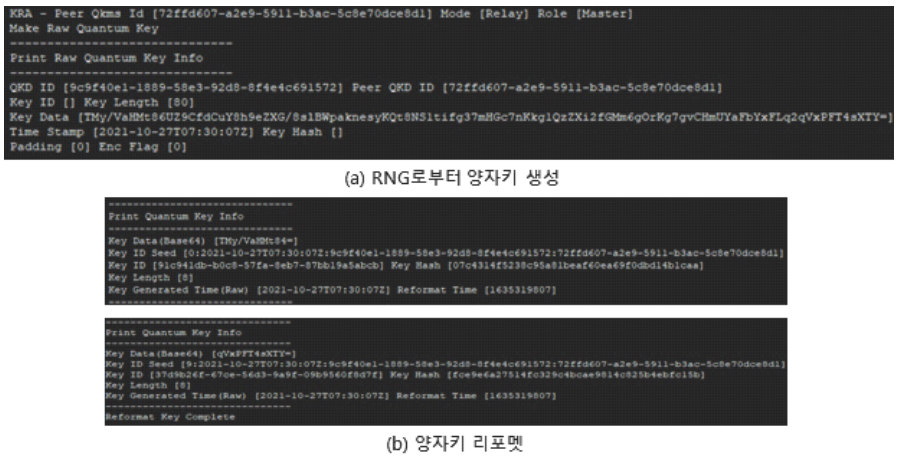


그림 8. QKMS1와 QKMS3 간의 암호화키 생성
Fig. 8. Encryption key generation between QKMS1 and QKMS3

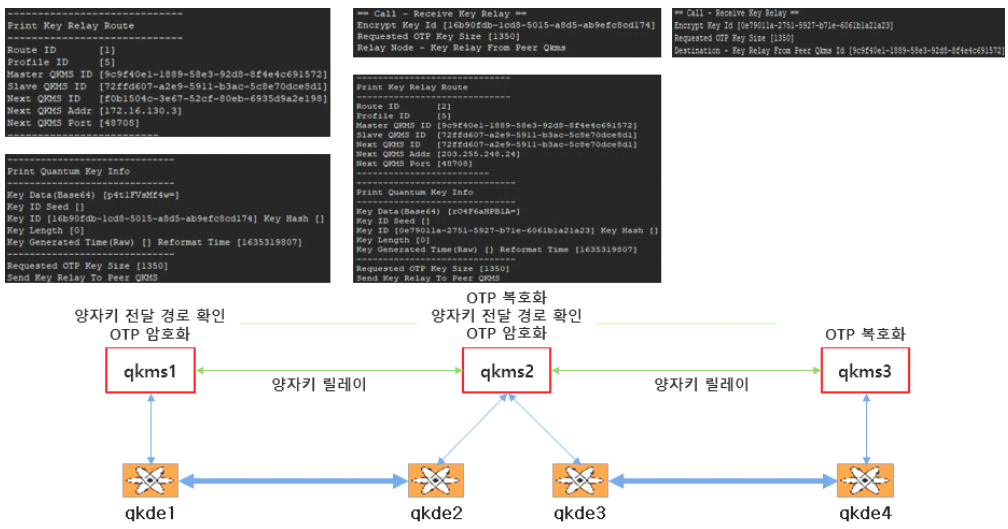


그림 9. 양자키 전달
Fig. 9. Quantum key relay


그림 10. QKMS1와 QKMS3에서 획득한 양자키 확인
Fig. 10. Verification of quantum key obtained by QKMS1 and QKMS3

수신한 QKMS3는 $Q_{key}^{s}(3,2)$에서 획득한 양자키를 활용하여 OTP 복호화를 수행하고 최종 목적지가 자신임을 확인한 이후 QKMS1과의 동기화 과정을 통하여 해당 암호화키들을 부 양자키 저장소 $Q_{key}^{s}(3,1)$에 저장한다. 마찬가지로 QKMS1 또한 QKMS3과의 동기화 과정을 통하여 부 양자키 저장소 $Q_{key}^{s}(1,3)$에 해당 암호화키들을 저장한다. 그림 9는 이러한 양자키 전달 과정과 이에 따른 각 QKMS에서의 관련 정보들을 보여주며, 그림 10은 양자암호통신망 부 양자키 관리 방안에 따라 획득한 키를 QKMS1과 QKMS3과 연계된 NE에서 서비스키 요청 과정을 통하여 동일한 양자키가 획득됨을 보인다.

## V. 결 론

본 논문에서는 양자키 부족 현상을 해결하고 이와 관련된 장애에 대응하여 안정적인 양자암호통신망 서비스 환경을 마련하기 위한 QKMS에서의 양자키 확장 구조와 양자키 관리 정책에 대하여 제안하였다. 또한 한정적인 양자키 자원을 활용하여 다양한 양자암호통신 서비스들의 요구사항에 따라 서비스키를 안정적이고 원활하게 제공하기 위한 서비스키 관리 방안에 대하여 제안하였다. 그리고 제안 방안들에 기반 한 양자키 관리 시스템과 통합제어기를 구현하여 양자암호통신망이 정상적으로 구동함을 확인하였다. 이를 통하여 양자암호통신망에서 발생할 수 있는 서비스 장애에 대응 가능한 체계를 구축함으로써 양자암호통신망 사용자에게 높은 보안 수준의 양자암호통신망 인프라 및 서비스를 제공할 수 있는 실질적인 환경 마련에 기여할 수 있기를 기대한다.

한편, 제안 방안의 실질적인 구현을 위해서는 동시에 다수의 양자암호통신망 서비스가 제공될 때 적절한 임계값을 설정하는 작업이 양자키 자원 최적화 및 서비스 QoS 지원 측면에서 상당히 중요하다. 이에 따라, 향후에는 본 논문에서 제시된 각 QKMS의 주 양자키 저장소 $Q_{key}^{q}(s,t)$와 부 양자키 저장소 $Q_{key}^{s}(s,t)$의 최소 양자키 보유량 임계값 $th_{key}^{p}(s,t)$, $th_{key}^{s}(s,t)$을 선정하는 연구를 수행할 예정이며, 이러한 전체 네트워크상의 모든 QKMS에서의 최적의 임계값을 설정하는 문제는 매우 복잡하기 때문에 인공지능 및 기계학습 기반으로 해결해보고자 한다.

## References

[1] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Secure Commun. and Asymmetric Cryptosystems*, Routledge, pp. 217-239, 2019. (https://doi.org/10.1145/359340.359342)

[2] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Rev.*, vol. 41, no. 2, pp. 303-332, 1999. (https://doi.org/10.1137/S0036144598347011)

[3] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Foundations of Comput Sci.*, pp. 124-134, 1994. (https://doi.org/10.1109/SFCS.1994.365700)

[4] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, no. 441, 2000. (https://doi.org/10.1103/PhysRevLett.85.441)

[5] R. Renner, "Security of quantum key distribution," *Int. J. Quantum Inf.*, vol. 6, no.

1, pp. 1-127, 2008. (https://doi.org/10.1142/S0219749908003256)

[6] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *arXiv preprint arXiv:2003.06557*, 2020. (https://doi.org/10.48550/arXiv.2003.06557)

[7] H. Park, et al., "Key derivation functions using the dual key agreement based on QKD and RSA cryptosystem," *J. KICS*, vol. 41, no. 4, pp. 479-488, 2016. (https://doi.org/10.7840/kics.2016.41.4.479)

[8] K. Lim, et al., "A review of continuous variable quantum key distribution," *J. KICS*, vol. 43, no. 1, pp. 152-160, 2018. (https://doi.org/10.7840/kics.2018.43.1.152)

[9] V. Scarani, et al., "The security of practical quantum key distribution," *Rev. Modern Phys.*, vol. 81, no. 3, 1301, 2009. (https://doi.org/https://doi.org/10.1103/RevModPhys.81.1301)

[10] M. Sasaki, et al., "Field test of quantum key distribution in the Tokyo QKD Network," *Optics Express*, vol. 19, no. 11, pp. 10387-10409, 2011. (https://doi.org/10.1364/OE.19.010387)

[11] S. J. Park, et al., "Design and implementation of a blockchain relay for quantum key distribution," *J. KICS*, vol. 46, no. 3, pp. 563-571, 2021. (https://doi.org/10.7840/kics.2021.46.3.563)

[12] *European Telecommunications Standards Institute web site*, Retrieved Apr. 29, 2022, from https://www.etsi.org/

[13] *ITU Telecommunication Standardization Sector web site*, Retrieved Apr. 29, 2022, from https://www.itu.int/en/ITU-T/Pages/default.aspx

[14] *Telecommunications Technology Association web site*, Retrieved Apr. 29, 2022, from https://www.tta.or.kr/tta/index.do

[15] Ministry of Science and ICT, "*Full-scale start of quantum cryptography communication pilot project to vitalize the quantum industry ecosystem*," 2021.

[16] TTA TTAK.KO-01.0214, "*Functional Architecture of the Quantum Cryptographic Transport Network*," Approved in 2019-12-11.

[17] ITU-T Y.3800, "*Overview on networks supporting quantum key*," Approved in 2019-10.

[18] ITU-T Y.3803, "*Key management for Quantum Key Distribution network*," Proposed in 2020-12.

[19] ETSI QKD 015, "*Control Interface for Software Defined Networks*," Approved in 2021-03.

[20] X. Ma, et al., "Quantum random number generation," *npj Quantum Information*, vol. 2, no. 1, pp. 1-9, 2016. (https://doi.org/10.1038/npjqi.2016.21)

[21] H. Krawczyk and P. Eronen, "*Hmac-based extract-and- expand key derivation function (hkdf)*," RFC 5869, May 2010.

**김 용 환** (Yong-hwan Kim)

2010년 8월 : 한국기술교육대학교 정보미디어공학과 석사
2015년 8월 : 한국기술교육대학교 컴퓨터공학과 박사
2016년 2월~현재 : 한국과학기술정보연구원(KISTI) 연구원
<관심분야> SDN/NFV, Network Virtualization, Mobility Management, Social Networks
[ORCID:0000-0003-3323-0323]

**심 규 석** (Kyu-Seok Shim)

2014년 : 고려대학교 컴퓨터정보학과 학사
2016년 : 고려대학교 컴퓨터정보학과 네트워크관리 전공 석사
2020년 : 고려대학교 컴퓨터정보학과 네트워크 관리 전공 박사
2020년~현재 : 한국과학기술정보연구원 박사후연구원
<관심분야> 네트워크관리, 양자키관리시스템, 양자 내성 네트워크 설계

**이 찬 균** (Chankyun Lee)

2009년 : KAIST, 전기 및 전자공학과 학사
2011년 : KAIST, 전기 및 전자공학과 석사
2016년 : KAIST, 전기 및 전자공학과 박사
2016년~2017년 : 삼성전자 차세대사업팀, 책임연구원
2017년 ~2019년 : 삼성전자 네트워크사업부, 책임연구원
2019년~현재 : 한국과학기술정보연구원, 선임연구원
<관심분야> 네트워크관리, 네트워크 토폴로지, 성능 모델링

**이 원 혁** (Wonhyuk Lee)

2001년 2월 : 성균관대학교 전기전자컴퓨터공학부 졸업
2003년 2월 : 성균관대학교 컴퓨터공학과 석사
2010년 8월 : 성균관대학교 전자전기컴퓨터공학과 박사
2003년 3월~현재 : 한국과학기술정보연구원 책임연구원
<관심분야> 네트워크 관리, 망 성능측정, 양자암호기반 통신망 구축관리
[ORCID:0000-0002-1571-9638]