KREONET 양자암호통신 구축을 위한 양자키관리 시스템 및 Q-SDN-Controller 기능 구현

심규석, 김용환, 이찬균, 이원혁
한국과학기술정보연구원
{kusuk007, yh.kim086, chankyunlee, livezone}@kisti.re..kr

The Implementation of Quantum Key Management System and Q-SDN-Controller Functions for KREONET Quantum Cryptography Network

Kyu-Seok Shim, YoungHwan Kim, Chankyun Lee and Wonhyuk Lee
Korea Institute of Science and Technology Information

요 약

다양한 연구데이터 전송에 사용되는 국가 과학기술연구망은 양자컴퓨터 개발 후의 소인수분해 기반 암호화 방식을 대체하기 위한 새로운 보안방식이 필요하다. 따라서 현재 국가 과학기술연구망에 양자암호통신을 적용하기 위한 연구가 진행되고 있다. 양자암호통신망을 구성하기 위해서는 양자키분배장치, 양자키관리시스템, 양자키암호화모듈이 구성되어야한다. 본 논문에서는 각 노드마다 설치된 양자키관리 시스템으로 구성된 양자암호통신망에서 중앙집중형 관리를 위한 양자키통합컨트롤러와의 연동방안을 제안하고, 양자암호통신망 관리를 위한 양자키통합컨트롤러 GUI 시스템을 소개한다. 양자키관리 시스템과 양자키통합컨트롤러와의 연동을 통해 양자암호통신을 구성하는 구성요소들의 상태 및 네트워크 토폴로지 관리 등 다양한 기능을 구현할 수 있으며, 장애가 발생하였을 때 대처할 수 있는 기능을 구현할 수 있는 것을 실험결과를 통해 증명할 수 있었다.

Ⅰ. 서 론

국가 과학기술연구망은 전국적으로 17개의 지역망 중심으로 네트워크로 연결되어있다. 국가 과학기술연구망에서는 다양한 연구데이터를 전송하고 있기 때문에 양자컴퓨터 개발 후의 소인수분해 기반 암호화 방식을 대체하기 위한 보안방식 개발이 필요하다[1]. 따라서 국가 과학기술연구망에 양자암호통신을 적용하기 위한 연구가 진행되고 있다[2].

본 논문은 국가 과학기술연구망에 양자암호통신을 적용하기 위해 양자키관리 시스템과 Q-SDN-Controller를 구축하여 연동하고, 양자암호 네트워크를 관리하기 위한 방안을 제안한다. 양자암호통신의 구성은 크게 3가지로 양자키분배장치(QKD, Quantum Key Distribution), 양자키관리 시스템(QKMS, Qunatum Key Management System), 양자키암호화모듈(Q-Encryptor)로 구성된다[3]. 그 중 양자키관리 시스템은 양자키분배장치에서 생성된 양자키를 저장 및 관리하고, 양자키암호화모듈로 보안요구사항에 적합한 키를 제공하고, 장거리에 있는 양자 노드에게 키를 전달하는 역할을 한다. 즉, 양자키분배장치의 네트워크화를 위해 필수구성요소이다.

양자키관리 시스템은 양자키를 저장, 관리, 전달하는 다양한 기능을 수행하고, 각 노드의 구성요소들을 관리하기 때문에 양자키관리 시스템을 통해 중앙집중형 관리가 가능하다. 해당 역할을 Q-SDN-Controller가 수행한다. 본 논문에서는 양자키관리 시스템, Q-SDN-Controller의 구성 및 기능들을 정의하고, 양자암호통신망 관리를 위한 Q-SDN-Controller의 GUI 프로그램을 제안한다.

본 논문은 서론에 이어 2장 본론에서는 양자키관리 시스템, Q-SDN-Controller의 구성 및 기능을 정의하고 GUI 프로그램을 제안하며, 3장 결론으로 논문을 마친다.

Ⅱ. 본론

양자키관리 시스템(QKMS)은 양자키분배장치에서 생성되는 양자키를 수신하여 저장하고, 효율적인 양자키 사용을 위해 서비스키를 생성하여 양자키 암호화 모듈로 전송하며, 장거리 양자암호통신을 위해 양자키관리 시스템간 키 전달을 수행한다. 또한, 각 노드에 포함된 양자키분배장치 및 링크의 상태 및 성능 정보를 수집하여 성능 및 장애들을 관리할 수 있다.

양자키통합컨트롤러(Q-SDN-Controller)는 양자키관리 시스템들과 연동되어 중앙집중형 관리를 가능하게 하는 장치이다. 양자키관리 시스템에서 수집한 각 구성요소의 상태 및 성능정보 그리고 연결된 링크들의 상태 정보들을 수신 받아 양자네트워크망을 관리하고, 장애가 발생하였을 경우 우회경로 설정 및 키전달 경로를 설정해줌으로써 네트워크 토폴로지 관리를 가능하게 한다.

다음 그림은 양자키관리 시스템과 양자키통합컨트롤러를 이용한 양자암호통신망 구성도이다. 그림과 같이 QKMS는 노드당 한 대로 해당 노드를 구성하는 양자키분배장치 및 링크상태를 수신받고, 양자키 전달 경로등을 설정할 수 있다. 해당 정보를 양자키관리 시스템에서 양자키통합컨트롤러로 전송함으로써 중앙집중형 양자암호통신망 관리를 가능하게 한다.

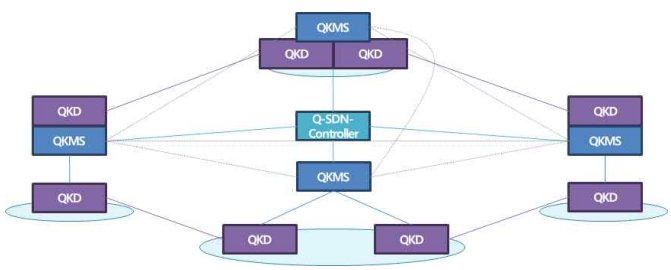

그림 1. 양자암호통신망 구성

양자암호통신망을 구성하는 구성요소의 연결 인터페이스는 다음 그림과 같이 7개의 인터페이스로 구성된다. 1은 양자키관리 시스템과 양자키분배 장치의 연결, 2는 양자키관리 시스템과 양자키암호화모듈의 연결, 3은 양자키관리 시스템간의 연결, 4는 양자키관리 시스템과 양자키통합컨트롤러와의 연결, 5는 양자키통합컨트롤러와 GUI 시스템간의 연결, 6은 양자키분배장치간의 연결, 7은 양자키암호화모듈간의 연결이다.

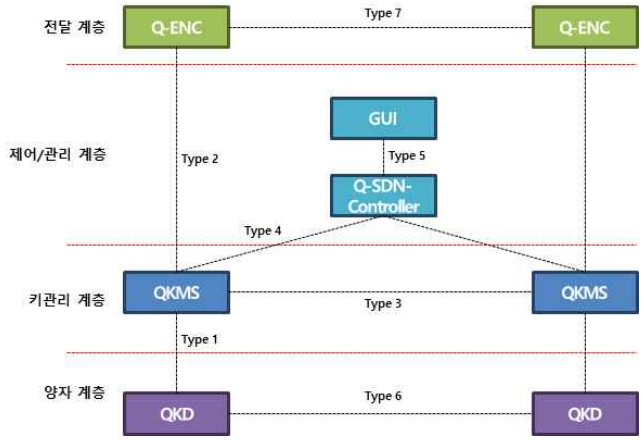

그림 2 양자암호통신망 구성요소 인터페이스

본 논문의 내용은 인터페이스 4와 5번으로 양자키관리 시스템과 양자키통합컨트롤러와의 연결, 그리고 양자키통합컨트롤러와 GUI의 시스템간의 연결로 인터페이스 4번은 양자키관리 시스템 및 양자키분배장치 관리 및 양자암호통신망 토폴로지 관리를 위해 상태정보 등을 제공하고, 양자키통합컨트롤러는 키전달경로 및 키 생성등을 관리할 수 있는 명령을 보낸다. 즉 양자키관리 시스템에서 상태정보를 확인하여 만약 장애가 발생했을 시 양자키통합 컨트롤러는 대체경로를 양자키관리 시스템에 전달하여 원활한 양자암호통신이 가능하도록 한다. 인터페이스 5번은 양자키통합 컨트롤러가 가진 정보들을 관리자가 쉽게 조회하고, 제어할 수 있는 GUI 시스템과의 연결이다.

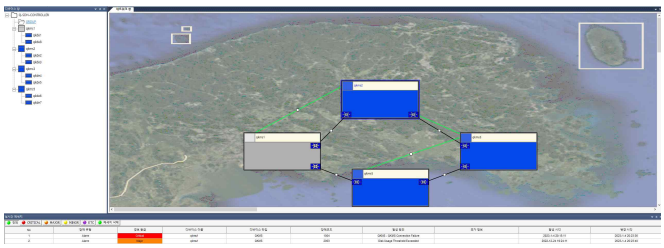

그림 3. GUI 시스템 네트워크 토폴로지 및 상태조회 화면

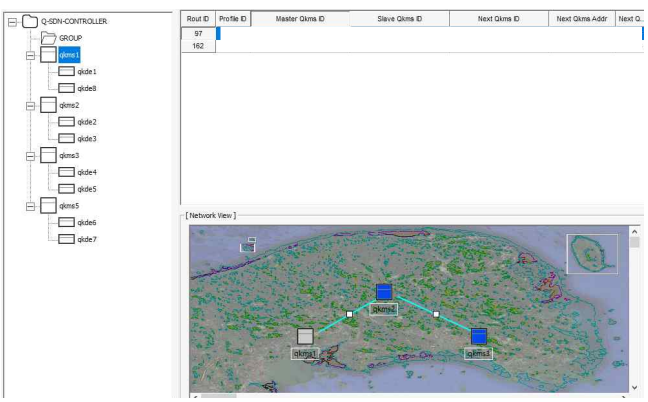

그림 4. 키 전달경로 설정 화면

다음 그림은 양자키통합컨트롤러의 GUI 시스템에서 네트워크 토폴로지와 상태정보를 조회한 결과이다. 다음과 같이 현재 4개의 노드로 구성되어 있으며, QKMS1과 2, QKMS2와 3, QKMS 3과 5 그리고 QKMS1, 5가 양자키분배장치로 대칭키를 생성하고 각 노드의 QKMS는 해당 대칭키를 저장한다. 그림4와 같이 QKMS1과 3의 양자암호통신이 가능하게 하기 위해 QKMS2를 이용하여 키전달경로를 설정하였으며, 그림3의 하단은 각 노드의 상태정보를 조회하고 장애가 발생했을 시 알림을 나타내는 화면이다. 만약 장애가 발생한다면 다음 과정과 같이 장애가 발생한 노드를 제외하고 새로운 경로를 계산하여 변경된 경로를 다시 QKMS로 전달한다.

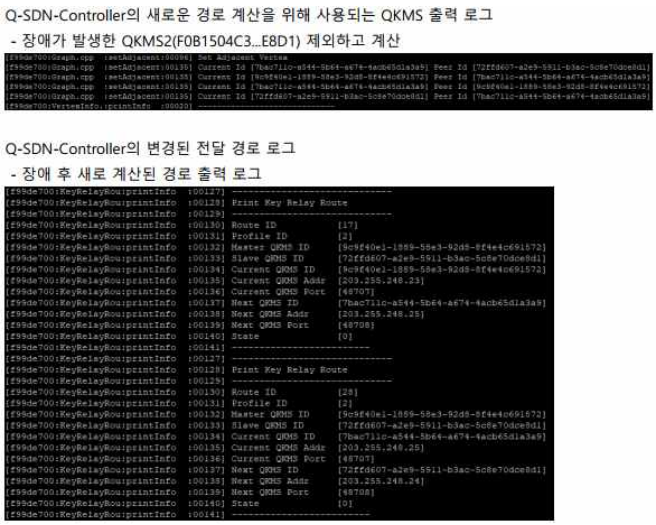

그림 5. 장애 발생 시 우회경로 설정

다음과 같이 양자키관리 시스템과 양자키통합컨트롤러를 구현하여 설치하였고, 구성요소의 상태 및 네트워크 토폴로지 정보를 조회 및 제어할 수 있으며, 장애가 발생하였을 때 대처할 수 있는 기능을 구현하였다.

Ⅲ. 결론

본 논문에서는 양자암호통신망을 구성하기 위한 양자키관리 시스템과 양자키관리 시스템을 중앙집중형 관리할 수 있는 양자키통합컨트롤러에 대해 소개하였고, 각 기능들을 정의하였다. 또한, 양자키통합컨트롤러와 연동하여 양자암호통신망 구성요소들의 상태 및 성능정보를 조회하고, 네트워크 토폴로지를 관리하며 다양한 기능을 구현한 것을 증명하였다. 마지막으로 장애가 발생하였을 때 대처할 수 있는 기능을 구현하였다.

ACKNOWLEDGMENT

본 연구는 2023년도 한국과학기술정보연구원(KISTI) 주요 사업 과제로 수행한 것입니다.

참 고 문 헌

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum Cryptography,” Rev. Mod. Phys., Vol.74, No.1, 2002, p.145

[2] 이원혁, 석우진, 박찬진, 권우창, 손일권, 김승해, 박병연, “양자암호기반의 통신망 구축 및 성능시험 검증연구”. KNOM Review, 2019, vol.22, No.02, pp39-47

[3] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus,“Field test of quantum key distribution in the Tokyo QKD Network”, Optics Express, Vol 19, Issue 11, 2011