Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.30, NO.5, Oct. 2020 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2020.30.5.771

암호장치의 송·수신자 역할 설정이 없는 양자키분배 시스템 설계

고 행 석,† 지 세 완, 장 진 각‡
ETRI 부설연구소 (연구원)

Design of Quantum Key Distribution System without Fixed Role of Cryptographic Applications

Haeng-Seok Ko,† Se-Wan Ji, Jingak Jang‡
The Affiliated Institure of ETRI (Researcher)

요 약

양자키분배(QKD)는 양자컴퓨터의 위협으로부터 안전하게 비밀키를 나누어 갖는 키공유 프로토콜 중 하나이다. 일반적으로 QKD 장치에 연결되는 암호장치는 경합조건 발생과 구현의 복잡성 때문에 송신자 또는 수신자의 역할을 설치할 때부터 적용한다. 기존 QKD 시스템은 링크용 암호장치에 주로 적용되었기 때문에 암호장치의 송·수신자 역할을 고정하여도 문제가 없었다. 암호장치와 QKD 장치가 공급하는 양자키의 종속성을 제거하여, QKD 네트워크로 유연하게 확장할 수 있는 새로운 QKD 시스템 및 프로토콜을 제안하였다. 기존 QKD 시스템에서는 암호장치가 요청하는 비밀키를 양자키로 직접 분배하였으나, 제안한 QKD 시스템에서는 난수로 생성한 비밀키를 암호장치에 분배한다. 두 QKD 노드 사이에서 미리 나누어 가진 송신용 및 수신용 양자키를 이용하여 비밀키를 암호화하고 전달하는 구조를 제안하였다. 제안한 QKD 시스템은 QKD 장치들 사이에서 공유한 양자키의 의존성을 제거하여 암호장치의 고정된 송·수신자 역할이 필요 없다.

ABSTRACT

QKD(Quantum Key Distribution) is one of the protocols that can make two distant parties safely share secure keys against the threat of quantum computer. Generally, cryptographic applications which are connected to the QKD device have fixed roles as a transmitter and a receiver due to the race condition and complexity of implementation. Because the conventional QKD system is mainly applied to the link encryptor, there are no problems even if the roles of the cryptographic devices are fixed. We propose a new scheme of QKD system and protocol that is easy to extend to the QKD network by eliminating quantum key dependency between cryptographic device and QKD node. The secure keys which are generated by the TRNG(True Random Number Generator) are provided to the cryptographic applications instead of quantum keys. We design an architecture to transmit safely the secure keys using the inbound and outbound quantum keys which are shared between two nodes. In this scheme, since the dependency of shared quantum keys between two QKD nodes is eliminated, all cryptographic applicatons can be a master or a slave depending on who initiates the cryptographic communications.

Keywords: QKD, Role of Cryptographic Application, Quantum Key, Key Sharing, Key Management

Received(07. 08. 2020), Modified(09. 15. 2020), Accepted(09. 15. 2020)

† 주저자, hsko@nsr.re.kr
‡ 교신저자, cstone@nsr.re.kr(Corresponding author)

I. 서 론

두 암호장치 사이에서 같은 암호키를 나누어 갖는 키분배는 전통적으로 어려운 문제이다. 같은 암호키를 안전하게 나누어 갖기 위하여 사전공유키(PSK; Pre-Shared Key)를 이용하는 방식과 암호와 복호를 서로 다른 키로 이용하는 비대칭 암호인 공개키암호 방식이 주로 사용되었다. 사전공유키 방식은 암호장치까지 신뢰할 수 있는 전달자에 의하여 공유키가 전달되어야 하고, 신뢰할 수 있는 관리자에 의하여 저장되고 운영되어야 한다. 따라서 사전공유키 방식은 공유키의 생성, 전달, 저장 등 키의 생명 주기 전 과정 동안 안전성을 보장해야 하는 관리의 어려움이 있다. 공개키와 비밀키 쌍으로 이루어진 공개키암호는 큰 두 수의 곱으로 이루어진 숫자를 인수분해하는 어려움과 이산대수 문제를 기반으로 설계가 되었다. 양자컴퓨터 시대가 도래하면, 인수분해와 이산대수 문제를 계산하여 암호키를 해독할 수 있으므로 공개키 암호는 보안에 취약한 것으로 알려져 있다[1][2]. 이에 따라 양자컴퓨터의 위협으로부터 안전하게 암호키를 분배하기 위하여 양자내성암호(PQC; Post Quantum Cryptographic)와 양자키분배(QKD; Quantum Key Distribution)에 관한 많은 연구가 이루어졌다. 양자내성암호는 양자컴퓨터로 계산하더라도 암호키를 찾는데 천문학적 시간이 걸리리라 기대되는 수학적 난제를 이용한 공개키 암호이다[6]. QKD는 양자물리학의 복제불가능성의 원리와 양자 상태의 측정 후 양자 상태가 붕괴하는 현상을 이용한다. QKD에서 송신자가 전송한 양자 상태의 광자를 도청자가 먼저 측정하게 되면, 양자비트에러율(QBER; Quantum Bit Error Rate)이 증가하기 때문에 도청자의 존재 여부를 확인할 수 있다. QKD를 이용하면 안전하게 양자키를 공유할 수 있으며, QKD 프로토콜은 조건 없이 안전한 정보이론적인 안전성(ITS; Information Theoretic Security)을 보장할 수 있다.

유럽에서는 산·학·연에서 연구한 양자암호통신 기술을 집대성하여 2004년 4월부터 2008년 10월까지 41개 기관을 중심으로 SECOQC(SEcure COmmunication based on Quantum Cryptography) 프로젝트를 수행하였으며, 이 연구 결과가 지금까지 ETSI, ISO, ITU 등 표준과 대부분의 양자암호 연구에 커다란 영향을 끼쳤다[1][2][3][4][5][9]-[23]. 최근에는 이러한 QKD 프로토콜의 안전성을 기반으로 QKD 장치를 SDN에 적용하거나, SDN을 이용하여 QKD 네트워크를 구성하는 연구가 활발하게 이루어지고 있으며[6][7][8], IPsec 등 기존 암호장치에 QKD를 적용하는 연구가 활발하게 진행되고 있다[9][10].

이 논문은 2장에서 배경 지식으로 QKD 시스템의 구성과 동작원리에 대하여 설명하고 기존 QKD 시스템의 문제점을 제시한다. 3장에서는 기존의 문제를 해결하기 위한 새로운 QKD 시스템과 프로토콜을 제안하고 새로운 QKD 시스템의 구조, 동작 원리와 특징에 관하여 기술한다. 4장에서는 결론으로 제안한 QKD 시스템의 특징과 장점을 설명한다.

II. 배 경

2.1 양자키분배 네트워크 구성

양자암호통신은 Fig. 1.과 같이 QKD 노드와 암호장치(SAE; Secure Application Entity)들의 조합으로 구성된다[11][12].

QKD 노드는 양자키를 생성하는 QKD 장치(QKDE; QKD Entity)와 양자키를 저장하고 암호장치의 요청에 따라 양자키를 암호장치로 전달하는 키관리장치(KME; Key Management Entity)로 구성된다. 양자키 노드는 1개 이상의 QKD 장치와 1개의 키관리장치로 구성된다. QKD 노드들은 모두 같은 방식의 QKD 장치를 사용하거나 다른 방식의 QKD 장치를 사용하는 복수의 QKD 장치들로 구성될 수 있다. QKD 노드에 복수의 QKD 장치를 적용해도 키관리장치는 일반적으로 1개를 운용한다. QKD 노드와 암호장치는 안전하게 관리되는 장소에 위치하며, 다수의 QKD 사이트가 서로 연결되어 양자키를 전달하는 QKD 네트워크를 구성하여 운용한

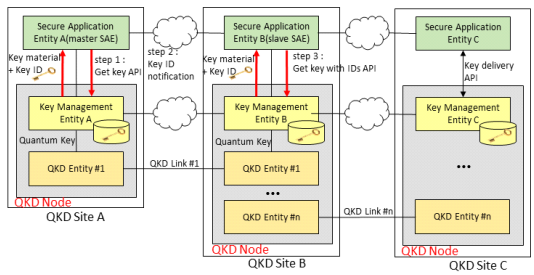

Fig. 1. QKD system and quantum key delivery protocol

다. QKD 장치 사이에는 점대점의 QKD 링크로 연결되어 있으며, QKD 링크는 광자를 전달하는 양자채널(quantum channel)과 키추출 정보를 전달하는 공개채널(public channel)로 구성되어 있다. 양자채널은 일반적으로 전용 광선로(dark fiber)를 이용한다. QKD 장치는 양자 상태가 부호화된 광자를 송신하는 송신장치(Alice)와 광자를 수신하고 양자 상태를 측정하는 수신장치(Bob)로 나누어지며 송·수신 장치가 한 개의 쌍으로 점대점으로 연결된 QKD 링크로 운용한다. 하나의 QKD 노드에는 1개 이상의 암호장치가 연결될 수 있으며, 암호장치는 마스터(송신자)와 슬래이브(수신자)로 역할(role)이 나누어져 있다. 마스터 암호장치는 키요청을 먼저 시작하고, 슬래이브 암호장치는 마스터 암호장치가 전달한 키 ID를 이용하여 키를 요청한다. 일반적으로 두 QKD 노드 사이에서 경합조건(race condition)을 방지하기 위하여 암호장치는 미리 선택된 마스터 또는 슬래이브의 역할을 가지고 있으며, QKD 노드로부터 공급받은 같은 양자키를 이용하여 암호통신을 수행한다.

2.2 양자키분배 시스템 동작

QKD 시스템의 송신장치에서 무작위로 선택된 기저와 난수값으로 부호화된 양자 상태의 광자를 양자채널로 전송하고, QKD 시스템의 수신장치는 기저를 무작위로 선택하여 광자의 양자 상태를 측정한다. 이때 송신장치는 광자 수 나누기 공격(photon number splitting attack) 등의 양자해킹을 대비하여 미끼(decoy) 신호를 무작위로 섞어서 수신장치로 송신한다. 송신장치가 생성한 양자 상태와 수신장치가 측정한 양자 상태의 결과를 raw 키로 저장하고, 송신장치가 전송한 디코이 정보, 송신장치와 수신장치가 선택한 기저 정보 등을 공개채널을 통하여 교환함으로써 걸러진 키(sifted key)를 생성한다. 이 과정에서 양자비트에러율을 측정하면 도청 여부를 판단할 수 있다. 걸러진 키를 오류정정 기법, 비밀증폭 기법 등을 이용하여 비밀키(양자키)를 생성하면, 점대점으로 연결된 두 QKD 장치는 같은 양자키를 갖게 된다. 두 QKD 장치에서 생성한 같은 양자키는 각각 키관리장치로 전달된다[13].

키관리장치는 QKD 장치로부터 양자키를 전달받고, 키 중계 및 암호장치와 연동 등의 역할을 한다. 일반적으로 QKD 장치에서 생성하는 양자키의 생성속도는 낮고 일정하지 않기 때문에 키관리장치에서 양자키를 버퍼에 저장한 후 암호장치로 전달한다[21]. 점대점으로 연결된 QKD 장치의 물리적 거리를 확장하거나, 점대점으로 직접 연결되지 않은 사이트 사이에서 키관리장치는 키중계 역할을 수행한다.

마스터 암호장치가 자신이 속한 키관리장치에 비밀키를 요청(get key)하면 키관리장치는 양자키와 양자키에 해당하는 키 ID를 마스터 암호장치로 보내준다. 마스터 암호장치는 슬래이브 암호장치로 키 ID를 전송하고, 키관리장치로부터 받은 양자키를 사용하여 암호통신을 준비한다. 슬래이브 암호장치는 마스터 암호장치로부터 키 ID를 받고, 자신이 속한 사이트의 키관리장치에게 키 ID를 이용하여 키요청(get key with key ID)을 한다. 키 ID로 키 요청을 받은 키관리장치는 키 ID에 해당하는 양자키를 찾아서 슬래이브 암호장치로 전달한다. 이러한 키공유 절차는 하나의 트랜잭션으로 처리된다. 마스터 암호장치와 슬래이브 암호장치는 동일한 양자키와 키 ID를 공유하게 되며, 공유한 양자키를 마스터키로 사용하여 암호통신을 수행한다[19][11]. 암호장치와 키관리 장치 사이에는 일반적으로 TLS(Transport Layer Security)가 사용되어 통신채널을 보호하고, 같은 사이트 내에서 하나의 서버 랙(rack)에 장착되어 물리적 보안으로 안전하게 관리된다[1][2][3][14].

QKD 네트워크를 구성하기 위해서는 QKD 노드뿐만 아니라 양자정보를 전달하는 신뢰노드(trusted node)도 필요하다. 신뢰노드는 양자채널 스위칭(quantum channel switching), 양자 리피터(quantum repeater), 신뢰 리피터(trusted repeater)가 있다[15]. 양자채널 스위칭은 광학 스위치를 이용하며, 안전하게 양자정보를 전달할 수 있으나, 스위치를 거치면서 신호의 감쇠가 생기기 때문에 전송거리가 짧아지므로 QKD 링크의 거리 확장에 사용할 수 없다. 양자 리피터는 양자키를 저장할 수 있는 양자 메모리가 필요하기 때문에, 현재의 기술로는 구현이 어렵다. 현실적으로는 양자키를 hop-by-hop으로 전달하는 신뢰 리피터가 양자키 전달 거리의 확장을 위한 유일한 방법이다.

그러나, hop-by-hop 방식의 신뢰노드가 공격을 받게 되면 양자키 정보가 노출될 수 있기 때문에 신뢰노드는 안전하게 관리된다는 가정이 필요하다[1][2][3]. 신뢰노드에 보안성을 강화하기 위하여 양자키를 이중화하는 방식[15]이나, QKD 노드에서

양자키를 저장하지 않고 연결되는 두 노드의 양자키 값을 XOR 하여 저장하는 방식[16] 등이 연구되었으나 보안성이 충분하게 확보되지는 못한 실정이다.

SECOQC에서 양자키의 중계는 안전한 QBB(Quantum BackBone) 또는 QKD 노드에서 hop-by-hop 방식으로 양자키로 암호화하여 전달하며[3][4], 대부분의 QKD 시스템은 이 방식을 적용하고 있다. 키를 중계하기 위한 hop-by-hop 방식은 신뢰노드의 로컬 양자키로 XOR 연산으로 복호와 암호를 반복하여 전달한다. 처음 전달하는 정보에 따라 Alice 양자키 전달($\oplus K_{local}$), 메시지 전달($M \oplus K_{local}$), 디피-헬만 키교환 전달($Y_A \oplus K_{local}$) 방식 등으로 나누어진다[2][3].

2.3 양자키분배 시스템의 문제점 고찰

QKD 시스템은 QKD 링크에 암호장치가 연결되는 형태에서 발전해 왔기 때문에 암호장치는 마스터 또는 슬래이브의 역할을 고정적으로 사용했다. [20]에서는 QKD가 서버와 원격지 서버 백업용 QKD 링크 암호장치에 연동되며, WAN, MAN에 적용된 QKD 네트워크도 점대점 링크를 연결한 유스 케이스를 보이고 있다. 이와같이 QKD 네트워크를 링크용 암호장치에 1대1로 연결할 경우 암호장치는 마스터/슬래이브 또는 서버/클라이언트 모델 적용에 적합하다.

SECOQC에서는 QKD 노드 사이에서 경합조건이 발생할 수 있어서 Q3P(Quantum Point-to-Point Protocol)를 마스터 또는 슬래이브로 고정적으로 설정하는 것처럼[2][15] 암호장치 사이에서도 경합조건이 발생할 수 있다. QKD 네트워크에서 암호장치의 역할을 미리 설정하지 않고 암호통신을 수행하는 경우, 한 암호장치가 요청한 키공유 트랜잭션이 완료되기 전에 상대 암호장치가 키요청 절차를 시작하게 되면, 요청한 양자키의 순서에 따라 양자키의 동기가 깨질 수 있고, 경합조건이나 교착상태(dead-lock)가 생길 수 있다.

SECOQC에서 QKD 노드는 QKD 장치에서 생성한 양자키를 암호장치로 전달하기 위한 메시지 암호키와 QKD 링크 사이에서 전달되는 정보를 인증하기 위한 인증키로 사용한다. 또한 hop-by-hop 방식으로 키를 중계할 때도 양자키를 사용한다. 양자키는 QKD 링크 사이에서 동기가 이루어져야 하고, 나아가서는 QKD 네트워크 전체에서 양자키 동기가 맞아야 한다.

그러나, QKD 네트워크 전체에서 양자키 동기를 맞추는 것은 매우 복잡하기 때문에 SECOQC에서는 화상회의 암호장치를 QKD 네트워크에 적용하기 위하여, 링크용 암호장치를 확장하는 개념으로 암호장치 앞단에 IPsec VPN으로 터널을 형성하고, QKD 노드에서 점대점 방식으로 양자키를 공급하는 방식을 적용하고 있다[1][2][3]. 또한, tokyo QKD network에서는 MPTMP(Multi Party To Multi Party)를 지원하는 다수의 보안 스마트폰에 양자키를 독립적으로 전달하기 위하여 센터 서버를 두고 센터 서버에서 세션 호출을 담당하고 각 암호장치로 암호키를 분배하는 방식을 적용하였다[17][18].

또 다른 문제점으로, QKD 노드에 다수의 암호장치를 연결하여 사용할 경우, 양자키 요청에 대한 처리성능이 낮은 문제가 있다. 하나의 암호장치가 키를 요청하게 되면, 키공유 트랜잭션이 종료될 때까지 다른 암호장치가 키요청을 사용할 수 없도록 QKD 노드는 키요청을 차단(blocking)한다. 그렇지 않으면 QKD 노드 사이의 양자키 동기가 깨질 수 있다. 이러한 키요청 차단으로 인하여 트랜잭션이 완료될 때까지 다른 암호장치는 QKD 노드를 사용할 수 없으므로 QKD 노드의 성능과 효율성이 저하될 수 있다[2][3][19][11].

QKD 네트워크를 유연하게 확장하려면, 암호장치를 쉽게 추가 및 제거할 수 있어야 하고, 기존 QKD 네트워크에 영향을 미치지 않으면서 QKD 노드를 추가할 수 있어야 한다. 암호장치는 링크용으로 제한하지 않아야 하며, 역할을 동적으로 운용할 수 있어야 한다. 이를 해결하기 위하여, QKD 네트워크에서 양자키 동기를 쉽게 유지할 수 있는 구조를 제안한다. 제한한 스킴은 QKD 노드의 추가가 용이하고 다양한 암호장치를 QKD 네트워크에 적용할 수 있으며 트랜잭션 처리에 따른 성능 저하 문제도 개선할 수 있다.

III. 새로운 양자키분배 시스템 제안

3.1 개요

이 논문에서 기존 QKD 시스템의 문제를 해결할 수 있는 새로운 QKD 시스템의 구조 및 프로토콜을 제안한다. 제안한 QKD 노드에 연동되는 암호장치는

마스터 또는 슬래이브 역할을 미리 정할 필요가 없다. QKD 시스템에 속한 모든 암호장치는 키요청을 먼저 시작할 수 있으며, 시작한 암호장치가 마스터가 되고, 키 ID를 받은 암호장치가 슬래이브로 동작한다. 또한, QKD 노드에서 키공유 트랜잭션이 처리 중이어도 키요청을 차단하지 않고 키와 키 ID를 지연 없이 제공하여 성능을 높일 수 있다.

기존 QKD 시스템은 QKD 장치가 생성한 양자키를 키관리 장치를 거쳐 암호장치로 전달하는 구조로 설계되어 있다. 이 방식은 양자키가 생산부터 소비되는 과정에서 같은 양자키를 QKD 장치, 키관리 장치, 암호장치가 암호/복호, 인증, 키 중계 등으로 사용하기 때문에 키동기를 유지하는 데 어려움이 있다.

이를 해결하기 위하여 새로운 QKD 시스템의 구조 및 프로토콜을 제안하였다. 제안한 스킴은 양자키의 생산을 담당하는 계층과 양자키를 소비하는 계층을 분리하였다. 암호장치는 양자키가 아닌 난수로 생성한 비밀키를 사용한다. 생성한 비밀키는 QKD 링크를 통하여 상대 QKD 노드로 전달되며, 양자키는 QKD 노드 사이의 채널을 보호하는 용도로만 사용하기 때문에 QKD 네트워크에서 양자키 동기를 쉽게 유지할 수 있다. 제안한 스킴은 QKD 노드에서 각각의 계층별로 양자키의 독립성을 부여함으로써, 양자키와 비밀키의 동기를 유지할 수 있다.

3.2 제안한 양자키분배 시스템 구성

제안한 QKD 시스템은 Fig. 2.와 같이 A, B 두 사이트에 QKD 노드와 암호장치(secure application)가 각각 연결되어 있다. QKD 노드는 1개 이상의 양자키분배 장치(QKD module)와 동수의 양자키 동기 관리(quantum key synchronization management) 장치, 1개의 양자키 통합(quantum key orchestration) 장치로 구성되고, 1개 이상의 암호장치가 QKD 노드에 연결된다. Fig. 3.은 복수의 QKD 장치와 동수의 양자키 동기 관리 장치, 1개의 양자키 통합 장치, 복수의 암호장치로 구성된 QKD 사이트의 예이다.

QKD 장치는 송신자와 수신자 역할의 장치가 점대점으로 연결된 1개의 세트로 구성된다. QKD 장치 사이에는 QKD 링크가 연결되어 있다. QKD 링크는 양자 상태의 광자를 전송하는 양자채널과 미끼 정보, 기저 정보 등을 전송하는 공개채널로 구성되어 있다. QKD 장치는 QKD 프로토콜을 통해 생성된

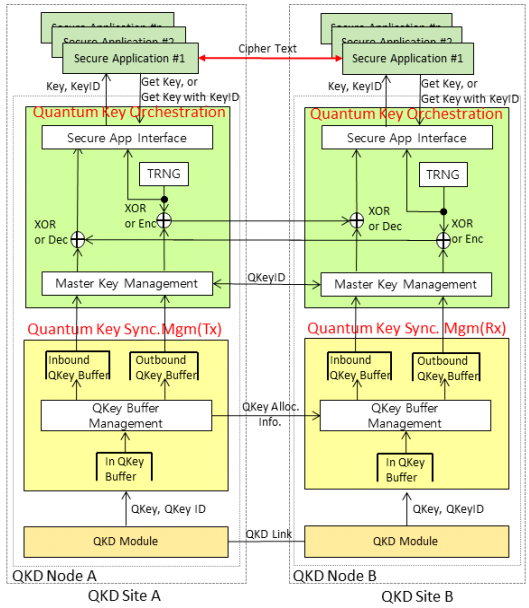

Fig. 2. Proposed QKD system structure and protocol

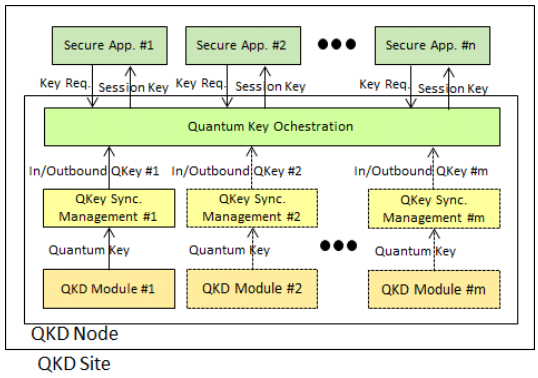

Fig. 3. Block diagram of QKD node with multiple QKDs and secure applications.

양자키와 양자키 ID를 양자키 동기 관리 장치로 전달한다.

양자키 동기 관리 장치는 입력 양자키 버퍼(input quantum key buffer), 양자키 버퍼 관리(quantum key buffer management) 블록, 송신용 양자키 버퍼(outbound quantum key buffer), 수신용 양자키 버퍼(inbound quantum key buffer)로 구성되어 있다. 입력 양자키 버퍼는 QKD 장치로부터 양자키와 양자키 ID를 받아서 저장한다. QKD 장치의 양자키 생성속도가 일정하지

않기 때문에 버퍼링이 필요하다. 양자키 버퍼 관리 장치는 입력 양자키 버퍼에 저장된 양자키와 양자키 ID를 송신용 양자키 버퍼와 수신용 양자키 버퍼에 저장하는 역할을 한다. 송신용 양자키 버퍼와 수신용 양자키 버퍼는 양자키 통합 장치에 양자키를 전달하기 위하여 사용된다. 양자키 동기 관리 장치는 연동되는 QKD 장치와 마찬가지로 송신자와 수신자 역할로 나누어진다. 송신자 역할의 양자키 동기 관리 장치는 송신용 양자키 버퍼와 수신용 양자키의 버퍼에 양자키와 양자키 ID를 저장하고, 저장한 정보를 수신자 역할의 양자키 동기 관리 장치로 전달한다. 수신자 역할의 양자키 버퍼 관리 장치는 전달받은 정보를 이용하여 송신용 양자키 버퍼와 수신용 양자키 버퍼에 QKD 장치에서 받은 양자키와 양자키 ID를 각각 저장한다.

양자키 통합 장치는 마스터키 관리(master key management) 블록, 암호(encryption) 블록, 복호(decryption) 블록, 실난수발생기(true random number generator), 암호장치 인터페이스(secure application interface) 블록으로 구성된다. 마스터키 관리 블록은 암호장치 인터페이스 블록, 암호화 블록, 복호화 블록, 실 난수 발생기를 제어한다. 또한, 상대 마스터키 관리 블록과 공개채널을 통하여 데이터 패킷을 송·수신한다. 암호화 블록과 복호화 블록은 배타적 논리합 또는 블록 암호를 사용한다. 배타적 논리합은 양자키의 생산량이 암호장치에서 요구하는 마스터키 소모량 보다 크면 사용할 수 있으며, OTP(One Time Pad)로 사용하기 때문에 양자키의 정보 이론적 안전성을 보장할 수 있다. 정보 이론적 안전성을 보장할 수 없지만 마스터키로 사용할 대량의 난수를 생성한 후 블록 암호로 양자키를 사용하여 마스터키를 암호화하면 양자키 생산 속도보다 더 많은 마스터키를 암호장치로 공급할 수 있다. 실난수발생기는 양자난수발생기 등을 사용하여 예측 불가능한 난수를 만들고 암호장치로 전달할 마스터키를 생성하기 위하여 사용한다. 암호장치 인터페이스는 암호장치와 물리적 및 논리적 인터페이스를 담당하고, 물리적 인터페이스를 통하여 전달된 논리적 인터페이스인 API(Application Program Interface) 명령을 해석하고 처리하는 역할을 한다.

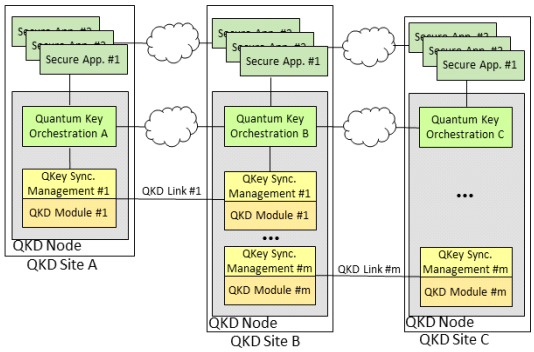

Fig. 4. Example of QKD networks

암호장치는 고유의 목적에 따라 링크용 암호장치, 전화기용 암호장치, VPN(Virtual Private Network) 등 다양한 암호장치를 사용할 수 있으며, QKD 노드로부터 마스터키를 받아 암호장치 사이에서 암호통신을 수행하기 위해 사용한다. 서로 다른 복수의 암호장치를 동시에 사용할 수 있다.

3.3 제안한 양자키분배 시스템의 동작

3.3.1 마스터키 생성

Fig. 2.의 QKD 시스템 구조에서 QKD 노드에 1개 이상의 QKD 장치를 적용할 수 있으며, BB-84 QKD, P&P QKD, MDI QKD 등 다양한 QKD 프로토콜을 사용할 수 있다. QKD 장치는 송신자와 수신자가 생성하고 측정한 무작위 값으로부터 raw 키, 걸러진 키 생성, 비밀증폭 등을 거쳐 두 QKD 장치가 공유하는 양자키와 양자키 ID를 생성한다. 각각 QKD 장치는 생성한 양자키와 양자키 ID를 양자키 동기 관리 장치의 입력 양자키 버퍼에 저장한다.

양자키 동기 관리 장치는 QKD 장치와 1대 1로 연동된다. 양자키 동기 관리 장치는 QKD 장치와 마찬가지로 송신자(A QKD 사이트)와 수신자(B QKD 사이트) 역할이 미리 나누어져 있다. A 사이트 양자키 동기 관리 장치의 양자키 버퍼 관리 블록은 입력 양자키 버퍼에서 양자키와 양자키 ID를 읽어서 송신 양자키 버퍼와 수신 양자키 버퍼가 비거나 넘치지 않도록 저장한다. 송신 양자키 버퍼와 수신 양자키 버퍼에 저장한 정보를 B 사이트의 양자키 동기 관리 장치로 전송한다.

B 사이트 양자키 동기 관리 장치는 A 사이트 양자키 동기 관리 장치가 보내온 정보를 이용하여 입력 양자키 버퍼에서 양자키와 양자키 ID를 읽어서 송신 양자키 버퍼와 수신 양자키 버퍼에 저장한다. A 사이트 양자키 동기 관리 장치의 송신 양자키 버퍼에

저장된 양자키 및 양자키 ID와 같은 양자키 및 양자키 ID가 B 사이트 양자키 동기 관리 장치의 수신 양자키 버퍼에 저장된다. 마찬가지로 A 사이트 수신 양자키 버퍼에 저장된 양자키 및 양자키 ID와 같은 양자키 및 양자키 ID가 B 사이트 송신 양자키 버퍼에 저장된다. 양자키 동기 관리 장치의 송신 양자키 버퍼와 수신 양자키 버퍼에 저장된 양자키와 양자키 ID는 상위의 양자키 통합 장치로 전달된다.

암호장치가 키요청을 하면 양자키 통합 장치는 난수로 만든 마스터키를 암호장치로 전달하고, 이 마스터키를 양자키로 암호화한 후 상대방 양자키 통합 장치로 전달한다. 이 과정을 통하여 두 QKD 노드의 양자키 통합 장치는 같은 마스터키를 공유한다. 양자키 통합 장치 내부의 마스터키 관리 블록이 이 과정의 전반적인 관리를 수행하며 마스터키 관리 블록의 주요 역할은 아래와 같다.

○ 송신용과 수신용 양자키와 양자키 ID 관리
○ 암호장치 인터페이스에서 받은 API 명령 처리
○ 실난수발생기, 암호화 블록, 복호화 블록 제어
○ 상대 사이트의 마스터키 관리 블록과 통신
○ 각 사이트로 연결되는 라우팅 테이블 관리
○ 각 사이트에 연동되는 암호장치의 ID 관리
○ 보안관리자(security officer) 접근 권한 관리
○ 암호장치와 보안 통신 관리

양자키는 양자키 통합 장치 사이에서 마스터키를 암호화하여 전달할 때 암호 및 복호용 키로 사용하기 때문에 두 QKD 노드 사이의 양자키의 동기를 쉽게 유지할 수 있다. 이러한 특성으로 인하여 기존 QKD 시스템보다 쉽게 송·수신자 역할이 없는 암호장치의 마스터키 공유, 키 중계(key relay), 그룹 암호통신 등의 응용을 처리할 수 있다.

3.3.2 마스터키 공유

Fig. 2.에서처럼 점대점으로 직접 연결된 두 A, B 사이트에서 암호장치가 마스터키와 마스터키 ID를 공유하는 프로토콜은 다음과 같다. A 사이트의 암호장치는 B 사이트의 암호장치와 암호통신을 하기 위하여 A 사이트의 양자키 통합 장치에게 B 사이트의 암호장치 ID를 매개변수로 사용하여 마스터키를 요청한다. 양자키 통합 장치는 암호장치의 마스터키 요청 명령을 받아서 해석하고, 실난수발생기로 마스터키를 생성한 후 마스터키와 마스터키 ID를 암호장치로 전달한다.

암호장치는 마스터키 ID를 B 사이트의 암호장치로 전달하고, B 사이트의 암호장치는 마스터키 ID를 매개변수로 사용하여 B 사이트의 양자키 통합 장치로 마스터키를 요청한다.

A 사이트의 양자키 통합 장치는 내부의 라우팅 테이블과 암호장치 ID를 이용하여 B 사이트까지의 라우팅 경로를 찾는다. 마스터키를 송신용 양자키 버퍼에 저장된 송신 양자키로 암호화하고, 암호화한 마스터키, 경로정보, 마스터키 ID, 양자키 ID를 데이터 패킷으로 만들어서 공개채널을 통하여 B 사이트의 양자키 통합 장치로 전송한다. B 사이트 양자키 통합 장치는 데이터 패킷을 수신하면 양자키와 양자키 ID를 확인하고 수신용 양자키 버퍼에 저장된 수신 양자키로 암호화된 마스터키를 복호화한 후 마스터키 ID와 같이 저장한다. B 사이트의 암호장치가 마스터키 ID를 매개변수로 마스터키를 요청하면, 암호키 통합 장치는 저장하고 있는 마스터키를 암호장치로 전달한다.

이 과정을 거쳐 A 사이트와 B 사이트의 암호장치는 같은 마스터키와 마스터키 ID를 공유할 수 있으며, 이 마스터키와 마스터키 ID를 이용하여 암호통신을 수행할 수 있게 된다.

A 사이트의 암호장치가 마스터키 요청을 시작하는 경우와 마찬가지로, B 사이트의 암호장치가 마스터키 요청을 시작하더라도 같은 절차에 의하여 마스터키를 공유할 수 있다.

3.3.3 키 중계

Fig. 4.는 QKD 네트워크 예이다. QKD 네트워크를 구성하면, 2개 이상의 QKD 장치가 있는 QKD 노드는 키 중계 기능이 필요하다. A 사이트의 암호장치가 C 사이트의 암호장치와 암호통신을 하는 과정은 다음과 같다. A 사이트의 암호장치는 C 사이트의 암호장치 ID를 매개변수로 A 사이트 양자키 통합 장치로 키를 요청한다. A 사이트 양자키 통합 장치는 암호장치의 ID를 이용하여 라우팅 테이블에서 마스터키 데이터 패킷을 전달할 라우팅 정보를 찾는다. 라우팅 정보를 읽어서 A 사이트의 양자키 통합 장치에서 C 사이트의 양자키 통합 장치로 마스터키를 전달하려면 B 사이트를 거쳐야 하는 것을 확인한다. A 사이트의 양자키 통합 장치는 실난수발생기를 이용하여 마스터키를 생성하고, 고유한 마스터

키 ID를 만든다. B 사이트와 연동되는 송신 양자키로 마스터키를 암호화하고, 암호화한 마스터키, 경로정보(A->B->C), 마스터키 ID, 양자 키 ID를 데이터 패킷으로 만들어 B 사이트의 양자키 통합 장치로 전달한다.

B 사이트 양자키 통합 장치는 A 사이트에서 온 패킷 내부의 경로 정보를 추출하여, 키 중계 역할을 확인한다. 키 중계를 하기 위하여 암호화된 마스터키를 A 사이트와 연결된 수신 양자키로 복호화하고, 다시 C 사이트와 연결된 송신 양자키로 암호화한다. B 사이트 양자키 통합 장치는 암호화한 마스터키, 경로정보(A->C), 마스터키 ID, 양자키 ID를 데이터 패킷으로 만들어 C 사이트의 양자키 통합 장치로 전달한다.

C 사이트의 양자키 통합 장치는 수신한 데이터 패킷에서 경로 정보를 확인하고 C 사이트가 최종 목적지 임을 확인한다. 마스터키를 B 사이트와 연동되는 수신 양자키로 복호화하고, 마스터키와 마스터키 ID를 저장한다.

A 사이트의 암호장치는 양자키 통합 장치가 제공한 마스터키와 마스터키 ID를 받아서, C 사이트의 암호장치로 마스터키 ID를 전송한다. C 사이트의 암호장치는 마스터키 ID를 매개변수로 사용하여 C 사이트 양자키 통합 장치로 키를 요청한다. C 사이트 양자키 통합 장치는 마스터키와 마스터키 ID를 암호장치로 전달한다. A 사이트의 암호장치와 C 사이트의 암호장치는 이 과정을 통하여 획득한 같은 마스터키와 마스터 키 ID를 이용하여 암호통신을 수행한다.

동일한 방식으로 QKD 노드 사이의 거리 확장을 위해 필요한 키 중계 기능을 담당하는 신뢰노드도 설계할 수 있다.

3.3.4 그룹 암호통신

제안한 QKD 시스템은 QKD 네트워크에 속한 모든 암호장치와 그룹 암호통신을 할 수 있다. 기존 QKD 시스템에서는 키 중계 기능을 이용하여 그룹 암호통신을 할 수는 있으나, 양자키 동기를 유지하기 위하여 매우 복잡한 구조와 프로토콜이 필요하다[1][2][3]. 그러나 제안한 스킴은 양자키와 마스터키의 연관성을 분리하였기 때문에 간단한 그룹키 공유 프로토콜로 그룹 암호통신을 할 수 있다. Fig. 4.와 같은 QKD 네트워크에서 암호장치들 사이에서 그룹 암호통신은 다음과 같이 수행할 수 있다. A 사이트의 암호장치는 복수의 암호장치와 그룹 암호통신을 수행하기 위하여 대상 암호장치의 ID를 매개변수로 사용하여 양자키 통합 장치로 그룹키를 요청한다. 양자키 통합 장치는 그룹키를 난수로 생성하고 그룹키 ID를 부여한 다음, 암호장치로 전달한다. 양자키 통합 장치는 암호장치의 ID를 이용하여 그룹키를 전달할 모든 경로를 탐색한다. A 사이트의 양자키 통합 장치는 B 사이트와 연계된 송신 양자키로 그룹키를 암호화하고, 암호화된 그룹키, 전달경로, 그룹키 ID, 송신 양자키 ID, 그룹 암호장치 ID를 데이터 패킷으로 묶어서 B 사이트로 전달한다. B 사이트의 양자키 통합 장치는 수신 양자키로 데이터 패킷의 그룹키를 복호화한다. B 사이트의 양자키 통합 장치는 패킷에 그룹 암호장치 ID 중 B 사이트에 속한 암호장치가 있는지를 확인한다. B 사이트에 속한 암호장치가 있으면 그룹키와 그룹키 ID를 저장하고, 패킷에서 B 사이트의 경로 정보와 암호장치 ID를 제거한다. C 사이트로 전달이 필요하면 그룹키를 C 사이트와 연계된 송신 양자키로 암호화하고, 암호화한 그룹키, 전달경로, 그룹키 ID, 송신 양자키 ID, 그룹 암호장치 ID를 데이터 패킷으로 묶어서 C 사이트로 전달한다. C 사이트는 데이터 패킷을 수신하면 수신 양자키로 그룹키를 복호화하고, 복호화된 그룹키와 그룹키 ID를 저장한다. 이 과정을 거쳐 그룹통신에 참여하는 모든 암호장치가 연동하는 QKD 통합 장치에는 같은 그룹키와 그룹키 ID를 가질 수 있게 된다.

처음 그룹 암호통신을 시작한 A 사이트의 암호장치는 모든 그룹 암호통신 대상 암호장치로 그룹키 ID를 전송한다. 그룹 암호통신에 참여하는 암호장치들은 연동하는 양자키 통합 장치에게 그룹키 ID를 매개변수로 그룹키를 요청하고 그룹키를 받아온다. QKD 네트워크의 구조에 따라 그룹 암호통신을 하려면 복수의 경로가 필요할 수 있다. 예를 들어, B 사이트에서 C 사이트 외의 다른 경로로 전달할 필요가 있으면, A 사이트의 양자키 통합 장치에서 복수의 경로를 모두 데이터 패킷으로 만들어서 B 사이트로 전달하고, B 사이트는 각 데이터 패킷에서 경로를 확인하고 해당 경로로 데이터 패킷을 전달한다.

IV. 결 론

이 논문에서는 기존 QKD 시스템에서의 활용성

및 성능이 제한되는 문제점에 대하여 분석하였으며, 해결방안으로 새로운 QKD 시스템의 구조와 프로토콜을 제안하였다. 제안한 스킴은 양자키의 생성과 사용에 있어서 계층별로 독립성을 부여함으로써 키동기를 쉽게 유지할 수 있다. 이로 인하여 제안한 스킴은 암호장치의 역할을 미리 결정하여 운용할 필요가 없으므로 운용의 효용성을 증대시킬 수 있으며, 키요청이 처리 중이어도 다른 키요청을 차단하지 않으므로 QKD의 성능을 높일 수 있다. 또한, 새로운 QKD 시스템의 구조와 프로토콜은 단순하고 일관성이 있는 구조로 인하여 확장이 용이하고, 키 중계, 그룹 암호통신 등을 쉽게 처리할 수 있는 장점이 있다.

References

[1] M. Dianati, R. Alléaume, M. Gagnaire and X. Shen, "Architecture and protocols of the future European Quantum key distribution network," Secur. Commun. Netw., vol. 1, no. 1, pp. 57-74, Jan. 2008.

[2] M. Peev et al., "The SECOQC quantum key distribution network in Vienna," New J. Phys., vol. 11, no. 7, Jul. 2009.

[3] M. Dianati and R. Alleaume, "Architecture of the secoqc quantum key distribution network," Proc. 1st Int. Conf. Quantum Nano Micro Technol. (ICQNM), pp. 13, Jan. 2007.

[4] M. Sasaki et al., "Field test of quantum key distribution in the Tokyo QKD network," Opt. Exp., vol. 19, no. 11, pp. 10387-10409, Aug. 2011.

[5] R. Alléaume et al., "Using quantum key distribution for cryptographic purposes: A survey," Theoretical Computer Science, vol. 560, part 1, pp. 62-81, Dec. 2014.

[6] A. Aguado et al., "The engineering of software-defined quantum key distribution networks," IEEE Commun. Mag., vol. 57, no. 7, pp. 20-26, Jul. 2019.

[7] Y. Cao, Y. Zhao, C. Colman-Meixner, X. Yu and J. Zhang, "Key on demand (KoD) for software-defined optical networks secured by quantum key distribution (QKD)," Opt. Exp., vol. 25, no. 22, pp. 26453-26467, Oct. 2017.

[8] Y. Zhao, Y. Cao, X. Yu and J. Zhang, "Software defined optical networks secured by quantum key distribution (QKD)," 2017 IEEE/CIC International Conference on Communications in China (ICCC), Qingdao, pp. 1-4, 2017.

[9] S. Marksteiner et. al., "On the Resilience of a QKD Key Synchronization Protocol for IPsec," Int. J. on Adv. in Secur., vol. 9, no. 3 & 4, pp. 90-100, Dec. 2016.

[10] S. Ghernaouti-Helie et al., "Using quantum key distribution within IPSEC to secure MAN communications," MAN 2005 conference, 2005.

[11] ETSI, "Quantum Key Distribution (QKD); Application Interface," ETSI GS QKD 004 V1.1.1, Dec. 2010.

[12] ETSI, "Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API," ETSI GS QKD 014, Feb. 2019.

[13] ISO/IEC, "Security requirements, test and evaluation methods for quantum key distribution - part 1: Requirements," ISO/IEC JTC1/SC27/WG3 working draft, Jan. 2020.

[14] ETSI, "Quantum Key Distribution (QKD); QKD Module Security Specification," ETSI GS QKD 008, Dec. 2010.

[15] L. Salvail et al., "Security of trusted repeater quantum key distribution networks," J. Comput. Secur., vol. 18, no. 1, pp. 61-87, Jan. 2010.

[16] P. Schartner and S. Rass, "How to

overcome the 'Trusted Node Model' in Quantum Cryptography," 2009 Int. Conf. on Computational Science and Engineering, pp. 259-262, Aug. 2009.
[17] A. Tajima et. al., "Quantum key distribution network for multiple applications," Quantum Science and Technology. 2(3), May 2017.
[18] A. Tajima et. al., "Quantum Key Distribution Network and Its Application," IEEE Photonics Conf. July 2018.
[19] ETSI, "Quantum Key Distribution (QKD): Components and Internal Interfaces," ETSI GS QKD 003, May 2018.
[20] ETSI, "Quantum Key Distribution (QKD): Use Cases," ETSI GS QKD 002, Jun. 2010.
[21] ETSI, "Quantum Key Distribution (QKD): Device and Communication Channel Parameters for QKD Deployment," ETSI GS QKD 012, Feb. 2019.
[22] ITU, "Overview on networks supporting quantum key distribution," ITU-T Y.3800. Oct. 2019.
[23] A. Mink et al., "Quantum Key Distribution (QKD) and Commodity Security Protocols: Introduction and Integration", Int. J. Netw. Secur. & Its Appli., vol. 1, no. 2, pp. 101-12, July 2009.

〈저자소개〉

고 행 석 (Haeng-Seok Ko) 정회원
1990년 2월: 충남대학교 컴퓨터공학과 학사
1992년 2월: 충남대학교 컴퓨터공학과 석사
2008년 8월: 충남대학교 컴퓨터공학과 박사
1992년 3월~2000년 1월: 국방과학연구소 선임연구원
2000년 2월~현재: ETRI 부설연구소 책임연구원
〈관심분야〉 암호모듈, 네트워크 보안, 양자암호

지 세 완 (Se-Wan Ji) 정회원
2001년 2월: 한국과학기술원(KAIST) 물리학과 학사
2003년 2월: 한국과학기술원(KAIST) 물리학과 석사
2009년 1월: 한국과학기술원(KAIST) 물리학과 박사
2009년 2월~2013년 1월: 고등과학원 연구원
2013년 2월~2016년 8월: Texas A&M University at Qatar 연구원
2016년 8월~현재: ETRI 부설연구소 선임연구원
〈관심분야〉 양자통신, 양자암호, 양자알고리즘

장 진 각 (Jingak Jang) 정회원
1999년 2월: 서강대학교 물리학과 학사
2001년 2월: 서강대학교 물리학과 석사
2013년 2월: 한양대학교 물리학과 박사
2001년 3월~현재: ETRI 부설연구소 책임연구원
〈관심분야〉 정보보호, 양자암호