https://doi.org/10.33778/kcsa.2021.21.1.003

양자암호 통신망에서 양자키 관리를 위한 통합 데이터 구조★

김 현 철*

요 약

양자 역학을 기반으로 하는 양자암호통신에서는 각각의 정보를 개별적인 광자에 실어 전송하기 때문에 일부만 도청하는 것이 기본적으로 불가능하며, 침입자가 광자를 불법적으로 가로채 수신자에게 재전송을 하여도 양자 복제 불가능성 원리에 의해 같은 정보를 광자에 실어 보내는 것이 불가능하다. 한편 네트워크 기반 다양한 서비스의 폭발적 증대와 함께 해당 서비스의 보안성 보장이 필수적으로 요구되면서 양자암호 통신망의 구축 및 관련 서비스가 다양한 형태로 추진되고 있다. 그러나 양자키 분배(QKD: Quantum Key Distribution) 기술의 발전과는 별개로 이를 활용한 네트워크 구축 및 다양한 양자암호 기반 서비스 제공 방안에 관해서는 많은 연구가 필요한 상태이다. 본 논문에서는 양자암호 장치를 기반으로, 다양한 양자암호 통신망 장비 간에 양자키를 전달하고 암호화된 전송환경 구현을 위한 통합 데이터 구조를 제안하였다.

Integrated Data Structure for Quantum Key Management in Quantum Cryptographic Network

Hyuncheol Kim*

ABSTRACT

In quantum cryptographic communication based on quantum mechanics, each piece of information is loaded onto individual photons and transmitted. Therefore, it is impossible to eavesdrop on only a part, and even if an intruder illegally intercepts a photon and retransmits it to the recipient, it is impossible to send the same information to the photon by the principle of quantum duplication impossible. With the explosive increase of various network-based services, the security of the service is required to be guaranteed, and the establishment of a quantum cryptographic communication network and related services are being promoted in various forms. However, apart from the development of Quantum Key Distribution (QKD) technology, a lot of research is needed on how to provide network-level services using this. In this paper, based on the quantum encryption device, we propose an integrated data structure for transferring quantum keys between various quantum encryption communication network devices and realizing an encrypted transmission environment.

Key words : Quantum Communication Network, Quantum Key Distribution, Quantum Cryptography

접수일(2021년 02월 28일), 게재확정일(2021년 3월 18일)

* 남서울대학교 컴퓨터소프트웨어학과 교수

★ 이 논문은 2020년도 남서울대학교 학술연구비 지원에 의해 연구되었음.

1. 서 론

전세계적으로 5G와 초고속 인터넷으로 대표되는 유무선 통신서비스의 급속한 확대에 따라 이러한 서비스들의 보안과 관련된 다양한 사항들은 공공서비스와 기업의 기밀정보 보호 및 다양한 개인정보보호 측면에서 그 중요성이 점차 확대되고 있다. 대부분의 기존 통신 시스템에서 채택하고 있는 비대칭 공개키 암호체계는 수학적인 “계산 복잡성”의 원리를 기반으로 하고 있다. 대표적 공개키 암호체계인 RSA의 원리는 매우 큰 수를 소인수 분해하는 것이 수학적으로 매우 난해하다는 점이다. 즉 소인수분해를 할 때 큰 수를 사용할수록 계산시간이 수학적으로 지수적으로 증가하게 된다는 것이다.

이러한 원리를 통신 시스템에 적용하면 송신자와 수신자가 충분히 큰 수의 소인수분해 해를 공개키와 비밀키로 사용하면 불법적인 암호문 해독이 현실적으로 매우 난해하다. 그러나, 최근 들어 양자컴퓨터 기술의 발전과 이를 기반으로 하는 다양한 소인수분해 알고리즘들이 개발됨에 따라 수학적 계산 복잡성에 기초한 암호체계들은 그 안전성에 심각한 위협을 받게 되었다. 즉 양자컴퓨터를 이용하면 RSA와 같은 암호체계는 어렵지 않게 해독이 가능한 것으로 판명되고 있다 [1][2].

이러한 추세를 반영하여 기존의 암호체계를 근본적으로 대체할 대안으로 등장한 양자암호(quantum cryptography) 기술은 수학적인 계산 복잡성에 암호체계의 안전성을 두지 않고, 양자 역학의 원리에 기초하여 도·감청이 근본적으로 불가능하므로 절대적인 안전성을 보장한다 [3][4].

양자암호통신 방식은 양자의 기본 특성을 이용해서 송·수신자 두 사람만 알고 있는 비밀키를 양자채널과 일반채널로 구성되는 통신선로를 통하여 교환할 수 있는 새로운 방식이며, 이를 양자키 분배(QKD: Quantum Key Distribution) 기술이라고 한다. 그러나 QKD 기술의 발전과는 별개로 이를 활용한 네트워크 구축 및 다양한 양자암호 기반 서비스 제공 방안에 관해서는 많은 연구가 필요한 상태이다 [5][6][7].

본 논문에서는 양자암호 장치와 IPSec 암호장치를 기반으로 하는 양자암호 통신망에서 다양한 양자암호 통신망 장비 간에 양자키를 전달하고 암호화된 전송 환경 구현을 위한 통합 데이터 구조를 제안하였다.

2. 양자암호통신

2.1 개요

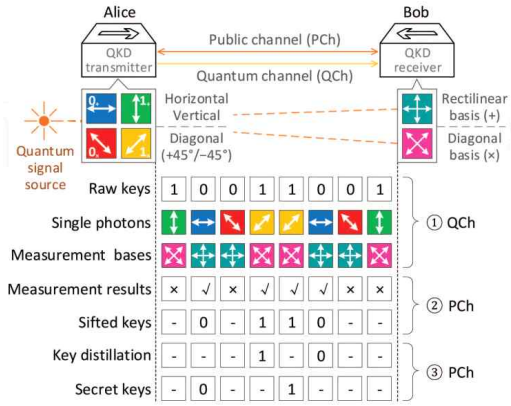
넓은 의미에서 양자암호통신은 양자 정보기술(quantum information technology)의 한 분야이며 양자 정보처리·정보통신 기술은 양자암호통신 기술과 양자 상태의 순간적인 원거리 이동을 수행하는 양자 원격전송 기술, 그리고 ‘양자 중첩’ 및 ‘양자 얽힘’의 원리를 바탕으로 대규모 연산을 수행하는 양자컴퓨팅 기술 등의 형태로 급속하게 발전하고 있다. 즉, 정보를 양자 상태에 직접적으로 매핑하여 처리하는 양자 정보기술은 기존의 기술로는 불가능한 다양한 일들을 수행할 수 있다.

이러한 양자 패러다임 변화 중에서도 양자암호통신 기술은 기술성숙도가 가장 높은 기술로서 현재 미국, 유럽, 일본 등 선진국을 중심으로 세계적으로 활발한 연구가 이루어지고 있다. 또한 양자암호통신 기술은 기본적으로 이미 매설된 통신 사업자들의 광섬유를 이용하기 때문에 손쉬운 대규모 상용화가 가능하다.

2.2 양자암호 프로토콜

RSA로 대표되는 비대칭 공개키 암호체계와 달리 대칭암호 체계에서는 암호키로 송·수신자가 미리 공유한 일회용 난수표(one-time pad)를 사용하여 안전한 통신을 보장한다. 양자암호통신에서는 양자 복제 불가 법칙에 기초하여 송·수신자 간에 일회용 난수표를 안전하게 분배하는 기술로서 “양자키분배(QKD)” 기술이라고 한다.

BB84 프로토콜로 명명된 최초의 양자암호 프로토콜은 1984년 IBM의 C. H. Bennett와 몬트리올 대학의 G. Brassard에 의해 발표되었다. (그림 1)에서와 같이 BB84에서는 두 개의 기저(basis)를 이루는 네 개의 양자 상태를 이용한다 [1][2][3][4]. BB84에서 송신자(Alice)는 ✢혹은 ✕ 중 한 개를 기저를 무작위로 선택하고 (1단계), 선택된 기저의 두 가지 양자 상태, 즉 0 혹은 1중에서 하나를 임의로 골라 수신자(Bob)에게 보낸다 (2단계). 따라서 총 4가지 형태의 키 비트가 생성된다.



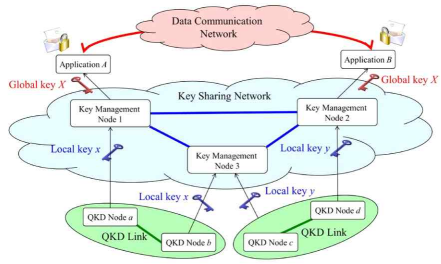
(그림 3) BB84 프로토콜 [2][3]

수신측 Bob도 역시 ✣, ✕ 두 가지 기저 중 하나를 무작위로 선택하여 (3단계), 수신된 양자 상태를 측정한다(4단계). 이때 Bob도 임의의 기저를 사용하기 때문에 0.5 확률로 틀린 기저를 사용하게 된다. 따라서 만일 송신 기저와 다른 기저를 사용하여 측정하였으면 0.5의 확률로 큐빗 0 또는 1로 측정하게 된다. 이후 Alice와 Bob은 선택한 기저를 public 채널을 통해 공유하는데, 선택한 기저가 같은 경우 Bob의 측정 결과는 Alice가 임의로 고른 양자 상태와 일치하며, 따라서 두 사용자가 같은 암호키(sifted key)를 갖게 된다(5단계).

3. QKD 기반 네크워크

3.1 QKD 기반 네트워크 구조

두 노드 간에 도청 공격에 대한 보안을 제공하는 QKD는 공유 난수를 암호화 키로 사용하는 매우 안전한 통신 기술이지만 극복해야 할 몇 가지 제약이 있다. 첫 번째는 키 공유 확산의 제약이다. 즉, 송·수신자 간에만 키가 공유되기 때문에 직접 연결된 두 노드만 암호화된 데이터를 전송할 수 있다. 두 번째 문제점은 키 공유 속도이다. 고정밀 광자 전송 및 감지의 어려움과 환경 변화에 따른 광섬유 특성의 변동으로 인해 실제 키 공유 속도는 약 1.9Mb/s 정도에 머물고 있다. 그러나 QKD가 제공하는 보안성 강화의 장점을 최대한 활용하려면 OTP 암호화가 필요하며, OTP에 필요한 키 공유 속도는 데이터 전송 속도와 같아야 한다.

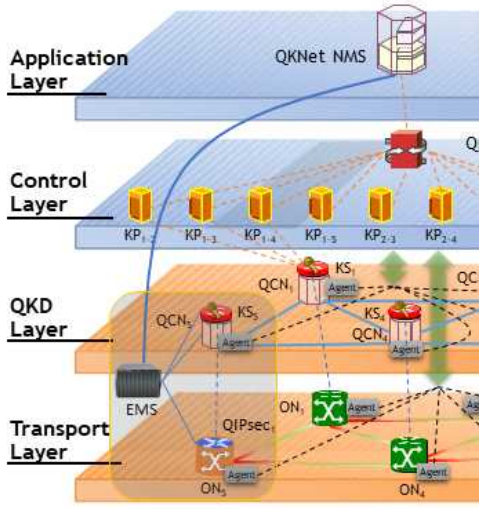


(그림 2) QKD 기반 네트워크 기본 구조

(그림 2)는 QKD 네트워크의 일반적인 구조를 나타내고 있다. QKD 네트워크는 QKD 노드, 키 관리 노드 및 애플리케이션의 세 가지 유형의 노드들로 구성된다. 플리케이션과 키 관리 노드 사이 및 키 관리 노드와 QKD 노드 사이의 통신은 기존 보안방식과 인증방식을 이용하여 보호되어야 한다.

3.2 QKD 기반 네트워크 구성요소

QKD 노드는 QKD 암호화 키를 공유하는 QKD 송·수신기이며 QKD 노드 간에 공유되는 암호화 키를 "로컬 키"라고 하며 로컬 키를 이용한 데이터의 보안은 직접 연결된 QKD 노드 간에만 유효하다. 한편 QKD 링크는 QKD 송·수신기를 연결하는 광섬유 링크이며 일대일 QKD 노드는 하나의 QKD 링크로만 연결될 수 있다 [5][6][7].



(그림 3) 제안된 양자암호 통신망 구성

키 관리 노드는 인접 QKD 노드 간에 공유되는 로컬 키를 관리하며 QKD 노드에서 생성된 로컬 키를 기반으로 인접한 QKD 노드와 암호화 터널을 생성할 수 있다. 마지막으로 키 공유 네트워크는 다수의 키 관리 노드와 이들 간의 터널 링크로 구성된다.

4. 제안된 양자암호통신망 구성

(그림 3)은 QKD 네트워크 통합운영을 위한 전체적인 구조를 나타내고 있다. 제안된 QKD 네트워크는 Transport 계층, QKD 계층, 제어 계층, 그리고 NMS를 포함하는 응용계층으로 구성된다.

- Transport 계층은 망에서 QE (Quantum Encryption)-capable 장치들로 구성되며, IPSec와 암호 처리 능력이 광전송 장치(ON: Optical Node)들로 구성된다.
- QKD 계층은 QCN (quantum communication node) 장치들과 키 서버(KS: Key Server)들로 구성된다.
- 제어 계층은 네트워크 컨트롤러와 키풀(KPs : Key Pools)로 구성된다. EMS (Element Management System)은 NMS로부터 다양한 관리적인 인터페이스를 제공하며, ON, QCN, 그리고 KS를 관리한다.
- 응용계층은 NMS를 E2E QE 서비스를 요청하는 응용으로 구성된다.

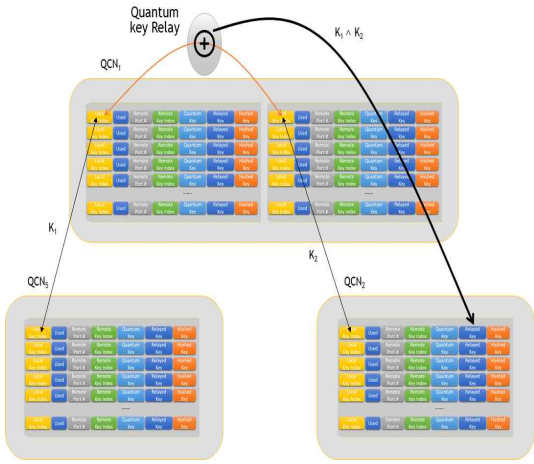
4.1 양자키 관리를 위한 데이터구조

QKD 계층은 QCN, KS, 그리고 컨트롤러 agent들의 집합으로 구성되며 전체적인 보안 측면에서 양자키는 QKD 계층을 벗어날 수 없다는 조건을 기본으로 한다.

KS는 (그림 4)에서와 같이 QCN으로부터 받은 양자키 정보를 기록하고, 해당 양자키의 hash 값을 생성하여 Key Index와 함께 저장한다. 양자키는 QKD 계층을 벗어날 수 없으므로, KS는 Key index와 hash 값을 KP로 전달한다.

QKD 키 생성률이 데이터 전송률과 비교해 현저히 낮고, 또 QKD 오류 상태를 대비하여 KS/KP/EMS/NMS는 키 재사용 기능을 제공한다. KP는 물리적인 위치와 상관없는 overlay 네트워크로 구축되며 KS로부터 양자키를 받아 관리한다.

(그림 4) QCN5에서의 KS5 구성 예



(그림 5) QCN1에서 양자키 릴레이와 전달을 지원하기 위한 구조

QKD 계층에서 생성된 양자키는 KS에서 관리되며, KP로는 Key ID와 Hash 값, 그리고 관련 정보만 전달된다. QKD 기반 연구망은 기본적으로 릴레이 노드를 지원한다. QKD 계층은 양자키 생성과 더불어 NMS/EMS 연동을 통해 생성된 양자키를 보안 채널을 통해 QIPsec 장비나 암호기능이 있는 전송 장비로 전달하는 기능을 수행한다.

(그림 5)는 QCN1에서 양자키 관리 및 양자키 릴레이 기능을 수행하기 위한 전체적인 데이터구조를 나타내고 있다.

6. 결 론

전세계적으로 5G와 초고속 인터넷으로 대표되는 유무선 통신서비스의 급속한 확대에 따라 이러한 서비스들의 보안과 관련된 다양한 사항들은 공공서비스와 기업의 기밀정보 보호 및 다양한 개인정보보호 측면에서 그 중요성이 점차 확대되고 있다. 대부분의 기존 통신 시스템에서 채택하고 있는 비대칭 공개키 암호체계는 수학적인 “계산 복잡성”의 원리를 기반으로 하고 있다. 대표적 공개키 암호체계인 RSA의 원리는 매우 큰 수를 소인수 분해하는 것이 수학적으로 매우 난해하다는 점이다. 즉 소인수분해를 할 때 큰 수를 사용할수록 계산시간이 수학적으로 지수적으로 증가하게 된다는 것이다.

QKD 기술의 발전과는 별개로 이를 활용한 네트워크 구축 및 다양한 양자암호 기반 서비스 제공 방안에 관해서는 많은 연구가 필요한 상태이다.

본 논문에서는 양자암호 장치와 IPSec 암호장치를 기반으로 하는 양자암호 통신망에서 다양한 양자암호 통신망 장비 간에 양자키를 전달하고 암호화된 전송환경 구현을 위한 통합 데이터 구조를 제안하였다.

참고문헌

[1] Yongli Zhao, et al., “Resource Allocation in Optical Networks Secured by Quantum Key Distribution” IEEE Communications Magazine, Vol 56, Issue 8, pp. 130-137, 2018.

[2] Yongli Zhao, et al., “Quantum Key Distribution (QKD) over Software-Defined Optical Networks,” IEEE Transactions on Broadcasting, IntechOpen access.

[3] YUAN CAO, et al. “Key on demand (KoD) for software-defined optical networks secured by quantum key distribution (QKD),” Optics Express, Vol. 25, No. 22, 2017.

[4] YUAN CAO, et al. “KaaS: Key as a Service over Quantum Key Distribution Integrated Optical Networks” IEEE Communications Magazine, Vol 57, Issue 5, pp. 152-159, 2019.

[5] JYUAN CAO, et al. “Resource Assignment Strategy in Optical Networks Integrated With Quantum Key Distribution,” IEEE Journal of Optical Communications and Networking, Vol. 9, Issue 11, pp. 995-1004, 2017.

[6] Alejandro Aguado, et al., “Virtual Network Function Deployment and Service Automation to Provide End-to-End Quantum Encryption,” IEEE Journal of Optical Communications and Networking, Vol. 10, Issue 4, pp. 421-430, 2018.

[7] Ririka Takahashi, et al.,, “A high-speed key management method for quantum key distribution network,” IEEE International Conference on Ubiquitous and Future Networks (ICUFN), 2019.

〔저자소개〕

김 현 철 (Hyuncheol Kim)
1990년 2월 성균관대학교 학사
1992년 2월 성균관대학교 석사
2005년 8월 성균관대학교 박사
2006년 9월 ~ 현재 남서울대학교 컴퓨터소프트웨어학과 교수
email : hckim@nsu.ac.kr