https://doi.org/10.33778/kcsa.2021.21.3.003

양자키분배와 IPSec을 결합한 네트워크 보안 장치 연구★

이 은 주*, 손 일 권*, 심 규 석*, 이 원 혁**

요 약

현존하는 대부분의 인터넷 보안 프로토콜은 소인수분해 문제의 수학적 복잡도에 기초한 고전적인 암호화 알고리즘에 의존하고 있으나, 이러한 고전 알고리즘은 양자 컴퓨터의 공격에 취약하다고 알려져 있다. 최근 양자 컴퓨팅 기술이 비약적으로 발전하면서 기존 통신의 물리 및 네트워크 계층 보안을 위해 양자키분배 기술을 적용하는 것이 국제적으로 필수적인 과제가 되고 있다. 본 연구에서는 성형 네트워크에 적용하기 위한 plug & play 방식의 양자키분배 장치를 제작하고, 생성된 양자키를 IPSec의 키 교환 과정에 이용함으로써 기존 IPSec 장치와 연동 실험한 결과를 보고하고자 한다.

Quantum Key Distribution System integrated with IPSec

Eunjoo Lee*, Ilkwon Sohn*, Kyuseok Shim*, Wonhyuk Lee**

ABSTRACT

Most of the internet security protocols rely on classical algorithms based on the mathematical complexity of the integer factorization problem, which becomes vulnerable to a quantum computer. Recent progresses of quantum computing technologies have highlighted the need for applying quantum key distribution (QKD) on existing network protocols. We report the development and integration of a plug & play QKD device with a commercial IPSec device by replacing the session keys used in IPSec protocol with the quantum ones. We expect that this work paves the way for enhancing security of the star-type networks by implementing QKD with the end-to-end IP communication.

Key words : Quantum Key Distribution, IPSec, IKE

접수일(2021년 04월 02일), 게재확정일(2021년 08월 28일)

★ 본 논문은 2021년도 한국과학기술정보연구원(KISTI)의 주요 사업 과제의 지원을 받아 연구되었음.

* 한국과학기술정보연구원

** 한국과학기술정보연구원(교신저자)

1. 서 론

양자키분배(quantum key distribution, QKD)란 양자물리학의 고유한 특성을 이용하여 송신자와 수신자 간에 공개된 채널을 통해 통신 암호 키를 안전하게 분배하는 것을 말한다. 비트 형태의 정보를 전송하기 위해 단일광자의 편광상태와 같은 양자 상태를 이용하며, 이 과정에서 공개 채널을 통한 도청을 시도하면 물리법칙에 의해 분배된 암호 키에 오류를 발생시키므로 도청자의 존재 여부를 밝혀낼 수 있다. 1984년 Bennet과 Brassard가 제안한 아이디어를 시작으로 실제 통신에 적용할 수 있는 양자키분배 장치 연구가 현재까지 활발하게 진행되고 있으며, 2000년대 중반부터는 유럽과 미국의 소수 업체들이 상용 양자키분배 시스템을 생산하고 있다.

본 논문에서는 국가과학기술연구망(KREONET)에 적용하기 위해 제작한 BB84 프로토콜 기반 plug&play 양자키분배 시스템에 대해 소개하고, 이를 네트워크 보안 기술의 하나인 IPSec의 키 교환 단계에 적용함으로써 양자컴퓨터의 공격에도 안전한 통신 시스템을 구현한 결과에 대해 보고하고자 한다.

2. 양자키분배

2.1 BB84 프로토콜

BB84 프로토콜[1]은 1984년에 Bennet과 Brassard가 제안한 최초의 양자키분배 프로토콜로써, 두 사람의 이름 첫 자를 따서 BB84 프로토콜이라고 불리게 되었다. 이 프로토콜은 광 채널을 통해 전송되는 단일광자들의 양자상태를 이용한다. 편광상태를 예로 들면, 송신자인 Alice는 광자의 편광상태를 네 가지 선형 편광(수평/수직, +45/-45도) 중의 하나로 준비한다. 수평-수직 기저와 대각선 기저 중 하나를 선택할 수 있고, 각 기저를 이루는 두 편광 방향에 각각 비트 0, 1을 부여한다. 수신자인 Bob은 Alice가 양자채널을 통해 보낸 광자의 편광상태를 측정하고자 하는데, 수평/수직 기저와 대각선 기저 중 하나를 무작위로 선택하여 측정한다. 검출기로 측정하는 과정에서 단일광자가 유실되기 때문에 측정은 단 한 번만 가능하며, Bob은 측정 기저와 결과를 기록한다. 그 후 Alice와 Bob은 공개된 고전 통신 채널을 통해 전송과 측정 시 이용한 편광 기저를 비교한다. 만약 Bob의 측정 기저가 Alice가 전송한 기저와 다를 경우 측정 결과를 확정할 수 없게 되므로 이때의 비트 정보를 버리게 되는데, 이 과정을 키 시프팅(key sifting)이라고 한다. 남은 비트의 경우 동일한 광자에 대해 같은 기저를 사용하였기 때문에 양쪽이 같은 비트 정보를 공유하게 된다. 이후 오류 보정과 비밀 증폭과 같은 후처리 과정을 통해 키의 일치도와 안정성을 높이고 나면 최종 키가 완성된다.

편광 인코딩을 이용한 첫 QKD 실험은 1989년에 Bennet[2] 등이 32 cm의 자유공간 양자 채널에서 구현했고, 4년 뒤 제네바 대학 Gisin의 그룹에서는 양자채널을 1 km 광섬유로 대체하여 통신거리를 확장한 결과를 보고하였다[3, 4].

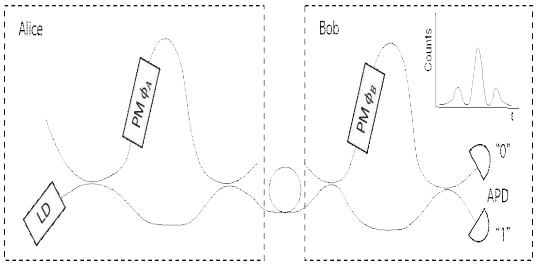
2.2 위상 인코딩을 이용한 QKD

앞서 소개한 빛의 편광상태를 이용하여 정보를 인코딩하는 방식은 자유공간에서 비교적 간단하게 구현할 수 있으나, 광섬유 케이블을 양자채널로 이용할 경우 광자들의 편광상태가 유지되지 않는다는 단점이 있다. 편광유지광섬유(polarization maintaining fiber)를 이용하는 방법도 있긴 하지만 수십 km 이상의 장거리 통신에 이용하기에는 가격이 고가이기 때문에 합리적인 선택은 아니다. 대신 이중 마하젠더 간섭계[5-10]로 동일한 프로토콜을 구현할 수 있는데, 편광 인코딩에 쓰였던 편광상태들은 마하젠더 간섭계의 두 경로 사이의 위상 차이로 치환된다. (그림 1)에 묘사된 바와 같이, Alice와 Bob은 각자가 가지고 있는 마하젠더 간섭계의 위상차를 조절할 수 있다.

만약 두 간섭계의 위상 차이가 같거나 π의 정수배일 경우에는 Bob의 간섭계 출력부에서 보강 또는 상쇄 간섭이 반드시 일어나므로 두 검출기 중 어디에서 검출될지 확정적으로 알 수 있다. 그러나 위상차가 이와 다른 값일 경우에는 양 검출기에서 광자가 무작위로 검출되게 된다. 편광 기반 프로토콜에서 Alice가 4개의 서로 직교하지 않는 편광상태 중 무작위로 하나를 준비했듯이, 여기서는 4개의 위상

$\left\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\right\}$ 중 하나를 선택하여 간섭계의 위상차 ϕ_A를 설정한다. 그리고 Bob이 앞서 측정 기저를 선택했듯이 자기가 가진 간섭계의 위상차 ϕ_B를 $\left\{0, \frac{\pi}{2}\right\}$ 중 하나로 설정한 후 간섭 결과를 두 개의 단일광자검출기로 측정한다. 위쪽 검출기에서 광자가 검출되면 비트 0, 아래쪽 검출기에서 검출되면 비트 1로 기록한다. 이후에는 고전 통신 채널을 통해 양자상태 준비(Alice)와 측정(Bob)에 사용한 위상 기저들을 비교한 후 같은 기저를 사용했을 때의 키만 남기고 나머지는 버린다. 이후 후처리 과정은 편광 기반 프로토콜과 동일하다.

위상 인코딩에 기초한 첫 QKD 시스템은 1993년에 Townsend[6] 등이 처음 발표했는데, 양자채널로 10 km 길이의 광섬유 스풀을 사용했다. 같은 그룹에서 1994년에 발표한 시스템은 Alice의 간섭계 출력부와 Bob의 간섭계 입력부에 존재하는 광섬유 빔 분할기를 편광 빔 분할기(Polarization beam splitter, PBS)로 대체하고 시간 다중화 대신 편광 다중화를 사용함으로써 간섭 신호와 상관없는 side peak(그림 1에서 중앙의 높은 peak를 제외한 나머지)들을 제거하였다.[8] 2004년에는 실리카 광집적소자에 구현한 간섭계 시스템을 이용하여 150 km 이상의 거리에서 시험해 보기도 했으며[11], 같은 해에 Toshiba Research Europe에서는 새로운 능동 간섭계 안정화 방법을 적용하여 1550 nm 파장에서 사용할 수 있는 자동화 시스템을 개발하고 122 km 거리에서 시험한 바 있다[12, 13].



(그림 1) 이중 마하젠더 간섭계를 이용한 BB84 QKD 실험 구성도.

2.3 Plug&Play 방식의 QKD

단일광자의 편광과 위상은 온, 습도와 같은 주변 환경 변화에 따라 변화할 수 있는데, 이를 방지하기 위해서는 능동 안정화 장치가 추가로 필요하다. 그러나 이는 전체 QKD 시스템을 복잡하게 하므로, 가능하면 능동소자 없이 편광/위상 변화를 보상하는 것이 바람직하다. 1997년에 Müller[14] 등은 위상 코딩을 이용하여 광학적, 역학적 섭동을 잡아낼 수 있는 QKD 장치를 제안한 바 있으며, 같은 해에 Zbiden[15] 등이 첫 실험 구현에 성공했다. 초기 시스템은 1300 nm 파장 대역의 광원을 이용했고[16-18], 1999년에 처음으로 1550 nm 대역 광원을 적용한 사례가 보고되었다[19]. 2002년에는 더 향상된 시스템을 이용하여 스위스 제네바와 로잔 사이 67 km 광섬유 링크를 통해 1550 nm 파장에서의 통신 실험이 이루어졌다[20]. 이 장치의 원리는 다음과 같다.

먼저 편광이 서로 수직하고 시간적으로 떨어져 있는 두 개의 강한 펄스를 Bob이 Alice에게 전송한다. Alice 쪽에 도착한 두 펄스는 패러데이 미러(Faraday mirror)라는 소자에서 반사되는데, 이 소자는 페러데이 편광 회전기(Faraday rotator)와 거울이 합쳐진 형태로써 반사 후 빛의 편광상태를 90도 회전시키는 역할을 한다. 이후 먼저 도착한 펄스의 위상(ϕ_A)을 $\left\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\right\}$ 4개 중 하나로 무작위로 변조하고, 광자 몇 개 수준으로 감쇠시킨다. 편광상태가 입사 전과 수직으로 바뀐 상태에서 다시 Bob의 간섭계로 되돌아가면 전송라인 광섬유 내의 복굴절로 인한 편광 변화가 보상되며 수평(수직) 편광 상태로 전송되었던 광자는 수직(수평) 편광 상태로 되돌아온다. Bob의 간섭계로 먼저 도착한 펄스는 비대칭 마하젠더 간섭계의 긴 경로를 지나고, 나중에 도착한 펄스는 짧은 경로를 지난다. 이 때 Bob은 두 경로 중 하나의 위상(ϕ_B)을 $\left\{0, \frac{\pi}{2}\right\}$ 둘 중 하나로 변조한 후 간섭을 측정한다. 이후의 과정은 2.2절의 이중 마하젠더 간섭계를 이용한 QKD와 동일하다.

"Plug & play" 시스템이라 불리는 이 실험 구성은 광 펄스 사이의 시간 지연 및 보상이 한 개의 비대칭

마하젠더 간섭계로부터 유도되기 때문에 별도의 안정화 장치가 필요하지 않다는 장점이 있다. 또한 수신부인 Bob에서 검출기뿐만 아니라 광원도 가지고 있기 때문에, 수신부를 중앙에 두고 다중화 과정을 통해 다수의 송신자와 통신할 수 있다면 단방향 QKD 장치보다 상대적으로 적은 리소스를 사용하면서 KREONET과 같은 성형 (star-type) 네트워크에 적용할 수 있을 것이다. 그러나 다음과 같은 사항들도 고려해보아야 한다. 우선 광 펄스가 Bob에서 Alice로 전송되었다가 다시 되돌아와야 하므로 전송 속도를 올리는 데 한계가 있다. 또, 강한 광 펄스의 레일리 후방 산란(Rayleigh backscattering)이 약한 펄스의 양자상태에 영향을 주어 오류율을 높일 수 있으므로 [17] 서로 반대 방향으로 진행하는 두 펄스열들이 만나지 않도록 타이밍을 조절해야 한다.

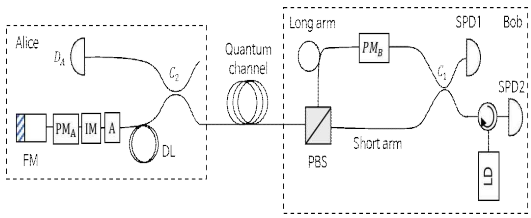
3. IPSec

IPSec은 데이터 패킷을 인증하고 암호화하여 네트워크 계층에서의 IP 통신을 보호하는 기술이다. IPSec은 데이터 인증, 재전송 공격 방지, 데이터 무결성을 보장하는 포괄적인 보안 해결책을 통해 IP 패킷의 데이터를 암호화한다. [21, 22] IPSec은 보안 프로토콜과 보안 연결(security associations, SA), 키 관리, 인증과 암호화 알고리즘으로 구성되어 있다.

IPSec에서의 키 관리를 위해 IKE (internet key exchange) 프로토콜을 수행하게 되는데, 이는 키 교환 및 SA 협상, 인증, 키 관리 서비스를 제공한다[22, 23]. IKE는 두 단계를 거쳐 실행되는데, 1단계(Phase 1)에서는 키 교환 보안 연결, 터널 수립에 필요한 보안 속성을 협상하여 안전한 통신 채널을 설정한다. 이 과정에서 VPN 장비 간 사용할 인증 방식과 암호화 방식, 키 교환 방식, 무결성 확인 방식, 보안 정책 시간 등을 설정한다. IKE SA 설정 과정에서 암호, 무결성 알고리즘에 대한 협상이 이루어지면, 디피-헬먼(Diffie-Hellman) 알고리즘을 이용하여 마스터 키를 생성하고 상호 인증 과정을 거친 후 IKE용 세션 키를 생성한다. 2단계(Phase 2)에서는 디피-헬먼 알고리즘으로 IPSec을 위한 세션 키를 생성하고, 생성된 세션 키를 사용하여 IPSec VPN 터널을 형성한다.

그러나 디피-헬먼 알고리즘은 소인수 분해 알고리즘의 계산 복잡도에 의존하기 때문에 RSA 암호시스템과 같이 향후 양자컴퓨터의 공격에 취약할 수 있다. 또한 통신하는 피어 사이에 배포될 수 있는 키의 충전 주기가 한정되어 있고, 생성된 키가 조건부로 안전하다는 것[24]도 약점으로 지적된다. 따라서 본 연구에서는 기존의 디피-헬만 알고리즘 기반의 키 생성과 배포를 양자키분배로 대체하여 네트워크상의 보안 문제를 해결하고자 하였다.

4. Plug&Play 양자키분배 장치 제작



(그림 2) Plug&Play 방식의 양자키분배 장치 구성도. FM : Faraday mirror, IM : intensity modulator, A : variable attenuator, PM : phase modulator, DL : delay lne

2.3절에서 소개한 Plug&Play 방식의 양자키분배 실험 구성도를 (그림 2)와 같이 설계하였다. Bob 쪽의 레이저 다이오드(laser diode, LD)에서 광 펄스를 생성하고, optical circulator(OC)를 통해 간섭계로 전달한다. 이 때 OC는 입사한 빛을 정해진 방향으로 순환시켜주는 역할을 하는데, 예를 들어 Port 1로 들어온 빛은 Port 2로만, Port 2로 들어온 빛은 Port 3으로만 진행할 수 있다. 덕분에 광원에서 나오는 광자와, Alice와 Bob의 간섭계를 거쳐서 돌아오는 광자를 효과적으로 분리할 수 있다. 들어온 빛을 50:50으로 나눠주는 광섬유 결합기(optical coupler) C_1을 통해 Bob의 간섭계를 지나면 편광상태가 서로 수직인 두 개의 분리된 펄스열이 만들어진다. 이 때 위상변조기 PM_B는 비활성화되어 있다.

두 펄스는 양자채널인 광섬유 스풀을 지난 후 Alice의 시스템에 도달하는데, 광섬유 결합기 C_2를 통해 신호가 나누어지면서 한 포트에서는 광 검출기

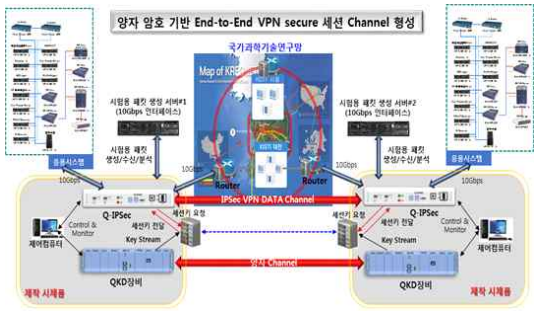
(photodiode)로 광신호 모니터링을, 나머지 포트에서는 위상 인코딩을 진행한다. 광섬유 스풀 DL이 쓰인 이유는 2.3절에서 설명했듯이 아직 감쇠가 안 된 강한 광신호의 후방 산란의 영향으로부터 인코딩된 양자 신호를 보호하기 위한 장치이다. 본 실험에서는 임의로 10 km 길이의 광섬유 스풀을 사용하였으나, 추가 실험을 통해 최적화된 길이의 스풀로 교체하면 더 빠른 키 발생율을 기대할 수 있을 것이다. 패러데이 미러(FM)에서 반사되고 나면 편광이 90도 회전하고, Alice는 나중에 도착한 광 펄스에 위상변조기 PM_A를 이용하여 네 가지 위상 중 하나를 골라 인가해 준다. 진폭변조기(IM)는 광자수 쪼개기 공격을 방지하기 위한 디코이(decoy) 상태 프로토콜[25, 26]을 적용하기 위해 사용되었다. 이후 광 감쇠기(attenuator)를 통과하면서 빛의 세기가 광자 몇 개 수준으로 감소한다.

앞서 FM 덕분에 편광상태가 90도 회전하고, 왔던 길을 그대로 되돌아갔기 때문에 광섬유 내부의 복굴절에 의한 영향이 상쇄된다. Bob의 간섭계를 떠날 때, 즉 PBS를 지날 때 광 펄스가 수평 편광, 수직 편광 순으로 출력되었다면, Alice를 거쳐 PBS로 다시 돌아올 때는 반대로 수직 편광, 수평 편광 순으로 입사된다. 먼저 들어온 수직 편광의 펄스는 PBS에서 반사되므로 아까와 반대로 더 긴 경로를 지나가며 Bob의 위상변조기 PM_B에 의해 위상 변화를 겪고, 수평 편광 펄스는 PBS를 투과하여 짧은 경로를 지나게 되므로 광 커플러 C_1에 서로 동시에 입사하면서 간섭한다. 이중 마하젠더 간섭계를 이용한 위상코딩 실험과 달리, 간섭계 경로 차에 의한 두 펄스 사이에 의한 시간 지연이 Alice의 인코딩 후 동일한 간섭계로 되돌아오면서 자동적으로 상쇄되므로 전체 시스템이 간소해지는 효과가 있다. Alice, Bob이 인가해준 위상의 차이가 0 또는 2π이면 광자가 SPD1에서 검출되고(비트 0), π면 SPD2에서 검출된다(비트 1).

그 외의 위상차를 가질 때는 SPD1이나 SPD2에 각각 50%의 확률로 랜덤하게 검출된다. Alice와 Bob이 선택한 양자상태 준비/측정 기저가 같을 경우 위상차가 0, π, 2π 중 하나가 되어 비트를 확정할 수 있으므로 이러한 경우의 비트 정보만 남기고 나머지는 삭제함으로써 raw 키를 생성할 수 있다.

4. 양자키 기반 IPSec 장치

양자키 기반 IPSec 연동 시스템은 대칭키를 생성하는 QKD 장치, QKD 장치로부터 키를 수신하여 장치 간 IP에 대한 단대단 보안 통신을 수행하는 Q-IPSec 장치 및 두 장치 간 키를 수신하여 관리하고 전달하는 역할을 수행하는 키 운용 장치(key management system, KMS)로 구성된다. 이 시스템의 목표는 QKD에서 생성한 키를 IPSec 네트워크 장치와 전송장치 등에 제공하여 안전한 연구망 서비스를 제공하는 것이다. 본 연구에서 제안하는 QKD 장치 및 Q-IPSec 연동 운영 장치의 목표 시스템 구성도는 다음(그림 3)과 같다.



(그림 3) KREONET에 적용하기 위한 양자키 기반 IPSec 장치 시스템 구성도

QKD 장치에서 생성한 키 정보는 KMS로 전달되고, KMS는 수신한 키 정보를 저장하며, 키 스트림으로부터 Q-IPSec 장치에 전달하기 위한 세션 키를 생성한다. Q-IPSec 장치로부터 세션 키에 대한 요청이 들어오면 KMS는 생성된 세션 키를 Q-IPSec 장치에 전달한다. 여기서 별도의 채널을 KMS 사이에 추가하여 양단에 교환되는 키 정보를 주고받음으로써 각 Q-IPSec 장치에 동일한 키를 전송할 수 있도록 하였다.

Q-IPSec 장치는 IP 계층 데이터 패킷의 보안을 유지하기 위한 VPN 장치로서, IKE에 의한 인증 및 키 교환을 수행한다. 키 교환 과정에서 장치 상호 간에 사용할 세션 키가 생성되는데, 세션 키는 세션이 생

성될 때마다 IKE 과정에 의해 생성되고, 서로 다른 서비스에 대해 각기 다른 키가 생성된다. IKE에 의해 서비스를 수행하는 Q-IPSec 양단 장치간의 키가 생성되면, 입력되는 데이터에 암호화 과정을 수행하며, 암호화된 데이터는 상대 장치에 의해 복호화되어 응용 시스템에 전달된다.

4.1 양자키 연동 장치 상위 블록 구성도

연동 장치는 (그림 4)와 같이 광학소자 제어부, 전처리부, 후처리부, 키 분배부, 키 교환부, 프레임 분석부, 암복호화부 및 암호통신부로 구성되어 있다. 이들 중 광학소자 제어, 전처리 및 후처리는 QKD 장치에서, 키 교환 및 프레임분석, 암복호화 및 암호화 통신은 Q-IPSec 장치에서 수행한다.

Q-IPSec 장치는 암복호를 수행하는 장치 간 동일한 구조와 형상을 가지나, QKD 장치는 QKD-Bob과 QKD-Alice로 구분되고 서로 다른 기능 구조를 가진다.

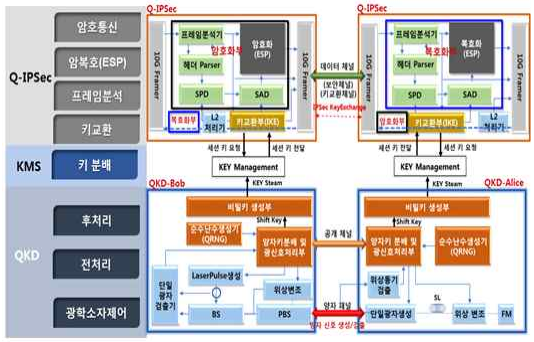
장치를 운영하기 위해서는 양자 채널, 공개 채널, 데이터 채널 이렇게 총 3개의 채널이 필요하다. 첫 번째로 양자 채널은 QKD에서 양자상태를 생성하고 검출하기 위한 물리적인 채널이다. 두 번째로 공개 채널은 QKD에서 키 시프팅 과정을 수행하기 위한 고전 통신 채널이다. 마지막으로 데이터 채널은 Q-IPSec 장치 간에 VPN 터널을 형성하여 암호화된 데이터를 송수신하기 위한 채널로서 IKE를 사용하는 키 교환 채널로도 사용된다.

QKD를 위한 광학소자 제어부는 QKD-Bob과 QKD-Alice의 LD, PM, IM, SPAD 등으로 구성되는 광학소자를 제어하기 위한 블록으로, 각 광학소자마다 제어를 위한 별도의 회로를 구성하며, 온도 제어와 광 펄스 생성, 위상 제어 등의 기능을 수행한다.

전처리부는 FPGA와 난수발생기(quantum random number generator, QRNG)로 구성되며, 난수 발생기에서 생성된 난수를 사용하여 signal과 decoy 펄스 및 각 광학소자를 제어하기 위한 디지털 신호를 생성한다. 생성된 디지털 신호는 Alice와 Bob 사이에 상호 동기화되어 동작한다. Bob에서는 LD를 제어하기 위한 주기적 디지털 신호를 생성하고 Alice로부터 수신된 광자를 검출하여 FPGA에 기록하고 키 생성부로 전달하는 기능을 한다. Alice의 FPGA는 PM과 IM을 제어하기 위한 디지털 신호 생성과 PD가 수신한 동기화 펄스를 검출하여 Bob과의 신호동기화를 수행한다. 후처리부에서는 광학소자 제어부와 전처리부로부터 생성된 raw-key에 후처리를 하여 비밀 키를 생성하고 키 분배부로 전달하는 역할을 한다. 키 분배부에서는 Q-IPSec 장치로부터 키 전달 요청이 들어왔을 때 일정 블록 크기(Q-IPSec에서 요청한 키 블록 크기)에 해당하는 비트 수만큼 전달해 준다.

Q-IPSec은 양자키를 사용하여 세션 단위로 데이터를 암, 복호화하여 전달하는 블록이며, 키 교환부, 프레임 분석부, 암복호부, 통신부로 구분된다. 키 교환부는 IKE를 수행하는 주체로서, 생성된 키 정보를 SPD와 SAD 데이터베이스에 저장하며, 내장된 MPSoC의 제어 명령에 따라 SPD, SAD 정보를 저장하거나 삭제한다.

프레임 분석부는 입력되는 Layer2 Ethernet 프레임으로부터 최대 5-tuple 정보를 추출하며, SPD 데이터베이스에 저장된 정보와 비교한다. SPD 데이터베이스는 저장된 정보와 수신된 플로우를 비교하고 SAD 데이터베이스를 참조하여 암복호 블록에 필요한 정보를 추출 후 데이터를 암복호 블록으로 전달한다. 암복호 블록은 SAD 데이터베이스로부터 전달받은 데이터를 참조하여 암복호 기능을 수행하는데, 암복호화된 데이터가 프레임 형태로 변환된 후 암호통신이 이루어진다.

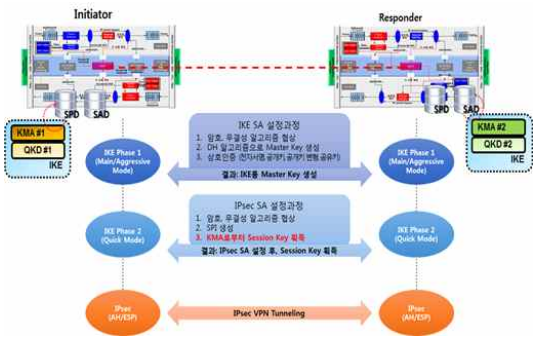


(그림 4) QKD + IPSec 연동 시스템의 구성 요소

4.2 양자키 연동 장치의 키 교환 구조

Q-IPSec의 키 교환 구조는 (그림 5)와 같은데, 앞서 3장에서 설명한 일반적인 IPSec과 IKE의 세션 키를 생성하는 방식에서 차이가 있다. IKE 1단계가 완료되면 IPSec 프로토콜 사용 및 암호화 방식에 대한 협상이 이루어지고 세션 키 생성 및 교환 과정에서 QKD에서 생성한 비밀키를 세션키로 사용한다. 생성된 키는 키 관리 에이전트에서 보관, 전달, 폐기 등의 과정을 거친다. Q-IPSec 키 교환을 위해서는 키에 대한 요청 및 키 전달 과정이 바뀌어야 하므로 관련된 IKE 알고리즘에 대한 수정 및 변경이 필요하다.

기존 IPSec의 경우 IKEv2 초기 교환 후 SW 기반 키를 사용하여 CHILD SA 정보를 교환하고 이후 생성된 SA를 이용하여 SAD를 생하고 데이터를 암복호화하여 송수신한다. Q-IPSec의 경우 IKEv2로 초기 교환 수행 후 SW 기반 키 대신 양자키를 사용하여 CHILD SA를 생성 및 교환한다.

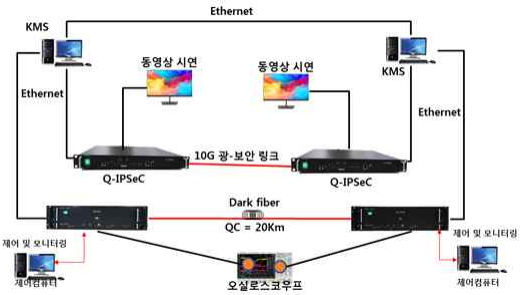


(그림 5) Q-IPSec 키 교환 절차

4.3 장치 연동 및 시험

QKD와 Q-IPSec 장치 연동 시험을 위해 (그림 6)과 같이 연동망 시스템을 구성하였다. 전체 시스템은 QKD 장치, Q-IPSec 장치, KMS, QKD 장치 제어를 위한 컴퓨터, QKD 내부 신호 모니터링을 위한 오실로스코프로 구성된다.

QKD 장치 사이의 양자 채널은 20 km로 설정하였고, 여기서 생성된 키는 QKD 장치 내부의 KMA를 통하여 KMS로 전달된다. Q-IPSec은 KMS로부터 키를 전달받아 IKE를 수행한다. 여기서 암호화 과정을 모니터링하기 위해 별도의 모니터링 PC를 사용하였다. 연동망 구성을 통해 QKD 장치에서 생성된 키 스트림이 KMS로 전달되고, Q-IPSeC의 키 교환을 통해 동영상 스트림이 암호화된 상태로 전달됨을 확인하였다. 20 km 양자 채널에서의 최종 키 생성률은 1kbps 이상으로 확인되었다.



(그림 6) 연동망 시스템 구조

5. 결 론

본 연구에서는 plug & play 방식의 불연속변수 QKD 장치와 IPSec 연동 장치를 개발하였다. QKD 장치 사이 전송거리를 20 km로 설정하여 시험을 진행한 결과 키 생성률이 1kbps 이상임을 확인하였다. Q-IPSec 장치는 QKD 장치에서 생성한 키를 KMS를 통해 수신하여 IKE의 세션 키로 활용함으로써 IP 데이터에 대한 보안을 수행한다. 최종적으로 연동 환경 구성 및 시험을 통해 QKD 장치에서 생성된 비밀키가 Q-IPSec 장치로 분배되고, 정상적인 암호화 통신이 수행됨을 확인하였다. 추후 QKD 시스템의 광손실 및 duty cycle 최소화를 통해 키 발생률을 높이면 KREONET에 안정적으로 적용할 수 있을 정도로 전송거리를 확정할 수 있을 것이라 기대한다.

참고문헌

[1] Charles H. Bennett, Gilles Brassard, Theoretical Computer Science, Vol. 560, Part 1 (2014).

[2] Bennett, C. H. and G. Brassard, Sigact News 20(4), 78 (1989).

[3] Müller, A., J. Bréguet, and N. Gisin, Europhys.

Lett. 23, 383 (1993).
[4] Bréguet, J., A. Müller, and N. Gisin, J. Mod. Opt. 41, 2405 (1994).
[5] C. H. Bennett, Phys. Rev. Lett. 68, 3121 (1992).
[6] Townsend, P., J.G. Rarity, and P. R. Tapster, Electron. Lett. 29, 634 (1993).
[7] Townsend, P., J.G. Rarity, and P. R. Tapster, Electron. Lett. 29, 1291 (1993).
[8] Townsend, P., Electron. Lett. 30, 809 (1994).
[9] Hughes, R., G. G. Luther, G. L. Morgan, and C. Simmons, Lecture Notes in Computer Science 1109,329 (1996).
[10] Dušek, M., O. Haderka, M. Hendrych, and M. Myˇska, Phys. Rev. A 60, 149 (1999).
[11] Kimura, T., Y. Nambu, T. Hatanaka, A. Tomita, H. Kosaka, and K. Nakamura, Jpn. J. Appl. Phys. 43, L1217 (2004).
[12] Gobby, C., Z.L. Yuan, and A. J. Shields, Appl. Phys. Lett. 84, 3762 (2004).
[13] Yuan, Z.L. and A. J. Shields, Opt. Exp. 13, 660 (2005).
[14] Müller, A., T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, Applied Physics Letters 70, no. 7 (1997).
[15] Zbinden, H., J.-D. Gautier, N. Gisin, B. Huttner, A. Muller, and W. Tittel, Electron. Lett. 33, 586 (1997).
[16] Ribordy, G., J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, J. Mod. Opt. 47, 517 (2000).
[17] Bethune, D., and W. Risk, IEEE J. Quantum Electron. 36, 340 (2000).
[18] Nielsen, P. M., C. Schori, J.L. Sørensen, L. Salvail, I. Damgård, and E. Polzik, J. Mod. Opt. 48, 1921 (2001).
[19] Bourennane, M., F. Gibson, A. Karlsson, A. Hening, P. Jonsson, T. Tsegaye, D. Ljunggren, and E. Sundberg, Opt. Express 4, 383 (1999).
[20] Stucki, D., N. Gisin, O. Guinnard, G. Ribordy and H. Zbinden, New J. Phys. 4, 41 (2002).
[21] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol," IETF RFC 2401 (1998).
[22] Ahmed Farouk, O. Tarawneh, Mohamed Elhoseny, J. Batle, Mosayeb Naseri, Aboul Ella Hassanien, and M. Abedl-Aty, "IPsec Multicast Architecture Based on Quantum Key Distribution, Quantum Secret Sharing and Measurement." In Quantum Computing : An Environment for Intelligent Large Scale Real Application, Springer International Publishing (2018).
[23] D. Harkins and D. Carrel, "The Internet Key Exchange," IETF RFC 2409 (1998).
[24] Marksteiner, Stefan & Maurhart, Oliver, A Protocol for Synchronizing Quantum-Derived Keys in IPsec and its Implementation. 10.13140/RG.2.1.4756. 4001 (2015).
[25] W.-Y. Hwang, Phys. Rev. Lett. 91, 057901 (2003).
[26] Zhao, Y., B. Qi, X. Ma, H.-K. Lo, L. Qian, Phys. Rev. Lett. 96, 070502 (2006).

[저자소개]

이 은 주 (Eunjoo Lee)
2010년 2월 한양대학교 물리학과 학사
2018년 2월 한국과학기술원 물리학과 박사
2018 ~ 2020 한국표준과학연구원 박사후연구원
2020~ 현재 한국과학기술정보연구원 박사후연구원
email : saranha@kisti.re.kr

손 일 권 (IlKwon Sohn)
2018년 고려대학교 공과대학 전기전자전파공학부 박사
2019년 한국과학기술정보연구원 박사후연구원
2019년 ~ 현재 한국과학기술정보연구원 선임연구원
email : d2estiny@kisti.re.kr

심 규 석 (Kyu-Seok Shim)
2014년 2월 고려대학교 컴퓨터정보학과 학사
2016년 8월 고려대학교 컴퓨터정보학과 석사
2020년 2월 고려대학교 컴퓨터정보학과 박사
2020~ 현재 한국과학기술정보연구원 박사후연구원
email : kusuk007@kisti.re.kr

이 원 혁 (Wonhyuk Lee)
2003년 성균관대학교 공과대학 컴퓨터공학과 석사
2010년 성균관대학교 공과대학 전자전기컴퓨터공학과 박사
2003년 ~ 현재 한국과학기술정보연구원 선임연구원
email :livezone@kisti.re.kr