편집위원 : 임용재 (한국방송통신전파진흥원)

물리계층의 신개념 보안통신기술, 양자암호통신

한상욱, 박병권, 김용수, 문성욱
한국과학기술연구원

요 약

본고에서는 차세대 보안통신기술인 양자암호통신에 대해 기술한다. 양자암호통신은 양자키분배와 암호통신으로 이루어지는데 양자키분배란 양자역학적 원리에 의해 비밀키를 송/수신자가 절대 안전하게 나누어 갖는 방법을 일컫는다. 나누어진 비밀키를 이용하여 현대암호 기법을 이용한 암호통신을 수행하면 도청으로부터 절대 안전한 보안통신 구현이 완성된다. 해외에서는 양자암호통신의 가능성과 중요성을 인식하고 집중적인 투자를 통해 연구개발을 진행하고 있으나 아직까지 국내에서는 체계적인 연구개발 활동이 미약한 상황이다. KIST는 2013년 25km 떨어진 송/수신자가 비밀키를 나누어가질 수 있는 BB84 양자키분배 프로토콜 기반 시스템 하드웨어를 구현하여 해외 학회에 전시 및 시연 했다. 추후 현대암호와의 융합연구 병행 기술개발을 추진한다면 조기에 양자암호통신 실용화가 가능할 것이라 기대된다. 절대 안전한 차세대 보안통신의 실현은 직접적으로는 국가적인 보안통신망의 확보를 가능하게 하고 간접적으로는 미래 초연결사회에서 활발한 지식 정보 교류를 가능하게 하여 새로운 사회 · 문화적 변화를 이끌어 내는 기반 기술이 될 것으로 기대한다.

Ⅰ. 서 론

안전한 정보교류를 위한 암호통신의 중요성은 동서고금을 막론하고 여러 가지 사례들을 통해 드러난다. 2차대전 연합국 승리에 결정적인 역할을 한 독일군 암호장비 애니그마 암호문 해독은 국가 안보와 직결되는 전쟁상황에서 암호통신의 중요성을 단명하게 보여 준다. 전 CIA 직원 스노든의 폭로에 의해 밝혀진 미국의 전방위적인 도청 사례들은 전문가뿐만 아니라 일반인들에게도 보안통신의 중요성을 각인시켜 주었다. 비단 국가적인 기밀정보의 보호뿐 아니라 개인 정보 보호의 중요성도 나날이 증가하고 있다. ICT 기술 발달에 따른 기존의 금융, 전자상거래 서비스의 활성화는 안전한 암호통신기술의 확보가 전제되어야 한다. 또한 향후 U-health와 같은 새로운 산업의 창출을 위해서도 안전한 통신체계의 확보가 선결조건이 된다. 최근 한국 정부의 핵심 정책인 창조경제란 "IT를 중심으로 산업과 산업, 산업과 문화를 융합해 지금껏 없던 새로운 산업을 일으키고 새로운 직업을 만들어 내는 게 창조경제의 실현"으로 정의되는데 이종 산업간의 융합을 위해 고급지식정보의 안전하고 빠른 교류가 필수임을 생각해 보면 국가 인프라로써의 국내 암호통신기술 개발의 중요성과 시급성을 확인할 수 있다.

현재 전세계적으로 차세대 보안통신기술로 양자암호통신을 활발히 연구 · 검증하고 있다. 본고에서는 먼저 양자암호통신이란 무엇이고 국내외 연구동향은 어떻게 되는지 살펴보도록 하겠다. 그리고 어떻게 안전성을 보장할 수 있는지 프로토콜 및 시스템에 대해 자세히 기술한 후 향후 응용방안에 대해 전망해 본다.

Ⅱ. 양자암호통신

양자암호통신은 멀리 떨어져 있는 두 사람이 통신상에서 암호 비밀키를 안전하게 나누어 갖고 이를 이용해 암호 통신을 수행하는 것이다. 양자암호통신은 〈그림 1〉과 같이 크게 두 부분으로 구성되는데 양자의 특성을 이용하여 비밀키를 송/수신자

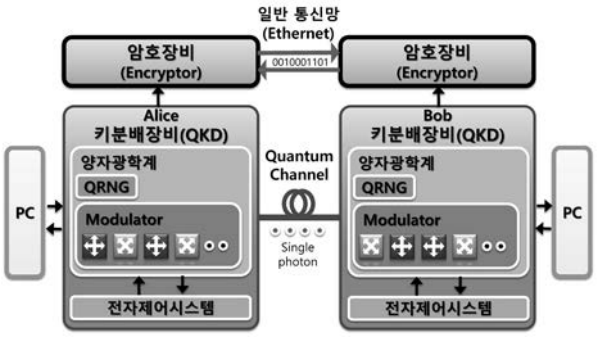


그림 1. 양자암호통신의 구성

그림 2. 양자의 특성

가 안전하게 나누어 갖는 양자키분배 (QKD, Quantum Key Distribution)와 나누어진 비밀키를 이용하여 암호통신을 하기 위한 데이터 암호화/복호화를 수행하는 암호장비로 구성된다. 흔히 양자암호라 하면 양자키분배만을 지칭하기도 한다.

양자암호통신의 안전성을 이해하기 위해서는 양자(量子, Quantum)의 고유한 특성을 알아야 한다. 양자는 에너지의 최소단위로서 〈그림 2〉와 같은 특성을 갖는 입자들을 일컫는다. 양자중첩이란 여러 상태가 확률적으로 하나의 양자에 동시에 존재하고 측정하기 전까지 정확한 양자상태를 알 수 없다는 특성이다. 양자얽힘은 둘 이상의 양자가 가지는 비고전적 상관관계로 두 양자가 서로 멀리 떨어져 있어도 존재하는 특성이다. 불확정성은 서로 다른 물리량이 동시에 정확하게 측정이 불가능한 특성이다. 여러 상태를 동시에 갖고 있고 이를 동시에 정확하게 측정할 수 없기 때문에 양자는 복제 불가능하다[1]. 복제 불가능성에 기반하여 양자암호는 비밀키 분배의 안전성을 보장받는다. 양자의 종류에는 광자, 전자, 이온, 원자 등 여러 가지가 있지만 양자암호통신에서는 빛의 최소단위인 광자를 이용한다. 자세한 동작 설명을 통한 안전성 보장 원리는 다음 단원에서 기술한다.

서두에 밝혔듯이 현재 전세계적으로 양자암호에 대한 활발한

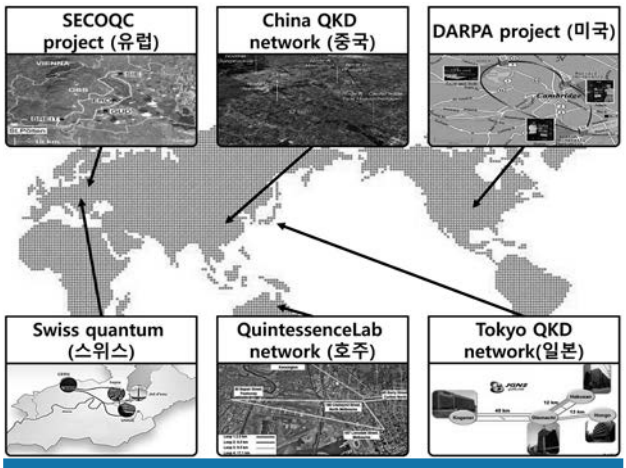


그림 3. QKD 상용화 테스트베드

표 1. 해외의 양자암호기술동향

구분	주요 정책 동향
유럽	• Qurope(Quantum Europe) 프로그램을 통해 유럽 양자정보통신 연구개발 로드맵을 제시하고 일관된 연구 수행 • EU는 미래기술(FET, Future Emerging Technologies) 사업에 Quantum Simulation을 선정, 525억 투자 • 영국은 2013년 Autumn Statement를 통해 양자기술 산업화에 2015년부터 5년간 4,800억 투자 발표
미국	• 2008년 국가양자정보과학비전(A Federal Vision for Quantum Information Science) 발표 후 NSF, IARPA, DARPA 등을 통해 年1조 투자
러시아	• 2010년 Russian Quantum Center를 설립하고 양자광학, 양자재료, 양자정보처리, 양자기술 등에 집중 투자
캐나다	• 캘거리大, 워터루大, 토론토大 등에 양자정보통신학과를 설치, 미래 ICT 선도를 위한 인재 집중 양성 • 워터루大 Quantum-Nano Center를 설립, 年500억 투자
중국	• 中과학기술부(MOST)는 2012년부터 5년간 양자기술, 나노기술 등에 2,900억 투자
일본	• FIRST 프로그램을 통해 양자정보처리(Quantum Information Processing)에 4년간 430억원 지원 • Riken, CREST 등을 통해 양자정보통신에 年 220억원 지원 • NICT는 2040년까지 기밀성이 보장된 사회를 위한 양자 로드맵에 따른 기술 개발을 진행 중
싱가포르	• 싱가포르국립대학을 통해 양자기술에 年1,300억 투자

연구 활동이 이루어지고 있다. 해외 기술 선진국에서는 80년대부터 본격적인 연구가 시작되어 90년대 연구용 시제품이 개발되었고 2000년대 이후부터는 〈그림 3〉과 같이 테스트베드를 구축하여 실환경 성능 검증을 하고 이를 통한 상용화 단계에 도달했다. 특히 표1에 보여지는 양자정보통신 (양자암호통신, 양자컴퓨터, 양자소자 등을 포함) 기술정책을 통해 국가전략기술로서 양자 기술을 집중육성하고 이를 활용한 선진 양자암호통신 기술 확보에 주력하고 있다.

이에 반해 국내 양자정보통신 기술은 90년대부터 2000년대 중반까지 학계를 중심으로 양자기술 원천연구가 이루어졌고 2010년까지 출연(연) 중심의 양자암호통신 기초연구가 진행되었다. 2011년 SKT Quantum Lab.의 설립과 2012년 출연(연) 최초의 양자기술 전문 연구센터인 KIST 나노양자정보연구센터의 개소 및 퀀텀포럼 창립 등 연구 여건이 개선되고는 있으나

그림 4. KIST 양자키분배 시스템

아직까지는 선진국과의 기술격차를 좁히지 못하고 있다. 〈그림 4〉와 같이 2013년 KIST가 세계 양자암호 학회인 Qcrypt에서 순수 국내 기술로 개발한 양자키분배 시스템을 전시 및 발표하는 성과를 내었고 정부에서도 양자 기술의 체계적인 발전을 위한 중장기 전략을 기획하는 등 양자정보통신 분야 기술 선진국으로 도약하기 위한 기반이 다져지고 있다.

Ⅲ. 양자키분배

양자암호통신을 이용한 안전한 보안통신의 핵심 기술은 비밀키를 실시간으로 통신상에서 안전하게 분배하는 기술이다. 비밀키를 양자의 특성을 이용하여 안전하게 분배하는 것을 양자키분배라 하는데 크게 프로토콜 부분과 시스템 하드웨어 부분으로 구분할 수 있다. 먼저 양자키분배 프로토콜에 대해 기술한다.

양자키분배 프로토콜은 1984년 BB84 프로토콜이 처음 제안된 이후로 다양한 프로토콜이 제안되어 왔다[2]. 〈그림 5〉에 나타난 것처럼 다차원 기저 기반 고효율 프로토콜과 시스템 양자해킹 대응 프로토콜이 제시되었다.[3]–[9] 그러나 아직까지도 BB84 프로토콜은 안전성 면과 구현가능성 면에서 가장 강력한 프로토콜로 대부분의 실제 시스템에 채용되고 있다. BB84 프로토콜 설명을 통해 양자키분배 시스템이 왜 도청으로부터 절대 안전한지에 대해 설명하도록 한다.

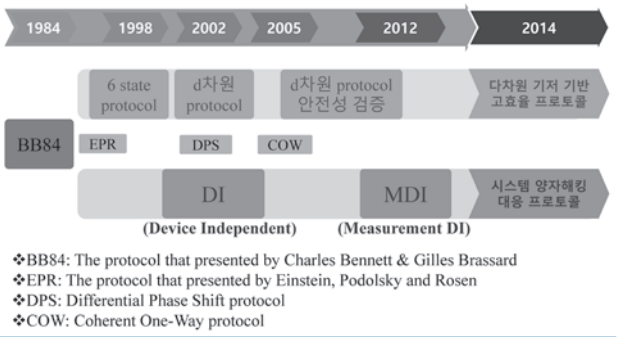


그림 5. 고효율 프로토콜의 발전 방향

양자의 한 종류인 단일광자를 이용하여 양자키분배를 구현하고 단일광자의 편광을 비밀키 전송을 위한 변조 수단으로 사용한다고 할 때 〈그림 6 (a)〉와 같이 송신자 Alice는 랜덤한 편광을 가진 단일광자를 수신자 Bob에게 전송한다. Alice와 Bob은 수직 · 수평기저에서 편광 0°, 90° 를 각각 Bit 0과 1로 약속하고, 대각기저에서는 편광 45°, 135° 를 각각 Bit 0과 1로 약속했다고 가정한다. Bob은 (b)와 같이 도달한 모든 단일광자에 대해 편광 기저를 랜덤하게 선택하여 측정을 수행한다. 이때 단일광자의 편광과 편광 기저가 일치하는 경우, 100%의 확률로 편광상태를 정확하게 측정하게 된다. 만약 단일광자의 편광과 편광 기저가 다른 경우, 50%의 확률로 측정오류가 발생하게 된다. 이후 Alice와 Bob은 〈그림 6 (c)〉와 같이 각자의 기저정보를 기존 통신망을 이용하여 공유한다. 최종적으로 〈그림 6 (d)〉와 같이 Alice와 Bob의 편광 기저가 같은 경우에 측정된 결과만 비밀키 생성에 이용하는 것으로 프로토콜을 완성한다.

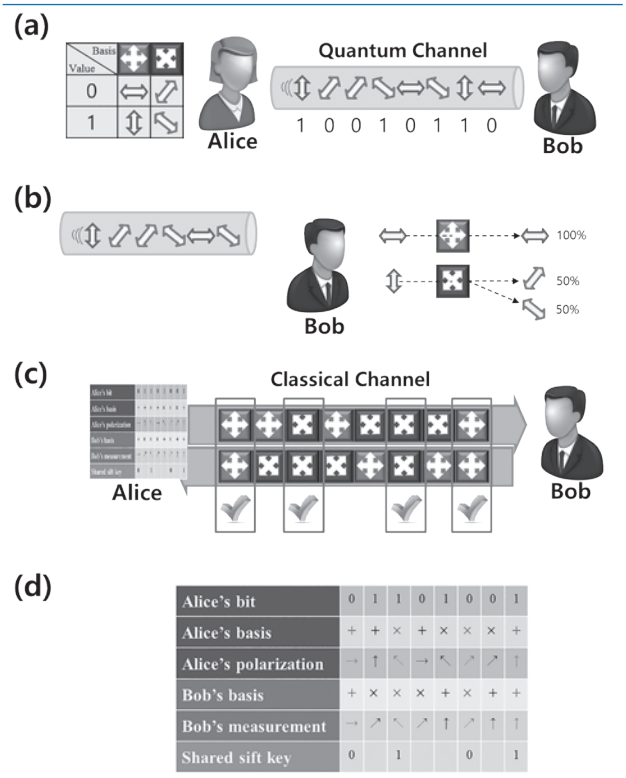
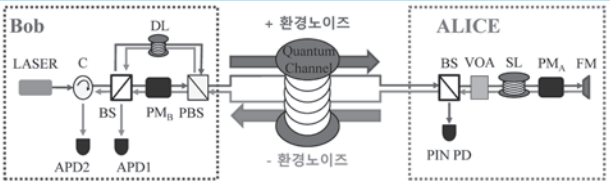


그림 6. BB84 프로토콜

만약 중간에 도청자 (Eve)가 있었다면 Eve는 본인의 존재를 Alice와 Bob이 눈치 챌 수 없도록 한 상태에서 비밀키 정보를 도청해야 한다. 기존 광 데이터 통신에서는 하나의 Bit 정보를 보낼 때 수백만개 이상(1mW, 1GHz기준)의 광자를 사용하여 보내므로 그 중 일부만 Wire tapping을 통해 빼냄으로써 손쉽게 도청을 할 수 있다. 그러나 양자키분배에서는 하나의 정보를 하나의 광자에 실어 보내기 때문에 일부만 발췌한다는 것이 원천적으로 불가능하다. 또한 중간에 광자를 가로챈 후 정보를 획득한 다음 같은 정보를 Bob에게 보내는 방법을 생각할 수도 있지만 이 경우 양자의 복제불가능성 원리에 의해 똑 같은 정보를 광자에 실어 보내는 것이 불가능하다. 잘못 복제된 임의의 광자를 Eve가 Bob에게 보낸다면 Alice와 Bob 사이에 최종적으로 생성된 키 에러율이 비정상적으로 커지게 되어 도청자의 유무를 Alice와 Bob이 쉽게 알아차릴 수 있다.

이러한 프로토콜을 실제로 양자키분배 시스템 하드웨어로 구현하는 방법은 여러 가지가 있다. 대표적으로 One way 방식



C: optical circulator, BS : beamsplitter, DL: delay line, SL : storage line,
PM : phase modulator, PBS : polarizing beamsplitter,
PIN PD : multi photon detector, VOA : variable optical attenuator,
APD1 and APD2 : single photon detectors, FM : Faraday mirror,

그림 7. Plug and play QKD system

과 Plug and Play라고 불려지는 Two way 방식이 있다.[10] [11] One way 방식은 고속 동작의 장점이 있지만 환경변화에 따른 시스템 동작의 안정성 측면에서 단점을 갖는다. 이에 반해 Plug and play 방식은 〈그림 7〉에서와 같이 먼저 수신부(Bob)에서 생성한 빛 신호가 송신부(Alice)에 도착하고 송신부에서는 비밀키 정보를 변조한 후 이를 단일광자 수준으로 빛 세기를 약화시켜 다시 수신부로 재전송한다. 이 과정에서 빛 신호는 환경 노이즈의 영향을 반대로 두 번 받기 때문에 자동 노이즈 보상이 이루어지게 된다. 따라서 비밀키 분배 속도에서는 단점이 있을지라도 시스템의 안정적인 동작에는 매우 유리한 방법이다.

QKD 시스템은 양자 광원과 간섭계, 변조기(PM) 그리고 검출기(APD)로 구성되는 양자광학 부분과 전자제어부로 이루어진다. 전자제어부는 크게 양자광학 부품들을 구동하기 위한 구

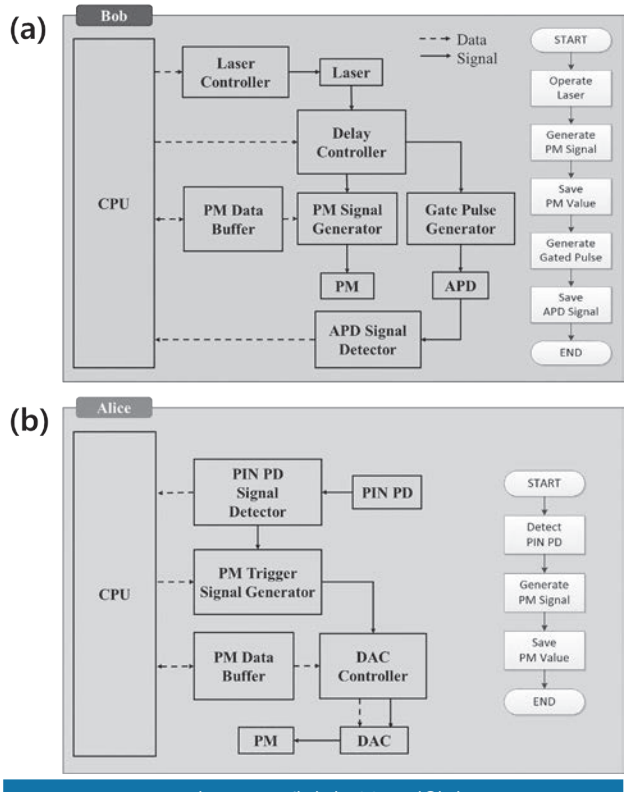


그림 8. QKD 제어회로부 동작원리

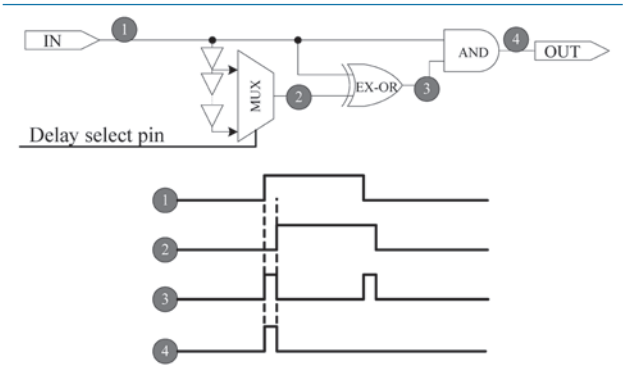


그림 9. 검출기 구동신호 생성

동회로부, 검출기에서 광신호에 따라 발생한 전기 신호를 처리하는 신호처리부, 외부 시스템과의 연결을 위한 인터페이스 그리고 전체 시스템을 제어하는 제어회로부로 나누어진다. 〈그림 4〉에 나타낸 KIST QKD 시스템은 환경변화에 강인한 Plug and play 방식으로 구현되었으며 위상 변조 기법을 이용하였다 [12]. 또한 시스템 성능에 가능 큰 영향을 미치는 단일광자검출기를 독자적으로 개발하여 안정적인 시스템 동작을 완성하였다 [13]. 〈그림 8〉은 Bob 과 Alice 각각의 제어회로부 구성과 동작 순서도를 나타낸다. 제어회로부는 FPGA내의 CPU와 각각의 Function block들을 구현하여 완성하였다. Bob의 CPU는 핵심 부품들인 Laser와 검출기, 그리고 변조기의 동작 시간을 직접 제어 하고 각각의 Function block들이 외부 드라이버 회로들이 순서에 맞게 구동 신호를 내보낼 수 있도록 제어한다. Alice의 CPU는 PIN PD의 출력신호에 동기를 맞춰 내부 변조기를 제어함으로써 Alice와 Bob 사이의 동기를 맞춰준다.

이러한 제어회로부는 매우 정밀한 시간 제어가 필수이다. 왜냐하면 QKD 시스템에서 가장 중요한 부품 중 하나인 단일광자검출기는 암전류 노이즈를 최소화 하기 위해 동작 시간을 수nsec 단위로 최소화 시켜 가져가야 하기 때문이다.[14]–

표 2. KIST 양자키분배 시스템 성능

시스템	시스템 크기	45 x 45 x 20 cm^3
	Quantum channel 길이	25 km
	Storage line 길이	15 km
송신부	Laser frequency	2 MHz
	Laser pulse width	3 ns
	Pulse Train frequency	2kHz
	Pulse in Pulse Train	140
수신부	Quantum efficiency	14 %
	Dark Count Probability	5 x 10–5
제어부	FPGA Clock frequency	800 MHz
성능	Key rate	1.5 kbps (Sifted Key)
	QBER	3% 이하

[18] KIST QKD 시스템에서는 수 nsec의 검출기 구동 신호를 0.6nsec의 resolution으로 제어하기 위해 〈그림 9〉와 같은 회로를 FPGA 내에서 구현하였다.

〈표 2〉는 KIST QKD시스템 성능을 나타낸다. 현대암호에서 비밀키 갱신 주기가 128bit/min인 것을 고려할 때 충분한 비밀키분배 속도를 가지고 있고 25km의 거리의 실제 광케이블을 이용하여 성능을 검증한 결과이다. 다음 단원에서는 실제로 양자키분배를 통해 안전하게 분배된 비밀키를 이용하여 양자암호통신을 수행할 때 필수적인 현대암호와의 융합에 대해 기술한다.

Ⅳ. 현대암호와의 융합을 통한 응용

양자암호통신을 완성하기 위해서는 〈그림 1〉에서 보이는 것처럼 안전하게 나누어진 비밀키를 암호장비와의 인터페이스를 통해 전달하고 암호장비에서 현대암호기법을 활용하여 암호화/복호화 작업을 수행해야 한다. 여러 암호 장비 중 현재 많이 보급되어 사용되고 있는 VPN (Virtual Private Network) 장비로의 응용이 가능하다.

VPN은 IPsec (Internet Protocol Security) 또는 SSL (Secure Sockets Layer)을 이용하여 구현한다. IPsec 기반 VPN의 경우 〈그림 10〉과 같이 ESP (Encapsulating Security Payload) packet을 만들기 위한 암호화 작업 시 양자키분배로 실시간 안전하게 분배된 비밀키를 사용한다면 보안성을 획기적으로 증대시킬 수 있다. SSL 기반의 VPN 장비에서는 〈그림 11〉에서처럼 Hand shake protocol을 사용한다고 할 때 암호화를 위한 Seed키를 공개키 대신 양자키로 대체한다면 한 단계 높은 보안성을 확보할 수 있을 것이라 기대된다.

새로운 양자키를 이용한 VPN과 같은 현대암호장비로의 응용을 위해서는 두 장비간 인터페이스 개발, 키관리 시스템 개발 등 새로운 기술 개발이 필요하다. 아울러 새로운 기술 개발이 유발할 수 있는 보안의 취약점을 선제적으로 대비할 수 있도록 연구개발이 이루어져야 할 필요도 있다.

현재까지는 양자키분배와 현대암호와의 융합을 위한 국내 연구개발 활동이 전무한 실정이다. 양자암호통신의 실적용을 위해서는 두 분야의 전문가 그룹의 협업 연구가 하루빨리 이루어

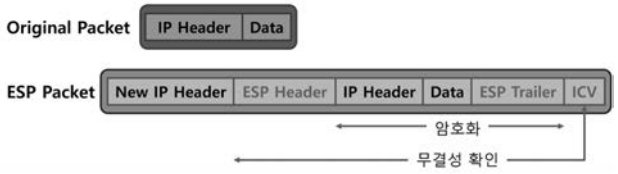


그림 10. IPsec 기반 ESP packet

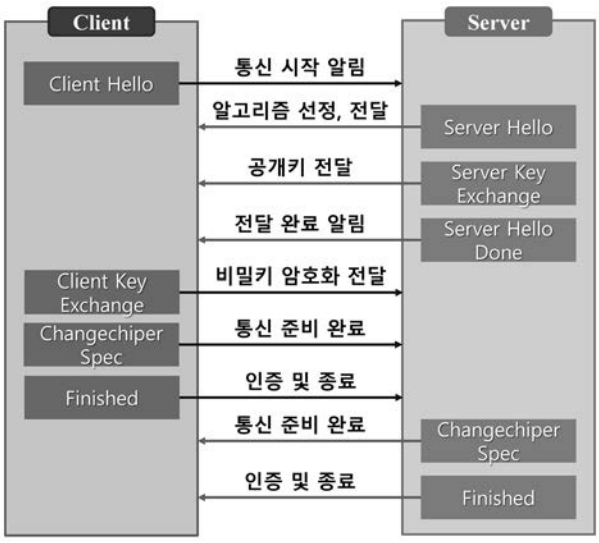


그림 11. Hand shake protocol

져야 할 것이다. 양자키분배 기술 자체의 고도화와 현대암호와의 융합을 위한 기술 개발이 동시에 이루어진다면 양자암호통신의 조기 상용화는 물론 선진국과의 기술격차 해소에 큰 밑거름이 될 것이다.

Ⅴ. 결 론

지금까지 차세대 보안통신 기술로 전세계적인 연구가 활발히 진행중인 양자암호통신이란 무엇인지 살펴보았다. 전통적인 IT 기술 선진국들은 물론 중국, 싱가포르, 캐나다, 호주 같은 국가들도 양자기술의 중요성을 인지하고 국가전략기술로 집중 육성하고 있다. 양자기술 중 상용화에 가장 근접한 기술인 양자암호통신은 비단 국가안보와 직결되는 기밀통신망의 보호뿐 아니라 미래 초연결사회에서 개인 사생활 보호를 통한 새로운 서비스 산업 창출의 기반이 된다는 점에서 집중적인 지원 속에 연구 · 개발이 진행되고 있다. 그동안 우리 나라는 정부의 산발적인 연구 지원과 연구 전략의 부재 때문에 선진국과의 기술 격차가 많이 벌어져 있는 상황이다. 체계적인 연구 추진을 위한 중장기 계획을 기반으로 학계, 출연(연), 산업계가 집중적인 연구 · 개발을 추진한다면 근시일 안에 가시적인 성과를 올릴 수 있다. 이는 최근 발표되는 수준 높은 양자 기술 관련 논문들과 양자암호 학회에서 전시된 시제품 등을 통해 그 가능성을 확인할 수 있다.

양자암호통신의 조기 상용화를 위해서는 양자기술 자체의 연구도 중요하지만 양자암호통신의 다른 한 축인 현대암호와의 융합연구도 동시에 추진되어야 한다. 이를 위해 양자암호 전문가 그룹과 현대암호 전문가 그룹이 협업할 수 있는 환경 조성이

필요한 시점이다.

차세대 보안통신인 양자암호통신의 조기 상용화는 과학기술뿐 아니라 사회적, 문화적인 새로운 변화를 이끌어낼 수 있는 기반이 되고 인터넷을 통한 안전한 정보의 교류는 금융, 전자상거래, U-health와 같은 서비스 산업의 발전을 가속화 시켜 양질의 경제 발전을 이끌어 낼 것이라 기대된다.

Acknowledgment

본 기고는 미래창조과학부 및 한국산업기술 평가관리원의 산업융합원천기술개발사업(정보통신)의 일환으로 수행하였음. [10044559, 양자암호통신 네트워크 구축을 위한 요소기술 개발]

참 고 문 헌

[1] W.K. Wooters and W.H. Zurek, "A Single Quantum Cannot be Cloned", Nature 299, 802, (1982).

[2] C.H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing", in Proc. of IEEE Int'l Conf. on Computers, Systems and Signal Proc., Bangalore, India, IEEE, New York, p.175, (1984).

[3] A. Ekert, Phys. Rev. Lett. 67, 661 (1991).

[4] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography", J. Cryptology 5, pp. 3-28 (1992).

[5] Inoue K, Walks E and Yamamoto Y, "Differential -phase-shift quantum key distribution", Phys. Rev. Lett. 89, 037902 (2002).

[6] A. Leverrier and P. Grangier, " continuous-variable quantum-key-distribution protocols with a nongaussian modulation", Phys. Rev. A 83, 042312 (2011).

[7] D. Mayers, A. Yao, Proc. of the 39th IEEE Conf. on Foundations of Computer Science, p. 503, (1998).

[8] H.-K. Lo et al. " Measurement-device-independent quantum key distribution", Phys. Rev. Lett. 108, 130503 (2012).

[9] H. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution", Phys. Rev. Lett. 94, 230504 (2005).

[10] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin,"Plug and Play systems for quantum cryptography", Appl. Phys. Lett. 70, pp. 793-795 (1997).

[11] D. Stucki, N. Gisin, O. Guinnared, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a plug & play system", New J. Phys. 4, 41.1-41.8 (2002).

[12] Min Ki Woo, Min Soo Lee, Byung Kwon Park, Osung Kwon, Yong-Su Kim, Il Young Kim, Sang-Wook Han, Sung Moon, "Development of Plug & Play Quantum Key Distribution System", Final Program of the Optical Society of Korea Summer Meeting, T3C-Ⅷ3 (2013).

[13] Min Soo Lee, Min Ki Woo, Byung Kwon Park, Osung Kwon, Yong-Su Kim, Il Young Kim, Sang-Wook Han, Sung Moon, "Development of Single Photon Detector for QKD System", Final Program of the Optical Society of Korea Summer Meeting, T3C-Ⅷ2 (2013).

[14] S.-B. Cho, and S.-K. Kang, "Weak avalanche discrimination for gated-mode single-photon avalanche photodiodes", Opt. Express 19, 18510-18515 (2011).

[15] Zhang, Jun, et al., "Practical fast gate rate InGaAs/InP single-photon avalanche photodiodes", App. Phys. Lett. 95, 1-3 (2009).

[16] S. Cova, M. Ghioni, A. Lotito, I. Rech, and F. Zappa, "Evolution and prospects for single-photon avalanche diodes and quenching circuits", J. Mod. Opt. 51, 1267-1288 (2004).

[17] A. Bouzid, J. B. Park, S. M. Kim, and S. moon, "Near Infrared Single photon Detector Using an InGaAs/InP Avalanche Photodiode Operated with a Bipolar Gating Signal", J. Jpn. Appl. Phys. 51, 034401 (2012).

[18] M. Ware, A. Migdall, J. C. Bienfang, and S. V. Polyakov, "Calibrating photon-counting detectors to high accuracy: background and deadtime issues", J. Mod. Opt. 54, 361-372 (2007).

약 력

한 상 욱

2006년 KAIST 전기및전자공학 박사
2006년~2009년 ㈜픽셀플러스 선임연구원
2009년~2012년 삼성종합기술원 전문연구원
2012년~현재 KIST 나노양자정보연구센터 선임연구원
관심분야: Quantum Optics/Information, APD

박 병 권

2012년 한국기술교육대학교 공학사
2013년~현재 KIST 나노양자정보연구센터 석박사 통합과정
관심분야: Quantum Optics/Information, FPGA, Coincidence counting

김 용 수

2012년 POSTECH 물리학 박사
2012년~2013년 NIST 박사후 연구원
2013년~현재 KIST 나노양자정보연구센터 선임연구원
관심분야: Quantum Optics/Information

문 성 욱

1986년 연세대학교 공학사
1988년 연세대학교 공학석사
1994년 연세대학교 공학박사
1989년~현재 KIST 나노양자정보연구센터 센터장
관심분야: Quantum Optics/Information, Nano system, MEMS