ETRI

2018
Electronics and
Telecommunications
Trends

무선 양자암호통신 시스템 및 부품 최신 기술 동향

Recent Technology Trends of Free-Space Quantum Key Distribution System and Components

윤천주 (C.J. Youn, cjyoun@etri.re.kr) 광통신부품연구그룹 책임연구원
고해신 (H. Ko, seagod.ko@etri.re.kr) 광통신부품연구그룹 연구원
김갑중 (K.-J. Kim, k.j.kim@etri.re.kr) 광통신부품연구그룹 선임연구원
최병석 (B.-S. Choi, chbs@etri.re.kr) 광통신부품연구그룹 책임연구원
최중선 (J.-S. Choe, jschoe@etri.re.kr) 광통신부품연구그룹 책임연구원

A quantum key distribution (QKD) provides in principle an unconditional secure communication unlike the standard public key cryptography depending on the computational complexity. In particular, free-space QKD can give a secure solution even without a fiber-based infrastructure. In this paper, we investigate an overview of recent research trends in the free-space QKD system, including satellite and handheld moving platforms. In addition, we show the key components for a free-space QKD system such as the integrated components, single photon detectors, and quantum random number generator. We discuss the technical challenges and progress toward a future free- space QKD system and components.

* DOI: 10.22648/ETRI.2018.J.330610

* 본고는 정부(과학기술정보통신부)의 재원으로 ETRI 출연금사업의 일환으로 수행된 연구임[17YB1110, 편광변조기반 무선양자통신 송수신부 핵심 부품 및 시스템 제어 선행 기술 개발].

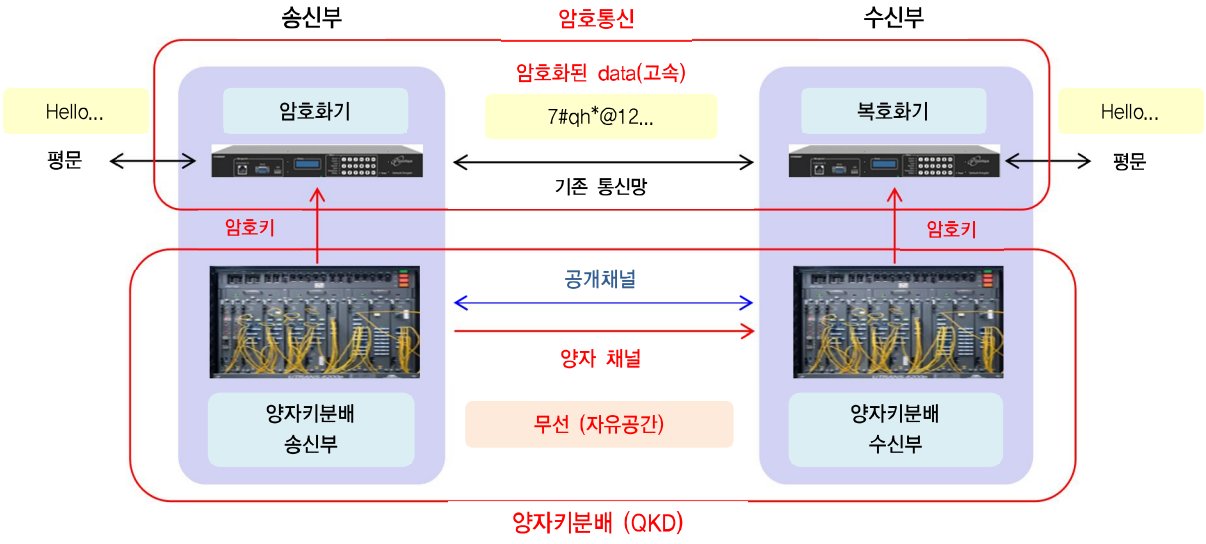
Ⅰ. 서론

인류는 문명의 발생 이래로 메시지의 내용이 원하지 않는 제 3자에게 누출되지 않도록 계속 노력해 왔으며 이를 위해 메시지를 암호화하여 수신자에게 전송함으로써 중간에 타인이 도청할 수 없도록 하고 있다. 최근에는 국가, 행정 및 군사 기밀, 금융기관 정보뿐만 아니라 사물 인터넷, 빅데이터, 개인의 민감한 금융 및 건강 정보 등과 같이 보안을 필요로 하는 정보가 더 많이 발생되고 있으며 인터넷과 통신 매체를 통하여 전송되고 있다. 따라서, 통신 보안은 중요성이 점점 더 증가하고 있으며 반드시 확보되어야 하는 기술이다.

현대 암호에서는 암호화키와 복호화키를 이용하여 데이터를 암호화 및 복호화를 하고 있으며 현재 사용하고 있는 RSA와 같은 공개키 암호 방식은 수학적인 계산 복잡성에 의존하고 있다. 즉 아주 큰 숫자를 소인수분해하는 문제는 현재의 기술로 계산 해독하는데 수 천년 이상 걸릴 수 있다는 사실에 근거를 두고 있다. 이것은 정보 이론적으로 안전하지 않으며 컴퓨팅 연산 능력 발전 및 새로운 알고리즘 개발로 해독될 개연성이 있다.

특히, 현재 전 세계에서 막대한 투자를 통하여 기술 개발 진행 중인 양자 컴퓨터가 개발되면 1994년 Bell Labs의 Peter Shor에 의해 제안된 양자컴퓨팅 알고리즘으로 현대 공개키 암호 방식은 더 이상 안전하지 않다는 것이 알려져 있다[1]. 그리고 데이터의 종류에 따라 짧은 시간 동안의 비밀 보장뿐만 아니라 수십년 이상 동안 비밀 유지를 필요로 하는 것이 있을 수 있으며 현재 보내는 데이터를 저장하여 미래의 개발될 기술로 해독될 가능성이 있으므로 미국 국가 안보국(US National Security Agency)은 양자컴퓨터의 위협을 심각하게 고려하여 최근 양자 시대에 동작할 수 있는 프로그램을 계획한다고 발표하였다[2]. 또한 현재의 정보 보안 인프라를 변환시키는 데에는 수년 이상의 시간이 소요될 수 있으므로 양자 시대에서도 안전한 통신 암호 기술이 빨리 적용될 필요가 있다.

이러한 양자 컴퓨터가 개발 되어서도 수학적인 계산 복잡성이 아닌 자연의 양자 물리학 법칙을 기반으로 하여 도청이 원천적으로 불가능한 무조건적인 안전성을 보장하는 기술이 양자키분배(QKD: Quantum Key Distribution) 기술이다. 양자키분배(QKD) 기술은 1984



(그림 1) 양자암호통신 시스템 구성도

년 IBM의 C. H. Bennett과 몬트리올 대학의 G. Brassard에 의해 처음 제안된 이래로 여러 양자암호프로토콜과 양자암호 프로토콜 안전성 증명에 대한 연구, 고속 및 장거리 양자키분배기술이 지속적으로 연구되고 있다[3]. 양자암호통신 시스템은 (그림 1)에서와 같이 현대 암호와 양자키분배 시스템의 융합이라고 할 수 있으며 양자키분배 송수신부로터 무조건적인 안전한 비밀키를 연속적으로 생성하여 암호화 및 복호화를 수행한다. 양자암호통신 기술은 양자 신호가 전송되는 양자 채널이 유선의 광섬유 기반인지와 자유 공간(대기)인지에 따라 유선 양자암호통신과 자유 공간 또는 무선 양자암호통신 기술로 구분할 수 있다.

본고에서는 무선 양자암호통신 시스템 국내외 기술동향과 무선 양자 암호 시스템을 구성하는 부품 기술 동향 및 전망에 대해 기술하고자 한다.

II. 무선 양자암호통신 시스템 기술 동향

1. 국외 기술 동향

이론적인 QKD 기술이 1984년에 제안 되었지만 처음 실험적으로 구현된 것은 실험실 내에서 32cm 자유 공간 양자 채널 링크를 통해 1989년에 이루어졌다[4]. 이후 90년대 후반부터 유선과 무선 양자암호통신이 실험적으로 구현되기 시작하여 각자 고속 장거리를 위한 기술이 연구되어 왔다.

무선 양자암호통신 기술은 2000년대 초반부터 몇몇 선진국을 중심으로 연구가 수행되어 왔다[〈표 1〉 참조]. 무선 양자암호통신 시스템은 대부분 1984년에 개발된 BB84 프로토콜을 기반으로 개발되고 있으며 수 백 미터 이내의 단거리에서 수 십 km 이상의 장거리와 위성을 이용한 천 km 이상의 초장거리 글로벌 양자암호통신 연구가 진행되고 있다. 2002년 미국 Los Alamos National Laboratory에서는 10km 가까운 거리에서 양자 신호를 송수신하는데 성공하였다. 이후 2007년에는

〈표 1〉 무선 양자암호통신 주요 국외 기술 개발 현황

년도	국가 (기관)	프로토콜	거리 (km)	키 생성률 (bps)	특이점
2002 [5]	미국	BB84	9.81	N/A	밤, 낮 신호 전송
2006 [6]	싱가포르	E91	1.5	630	얽힘 기반
2007 [7]	오스트리아, 독일 등	BB84 (decoy), E91	144	128 (decoy)	장거리
2009 [8]	스위스 등 (SECOQC)	BB84	0.08	17,400	실 환경 데모
2009 [9]	싱가포르	BBM92	0.35	385	낮 환경, 얽힘 기반
2013 [10]	중국	BB84 (decoy)	20, 40	268.9 159.4	이동체 – 기지국
2013 [11]	독일	BB84	20	7.9	비행기 – 기지국
2015 [12]	캐나다	BB84 (decoy)	0.65	40	자동차 – 기지국
2017 [13]	중국	BB84 (decoy)	1,200	1,100 (Sifted)	인공위성 기반
2018 [14]	중국, 오스트리아	BB84 (decoy)	7,600	3,000 (Sifted) at ~1,000km	인공위성, 대륙간

오스트리아와 독일을 포함한 연구진이 지상 두 기지국에서 최장거리인 144km 거리에서 128bps 수준의 키를 생성할 수 있는 무선 지상 양자 암호통신이 가능함을 보여주었다.

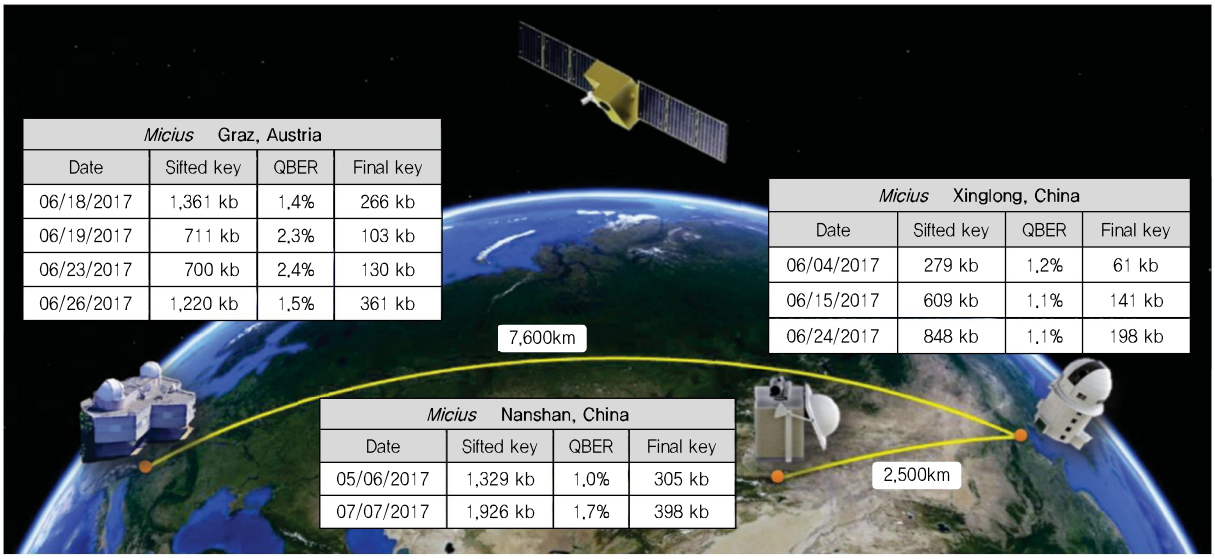
2010년대에는 움직이는 이동체와 고정 기지국간의 연구가 활발하게 수행되었는데, 독일과 중국, 캐나다 등에서 각각 비행기, 열기구, 자동차와 기지국 간의 양자암호통신 결과가 보고되었다. 이러한 이동체와 고정 기지국간의 연구는 지상 고정 기지국과 저궤도 위성간의 양자암호통신을 수행할 수 있는 기반 기술에 활용될 수 있다. 또한 실시간 빔 트래킹 기술을 활용하여 고속으로 움직이는 이동 플랫폼과 지상 기지국 간의 양자 신호를 추적하고 복원하는 기술이 요구된다. 빔 트래킹 기술은 양자 신호와 동일한 경로를 가지는 보조 빔을 활용하여 양자 신호의 경로를 수신기의 단일 광자 검출기에 항상 일정하게 입사되도록 제어하는 기술로, 보조빔의 경로를 실시간으로 제어할 수 있는 빠른 움직임 거울(Fast

Steering Mirror), 공간 위치를 측정하는 위치 센서와 제어 구동부 등으로 구성된다. 또한, 실제 양자 신호만을 복원하고 추출해야 하므로 보조빔을 효과적으로 제거하는 기술과 보조빔 신호를 이용한 초정밀 양자 신호 제어 기술이 요구된다.

중국은 2016년에 세계 최초로 양자암호통신용 인공위성을 발사에 성공하였고, 2017년과 2018년에 이를 활용한 초장거리 무선 양자암호통신 결과를 발표하였다[13], [14]. 2016년에 발사한 MICIUS 인공위성을 이용하여 2017년에 세계 최초로 저궤도 인공위성(송신부)과 지상 기지국(수신부) 간의 양자암호통신 실험 결과를 Nature 저널지에 보고하였는데 약 500km에서는 약 12 kbps, 1,200 km 떨어진 거리에서는 약 1.1kbps 수준의 시프티드 키속도(Sifted Key Rate)를 생성하였다. 또한 2018년에는 (그림 2)에서 보여지듯이 중국 Xinglong과 오스트리아 Graz사이에서 지상으로는 7,600km에 이르는 거리의 두 기지국의 양자암호통신을 MICIUS 인공위성을 신뢰 노드(Trusted Node)로 활용하여 성공적으로 수행한 결과를 발표하였으며, 이는 초장거리 글로벌 양자네트워크의 실현 가능성을 보여주었다.

중국 이외에도 인공위성 기반 양자암호통신 기술 개발을 위하여 인공위성을 이용한 양자 신호 전송 수준의 기반 기술 연구는 세계적으로 활발하게 연구 개발되고 있다. 이탈리아와 싱가포르는 2016년, 각각 중궤도 위성(LAGEOS-2)과 저궤도 위성(GALASSIA)을 활용한 양자 전송 실험을 수행하여 성공적으로 양자 상태 복원을 확인하였다[15], [16]. 또한 2017년에는 일본과 독일에서 각각 저궤도 위성(SOCRATES), 정지궤도 위성(ALPHASET)을 활용하여 편광 상태 복원 및 양자 결맞음 특성을 확인하였고 그 결과를 보고 하였다[17], [18]. 이는 향후 인공위성 기반 양자통신을 수행할 수 있는 기반 기술을 확보하였음을 의미한다. 이 외에도 미국의 CAPSat, 영국의 CQuCom, 프랑스의 Nanobob, 캐나다의 QEYSSat, NanoQEY 등 선진국을 중심으로 인공위성 기반 양자통신을 위한 기술 개발 프로젝트가 진행되고 있다[19]. 이에 따라 글로벌 양자 네트워크에 관한 기술은 더욱 빠르게 발전할 것으로 전망된다.

영국은 UK National Quantum Technologies Pro-



(그림 2) 인공위성 기반 대륙간 무선양자암호통신 (2018 중국)

[출처] Reprinted with permission form S.-K. Liao et al., "Satellite-Relayed Intercontinental Quantum Network," *Phys. Rev. Lett.*, vol. 120, no. 3, 2018, Article no. 030501.

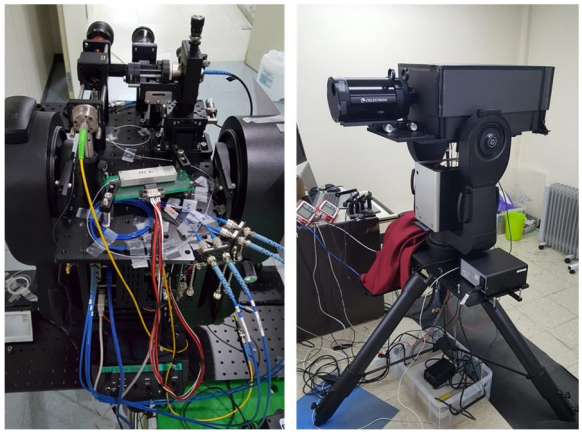
gramme(UKNQT)에 따라 영국 정부가 5년간 2억 7천만 파운드를 지원하여 Sensors and Metrology Hub(허브), Quantum Enhanced Imaging(QuantIC) 허브, Networked Quantum Information Technologies(NQIT) 허브, Quantum Communication 허브의 4개의 허브를 운영 중에 있다[20]. 양자 통신(Quantum Communication) 허브는 York 대학의 Tim Spiller 교수가 허브 리더이며 4개의 대형 Work Package(WP1: Short Range Consumer QKD, WP2: Chip Scale QKD, WP3: UK Quantum Networks, WP4: Next Generation Quantum Communication)로 구성되어 있다. Work Package 1에서는 단거리 무선 소비자 양자암호통신 과제에서 (그림 3)에서와 같이 단거리에서 ATM기와 모바일 단말과 같이 소형 이동체와 고정 기지국간의 응용을 고려하여 연구를 진행하고 있다. Work Package 2에서는 19인치 랙 규모의 부피가 큰 유선 양자암호통신 시스템을 소형화하기 위해서 집적화 칩 형태의 유선 양자암호통신 부품 및 시스템 형태의 연구가 진행되고 있다. Work Package 3에서는 브리스톨 대학과 캠브리지 대학의 매트로 양자암호통신 시스템, 양자 액세스망을 위한 양자암호통신과 이를 연결하는 백본 양자암호통신 시스템 구축 연구를 진행중이며 Work Package 4에서는 양자 중계기와 양자 디지털 서명과 같은 미래 양자 통신 기술에 대한 기본 기술을 연구하고 있다.

(그림 3) Short Range Consumer QKD 예시

2. 국내 기술 동향

국내의 유선 양자암호통신 연구는 ㈜SKT, 한국전자통신연구원(ETRI), 한국과학기술연구원(KIST), 한국과학기술원(KAIST), 국가보안연구소(NSR) 등에서 이루어져 왔지만 무선 양자암호통신의 연구 개발은 국외에 비해 매우 늦게 진행되었다. 지난 2015년부터 ETRI-KIST 정부출연연구소 공동 연구로 무선 양자암호통신 부품 및 시스템 기술 관련 연구가 수행되었다. ETRI는 자체 기술로 개발한 평판형 도파로 기반 초소형 편광부호화 칩과 소형 광학계 기반 편광 모듈을 활용하여 편광 기반 BB84 무선 양자암호통신 시스템을 구축하였다[(그림 4) 참조], [21].

ETRI의 무선 양자암호통신 시스템은 100MHz 속도 이상으로 구동할 수 있는 시스템으로 디코이 기술을 적용하여 광자수 분해 공격(Photon Number Splitting Attack)에도 안전성을 확보하였다. 또한 ETRI 무선 양자암호통신 시스템은 초정밀 빔 트래킹 기술을 개발 적용하여 안정적으로 무선 양자 신호를 송수신 할 수 있도록 개발되었다. 일반적으로 낮에는 단일 광자 세기보다 훨씬 높은 세기를 갖는 태양광 빛에 의해 무선 양자암호통신 신호 전송 및 복원이 어렵다. ETRI는 스펙트럼, 공간적, 시간적 영역에서 광잡음 초저감기술을 통해 낮에도 무선 양자 신호를 복원할 수 있는 기술을 개발하였



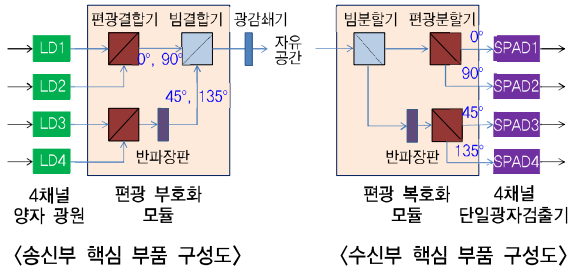
(그림 4) ETRI 무선 양자키분배 송신부 및 수신부 시스템

다. ETRI 시스템은 약 300m 거리의 낮 환경에서도 우수한 3.5% 정도의 양자비트오류율(QBER)과 190kbps 수준의 양자 키 생성이 가능함을 보였고, 현재 장거리 전송을 위한 기반 기술을 연구하고 있다. 또한 ETRI 연구진은 다중 레이저 광원을 이용한 무선 양자암호통신에서 광원의 구동 방식 특성에 따른 양자 통신 시스템의 해킹 가능성을 처음으로 제시하였고, 광원 해킹을 제거할 수 있는 기술과 성능 개선 방법을 보고하였다[22], [23].

많은 선진국들이 이동형 무선 양자암호통신 기술과 인공위성 기반 양자암호통신 관련 기술 개발하는 상황을 고려하면 국내 무선 양자암호통신 기술은 선진국들에 비해 뒤쳐져 있다. 지속적인 연구와 투자를 바탕으로 빠른 기술 개발과 원천 기술 및 선도 기술 확보가 매우 시급한 상황이라고 할 수 있다.

Ⅲ. 무선 양자암호통신 부품 기술 동향

BB84 양자암호프로토콜 기반으로 무선 양자암호통신 시스템을 구성할 경우 양자키분배 양자 채널 송신부 핵심 광부품과 수신부 핵심 광부품을 (그림 5)에 나타내었다. 무선 양자키분배의 양자 채널 송신부 핵심 광부품으로서는 4채널의 광원, 편광결합기, 반파장판, 빔결합기, 광감쇄기 등이 있으며 수신부 핵심 광부품으로서는 빔분할기, 반파장판, 편광분할기, 4채널 단일광자검출기 등이 있다. 그 외 양자 난수 발생기, 공개 채널용 광부품 기술, 공개 채널과 양자 채널 통합 기술 등이 필요하다. 본 장에서는 무선 양자암호통신용 핵심 부품으로서

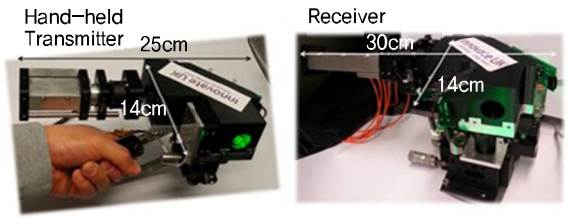


(그림 5) 무선 양자키분배 송수신부 핵심 부품 구성도

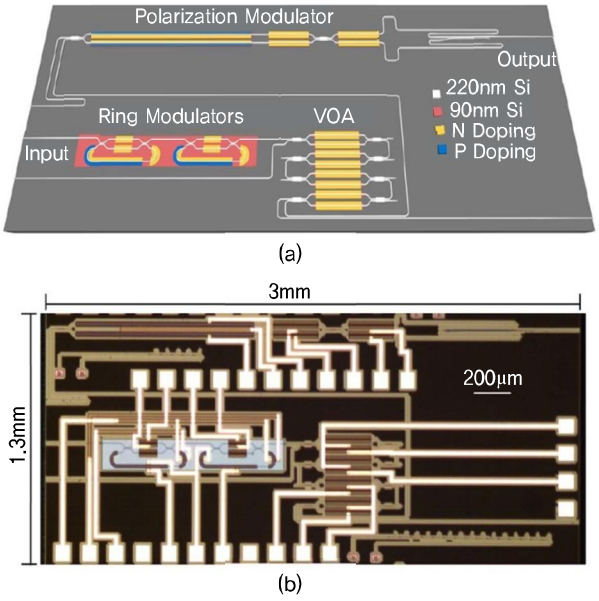
특히 무선 양자키분배용 집적화 부품 기술과 단일 광자 검출기 기술, 양자 난수 발생기 기술 동향을 살펴본다.

1. 무선 양자암호통신 집적화 부품 기술 동향

무선 양자암호통신 부품들은 고가이지만 대부분 상용 광학 부품들로 구성될 수 있다. 대부분의 무선 양자암호통신 시스템에 사용되는 광학 부품들은 우수한 성능을 가지며 고가인 부피가 큰 개별 광학 부품들이 사용된다. 그리고 시스템은 이러한 양자 광학 부품들을 고정밀 및 안정적인 광정렬과 광연결을 통하여 이루어진다. 이러한 것은 제작에 많은 비용과 시간이 요구되며 소형 무선 양자암호장치를 필요로 하는 다양한 응용 분야에는 사용 제약을 받게 된다. 따라서, 소형이면서 안정적이고 저가로 구현할 수 있는 집적화 칩 기반의 무선양자암호통신 부품 연구가 요구된다. 영국 옥스포드 대학에서는 2017년 (그림 6)에서와 같이 모바일 결제나 현금 자동 입출금기(automated teller machine, ATM)와 같은 근거리 보안통신을 위한 양자암호통신 모듈을 보고하였다[24]. 이러한 연구는 2015년에 있었던 전세계 20억 달러 손실이 있었던 은행카드 복제(ATM skimming)와 같은 보안 문제를 해결할 수 있을 것으로 예상된다. 이 시스템은 작은 크기의 개별 자유 공간 광학 부품들로 구성하여 소형 무선 양자암호통신 송수신부 초기 프로토타입 형태로 만들었지만 아직 부피가 크며 개선해야 할 많



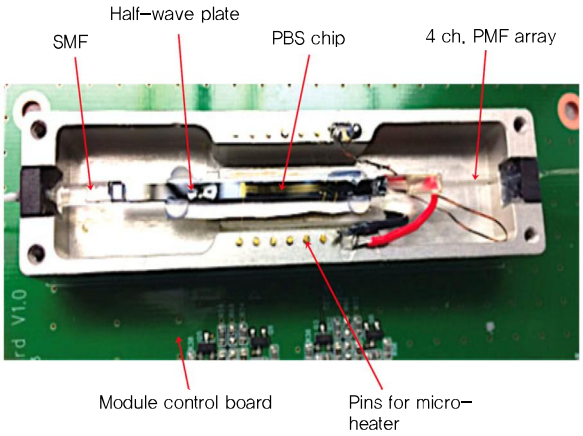
(그림 6) 핸드헬드(hand-held) 형태의 송신기 및 수신기[14]



(그림 7) 실리콘포토닉스 기반 양자암호통신용 송신기 칩[26]

은 것을 가지고 있다. 이를 소형화 및 경량화를 위해서는 집적화 칩 형태의 연구가 요구된다.

2015년 독일의 Ludwig-Maximilian 대학에서는 핸드헬드(hand-held) 양자키분배 송신 모듈을 위해서 femtosecond laser writing 기술을 이용하여 붕규산염 유리(borosilicate glass)에 평면형 도파로 제작 기술을 보고하였다[25]. 이 도파로와 4개의 광원과 4개의 초소형 편광판(polarizer)을 이용하여 양자키분배 송신 모듈 결과를 보고하였다. 또한 캐나다의 토론토 대학은 2016년 편광 부호화 양자키분배 송신기를 위한 실리콘 포토닉스(silicon photonics) 기반의 송신기 칩을 보고하였다[26]. 실리콘 포토닉스 기술은 전자 소자 등의 제작을 위해 사용되었던 성숙된 실리콘 공정 기술을 이용하여 초소형 크기의 광정렬이 필요 없는 광집적회로를 제작할 수 있는 기술이다[(그림 7) 참조]. 그러나 보고된 기술은 주로 유선 양자암호통신 파장대역인 1,550nm 파



(그림 8) ETRI 실리카 도파로 집적화 칩기반 편광 모듈

[출처] J.S. Choe et al., "Silica Planar Lightwave Circuit Based Integrated 1 × 4 Polarization Beam Splitter Module for Free-Space BB84 Quantum Key Distribution," *IEEE Photon. J.*, vol. 10, 2018, Article no. 7600108

장에서 동작하며 10MHz의 저속 시스템 속도와 5km의 유선 광섬유를 통해서 기본 성능 결과가 보고 되었다.

영국 Bristol 대학도 2017년 실리콘 포토닉스 기술을 사용하였으며 캐리어 공핍 변조와 열 변조를 이용하여 고속 편광 부호화를 할 수 있는 집적화 칩 기술을 보고하였다[27]. 그러나 이 연구 또한 1,550nm 파장 대역에서 동작하는 송신기 칩이다. 현재 무선 양자암호통신 시스템이 사용하고 있는 광자 검출기 효율이 높은 850nm 이하의 파장 대역에서 동작하는 집적화 칩 및 부품 기술 개발이 요구된다.

국내 ETRI 연구 그룹은 (그림 8)에서 볼 수 있듯이 2018년 무선 양자암호통신에서 실리카 기반 평면형 도파로 형태의 편광부호화 집적화 칩 및 모듈 기술을 보고하였다[21]. 이 칩은 2개의 편광빔결합기, 반파장판, 빔결합기가 하나의 칩 기반에서 제작된 것으로 785nm 파장대역에서 동작한다. ETRI는 이 편광부호화 집적화 부품을 무선양자암호 송신부 시스템에 장착하여 낮 환경에서도 성공적으로 동작함을 시연하였다.

무선 양자암호통신을 위한 집적화 칩 기반 부품 기술은 아직 일부 핵심 부품만 집적화할 수 있는 수준이며

동작 파장도 제한적이다. 집적화 칩 기반의 부품 기술은 광학계간의 광정렬이 필요 없고 대량 생산 및 저비용으로 제작할 수 있는 기술이며 소형 플랫폼과 같은 다양한 응용에 사용될 수 있다. 무선 양자암호통신 송수신부 전체를 칩기반 집적화 기술로 개발하는 연구는 매우 어려운 고난이도의 기술을 요구하지만 선도 및 원천 기술 확보를 위해서 지속적인 연구가 필요하다.

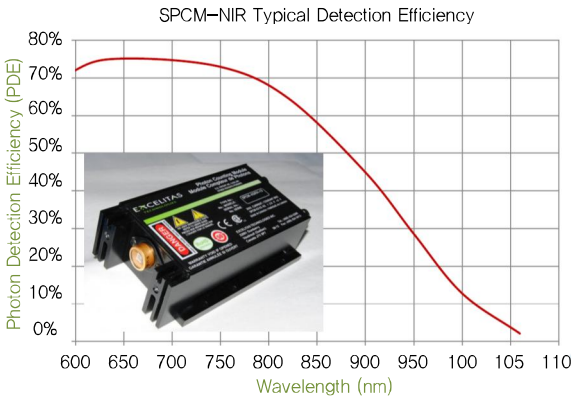
2. 단일광자검출기 기술 동향

무선 양자 암호 통신의 광자 검출기로 사용될 수 있는 소자로는 PMT(photomultiplier tube), SPAD (single-photon avalanche detector), SNSPD(superconducting nanowire single-photon detector) 등이 있다. PMT는 높은 이득을 갖는 진공 튜브를 이용해 광검출을 하는 소자로서 넓은 검출 면적을 가지고 있는 장점이 있으나 광을 전자 신호로 바꿔주는 photocathode 물질에 따라 약간의 차이는 있으나 근적외선 이상의 파장에서는 광자 검출 효율이 낮아 무선 양자 암호 시스템 적용에 제한적이다. SNSPD는 광흡수에 의해 초전도 상태가 파괴되면서 나타나는 저항의 증가를 이용해 단일광자를 검출하는 방식이다. 재료 및 나노와이어의 폭 등의 조정을 통해 1,550nm에서도 광자 검출 효율을 90% 이상을 얻을 수 있고, 암계수율은 100Hz 이하, 타이밍 지터는 30ps 등 성능면에서는 가장 우수한 특성을 보이는 소자이다. 하지만 수광부의 크기가 수십μm정도로 작고, 나노와이어의 방향에 따른 편광 의존성을 가질 수 있으며 초전도 상태를 유지하기 위해서는 극저온(< 3K)에서 동작을 해야 하는 단점을 가지고 있다.

SPAD는 반도체 다이오드 구조를 이용해 단일광자를 검출하는 소자로 항복(breakdown) 전압 이상으로 바이어스를 인가한 상태에서 광자가 입력되면 전자-정공쌍이 생성되게 되고, 높은 전압에 의한 impact ionization에 의해 이들이 증폭이 되는 avalanche 현상에 의한 신호가 발생된다[28]. 또한 광자를 검출, quenching 하고 다시 빨리 원래 상태로 복귀시키는 광자 검출 전자회로가 중요하며 크게 수동 quenching 회로와 능동 quenching 회로로 나눌 수 있다. 수동 quenching 회로는 간단하나 큰 저항값과 기생 커패시턴스 성분으로 인해 reset에 많은 시간이 걸리게 되므로 동작 속도가 낮지만 active quenching 회로에서는 빠른 동작 속도를 위해 avalanche를 감지하는 comparator를 이용해 다이오드에 걸리는 전압을 조절해 quenching 및 reset 시간을 단축시켜 준다. 그러나 quenching을 하기 위한 feed-back 회로의 경로에 의한 지연시간이 발생할 수 있으며 이를 보완하기 위해 두 가지를 혼합한 형태의 quenching 회로도 많이 연구되고 있다.

SPAD의 성능을 나타내는 파라미터들에는 광자 검출 효율, 암계수율, after-pulse 확률, 타이밍 지터 등이 있으며 SPAD 어레이(Array)에서는 누화율 및 fill-factor 등이 추가된다. (그림 9)에 Excelitas 사의 최근 상용 Si-APD 기반 단일 광자 검출기의 파장에 따른 광자 검출 효율을 나타내었다.

실리콘 SPAD는 전용 공정을 이용해 우수한 성능의 소자만을 제작하는 방식과 CMOS(complementary metal-oxide-semiconductor) 공정을 이용해 소자뿐만 아니라 주변의 전자 회로를 같이 제작하는 방식으로 분류된다. 전용 공정을 이용하는 소자는 다시 planar 타입과 non-



(그림 9) Si-APD 기반 SPAD의 광자 검출 효율

[출처] Excelitas, "NIR SPAD brochure,"

planar 타입으로 분류할 수 있다. Planar 타입 전용 공정을 이용한 소자는 Micro Photon Device사의 제품이 대표적이며 광자 검출 효율 불균일성 개선, 긴 diffusion tail 특성 개선, 900nm 파장 영역까지 검출 효율을 증가시키려는 연구가 진행되어 왔다[29]. 전용 공정 중 non-planar 타입의 제품을 생산하는 대표적인 업체는 Excelitas사로서 약 30μm 정도로 기판을 얇게 만들어 후면을 통해 빛이 조사되는 방식이다. 이러한 종류의 소자는 상당히 넓은 active 지름(~180μm)을 갖고 있고 낮은 도핑량을 갖고 있는 guard ring으로 인해 edge breakdown을 막을 수 있는 장점이 있는 반면 높은 breakdown 전압을 갖고 있어 avalanche 신호가 발생하였을 때 전력 소모가 큰 단점을 가지고 있다[30].

〈표 2〉에 전용 공정을 이용하여 상용으로 판매하고 있는 Si-APD 기반 SPAD의 성능을 나타내었다. 회사마다 성능 특성이 다양하며 모든 성능 파라미터가 우수한 특성을 보유한 회사는 없는 것을 확인할 수 있다. Si-APD 기반 SPAD는 1.55μm 파장 대역에서 사용되는 InGaAs-APD 기반 SPAD 보다 우수한 성능을 나타내지만 광자 검출 효율이 SNSPD보다는 낮으며 광자 검출 효율, 암계수율, 타이밍 지터, 최대 속도 등의 면에서 추가 개선이 필요하다.

전용 공정을 이용한 소자와 함께 CMOS 표준 공정을 이용한 소자 제작의 시도가 최근 계속 연구되어 왔는데 이는 실리콘 공정을 이용하여 Si-SPAD와 CMOS 전자회로를 일체형 소자로 만들 수 있는 장점에 기인한다.

〈표 2〉 상용 Si-APD 기반 SPAD 모듈의 성능 비교

	최대 광자 검출 효율 (%@nm)	암계수율 (cps@RT)	After-pulse 확률 (%)	타이밍 지터 (ps@nm)	최대 속도 (Mcps)
Excelitas	65(650)	25	0.5	350(825)	37
Laser Componetns	70(670)	10	0.2	1,000 (N. A.)	20
MPD	60(650)	25	N. A.	100(850)	12
IDQ	80(800)	200	N. A.	400(650)	1

표준 CMOS 공정을 이용해 SPAD를 제작할 경우 공정에 사용되는 재료 및 공정 자체가 SPAD 동작에 필요한 만큼 불순물 농도가 적어야 하고 공핍층에서 band-to-band tunneling 효과가 발생하지 않을 만큼 전기장 세기가 작아야 한다. 고전압 0.35μm CMOS 공정을 이용한 소자의 경우 20μm 지름 SPAD 칩에서 450nm 파장에서 35% 광자 검출 효율, 암계수율이 1,000cps인 결과가 보고되었다[31]. 이 방법의 단점으로는 avalanche를 유발하는 것이 정공이어서 기본적으로 광자 검출 효율이 상대적으로 낮다는 것과 깊게 확산된 guard ring으로 인해 불균일한 광자 검출 효율을 들 수 있다. 또한, 고밀도 및 높은 fill-factor를 갖는 SPAD 어레이를 제작하기 위해서는 deep-submicron(DSM) CMOS 공정이 필수적으로 요구되지만 구현하기가 어렵다. 90nm CMOS 공정을 이용한 칩의 경우 제작 공정이 어렵지만 690nm 파장에서 44%, 850nm에서 20%의 광자 검출 효율과 암계수율이 70cps를 얻은 결과가 보고되었다[31], [32]. 표준 CMOS 공정을 이용한 Si-SPAD는 전용 공정을 이용한 방법에 비해 성능 개선이 많이 필요하지만 향후 소형화 및 집적화 방식의 무선 양자암호통신 모듈을 위해서 지속적인 연구가 필요한 기술이다.

3. 양자 난수 발생 기술 동향

난수는 특정한 순서나 규칙을 가지지 않는 수라고 정의할 수 있으며, 따라서 예측 불가능함을 그 특징으로 가진다. 이러한 예측 불가능성은 많은 분야에 이용될 수 있는데, 전산 모사, 게임, 스마트 네트워크, 인공 지능, 암호화 등이 그 예이다[33].

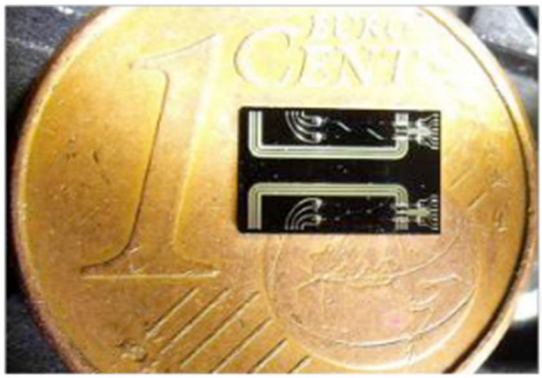
난수는 크게 의사난수(pseudo-random number)와 진정난수(true random number)로 구분할 수 있다. 의사난수는 생성되는 수열에서 다음에 나타날 수는 생성기의 내부 상태에 의해 확정적으로 결정되며, 어떤 시점에서 과거와 동일한 내부 상태가 발생할 경우 앞서의 수열이 반복되어 나타나므로 예측 불가능성 측면에서 불완전

하다는 단점을 가진다. 진정 난수는 예측 불가능하거나 최소한 예측하기 어려운 물리적 과정을 측정하는 방법을 사용한다. 진정 난수 생성기 중 양자역학적 현상에 의한 근본적인 불확정성을 사용하는 것이 양자 난수 발생기이다. 즉, 완전한 예측 불가능성을 제공하는 것이 양자 난수 발생기(QRNG: Quantum Random Number Generator)이다. 양자 난수 발생기는 진정 난수이면서 초고속 및 초소형 형태로의 연구가 진행중이다.

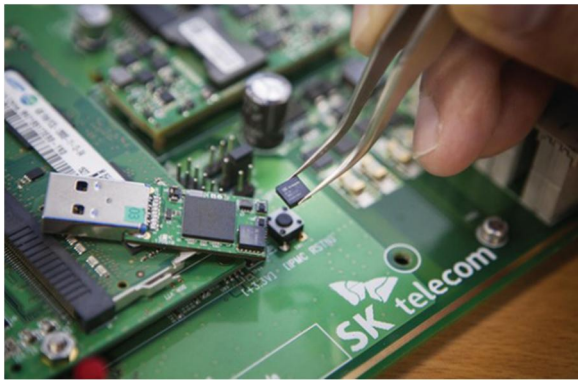
현재의 양자 난수 발생기는 대부분 광학을 기반으로 하고 있다. 빛의 양자 상태에는 여러 파라미터가 가지는 근본적인 무작위성(randomness)때문에 다양한 방식의 난수 생성기의 구현이 가능하기 때문이다. 광학을 이용한 양자 난수 발생기에는 방식에 따라 광경로 분할, 광자 도달 시간 차이, 광자 계수, 진공 요동, 위상 잡음, 자발적 방출을 이용한 방법 등 다양하게 보고되었다[33]. 스페인 바로셀로나 대학의 C. Abellan 등은 InP PIC로 QRNG를 구현하였다[34]. 반도체 공정 기술을 이용하여 InP 광집적회로로 위상 잡음 측정 방식의 QRNG를 구현한 칩 결과를 보고하였다. (그림 10)과 같은 매우 작은 칩에 두 개의 레이저 다이오드와 광도파로를 이용한 간섭계에서 두 레이저의 빛이 간섭하면서 이득 스위칭을 할 때 레이저의 랜덤한 위상에 의해 난수를 생성하는 원리를 이용하였으며 Gb/s 속도가 가능함을 보고하였다.

또한 레이저의 위상 잡음을 측정하여 양자 난수를 발생시키는 방식도 주목을 받고 있다[35]. 레이저 다이오드가 문턱 전류 근처에서 동작할 때 높은 자발적 방출의 비중이 높아서 양자 잡음에 의해 위상 잡음이 정해진다. 또, 위상 잡음은 비대칭 간섭계에 의해 세기 잡음으로 변환 가능하여 광검출기로 측정할 수 있다. 그 다음 난수 추출기를 통과한 후 3.2Gbps 속도의 양자난수 비트열이 최종적으로 얻어졌다.

국내 SK 텔레콤은 스위스의 IDQ사와의 공동 개발을 통해 LED, CMOS 이미지 센서, ASIC을 이용하여 (그림 11)에서 보듯이 칩 형태의 작은 QRNG 칩을 발표하였다. LED에서 발생하는 광자의 개수가 시간에 대해 랜덤하며(양자 잡음 또는 산탄 잡음), 평균 광자 수의 분포는 포아송 분포를 따른다는 성질을 이용했다[36]. CMOS 이미지 센서의 픽셀들이 LED에서 발생한 광자를 흡수하여 그 수를 측정함으로써 미가공된 난수열을 얻는다. 이 난수열에 난수성 추출 알고리즘을 적용하여 최종적인 양자 난수를 생성한다. 이 QRNG는 그 크기가 5mm×5mm×2mm로 초소형이지만 상대적으로 1.5Mbps



(그림 10) InP 반도체 광회로 기반 양자 난수 생성기[34]



(그림 11) LED 출력 및 CMOS 이미지 센서 기반 양자 난수 생성기

[출처] Reprinted with permission from SKtelecom, https://www.sktelecom.com/advertise/press_detail.do?idx=4197

의 낮은 속도로 난수 비트열을 생성한다.

물리적인 시스템을 이용한 난수 생성기는 측정 및 생성 부품의 불완전성 때문에 출력이 편향되거나 상관관계가 존재할 수 있다. 이런 문제를 해결하기 위해 측정을 통해 얻어진 난수열에 후처리를 가하여 균일한 분포의 난수열이 되도록 한다. 이러한 목적을 위해 고안된 것이 무작위성 추출기(randomness extractor)이며, Von Neumann, Trevisan 추출기를 비롯한 여러 가지 알고리즘이 사용되고 있다[37]. 또한 최근에는 물리적 소자가 불완전하더라도 비록 저속이지만 소자에 의존하지 않고 양자역학적으로 난수를 생성할 수 있는 self-testing QRNG 형태에 대한 연구도 보고되고 있다[38]. 그리고 물리적인 양자 난수 생성기에서 생성된 난수열이 올바르게 동작하는지 테스트 및 검증될 필요가 있다. 난수성 테스트의 일반적인 방법은 통계적인 테스트를 사용하는 것이다. 통계적인 난수 테스트 방법으로서 NIST, TestU01, DieHard 등의 방법이 사용되고 있다[39].

최근 양자 난수 발생기는 초소형에 대한 연구가 많이 진행되고 있지만 고속 양자암호통신에 사용되기 위해서는 초고속 양자 난수 발생기가 필요하다. 따라서, 향후 Gb/s급 이상의 초고속이면서 초소형에 대한 양자 난수 발생 기술이 연구될 필요가 있다.

Ⅳ. 결론

최근 정보 통신 기술의 비약적인 발전과 함께 인공지능, 클라우드 서비스, 빅데이터, 사물 인터넷, 지능형 자동차 등 다양한 응용 분야가 발생하고 있으며 앞으로 정보 통신의 발전은 더욱 가속화 될 것이다. 정보 통신 발전과 함께 보안 기술은 사회적 및 개인적 관점에서 점점 더 중요해지고 있다. 또한, 현대 암호 체계를 해독할 수 있는 양자컴퓨터의 개발이 수년 내에 가시화 될 가능성에 의해서 양자암호통신 기술에 대한 중요성은 점점 증가하고 있다.

본고에서는 차세대 통신 보안 기술이면서 양자역학적 원리에 의해 무조건적인 보안성을 보장하는 양자 암호통신의 개념, 중요성 및 기술 동향에 대해서 살펴 보았다. 특히, 광섬유 구축이 없는 대기 환경에서 동작할 수 있으면서 궁극적으로 글로벌 양자암호통신을 가능하게 하는 무선 양자암호통신 시스템의 최신 국내외 기술, 핵심 부품 요소 기술의 동향 및 발전 전망에 대해서 기술하였다. 무선 양자암호통신 기술 선진국들은 현재 초대규모 투자를 통해 위성을 이용한 초장거리 글로벌 양자암호통신 기술 개발을 시작하였고 이동형 소형 단거리 무선 양자암호통신 기술 등 다양한 연구를 진행 중에 있다. 국내의 양자암호통신 기술은 기술 선진국 대비 연구 환경, 인프라, 보유 기술 등이 미흡하지만 국가 전략적 과학 기술 측면에서 추진되어야 하는 기술이다. 무선 양자암호통신 기술을 보유하지 못 할 경우 국외에 기술 종속이 우려되거나 기술적, 경제적 기술 도입 어려움이 예상된다. 또한 주도권 확보를 위한 독자적인 원천, 선도 기술 개발 및 실제 다양한 분야에서 적용할 수 있는 기술이 빠른 시일 내에 개발 되어야 할 것으로 전망된다.

약어 정리

BS	Beam Splitter
LD	Laser Diode
PBS	Polarization Beam Splitter
PMT	Photo-Multiplier Tube
QKD	Quantum Key Distribution
QRNG	Quantum Random Number Generator
RSA	Rivet, Sharmir, Adleman
SNSPD	Superconducting Nanowire Single-Photon Detector
SPAD	Single Photon Avalanche Diode

참고문헌

[1] P.W. Shor, “Algorithms for Quantum Computation: Discrete Logarithms and Factoring” *Proc. Annu. Symp. Foundations Comput. Sci.*, Santa Fe, NM, USA, Nov. 20-

22, 1994, pp. 124–134.

[2] https://www.iad.gov/iad/news/changes-to-cnsa-suit-and-quantum-computing-policy.cfm

[3] C.H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Proc. IEEE Int. Conf. Comput., Syst., Signal Process.*, Banalore, India, Dec. 9–12, 1984, pp. 175–179.

[4] C.H. Bennett and G. Brassard, "Experimental Quantum Cryptography: The Dawn of a New Era for Quantum Cryptography: the Experimental Prototype is Working!" *ACM Sigact News*, vol. 20, no. 4, Nov. 1989, pp. 78–80.

[5] R.J. Hughes et al., "Practical Free-Space Quantum Key Distribution over 10 km in Daylight and at Night," *New J. Phys.*, vol. 4, 2002, pp. 43:1–43:14.

[6] I. Marcikic, A. Lamas-Linares, and C. Kurtsiefer. "Free-Space Quantum Key Distribution with Entangled Photons," *Applied Phys. Lett.*, vol. 89, no. 10, 2006, pp. 101122:1–101122:4.

[7] T. Schmitt-Manderbach et al., "Experimental Demonstration of free-Space Decoy-State Quantum Key Distribution over 144 km," *Phys. Rev. Lett.*, vol. 98. 2007, pp. 010504:1–010504:2.

[8] M. Peev et al., "The SECOQC Quantum Key Distribution Network in Vienna," *New J. Phys.*, vol. 11, 2009, Article no. 075001.

[9] M.P. Peloso et al., "Daylight Operation of a Free Space, Entanglement-Based Quantum Key Distribution System," *New J. Phys.*, vol. 11, 2009, Article no. 045007.

[10] J.-Y. Wang et al., "Direct and Full-Scale Experimental Verifications Towards Ground-Satellite Quantum Key Distribution," *Nature Photon.*, vol. 7. no. 5, 2013, pp. 387–393.

[11] S. Nauerth et al., "Air-to-Ground Quantum Communication," *Nature Photon.*, vol. 7, 2013, pp. 382–386.

[12] J.-P. Bourgoin et al., "Free-Space Quantum Key Distribution to a Moving Receiver," *Opt. Express*, vol. 23, no. 26, 2015, pp. 33437–33447.

[13] S.-K. Liao et al., "Satellite-to-Ground Quantum Key Distribution." *Nature*, vol. 549, no. 7670, 2017, pp. 43–47.

[14] S.-K. Liao et al., "Satellite-Relayed Intercontinental Quantum Network," *Phys. Rev. Lett.*, vol. 120, no. 3, 2018, Article no. 030501.

[15] D. Dequal et al., "Experimental Single-Photon Exchange Along a Space Link of 7000 km," *Phys. Rev. A*, vol. 93, no. 1, 2016, Article no. 010301.

[16] Z. Tang et al., "Generation and Analysis of Correlated Pairs of Photons aboard a Nanosatellite," *Phys. Rev. App.*, vol. 5, no. 5, 2016, Article no. 054022.

[17] H. Takenaka et al., "Satellite-to-Ground Quantum-Limited Communication Using a 50-kg-Class Microsatellite," *Nature Photon.*, vol. 11, no. 8, 2017, pp. 502–508.

[18] K. Günthner et al., "Quantum-Limited Measurements of Optical Signals from a Geostationary Satellite," *Optica*, vol. 4, no. 6, 2017, pp. 611–616.

[19] I. Khan et al., "Satellite-Based QKD," *Opt. Photon. News*, vol. 29, no. 2, 2018, pp. 26–33.

[20] http://uknqt.epsrc.ac.uk/

[21] J.S. Choe et al., "Silica Planar Lightwave Circuit Based Integrated 1 × 4 Polarization Beam Splitter Module for Free-Space BB84 Quantum Key Distribution," *IEEE Photon. J.*, vol. 10, 2018, Article no. 7600108.

[22] H. Ko et al., "Critical Side Channel Effects in Random Bit Generation with Multiple Semiconductor Lasers in a Polarization-Based Quantum Key Distribution System," *Opt. Express*, vol. 25, no. 17, 2017, pp. 20045–20055.

[23] H. Ko et al., "High-Speed and High-Performance Polarization-Based Quantum Key Distribution System Without Side Channel Effects Caused by Multiple Lasers," *Photon. Res.*, vol. 6, no. 3, 2018, pp. 214–219.

[24] H. Chum et al., "Handheld Free Space Quantum Key Distribution with Dynamic Motion Compensation," *Opt. Express*, vol. 25, 2017, pp. 6784–6795.

[25] G. Vest et al., "Design and Evaluation of a Handheld Quantum Key Distribution Sender Module," *IEEE J. Sel. Top. Quantum Electron.*, vol. 21, 2015, Article no. 6600607.

[26] C. Ma et al., "Silicon Photonic Transmitter for Polarization-Encoded Quantum Key Distribution," *Optica*, vol. 3, 2016, pp. 1274–1278.

[27] P. Sibson et al., "Integrated Silicon Photonics for High-Speed Quantum Key Distribution," *Optica*, vol. 4, 2017, pp. 172–177.

[28] S. Cova et al., "Avalanche Photodiodes and Quenching Circuits for Single-Photon Detection," *Appl. Opt.*, vol. 35, 1996, pp. 1956–1976.

[29] A.L. Lacaita, M. Ghioni, and S. Cova, "Double Epitaxy Improves Single-Photon Avalanche Diode Performance," *Electron. Lett.*, vol. 25, June, 1989, pp. 841–843.

[30] S. Cova et al., "Semi-Conductor Based Detectors," *Exp. Methods Phys. Sci.*, vol. 45, 2013, pp. 83-146.

[31] E.A.G. Webster et al., "A Single-Photon Avalanche Diode in 90-nm CMOS Imaging Technology With 44% Photon Detection Efficiency at 690 nm," *IEEE Electron Device Lett.*, vol. 33, no. 5, 2012, pp. 694-696.

[32] M.A. Karami et al., "A New Singlephoton Avalanche Diode in 90 nm Standard CMOS Technology," *Opt. Exp.*, vol. 18, no. 21, Oct. 2010, pp. 22158-22166.

[33] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum Random Number Generators," *Rev. Mod. Phys.*, vol. 89, no. 1, Feb. 2017, Article no. 015004.

[34] C. Abellan et al., "Quantum Entropy Source on an InP Photonic Integrated Circuit for Random Number Generation," *Optica*, vol. 3, no. 9, 2016. pp. 989-994.

[35] X.G. Zhang et al., "Fully Integrated 3.2 Gbps Quantum Random Number Generator with Real-Time Extraction," *Rev. Sci. Instrum.*, vol. 87, no. 7, 2016, pp. 1-3.

[36] B. Sanguinetti et al., "Quantum Random Number Generation on a Mobile Phone," *Phys. Rev. X*, vol. 4, no. 3, 2014, pp. 1-6.

[37] L. Trevisan, "Extractors and Pseudorandom Generators," *J. ACM*, vol. 48, no. 4, 2001, pp. 860-879.

[38] T. Lunghi et al. "Self-*testing quantum random number generator*," *Phys. Rev. Lett.*, vol. 114, 2015, Article no. 150501.

[39] A. Rukhin et al., "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," NIST Special Publication 800-22, Revision 1.a., 2010.