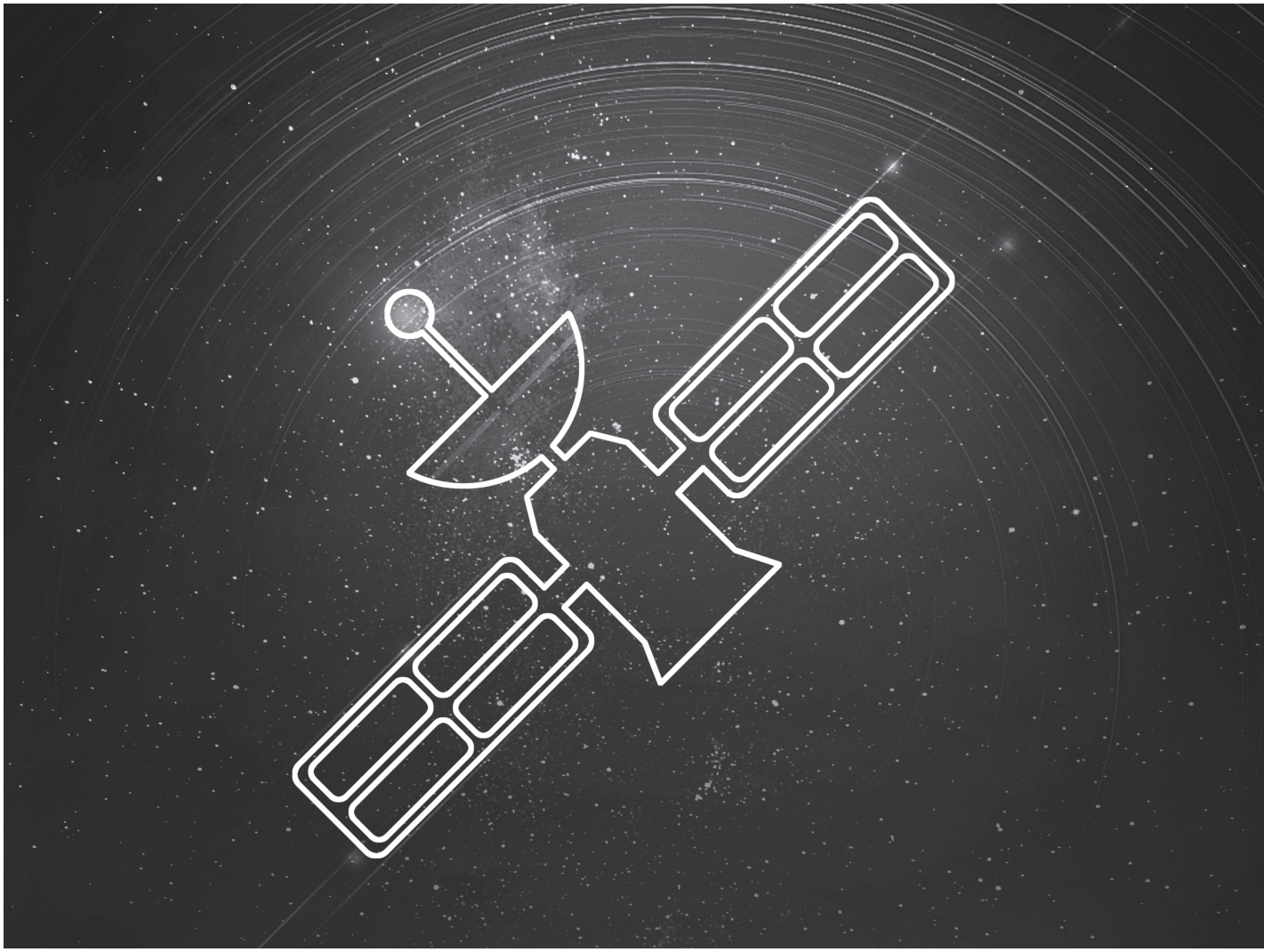

일본에 대한 위성 양자 암호관련기술의 연구개발

글 Hiroyuki Endo 연구원, Mikio Fujiwara 연구매니저,
Masahiro Takeoka 센터장, Masahide Sasaki 주임연구원 /
(국연) 정보통신연구기구 미래 ICT연구소 양자 ICT첨단개발센터
번역 유정훈 / 그린광학 사업개발그룹장

1. 처음

정보 네트워크에 의해 나날의 생활의 편리성이 높아지는 한편, 신용카드 암호 등 그곳에서 거래되는 정보를 노리는 범죄도 만연하게 되었다. 그 때문에 정보 보안에 대한 관심이 어느 때 보다 높아지고 있다.

현재 네트워크의 보안은 암호화, 인증 등의 기능을 가지는 암호 알고리즘의 집합체에 의해 유지되고 있지만, 이들 안전성은 도청자의 계산기 능력에 의존하고 있고, 기술의 진보에 동반해 저하해 간다(계산량적 안전성). 외교 · 방위 등의 국가의 안전에 관한 정보와 의료 · 게놈 데이터 등의 인간의 생명에 관한 정보의 보안을 유지하기 위해서는 안전성이 기술의 진보에 대해서 저하하지 않는 것을 정보 이론적으로 증명할 수 있는(정보이론적 안전성) 기술이 필수로 된다.

이와 같은 기술로서 양자 암호[1~3]를 들 수 있다. 양자 암호에서는 최초로 광자의 양자역학적인 성질을 이용해서 떨어진 2지점 간에서 키를 공유한다. 이와 같은 키 공유는 양자 키 분배(QKD: Quantum Key Distribution)라고 하고, 물리학적으로 허용되는 여러 도청법에 노출되어도 안전한 것이 나타나고 있다. 이어서 공유한 키를 사용해서 Vernam의 원타임 패드 암호에 의해 평문을 암호화한다. 이 방법에서는 평문과 같은 길이의 키가 사용되고, 한번 사용된 키는 두 번은 사용되지 않는다. 이 규칙 하에서 Vernam의 원타임 패드 암호는 정보 이론적으로 안전한 것이 나타나있다[4].

실용화를 의식한 광섬유 네트워크가 구축되는 등, 세계적 연구기관 · 기업에 의해 연구개발이 진행하고 있는 양자 암호이지만, 매우 강력한 안전성과 교환, 전송거리 및 키 생성 속도에 과제를 포함하고 있다. 섬유중의 광자 흡수에 의해 50 km의 섬유에서 약 1 Mbit/초의 키 생성 속도를 달성할 수 있는 시스템에서도 100 km의 전송거리에서는 키 생성 속도는 약 1 kbit/초로 감소한다[5]. 신뢰할 수 있는 국사에 의한 키의 중계는 유효한 수단으로 포착되고 있고, 중국에서는 32거점에 의한 키 중계에 의해 북경에서 상해까지의 거리 2000 km를 연결하는 양자 암호통신을 실시했다[6]. 그래도 대륙 간 스케일의 양자 암호통신은 매우 어렵다. 그래서 최근에서는 양자 암호통신의 전송거리를 더욱더 신전시키기 위한 수단으로서 인공위성에 의한 양자 암호, 즉 위성 양자 암호가 주목되고 있다. 대기가 없는 우주공간에서는 광자의 흡수와 산란을 사실상 무시할 수 있다. 그 때문에 지상 섬유계와 비교해서 전송거리를 크게 늘리는 것을 기대할 수 있다.

본고에서는 일본에서 실시된 위성 양자 암호에 관련한 기술을 검토한다. 이하, 제2절에서는 양자 암호의 심장부라고도 할 수 있는 QKD의 기초사항을 확인하고, 제3절에서 각국에서 위성 양자 암호의 연구개발에 대해서 말하겠다. 그리고 제4절과 제5절에서는 정보통신연구기구(NICT)가 행해온 초소형 위성에 의한 양자통신실험과 양자 암호와 관련한 기술인 물리 계층 암호에 대해서 각각 말하겠다.

2. 양자 키 분배

QKD의 첫 번째 단계는 송신자(앨리스)가 키의 소(素)로 되는 난수 비트를 단일광자의 편광과 위상 등으로 부호화해서 정규수신자(보브)로 전송하는 양자통신이다. 보브는 보내져온 광자의 양자상태를 식별하는 것에서 난수 비트를 복조한다. 이렇게 해서 시프트 키라고 불리는 난수열이 앨리스와 보브 간에서 공유된다. 이어서 키 증유 처리라고 하는 신호처리가 행해진다. 여기에서는 광자의 전송과정에서 생긴 앨리스의 시프

트 키와 보브의 시프트 키 간의 비트 에러율에 대해서 시프트 키의 일부를 인증된 공개통신로에서 주고받으면서 정정한다. 또 이브에 부분적으로 유출된 정보를 삭제하기 위한 처리도 행해진다. 이상의 스텝을 통해 앨리스와 보브 간에서 키가 공유된다. 이브는 전송되어 있는 광자에 대해서 도청 · 변조 등의 공격을 행한다. 그러나 양자역학의 원리에서 단일광자와 부호화되어 있는 난수 비트에 대해서 이들 공격을 전혀 흔적을 남기지 않고 행할 수 없다. QKD의 경우, 이 흔적은 시프트 키에 대한 비트 에러율의 증가로서 나타나고, 그곳에서 도청자에게 누설해있는 정보량의 상한을 계산할 수 있다. 그 때문에 QKD의 안전성을 물리적으로 가능한 모든 공격에 의해 정보 이론적으로 증명할 수 있다.

3. 위성 양자 암호연구개발의 해외동향

앞서 말했듯이 인공위성은 양자 암호의 전송거리를 크게 늘리는 방법으로서 주목 받고 있으며, 많은 연구기관이 대거 위성 양자 암호의 연구개발에 몰두하고 있다.

세계에 앞서 위성 양자 암호를 성공시킨 것은 중국과학기술대학이다. 그들은 2016년 8월에 중량 600 kg의 양자과학위성 "묵자"를 저궤도에 발사했다. 장기간을 걸쳐 개발한 세계최고정도의 포착 추적 기술을 구사하는 것에서 2017년 6월에는 2지점 간에서 양자 얽힘 상태의 공유에 성공했다[7]. 그리고 같은 해 8월에는 키 생성 속도 약 1 kbit/초 정도의 위성–지상국 간 QKD를 실시하고[8], 2018년 1월에는 "묵자"를 중계노드로 하는 중국–오스트리아 간에서의 양자 암호통신을 행했다[9].

거의 같은 시기에 막스 플랑크연구소와 독일 항공우주센터에 의해 미약한 코히런트상태 펄스의 식별실험이 실시되었다[10]. 이 기술은 QKD의 프로토콜의 일종인, 연속량 QKD의 기초로 된다. 또한 2017년 3월에는 유럽우주기관이 주체로 되어 위성광통신의 국제프로젝트 "ScyLight"를 설립했다. 14국가가 참가하는 이 프로젝터에서는 위성광통신 기술뿐만 아니라 위성 양자 암호기술의 연구개발 및 그 시장개척에도 장기적으로 대처할 계획이다.

그 외 양자정보기술의 벤처기업인 ID Quantique으로 투자하고, 2022년까지 양자통신위성의 발사를 계획하고 있는 한국의 SK Telecom과 위성 양자 암호개발 프로젝터 "QEYSSat"를 시작한 캐나다의 워털루 대학, 그리고 2016년 시점에서 이미 양자통신을 위한 초소형 위성을 발사한 싱가포르의 S–fifteen space system 등, 세계 각국에서도 위성 양자 암호의 개발이 시작되고 있다. 어느 기관도 막대한 자금을 근거로 연구개발을 진행하고 있고, 이 분야에 대한 국제적인 리더십의 획득을 노리고 있다.

4. 초소형 위성에 의한 위성-지상국 간 양자통신실험

이 절에서는 NICT가 행해온 위성 양자 암호를 향한 연구개발에 대해서 말하겠다. 중국이 "묵자"위성을 발사했을 때와 거의 동시기에 NICT는 고도 628 km를 주회하는 저궤도위성과 NICT 코가네이 본부에 건조한 지상국 사이에서 위성–지상국 간에서의 양자통신의 실증실험을 행했다[11]. 본 실험에서 사용된 위성 "SOCRATES"는 소형위성 표준버스기술의 실증과 선진적인 미션/요소기술의 궤도상 실증기회의 제공을 목적으로서 ㈜AES에 의해 개발되었다. 크기가 약 50 cm^3, 질량이 약 50 kg정도이며 초소형 위성으로 분류된다.

그림1 중앙상부에 나타났듯이 "SOCRATES"에는 소형위성에 대한 광 공간 통신기술의 실증을 목적으로서 NICT 우주통신연구실에서 개발된 소형 광 트랜스폰더 "SOTA(Small Optical TrAn–sponder)"가 탑재되어 있다. "SOTA"에는 여러 가지 실험을 상정해서 복수종류의 레이저가 탑재되어 있지만, 본 실험에서는 비교적 쉬게 조달 가능한 Si 베이스의 단일광자검출기를 사용하기 때문에 파장 800 nm대의 직선편광 펄스레이저가 사용되었다(그림1(a)의 Tx2와 Tx3). QKD에 필요한 비직교상태의 생성을 실현하기 위해 양자의 편광이 상대적으로 약 45°(실장상은 44°) 경사지게 설치되어 있다.

"SOTA"에서 송신된 펄스는 우주공간과 대기를 전파하고, 지상국에 있는 구경 1 m의 반사식 망원경(그림1(b))에 의해 그 나스미스 초점에 설치된 양자수신기로 집광된다(그림1(c)). 이 양자수신기는 비직행인 편광상태를 식별할 수 있도록 설계되어 있다. 송신광펄스가 의사 난수열에 기초해서 생성되어 있는 것, 송신펄스당의 광자수가 단일광자레벨이 아닌 것에서 상기의 셋업에서는 QKD실험은 행하지 않는다. 그러나 양자수신기에 대한 펄

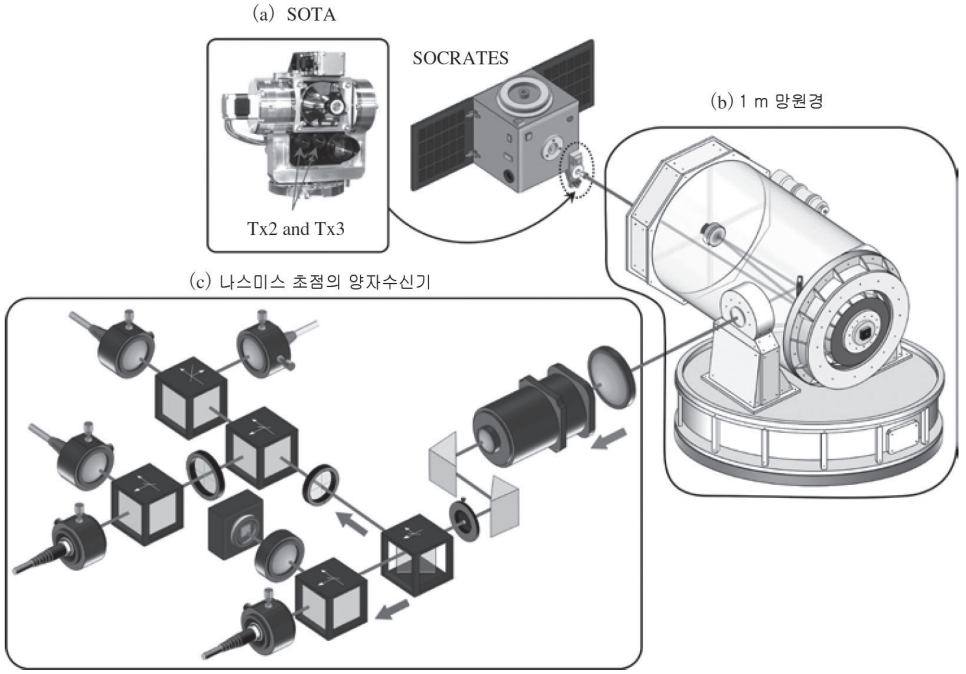

그림1: SOTA를 이용한 양자 통신 실험 설정 개요 그림[11]
(a) SOTA의 사진. (b) NICT 코가네이 지상국에 설치된 1 m 망원경. (c) 1 m 망원경 나스미스대에 설치된 양자 수신기. 각 광학 부품에 대한 자세한 내용은 문헌 11)을 참조하고 바란다.

스당의 평균광자수가 0.146으로 매우 미약했기 때문에 양자통신실험이라고 자리매김할 수 있다.

양자수신기가 비직교인 편광상태를 식별할 수 있는 것의 확인을 위해 위성 고도에 따라 1 m 망원경의 각도가 변화하는 것에 생기는 편광의 상대적인 변화를 검증했다. 그림2의 파선은 Tx2 및 Tx3이 송신한 펄스 편광의 상대적인 변화를 "SOCRATES"의 궤도요소에서 예측한 커브이다. 한편 이 그림의 마커는 실험데이터에서 복원된 편광변화이다. 22:58의 후반쯤에서 양자가 매우 잘 일치하고 있기 때

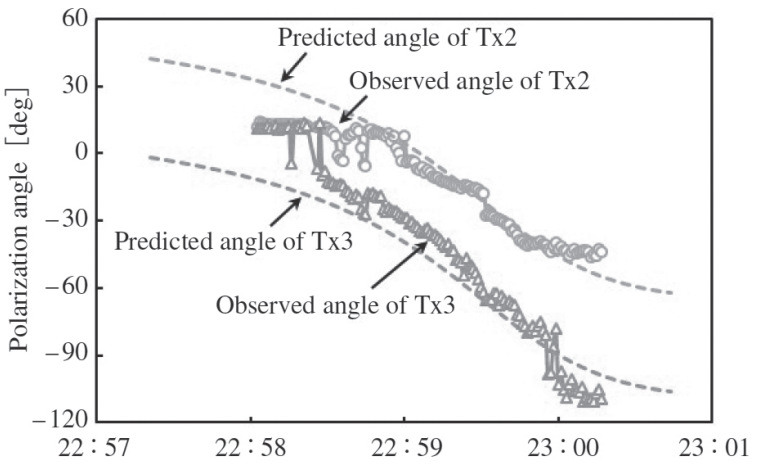

그림2: Tx2, Tx3의 양자수신기 출력에서 얻어진 상대편광각 및, 궤도계산에서 예상되는 상대편광각[11].

문에 비직교인 편광상태의 식별에 성공했다고 결론할 수 있다.

전술과 같이 본 실험은 어디까지나 양자통신의 실증실험이고, QKD의 실증실험은 아니다. 그러나 얻어진 실험데이터에서 QKD 프로토콜의 일종인 B92[12]를 상정해서 양자비트 에러율을 계산한 결과, 본 실험의 셋업에 의한 그 실시가능성을 확인할 수 있었다. 본 실험은 "묵자"보다도 압도적으로 소형 위성과 지상국 간에서 양자통신을 성공시키고 있다. 한편 중국 실험에 앞서 성과를 공표할 수 있었던 점에 큰 의의가 있다.

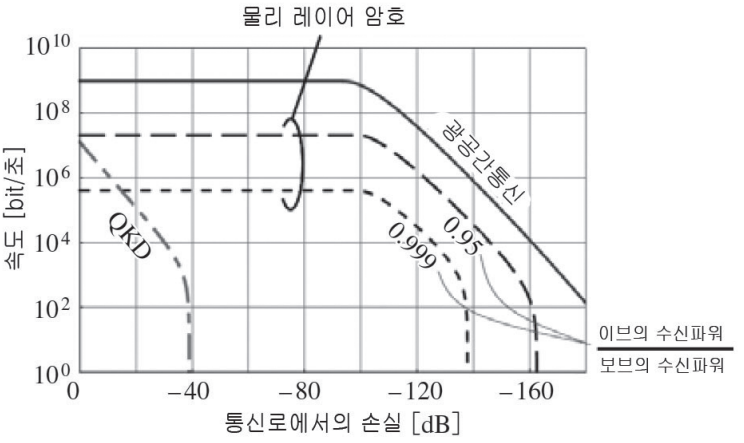

그림3: 물리 계층 암호와 QKD, 광공간통신의 속도 비교[17]

5. 광 공간 통신에 의한 비밀 키 공유

저궤도위성–지상국 간 통신의 스루풋을 구할 때, 위성이 고속으로서 지구를 공전하고 있는 것에서 지상국과의 통신가능시간이 몇 분에서 십수 분 정도인 것을 고려할 필요가 있다. 예를 들면 중국의 "묵자"에 의한 QKD 실험에서 키 생성 속도는 1 kbit/초 정도였지만, 1일의 통신가능시간을 10분정도로 가정하면 1일당의 키 생성 총량은 600 kbits 정도로 추정된다.

이 스루풋은 국가기밀정보와 같이 높은 기밀성이 요구되는 정보를 지키는 것에는 충분하다. 그러나 매일 거래되는 대량의 트래픽을 지탱하기에는 너무 적다. 그와 같은 고도한 기밀성이 요구되지 않는 용도에는 안전성에 약간의 조건이 부과하더라도 보다 대량의 키를 생성할 수 있는 것이 좋다.

이상의 관점 하에 NICT에서는 물리 계층 암호라는 기술의 연구 · 개발을 행했다. 이 기술은 통신에 특유한 물리적 특징에 기초해서 도청자의 도청능력을 가정하고, 정보이론적으로 안전한 은닉 메시지전송[13,14]과 암호 키의 공유[15,16]를 실현하는 것이다. 예를 들면 위성 광 공간 통신에서는 앨리스와 보브 통신은 확산이 좁은 광 빔에 의해 상호 전망을 확보한 상에서 행해진다. 이 "물리적 특징"하에서는 이브의 공격은 전망 밖에서의 것에 한정할 수 있고, "물리학적으로 가능한 여러 공격방법도 갖춰진 이브"에 대해서도 보증되는 QKD의 너무 강력한 안전성을 완화시킬 수 있다.

그림3에 데코이 BB84 프로토콜에 의한 QKD와 정보이론적으로 안전한 방법을 사용하

지 않는 광 공간 통신, 그리고 물리 계층 암호의 전송 속도를 나타낸다[17]. QKD의 키 생성 속도는 저궤도위성–지상국 간에서의 손실에 대응하는 −40 dB부근에서 급격히 감소한다. 한편 물리 계층 암호는 QKD보다도 장거리에서의 은닉 통신을 실현할 수 있다.

NICT에서는 물리 계층 암호의 일종인 비밀 키 공유[15,16]라고 하는 방법의 실증실험을 실시했다[18,19]. 이것은 QKD와 같이 난수를 공유한 후에 공개통신로에 의한 키 증유처리를 실시하는 것에서 정보이론적 안전에 키를 생성하는 방법이다. 그러나 난수의 공유는 반드시 양자적은 아니고 통상의 광통신과 같이 광 신호에서 행해진다. 양자역학의 원리를 사용하지 않기 때문에 앨리스와 보브 간의 비트에러에서 이브에 대해서 누설된 정보량을 예측하는 것은 곤란하다. 이 사실이 비밀 키 공유의 기술적인 허들을 높여왔다.

그림4에는 우리들이 광 공간 통신에 대한 비밀 키 공유의 실증실험을 행한 광 공간 통신 테스트 베드의 사진을 나타냈다. 이 테스트 베드는 송신기의 앨리스가 두어진 전통대(電通大)와 두 개의 수신기가 두어진 NICT 간에서 7.8 km의 수평광 링크를 구성한다. 지구를 둘러싼 대기 두께가 10 km정도인 것을 고려하면 7.8 km라는 거리를 수평전파하는 광은 위성–지상국 간을 수직 전파하는 광과 비슷하거나 혹은 그 이상의 대기 요란의 영향을 받는 것으로 된다. 그 때문에 여러 광 공간 통신에 관한 기술의 위성탑재가능성 검증에 본 테스트 베드를 사용할 수 있다.

앨리스는 파장 1550 nm의 eye safe 레이저를 10 MHz의 대역에서 on–off 변조하는 것에서 물리 난수 원에서 생성된 난수열을 전송한다. NICT측의 두 개의 수신계 중, 6층의 계는 보브 역할을 담당한다. 보브가 복조한 난수비트열과 앨리스가 전송한 난수비트열을 PC상

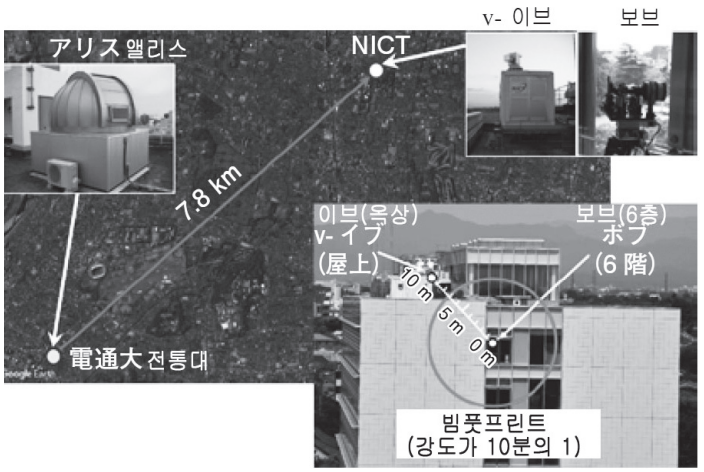

그림4: 광 공간 통신 테스트 베드[18 21)]

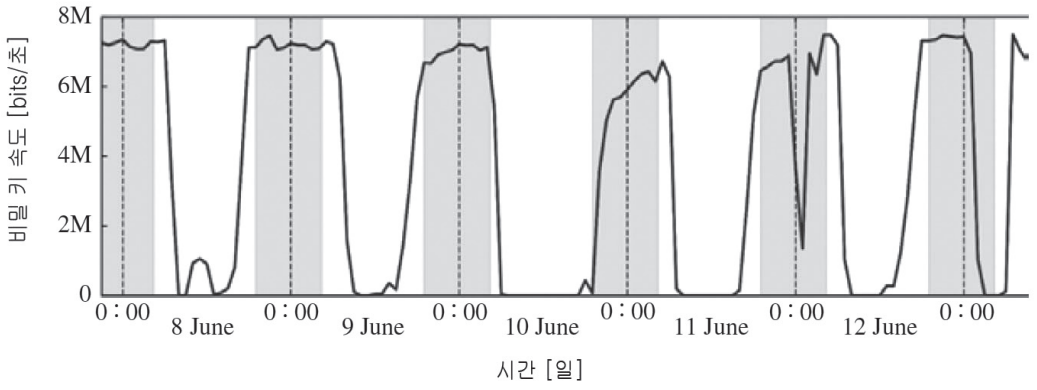

그림5: 2017년 6월에 실시된 비밀 키 공유의 실증실험결과[19)].
음영부는 일몰부터 일출까지의 시간을 나타내고 있다.

에 실장한 키 증유 처리에 입력해서 키를 생성한다. 한편 v(virtual)–이브계라고 하는 옥상의 계는 빔의 끝에서 누설되고 있는 파워를 검출하는 것에서 보다 떨어진 위치에 있는 도청에 노출되는 정보량의 상한을 주기 위한 프로브 시스템으로 기능한다. 이 프로브 시스템의 도입에 의해 비밀 키 공유의 실현가능성을 높일 수 있었다.

그림5에 5일간에 걸쳐 행해진 비밀 키 공유 실험의 결과를 나타냈다. 이 실험에서는 100 ms 간의 비밀 키 전송을 5분마다 행하고, 그곳에서 키 생성 속도를 예측했다. 이 그림에 나타냈듯이 심야에는 평균해서 7 Mbit/초의 키 생성 속도를 실현할 수 있다. 이것은 위성 양자 암호의 결과와 비교해서 압도적으로 고속이다. 한편, 아침으로 되면 키 속도는 10으로 급격히 저하한다. 이것은 아침저녁의 기온 차에 의해 일어나는 건물과 실험장치의 열팽창에 의한 광축의 편차가 원인이라고 생각되고, 정기적인 정렬조절과 선진적인 광축보정기술에 의해 회복가능하다. 또 심야에서도 키 생성 속도가 급격히 저하하고 있는 시간대가 있지만, 이것은 강우에 의해 광통신이 차단되었기 때문인 것이 날씨데이터를 참조하는 것에서 명확히 되어 있다.

6. 이후의 전망

현재, NICT는 총무성이 내세운 ICT중점기술의 연구개발 프로젝터의 하나인 "위성통신에 대한 양자 암호기술의 연구개발"에 참여하고 있다. 본 프로젝트에서는 각국보다도 앞서 실증한 초소형 위성에 대한 양자통신의 노하우와, 광 공간 통신에 대한 물리 계층 암호라는 일본 독자의 기술개발에서 얻어진 지식을 바탕으로 초소형 위성에 탑재 가능한 양자 암호기술과 휴대형 광 지상국을 조합시킨 시스템의 개발이라는 세계 최초의 시도에 노력하고 있다. 이 연구개발에 의해 실용적이고 시장경쟁력이 있는 이동체 양자 암호통신 기술의 확립을 목표로 하고 있다.

감 사

본 해설문에서 소개한 연구의 일부는 종합과학기술회의 · 이노베이션회의에 의해 제도 설계된 혁신적 연구개발추진프로그램(ImPACT)의 지원을 받아 실시되었다.

참고논문

1) C. H. Bennett, and G. Brassard, “Quantum cryptography: public key distribution and coin tossing,”in Proc. of IEEE International Conference on Computers Systems and Signal Processing, Bangalore India, pp. 175-179, 1984.
2) A. K. Ekert,“Quantum cryptography based on Bell ' s theorem,”Phys. Rev. Lett., vol. 67, no. 6, pp. 661-663, 1991.
3) N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,”Rev. Mod. Phys., vol. 74, no. 1, pp. 145-195, 2002.
4) C. Shannon, “Communication theory of secrecy systems,”Bell Syst. Tech. J., vol. 28, no. 4, pp. 656-715, 1949.
5) A. R. Dixon, et al., “High speed prototype quantum key distribution system and long term field trial,”Opt. Express, vol. 23, no. 6, pp. 7583-7592, 2015.
6) J. Qiu,“Quantum communications leap out of the lab,”Nature, no. 508, vol. 7497, pp. 441-442, 2014.
7) J. Yin, et al., “Satellite-based entanglement distribution over 1200 kilometers,”Science, vol. 356, no. 6343, pp. 1140-1144, 2017.
8) S. -K. Liao, et al., “Satellite-to-ground quantum key distribution,”Nature vol. 549, no. 7670, pp. 43-47, 2017.
9) S. -K. Liao, et al., “Satellite-relayed intercontinental quantum network,”Phys. Rev. Lett., vol. 120, no. 3, pp. 030501, 2018.
10) K. Gunthner, et al.,“Quantum-limited measurements of optical signals from a geostationary satellite,”Optica, vol. 4, no. 6, pp. 611-616, 2017.
11) H. Takenaka, et al., “Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite,”Nat. Photonics, vol. 11, pp. 502-508, 2017.
12) C. H. Bennett, “Quantum cryptography using any two nonorthogonal states,”Phys. Rev. Lett., vol. 68, no. 21, pp. 3121-3124, 1992.
13) A. D. Wyner,“The wire-tap channel,”Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355-1387, 1975.
14) I. Csiszar and J. Korner. “Broadcast channels with confidential messages.”IEEE Trans. Inform. Theory, vol. 24, no. 3, pp. 339-348, 1978.
15) U. M. Maurer, “Secret key agreement by public discussion from common information,”IEEE Trans. Inform. Theory, vol. 39, no. 3, pp. 733-742, 1993.
16) R. Ahlswede and I. Csiszar, “Common randomness in information theory and cryptography. I. Secret sharing,”IEEE Trans. Inform. Theory, vol. 39, no. 4, pp. 1121-1132, 1993.
17) H. Endo, T. S. Han, T. Aoki, and M. Sasaki, “Numerical study on secrecy capacity and code length dependence of the performances in optical wiretap channels,”IEEE Photon. J., vol. 7, no. 5, pp. 7903418, 2015.
18) M. Fujiwara, et al., “Free-space optical wiretap channel and experimental secret key agreement in 7.8 km terrestrial link,”Opt. Express, vol. 26, no. 15, pp. 19513-19523, 2018.
19) H. Endo, et al. “Free space optical secret key agreement,”Opt. Express, vol. 26, no. 18, pp. 23305-23332, 2018.
20) H. Endo, et al., “Free-space optical channel estimation for physical layer security,”Opt. Express, vol. 24, no. 8, pp. 8940-8955, 2016.
21) 遠藤寛之 他“光空間通信における物理レイヤ暗号～実環境における性能推定と符号化～ ,”信学技法, vol. 116, no. 183, pp. 7-12, 2016.