논문 21-46-05-15 The Journal of Korean Institute of Communications and Information Sciences '21-05 Vol.46 No.05
https://doi.org/10.7840/kics.2021.46.5.900

시분할 직교 호모다인 검출을 이용한 연속변수 양자암호키분배

오 준 상•, 임 경 천*, 이 준 구°

Continuous Variable QKD with Time Division Quadrature Homodyne Detection

Junsang Oh•, Kyongchun Lim*, June-Koo Kevin Rhee°

요 약

연속변수 양자암호키분배 (continuous-variable quantum key distribution, CVQKD) 시스템에서, 편광 분할을 이용한 기존 직교 호모다인 검출 (quadrature homodyne detection, QHD) 시스템은 기존의 호모다인 검출(homodyne detection, HD) 방식 대비 비밀키 생성률을 높일 수 있다. 우리가 제안한 시분할 직교 호모다인 검출 (time-division quadrature homodyne detection, TDQHD) 시스템은 두 개의 호모다인 간섭계로 직교 호모다인 검출을 하는 기존 방식과 달리, 시분할 방식을 도입하여 하나의 호모다인 간섭계만으로 동시에 두 개의 직교하는 기저에 대한 양자 연속변수 검출을 가능하게 한다. 이 방식은 직교 호모다인 검출과 동일하게 기존 호모다인보다 향상된 비밀키 생성률을 얻을 수 있게 한다. 추가로 실제 시스템 구현에 있어, 기존 호모다인 검출에서 검출 기저 선택을 위해 사용하는 임의의 위상 변조가 필요 없으며, 수신부를 편광에 독립적으로 구현할 수 있어 광섬유의 편광 흔들림에 의한 영향이 해소된다.

Key Words : quantum key distribution, continuous variable quantum key distribution, heterodyne detection, time division multiplex, quadrature detection

ABSTRACT

In the continuous-variable quantum key distribution (CVQKD) system, quadrature homodyne detection (QHD) can increase the secret key rate compared to the conventional homodyne detection (HD). Our new scheme of time-division quadrature homodyne detection (TDQHD) enables simultaneous detection of two quadratures with only one single homodyne interferometer in a time-division manner, unlike conventional QHD. In addition, in implementing the actual system, the need for a random phase modulation used for selection of the detection quadrature in the HD is eliminated, and hence practically the TDQHD can be implemented polarization independent, eliminating the impairment caused by polarization drifts in the fiber transmission system.

※ 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터지원사업(IITP-2021-2018-0-01402)의 연구결과로 수행되었습니다.

• First Author : Korea Advanced Institute of Science and Technology School of Electrical Engineering & AI Quantum Computing ITRC Center, js.oh@kaist.ac.kr, 학생회원

° Corresponding Author : Korea Advanced Institute of Science and Technology School of Electrical Engineering & AI Quantum Computing ITRC Center, rhee.jk@kaist.ac.kr, 정회원

* Electronics and Telecommunications Research Institute Quantum Optics Research Section, lim.kc@etri.re.kr, 정회원

논문번호 : 202101-014-A-RE, Received January 1, 2021; Revised February 8, 2021; Accepted February 9, 2021

Ⅰ. 서 론

연속변수 양자암호키분배는 높은 파워를 갖는 국부 진동자(local oscillator, LO)와 수 개 또는 수십 개의 평균 광자 수를 갖는 양자 상태(quantum state)의 호모다인 검출(homodyne detection, HD)을 통하여 암호키를 교환한다. 호모다인 간섭계를 이용한 검출 방식은 빛의 위상 또는 진폭을 광자잡음한계로 측정할 수 있고[1] 높은 검출 효율을 갖는 균형 검출기를 사용하기 때문에 양자암호키분배 프로토콜 중 높은 암호키 전송률에 접근할 수 있는 효율적인 방법으로 알려져 있다. 또한, 일반적인 광통신에서 사용되는 결맞음 검출기를 사용하기 때문에 높은 상용화 가능성을 갖는다고 판단된다. 기존의 헤테로다인 검출[2], 즉 직교 호모다인 검출 (quadrature homodyne detection, QHD) 방식은 수신 신호를 분할하여 2개의 호모다인 간섭계를 통해 각 동기위상 (Q) 과 직교위상 (P) 검출을 한다. 직교 호모다인 검출 시스템은 암호키 전송률을 높일 수 있지만, 실제 시스템을 구현할 때, LO와 양자 신호의 편광 분할 다중화 방식을 사용하기 때문에 정밀한 편광 제어가 필요하다. 본 논문에서는 시분할 방식을 이용하여 기존의 직교 호모다인 검출 시스템과 같이 향상된 암호키 전송률을 갖고, 추가적으로 편광 흔들림에 무관한 단일 간섭계를 이용하여 실제 구현에서 갖는 어려움을 해소한 시분할 직교 호모다인 검출 방법을 소개한다.

Ⅱ. 시분할 직교 호모다인 검출

2.1 프로토콜 설명

제안한 방식은 가우시안 변조 결맞음 상태(gaussian modulation coherent state, GMCS) 프로토콜[3]을 기반으로 한다. 그림 1은 시분할 직교 호모다인 검출 시스템의 개략적 실험 셋업을 나타낸다. 설명에 앞서, 양자 신호와 LO 펄스를 송신부에서 광 진폭 변조기를 통해 생성하기 때문에 높은 파워를 갖는 LO 펄스를 수신자에게 전송하게 된다. 최근 이런 경우에 대한 도청자의 공격을 분석한 논문들이 나와 있지만[4-7], 다양한 해결책이 있어 본 논문에서는 이를 고려하지 않겠다.

송신자(Alice)는 두 단계로 나누어 수신자(Bob)에게 신호를 전달한다. 먼저, Alice는 광 펄스를 생성하는 첫 번째 광 진폭 변조기를 이용하여 세기가 강한 LO와 세기가 약한 양자 신호를 펄스 형태로 교대로 생성한다. 첫 번째 단계에서는 데이터 변조는 하지 않는다. 두 번째 단계에서는 광 진폭 변조기와 위상 변조기를 이용하여 (Q, P) 데이터 변조를 한다. 이때, 데이터 변조는 양자 신호 펄스에만 적용된다. 위의 두 단계를 거쳐 LO와 양자 신호는 양자 채널을 지나 Bob에게 전달된다. Bob에 도착하는 광 펄스들은 앞서 생성된 LO와 양자 신호의 시간 간격에 해당하는 τ의 광로차를 갖는 비대칭 마이컬슨 간섭계를 지나 검출된다. 시분할 직교 호모다인 검출이 이루어지기 위해 수신부 간섭계 내부 광 경로차에 의한 위상 차이, δ를 45°로 일정하게 제어한다. 실제 시스템에서는 편광 흔들림에 무관하도록 마이컬슨 간섭계를 사용하지만, 다음 항부터는 내용의 이해를 돕기 위해 마하-젠더 간섭계를 통해 설명한다.

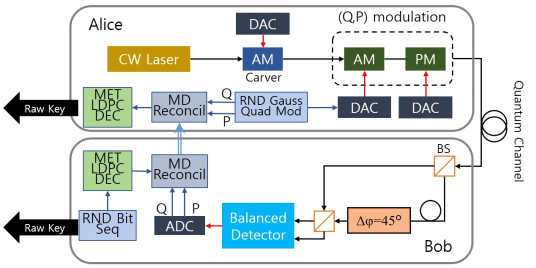

그림 1. 시분할 직교 호모다인 검출을 이용한 연속변수 양자암호키분배 시스템. CW Laser, 연속파 레이저; AM, 광 진폭 변조기; PM, 광 위상 변조기; DAC, 디지털 아날로그 변환기; ADC, 아날로그 디지털 변환기; BS, 빛살 가르개.
Fig. 1. CV QKD system with TDQHD. CW laser, continuous wave laser; AM, amplitude modulator; PM, phase modulator; DAC, digital to analog converter; ADC, analog to digital converter; BS, beam splitter.

2.2 시분할 직교 호모다인 검출

이 절에서 우리는 양자 이론을 이용하여 시분할 직교 호모다인 검출을 설명한다. 시분할 직교 호모다인 검출은 Alice가 전송한 하나의 양자 신호에 대해 두 개의 연속적인 호모다인 검출로 정의된다. 간섭계를 통과하기 전 세 개의 광신호 펄스를 표현하는 필드 연

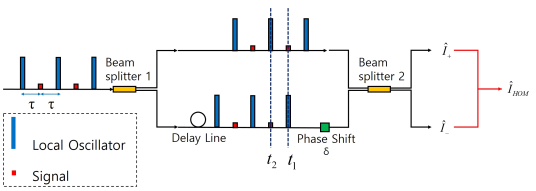

그림 2. 수신부에서 LO와 양자 신호 펄스의 동작. 비대칭 간섭계는 시간 τ에 해당하는 지연 길이를 가지며 광 경로차에 따른 위상 차이는 위상 편이 δ로 나타냄.
Fig. 2. The characterization of LO and signal pulses in receiver. The asymmetric interferometer has a delay line corresponding to time τ, and the phase difference according to the optical path difference is represented by the phase shift δ.

산자를 다음과 같이 정의한다.

$$\hat{E} = \hat{a}_{LO}e^{iwt} + \hat{a}_S e^{iw(t-\tau)} + \hat{a}_{LO}e^{iw(t-2\tau)}. \quad (1)$$

위 식에서 $\hat{a}_{LO}$와 $\hat{a}_S$는 LO와 양자 신호 펄스의 소멸 연산자를 나타낸다. 식(1)의 필드 연산자는 그림 2의 첫 번째 빛살 가르개(beam splitter, BS)를 지나 두 개의 필드 연산자로 나눠진다.

$$\hat{E}_u = \frac{i}{\sqrt{2}}(\hat{a}_{LO}e^{iwt} + \hat{a}_S e^{iw(t-\tau)} + \hat{a}_{LO}e^{iw(t-2\tau)}), \quad (2)$$

$$\hat{E}_l = \frac{1}{\sqrt{2}}(\hat{a}_{LO}e^{iwt} + \hat{a}_S e^{iw(t-\tau)} + \hat{a}_{LO}e^{iw(t-2\tau)}). \quad (3)$$

위 식에서 $\hat{E}_u$와 $\hat{E}_l$은 간섭계의 위팔과 아래팔을 지나는 필드 연산자를 나타낸다. 그리고 아래팔에서는 LO와 양자 신호가 간섭하게 만드는 시간 τ에 해당하는 지연과 광 경로차에 의한 위상 차이, δ를 적용한 필드 연산자를 아래와 같이 새로 정의한다.

$$\hat{E}_l' = \frac{1}{\sqrt{2}}(\hat{a}_{LO}e^{i(w(t-\tau)+\delta)} + \hat{a}_S e^{i(w(t-2\tau)+\delta)} + \hat{a}_{LO}e^{i(w(t-3\tau)+\delta)}). \quad (4)$$

두 번째 BS를 통해 나온 간섭계 출력은 LO와 양자 신호는 간섭으로 만들어지며 이 간섭 신호는 균형 검출기를 통해 검출된다. 균형 검출기는 보강 간섭 신호를 검출하는 (+)광다이오드의 전류와 상쇄 간섭 신호를 검출하는 (-)광다이오드의 전류의 차이를 최종적으로 출력한다.

시간 $t_1\,(t=\tau)$에서 (+)전류와 (-)전류 그리고 최종 출력 전류를 살펴보자. (+)전류는 아래 식과 같이 나타낼 수 있다.

$$\begin{aligned}\hat{I}_+ &= \frac{q}{4T}(\hat{a}_S + \hat{a}_{LO}e^{i\delta})^\dagger(\hat{a}_S + \hat{a}_{LO}e^{i\delta}) \\ &= \frac{q}{4T}(\hat{a}_S^\dagger\hat{a}_S + \hat{a}_{LO}^\dagger\hat{a}_{LO} + \hat{a}_S^\dagger\hat{a}_{LO}e^{i\delta} + \hat{a}_{LO}^\dagger\hat{a}_S e^{-i\delta}).\end{aligned} \quad (5)$$

위 식에서, q는 전자의 전하량을 나타내며, T는 검출기 대역폭을 시간 주기로 나타낸 것이다. 마찬가지로 시간 $t_1\,(t=\tau)$에서 (-)전류를 구할 수 있다.

$$\begin{aligned}\hat{I}_- &= \frac{q}{4T}(\hat{a}_S^\dagger\hat{a}_S + \hat{a}_{LO}^\dagger\hat{a}_{LO} \\ &\quad - \hat{a}_S^\dagger\hat{a}_{LO}e^{i\delta} - \hat{a}_{LO}^\dagger\hat{a}_S e^{-i\delta}).\end{aligned} \quad (6)$$

균형 검출을 통한 시간 $t_1\,(t=\tau)$에서 차동 출력 전류는 식(4)와 식(5)의 차이로 구할 수 있다.

$$\begin{aligned}\hat{I}_{t_1} &= \hat{I}_+ - \hat{I}_- \\ &= \frac{q}{2T}(\hat{a}_S^\dagger\hat{a}_{LO}e^{i\delta} + \hat{a}_{LO}^\dagger\hat{a}_S e^{-i\delta}).\end{aligned} \quad (7)$$

이때, LO는 고전적 상태로 간주할 수 있으므로 소멸 연산자를 LO의 진폭으로 대신 쓸 수 있다.

$$\begin{aligned}\hat{I}_{t_1} &= \hat{I}_+ - \hat{I}_- \\ &= \frac{q}{2T}(\hat{a}_S^\dagger A_{LO}e^{i\delta} + A_{LO}\hat{a}_S e^{-i\delta}) \\ &= \frac{qA_{LO}}{2T}[\cos\delta(\hat{a}_S + \hat{a}_S^\dagger) - i\sin\delta(\hat{a}_S - \hat{a}_S^\dagger)].\end{aligned} \quad (8)$$

위의 식은 연속변수 양자암호키분배에서 사용되는 $\hat{q} = (\hat{a}_S + \hat{a}_S^\dagger)/2$ 와 $\hat{p} = (\hat{a}_S - \hat{a}_S^\dagger)/2i$의 직교 연산자를 사용하여 다시 표현할 수 있다.

$$\hat{I}_{t_1} = \frac{qA_{LO}}{T}[\cos\delta\,\hat{q} - \sin\delta\,\hat{p}]. \quad (9)$$

마찬가지로, 시간 $t_2\,(t=2\tau)$에서 차동 출력 전류를 구할 수 있다.

$$\hat{I}_{t_2} = \frac{qA_{LO}}{T}[\cos\delta\,\hat{q} + \sin\delta\,\hat{p}]. \quad (10)$$

최종 출력 전류는 간섭계의 위팔과 아래팔의 광 경로차에 따른 위상 차이 값, δ에 따라서 달라진다. 측정된 값을 통해 헤테로다인 검출과 같이 우리가 일반적으로 사용하는 (Q, P)변조값을 얻으려면 δ는 45°로 고정되어야 하며 이때, 시간 t_1과 시간 t_2에서의 출력 전류는 다음과 같다.

$$\hat{I}_{t_1} = \frac{qA_{LO}}{T\sqrt{2}}(\hat{q}-\hat{p}), \tag{11}$$

$$\hat{I}_{t_2} = \frac{qA_{LO}}{T\sqrt{2}}(\hat{q}+\hat{p}). \tag{12}$$

따라서 각 시간에서 검출한 출력 전류의 합과 차를 통해 Q 직교 좌표의 변조값과 P 직교 좌표의 변조값을 식(10)으로부터 구할 수 있으며, 시분할을 통한 직교 호모다인 검출이 헤테로다인 검출과 동일한 결과를 얻을 수 있음을 확인할 수 있다.

$$\hat{I}_{t1} + \hat{I}_{t_2} = \frac{qA_{LO}}{T\sqrt{2}}\hat{q}, \tag{13}$$

$$\hat{I}_{t1} - \hat{I}_{t_2} = \frac{qA_{LO}}{T\sqrt{2}}\hat{p}. \tag{14}$$

Ⅲ. 시분할 직교 호모다인 검출의 무한키 조건 보안성 분석

GMCS 프로토콜에 기반한 세 가지 연속변수 양자암호키분배 시스템을 비교한다. 그림 3은 호모다인, 직교 호모다인, 그리고 시분할 직교 호모다인 검출을 이용한 연속변수 양자암호키분배 시스템의 수신부 회로도를 나타낸다.

그림 3(a)의 호모다인 검출 시스템은 하나의 호모다인 간섭계로 LO의 위상을 0° 또는 90°로 무작위 변조시켜 Q 직교 변조값과 P 직교 변조값을 얻는다. 그림 3(b)의 직교 호모다인 검출 시스템의 경우, 수신광을 직교하는 편광으로 분리하여 두 개의 호모다인 간섭계로 Q 직교 변조값과 P 직교 변조값을 얻는다. 그림 3(c)의 시분할 직교 호모다인 검출 시스템은 임의의 LO 위상 변조 없이 비대칭 간섭계 내의 광 경로차에 의한 위상 차이 δ를 45°로 고정해 하나의 양자신호에 대해 두 개의 연속적인 호모다인 검출을 수행하여 (Q, P) 변조값을 얻는다.

무한키 조건에서 역방향 조정 (reverse reconciliation)을 사용한 비밀키 생성률 K_R은 다음과 같다.

$$K_R = \beta I_{AB} - \chi_{EB}. \tag{15}$$

여기서 β는 조정 효율 (reconciliation efficiency), I_{AB}는 Alice와 Bob 사이의 상호정보량 그리고 χ_{EB}는

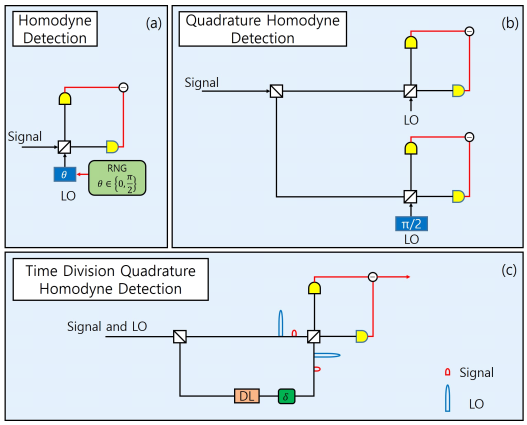

그림 3. (a)호모다인 검출, (b)직교 호모다인 검출 그리고 (c)시분할 직교 호모다인 검출의 수신부 회로 비교.
Fig. 3. Schematic comparison of receiver with (a)HD (b)QHD and (c)TDQHD.

도청자(Eve)와 Bob 사이의 Holevo 한계를 나타낸다.

Alice와 Bob 사이의 상호정보량은

$$I_{AB} = \log_2(1+SNR) = \log_2\left(1+\frac{\frac{1}{2}T_t V_A}{1+\frac{\xi}{2}}\right), \tag{16}$$

Eve와 Bob 사이의 Holevo 한계값은

$$\chi_{EB} = S_E - S_{E|B}, \tag{17}$$

로 주어진다. 여기서 T_t는 검출기 효율을 포함한 전체 전송률, V_A는 Alice의 변조 분산, ξ는 초과 잡음 (excess noise), S는 폰노이만 엔트로피를 나타낸다. 비밀키 생성률의 자세한 계산[8, 9]을 참고한다.

이제 제안한 방식의 성능을 확인하기 위해 앞서 살펴본 GMCS 프로토콜을 기반으로 비밀키 전송률을 비교해 볼 것이다. 수신기의 SNU (shot noise unit)를 기준으로 측정되는 변조 분산 V_A는 광섬유 길이에 따라 정해지는 채널 손실에 대하여 비밀키 전송률이 최대화되도록 최적화 되었으며, 조정 효율 β는 97%, 초과 잡음 ξ는 0.01 SNU로 설정하였다. 그림 4는 무한키 조건에서 얽힘 복제 공격에 대한 비밀키 전송률을 세 가지 검출 방식에 대하여 비교하는 그래프이다. 시분할 직교 호모다인 검출은 직교 호모다인과 마찬가지로 기존 호모다인 검출 방식과 비교해 향상된 비밀키 생성률을 가지며, 특히 20km 내에서 좋은 효율을 보여 단거리 보안통신에 적합한 해결책이 될 수 있다.

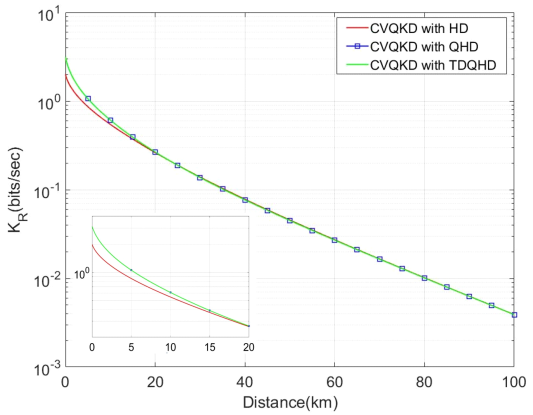

그림 4. 무한키 조건에서 얽힘 복제 공격에 대한 호모다인 검출(붉은선), 직교 호모다인 검출(파란색 네모) 그리고 시분할 직교 호모다인 검출(초록선) 방식의 비밀키 생성률 비교.
Fig. 4. Comparison of asymptotic secret key rate against Entangling Cloner Attack with HD(red curve), QHD(open blue square) and TDQHD(green curve).

Ⅳ. 결 론

본 논문에서는 시분할 직교 호모다인 검출을 이용하여 단일 호모다인 간섭계에서 두 직교 기저를 한꺼번에 측정할 수 있는 실용적인 연속변수 양자암호키 분배 방식을 제안하였다. 제안한 시분할 직교 호모다인 검출은 기존 호모다인 검출과 비교하여 대부분의 범위에서 암호키 전송률을 향상한다. 또한, 시스템을 구현하는 관점에서, 호모다인 검출을 이용한 연속변수 양자암호키분배 시스템과 비교하였을 때, 필수적인 무작위 기저 선택 과정을 제거할 수 있고 헤테로다인 검출을 이용한 양자암호키분배 시스템과 비교하였을 때, 편광 BS 등과 같은 편광 제어에 필요한 부품이 필요 없어 시스템을 단순화 할 수 있다. 이러한 장점을 통해 제안한 시분할 직교 호모다인 검출 시스템은 저가형 양자암호키분배 시스템에 적합한 효율적인 해결 방법이 될 수 있다.

Reference

[1] K. Cho, "Ultra-precision measurements using interferometers and their applications," *New Physics: Sae Mulli*, vol. 70, no. 3, pp. 199-211, Mar. 2020.

[2] C. Wittmann, J. Furst, C. Wiechers, D. Elser, D. Sych, and G. Leuchs, "Quantum key distribution with heterodyne detection," *CLEO/Europe-EQEC 2009*, Munich, Germany, Aug. 2009.

[3] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Physical Rev. Lett.*, vol. 88, no. 5, p. 057902, Jan. 2002.

[4] X.-C. Ma, S.-H. Sun, M.-S. Jiang, and L.-M. Liang, "Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol," *Physical Rev. A*, vol. 87, no. 5, p. 052309, May 2013.

[5] J.-Z. Huang, Z.-Q. Y. Christian Weedbrook, H.-W. L. Shuang Wang, W. Chen, and Z.-L. H. Guo Cong Guo, "Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack," *Physical Rev. A*, vol. 87, no. 6, p. 062329, Jun. 2013.

[6] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, "Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution," *Physical Rev. A*, vol. 87, no. 6, p. 062313, Nov. 2013.

[7] J.-Z. Huang, S. Kunz-Jacques, P. Jouguet, C. Weedbrook, Z.-Q. Yin, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, "Quantum hacking on quantum key distribution using homodyne detection," *Physical Rev. A*, vol. 89, no. 3, p. 032304, May 2014.

[8] J. Lodewyck, M. Bloch, R. Garcia-Patron, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, "Quantum key distribution over 25 km with an all-fiber continuous-variable system," *Physical Rev. A*, vol. 76, no. 4, p. 042305, Oct. 2007.

[9] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, "Continuous-variable quantum key distribution with Gaussian modulation—the theory of practical implementations," *Advanced Quantum Technol.*, vol. 1, no. 1, p. 1800011, Jun. 2018.

오 준 상 (Junsang Oh)

2014년 8월 : 한국과학기술원 전기및전자공학부 학사
2016년 8월 : 한국과학기술원 전기및전자공학부 석사
2016년 9월~현재 : 한국과학기술원 전기및전자공학부 박사과정

<관심분야> 양자암호통신, 양자컴퓨팅, 양자기계학습

[ORCID:0000-0002-1769-7911]

임 경 천 (Kyongchun Lim)

2012년 2월 : 성균관대학교 전자전기컴퓨터공학과 학사
2014년 2월 : 한국과학기술원 전기및전자공학부 석사
2019년 2월: 한국과학기술원 전기및전자공학부 박사
2019년 3월~현재 : 한국전자통신연구원 양자광학 연구실 선임연구원

<관심분야> 양자통신, 양자 암호키 분배, 양자 정보 이론

이 준 구 (June-Koo Kevin Rhee)

1988년 2월 : 서울대학교 전기공학과 공학학사
1990년 8월 : 서울대학교 전기공학과 이학석사
1995년 8월 : Univ. of Michigan Electrical Engineering, 박사
2005년 3월~현재 : KAIST 전기및전자공학부 부교수, 정교수

<관심분야> 양자컴퓨팅, 양자통신, 양자기계학습, 광통신

[ORCID:0000-0001-7151-017X]