시분할 직교 호모다인 검출을 이용한 연속변수 양자암호키분배

오준상 [1], 임경천 [2], 이준구 [1]*

[1] KAIST, 전기및전자공학부

[2] ETRI, 양자광학연구실

js.oh@kaist.ac.kr, lim.kc@etri.re.kr, rhee.jk@kaist.ac.kr

요 약

연속변수 양자암호키분배 (Continuous-Variable Quantum Key Distribution - CVQKD) 시스템에서 직교 호모다인 검출 (Quadrature Homodyne Detection - QHD)은 기존의 CVQKD 호모다인 검출과 비교하여 암호키 전송 속도를 향상시킬 수 있다. 본 논문에서는 시분할 직교 호모다인 검출 체계를 제안하여 단일 호모다인 간섭계에서 두 개의 직교하는 기저에 대한 검출을 시분할 방식으로 동시에 측정는 방버을 제시한다. 더불어 제안하는 검출 방식은 실제 시스템을 구현하는데 있어, 기존 호모다인 검출의 기저 선택을 위해 사용하는 랜덤 위상 변조가 필요 없으며, 수신부가 편광 의존성이 없어 편광 제어가 필요하지 않다.

Ⅰ. 서 론

연속변수 양자암호키분배에서 송신자는 결맞음상태 레이저 광원 (Coherent Laser Source) 을 이용하여 수 개의 평균 광자 수를 갖는 펄스를 전송하고 수신자는 검출 효율이 높은 호모다인 검출을 통하여 이를 측정하기 때문에 높은 암호키 전송률에 접근하는 효율적인 방법으로 간주되었다. 또한 2011 년 제안된 Multi-Dimensional Reconciliation 방식[1]을 이용하여 후처리 효율을 96% 이상으로 올리면서 100km 이상의 거리에서도 암호 통신이 가능하게 하였다. 이러한 장점들 때문에 연속변수 양자암호키분배는 높은 상용화 가능성을 갖는다고 판단되며 활발한 연구가 진행되고 있다. CVQKD 에서 헤테로다인 검출 (Heterodyne Detection) [2], 즉 직교 호모다인 검출 (QHD) 방식은 직교하는 편광을 분할하여 2 개의 광 간섭계를 통해 직교하는 두 기저에 대한 측정을 함으로써 암호키 전송률을 높일 수 있다. 이 시스템 실제 구현하기 위해서는 빛의 편광 제어가 중요하고 두 개의 간섭계가 필요한데, 본 논문에서는 편광 흔들림에 무관한, 단일 간섭계만으로 구성된 새로운 시분할 (time-division) QHD (TDQHD) 검출 방식을 소개한다.

Ⅱ. 시분할 직교 호모다인 검출 (TDQHD) 방법

본 논문에서는 시분할 송수신 방법에 기반하여 기존의 직교 호모다인 검출 방식과 동일한 효과를 갖는 새로운 CVQKD 검출 방식을 소개한다. CVQKD 채널은 기존 GMCS(Gaussian Modulation Coherent State) 프로토콜[2]을 기반으로 한다. 그림 1 은 시분할 직교 호모다인 검출 (TDQKD) 방식 실험의 개략적인 설계를 나타낸다. 양자 신호와 국부 발진 신호 (LO)는 동일한 레이저로부터 변조기를 지나 동일한 시간 간격 τ 로 인터리빙된다. 수신부에서 별도의 국부 발진 신호를 사용하지 않을 경우에 대한 Eve 의 공격을 분석한 논문들이 있지만[3-6], 본 논문에서는 개념적인 설명을 위해 이를 고려하지 않겠다.

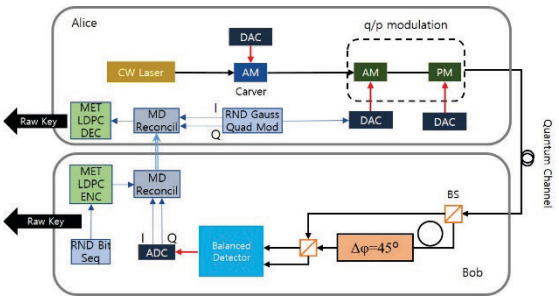

그림 1. 도식화한 시분할 직교 호모다인 검출 연속변수 양자암호키분배 시스템. AM, amplitude modulator; PM, phase modulator; DAC, digital to analog converter; ADC, analog to digital converter; BS, beam splitter 를 나타낸다.

Alice는 두 단계를 거쳐 신호를 Bob에게 전송한다. 먼저, Alice 는 carver 역할을 하는 첫번째 진폭 변조기를 통해 양자 신호 펄스와 국부 발진 (LO) 펄스를 차례대로 생성한다. 이때, 양자 신호는 *q/p* quadrature 변조 값을 가지지 않는다. 두번째 단계에서는, 진폭 변조기와 위상 변조기를 통해 양자 신호 펄스에만 *q/p* 변조를 적용한다. 변조된 양자 신호와 국부 발진 신호는 같은 양자 채널을 지나 Bob 에게 전달된다. Bob 에게 도착한 신호들은 양자 신호와 국부 발진 신호 간격에 해당하는 지연을 갖는

간섭계를 통과하여 검출된다. 이 때, 간섭계 내부의 위, 아래 광로를 지나는 신호 간 위상 차이는 일정하게 유지되어야 한다. 실제 실험에서는 균형 검출기에서 검출되어 나온 전기 신호를 통해 간섭계와 검출기 간 피드백 회로를 구성하여 일정하게 유지시킨다.

제안한 방식에서는, 하나의 양자 신호에 대하여 2 번의 검출 결과가 나오며, 이는 간섭계 내부의 위상차를 δ라 하였을 때, 다음과 같은 전류 오퍼레이터를 얻는다.

$$\hat{I}_{t_1} = \frac{qA_L}{\tau}[\cos\delta\,\hat{q} - \sin\delta\,\hat{p}],$$

$$\hat{I}_{t_2} = \frac{qA_L}{\tau}[\cos\delta\,\hat{q} + \sin\delta\,\hat{p}]. \qquad (1)$$

q는 전하량, A_L는 국부 발진 신호 크기, $\hat{q}$, $\hat{p}$ 는 quadrature operator를 나타낸다. 이 때, 헤테로다인 검출과 동일한 효과를 갖기 위해서 간섭계 위상차 $\delta = 45°$ 가 되어야하며 해당 경우의 암호키 전송률을 무한한 키에 대해서 기존의 호모다인 검출과 헤테로다인 검출과 비교해보았다.

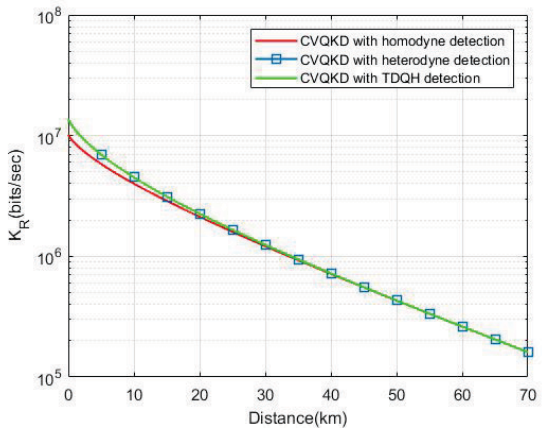

그림 2. 호모다인 검출(빨간색), 직교 호모다인 검출(파란색과 사각형), 및 시분할 직교 호모다인 검출(녹색)에 대한 암호키 전송률 비교, 전송하는 신호의 파워는 각 거리별로 최적화하였으며, 후처리 효율은 97%, 추가 잡음은 0.01(Shot Noise Unit)으로 설정하였다.

Ⅲ. 결론

본논문에서는 시분할 직교 호모다인 검출을 이용하여 단일 호모다인 간섭계에서 두 직교 기저를 동시에 측정할 수 있는 실용적인 연속변수 양자암호키분배 방식을 제안하였다. 제안한 시분할 직교 호모다인 검출은 기존 호모다인 검출과 비교하여 대부분의 범위에서 암호키 전송률을 향상시킨다. 또한 시스템을 구현하는 입장에서는, 호모다인 검출을 이용한 연속변수 양자암호키분배 시스템과 비교하였을 때, 필수적인 무작위 기저 선택 과정을 제거할 수 있고 헤테로다인 검출을 이용한 양자암호키분배 시스템과 비교하였을 때, 편광 빔스플리터 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 답안이 될 수 있다.

ACKNOWLEDGMENT

"본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학 ICT 연구센터지원사업의 연구결과로 수행되었음" (IITP-2020-2015-0-00385)

참 고 문 헌

[1] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor and P. Grangier, "Multidimensional reconciliation for a continuous-variable quantum key distribution," Physical Review A, vol. 77, no. 4, Apr. 2008.

[2] C. Wittmann, J. Furst, C. Wiechers, D. Elser, D. Sych, and G. Leuchs, "Quantum Key Distribution with Heterodyne Detection," CLEO/Europe - EQEC 2009 - European Conference on Lasers and Electro-Optics and the European Quantum Electronics Conference, 2009.

[3] F. Grosshans and P. Grangier, "Continuous Variable Quantum Cryptography Using Coherent States," Physical Review Letters, vol. 88, no. 5, 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 Review A, vol. 87, no. 5, Sep. 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 Review A, vol.87, no. 6, June, 2013.

[6] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, "Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution," Physical Review A, vol. 87, no. 6, 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 Review A, vol. 89, no. 3, May 2014.