연속 변수를 이용한 양자 키 분배 시스템의 보안성 증폭

이선의*, 김진영*

Privacy Amplification of Quantum Key Distribution Systems Using Continuous Variable

Sun Yui Lee*, Jin Young Kim*

요 약

연속 양자 변수를 이용한 QKD 시스템은 높은 키 생성률을 보장하는 실질적인 솔루션으로 고려되어져 왔다. 불연속 QKD 시스템과 연속 변수 QKD 시스템의 차이를 설명한다. 연속 변수가 불확정성의 원리를 만족하는 이론을 설명하고 이를 검출하기 위한 호모다인 검출기의 원리를 설명한다. 이를 이용하여 QKD시스템에서 비밀키의 길이가 변화는 과정을 설명하고 보안성 증폭을 위하여 노출되는 키의 정보량을 알아본다.

Key Words : QKD(Quantum Key Distribution), CV-QKD(Continuous Variable QKD), DV-QKD(Discrete Variable QKD) , Homodyne detector.

ABSTRACT

The continuous variable quantum key distribution has been considered to have practical solution to provide high key rate. This paper explains the difference between DV-QKD and CV-QKD schemes. It describes CV-QKD as a theory that satisfies the uncertainty principle using continuous variable and homodyne detector. We shows varying length of secret key in QKD systems and amount of the exposed information to amplify privacy.

I. 서 론

연속 변수(Continuous Variable)를 사용한 양자 키 분배(Quantum Key Distritbution) 시스템은 높은 모듈레이션 성능과 검출 속도를 가지고 있어 양자 통신의 실용적인 연구 분야로 주목 받고 있다. 불연속 양자 변수를 사용하는 시스템은 single photon 발생 시키고 측정해야 하기 때문에 기술적으로 극복해야할 문제들이 많지만 연속 변수는 레이저 빔의 진폭 및 위상을 사용하여 구현이 쉬운 장점이 있다.

이와 같은 연속 변수 양자 모델은 squeezed states[1] 또는 entangled states[2], coherent states[3]를 사용한다. squeezed states와 entangled states는 양자 채널에서의 노이즈에 매우 민감하기 때문에 장거리 양자 정보 통신에서는 coherent states가 더 적합하다. 이와 같이 연속 양자 변수 모델은 양자 채널의 노이즈에 민감하기 때문에 다양한 개선 방법이 연구되어 왔다[4]. 또한 coherent states를 이용한 진폭과 위상 정보를 인코딩하여 실험한 다양한 연구가 진행되고 있다[5].

single photon을 사용한 시스템과 달리 양자 관성 노이즈를 활용하여 도청자로부터 정보를 보호한다[6]. 하지만 이와 같은 특징으로 인하여 서로 공증된 사용자간의 노이즈를 유발한다. 이 에러를 보정하기 위하여 기존의 에러 정정 부호를 사용하는 데 전송자 엘리스와 수신자 밥 사이의 에러를 정정할 수 있고 일부 정보를 도청자인 이브로부터 비밀키를 보존할 수 있다. 양자 키 분배 시스템에서는 두 통신자 사이의 에러를 정정할 수 있고 도청자가 에러 정정 후의 정보를 모르게 할 수 있다. 본 논문에서는 에러 정정 후의 보안성 증폭을 위하여 엘리스와 밥 그리고 이브간의 정보량의 조건을 비교한다. 또한 연속 변수 양자 키 분배 방식의 과정을 살펴본다.

※본 연구는 미래창조과학부 및 정보통신기술진흥센터의 정보통신·방송 연구개발사업의 일환으로 수행하였음. [1711028311, 양자암호통신망 구축을 통한 신뢰성 검증기술 및 QKD 고도화를 위한 핵심요소기술 개발]

*광운대학교 전파공학과 소속 유비쿼터스 통신 연구실(sunyuil22@naver.com), (jinyoung@kw.ac.kr)

접수일자 : 2016년 7월 13일, 수정완료일자 : 2016년 8월 9일, 최종게재확정일자 : 2016년 8월 30일

Ⅱ. 본론

연속 변수를 이용한 양자 키 분배 프로토콜은 대표적으로 coherent states를 이용하여 기저를 선택하는 방식이 있다. 이 과정은 먼저 전처리 단계로 가우시안 분포의 임의의 수 X_A, P_A를 정하고 각각 진폭과 위상으로 모듈레이션을 수행한다. 그림 1은 진폭과 위상을 이용한 양자 상태를 전송하는 것을 나타낸다. 이 신호는 $|X_A + iP_A>$으로 송신자가 결맞는 상태를 수신자에게 보낸다. 수신자는 임의로 X또는 P의 쿼드러처 값을 선택하여 특정한다. 도청이 가능한 일반 채널을 통하여 일반 통신 방식으로 수신자가 진폭과 위상 중 선택한 측정 순서를 송신자에게 알려주고 관계없는 데이터를 버리게 된다.

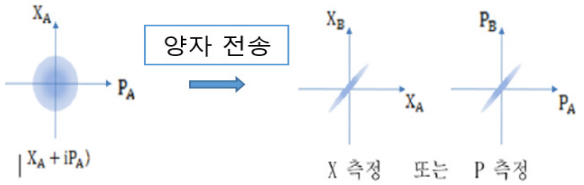

그림 1. 연속 변수를 이용한 양자 상태 전송
(X : 진폭, P 위상)

양자의 물리적 성질에 의해서 진폭을 측정하게 되면 위상에 대한 정보를 버리게 되기 때문에 보안성을 보장할 수 있게 된다. 이 과정을 마친 후의 송수신자간에 Gaussian Variable을 공유한 것들 중에 임의의 변수를 골라 sifted key로 사용하여 비교한다. 임의의 변수를 교환해 sifted key를 비교하여 에러율과 양자 채널의 전송 효율을 계산하게 된다. 이 정보 정제 과정을 거친 비트들을 에러 정정 기법으로 오류를 정정하고 비밀성 증폭을 수행한다.

Ⅲ. 호모다인 검출기

Homodyne detector는 양자 광학 장치의 하나로 연속 변수를 측정할 수 있는 장치이다. 여기서 쿼드러처 연산자는 조화 진동자의 생성 연산자와 소멸 연산자의 선형 결합을 말한다. 이 장치에서 입력 신호 (결맞는 상태의 약한 신호 펄스; a) 는 빛 가르개 (beam splitter) 의 도움으로 강한 기준 펄스 (local oscillator field; aL) 와 중첩된다. 빛 스플리터의 두 출력 모드 (d1, d2) 는 두 광 검출기 (photodetector; D1, D2) 가 측정한다. 결과적으로 광전류(photocurrent)는 두 광 검출기의 차이가 되고, 우리가 측정할 수 있는 신호는 두 출력 모드 (d1, d2) 에 있는 광자 수의 차이에 비례한다. CV-QKD 프로토콜의 첫 번째 단계는 송신자가 송신할 데이터를 부호화(encoding) 하는 것이다. 즉, 임의의 수 발생기 (RNG; random number generator) 로부터 가우시안 분포로 만들어진 임의의 수 (연속 변수) 를 위상 변조기 (phase modulator) 및 진폭 변조기 (amplitude modulator) 에 적용한다. 각각의 변조기는 신호 펄스의 위상 쿼드러처 및 진폭 쿼드러처 성분을 매우 약하게 변조해 준다. 이렇게 약하게 변조된 신호 펄스를 (강한 기준 펄스와 함께) 양자 채널을 통해 수신자에게 보낸다. 그래서 송신자는 임의의 연속 변수 데이터를 약한 레이저 펄스 (결맞는 상태) 에 실어서 양자 채널을 통해 수신자에게 보내는 것이다. 그러면 수신자는 균등 (balanced) 호모다인 검출기로, 위상 쿼드러처 성분 또는 진폭 쿼드러처 성분의 연속 변수 값 둘 중 하나를 임의로 측정한다. 따라서 결국 수신자는 자신이 측정한 변수를 송신자와 공유하게 되는 것이다. 이러한 과정이 호모다인 검출기를 이용해 진행되는데, 그림 2에서 그것을 보여주고 있다.

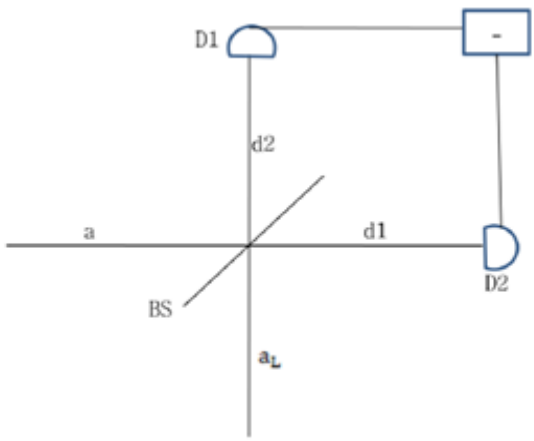

그림 2. 호모다인 검출기

Ⅳ. 키 교환

기존의 싱글 포톤을 이용한 QKD 시스템은 광자의 편광을 이용하여 키를 교환한다. 수직, 수평인 편광과 45도, 135도 편광을 이용하여 구분된 기저를 통하여 양자 채널을 통하여 광자를 전송하고 송수신자는 이 광자를 빔스플리터를 이용하여 측정한 후 큐비트를 판단한 후 일반 도청가능한 통신 채널을 통하여 서로 광자의 기저를 판단한 정보를 교환하게 된다. 만약 다른 기저로 판단한 정보가 있으면 모두 버리게 되고 같은 기저를 사용하여 측정하였지만 비트가 다른 정보를 통하여 도청자의 유무를 판단하게 된다. 이를 통하여 양자 통신의 보안성을 보장할 수 있다. 왜냐하면 도청자는 송수신자가 임의로 선택한 광자의 편광을 알 수 없기 때문에 광자를 중간에 가로채어 측정한 후 재 전송하게 되면 필연적으로 50%의 확률로 잘못된 정보를 전송하게 된다. 연속 변수를 사용한 QKD 시스템도 이와 유사한 방식으로 키 교환을 실시한다. 송신자는 그림 2와 같이 위상 및 진폭의 연속 변수에 임의의 정보를 실어서 보내게 되고 수신자는 둘 중 하나의 기저를 선택하여 측정하게 된다.

퀴드러처 진폭의 이상적인 측정값이 생성하는 SNR. (Signal-to-noise)은 식 1과 같다.

$$(S/N)^{\pm} = \frac{V_s^{\pm}}{V_n^{\pm}}, \qquad (1)$$

동시에 위상과 진폭을 모두 측정하게 되는 경우의 식 2를 초과하는 SNR을 얻을 수 없게 된다.

$$(S/N)_{\sim}^{\pm} = \left(\frac{\eta^{\pm} V_s^{\pm}}{\eta^{\pm} V_n^{\pm} + \eta^{\mp} V_m^{\pm}} \right) S/N^{\pm}, \qquad (2)$$

여기서 $V_s^{\pm}$와 $V_n^{\pm}$는 각각 광신호 캐리어의 관련된 주파수의 진폭(+)과 위상(-)의 신호와 잡음 파워이다. $V_m^{\pm}$은 위상과 진폭을 분리할 때 발생하는 피할 수 없는 양자 잡음이다. $\eta^{\pm}$는 스플리터 비율로 50:50의 빔스플리터를 예로 들면 $\eta^{+} = \eta^{-} = 0.5$ 이다.

Coherent 광신호의 QNL(Quantum Noise Limit)에 대한 일반화된 스펙트럼 파워는 $V_n^{\pm} = 1$ 이다. 양자 통신에서 사용하는 Coherent 광신호는 스플리터 비율이 0.5일 경우 두 위상과 진폭에 SNR은 반드시 시스템에 영향을 미친다. The Hartley- Shannon law에 따르면 만약 고정된 대역폭에서의 정보가 대응하는 비율의 채널 용량과 SNR이 감소된 통신 채널에서 전송중이라면 에러는 필연적으로 수신기에 나타난다 [7]. 그러므로 양자 연속 변수를 사용하는 CV-QKD 시스템에서의 키 교환은 위와 같은 특성을 바탕으로 도청자에 의한 위상과 진폭의 동시 측정은 전송에 에러를 발생시키기 때문에 보안성이 보장된다.

Ⅴ. Key Sifting

초기의 키 교환을 마치고 부터는 Key Sifiting은 일반 통신 채널을 통하여 정보 교환이 이루어 진다. 양자 채널을 통과한 큐비트 정보는 레이저와 같은 광자를 주로 이용한 광학 장치를 통해 정보를 교환한다. 이 초기 키를 가지고 일반 채널을 통하여 수신자가 측정한 기저 정보를 송신자에게 전달하여 키를 걸러내게 된다. 송신자가 전달받은 측정 정보를 이용하여 일치하지 않는 정보를 버린다. 그림 3은 양자 채널을 통한 정보가 어떻게 달라지는 지를 보여준다. 양자 채널을 통하여 큐비트를 전송하는 과정인 초기 키 교환을 보면 손실이 있는 채널을 나타낸 점선을 통과한 양자 정보는 상당한 손실이 있는 것을 알 수 있다. 그리고 이 손실을 뺀 정보를 통하여 초기 키를 얻게 되고 여기서 일반 채널은 굵은 실선으로 일반 채널을 나타낸다. 키의 길이를 보면 키 정보를 송수신자가 같은 기저로 측정한 것만 남기고 나머지를 버리기 때문에 약 절반 정도의 sifted key 만이 남게 된다.

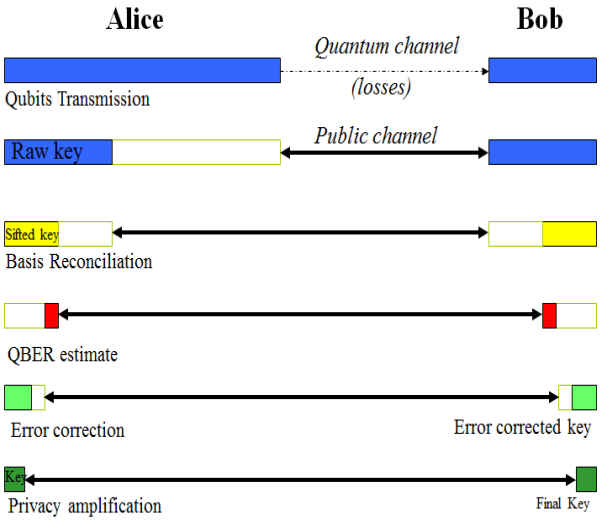

그림 3. QKD 시스템의 비밀키 생성 과정 및 키 길이 변화

Ⅵ. 에러 정정 및 보안성 증폭

분별해낸 sifted key가 송수신자 양쪽에 동일하면 그대로 비밀키(secret key)로 직접 사용할 수 있다. 하지만 양자 채널을 통과하여 손실되고 측정한 기저가 달라 버려진 부분과 도청으로 유발된 에러까지 고려하게 되면 확인해 보기 전에는 알 수 없다. 이를 확인하기 위하여 키의 일부분을 일반 공용 채널을 통하여 교환하게 된다. 이는 에러율을 확인하는데 이용하지게 되지만 공용 채널을 통했기 때문에 확인 후에 버리게 되는 비트이다. 도청자가 측정 후 재전송을 통하여 발생시킨 에러도 QKD 시스템에는 포함되기 때문에 전체 에러율을 측정하기 위해서 교환하게 되는 키의 길이를 최소화하는 것이 중요하다. 이 공개되어 버리는 비트들로 QBER(Qubit Bit Error rate)을 계산하여 일정 기준을 초과하게 되면 도청자가 많은 정보를 가져간 것으로 암호 키를 충분히 추정할 수 있게 되어 다시 키 교환 과정을 처음부터 수행한다. 이 기준값을 정하는 것이 정보 보안의 QKD에서의 어려운 점이다. 양자 채널은 노이즈에 민감하기 때문에 일정 이상의 에러는 항상 존재하고 도청자가 도청했을 시에 발생하는 에러또한 포함하여야 하기 때문이다. QBER 값이 일정 수준을 넘지 않는다 가정하면 정보 누출이 적다 판단하고 오류 정정을 시작한다. DV-QKD에서는 통신에 사용하는 정정 기법들을 사용할 수 있다. CV-QKD는 연속 변수를 이용하기 때문에 기존의 방법을 이용하기 위해서는 연속 변수를 양자화(quantization)하는 과정을 거쳐야 한다. 그 후 오류 정정을 한 키의 일부를 다시 송수신자간에 비교하여 오류 정정 비율을 확인하고 교환하는 데 사용한 키는 버린다. 정정을 끝내고 신뢰할 수 있는 키를 이용하여 보안성 증폭을 수행한다.

Ⅶ. 노출 정보량 분석

실제 구현에 있어서는 실현적인 가능성을 고려해야 한다. 이는 암호 키를 만드는 데 있어서 키 생성 속도는 중요한 성능 중 하나이다. 필요에 의해서 공용 채널을 통하여 노출되는 정보량을 줄임으로 인해서 보안성을 증폭할 수 있고 버리게 되는 정보를 줄이게 되어 키 생성 속도를 증가시킬 수 있게 된다. 이를 위해서 송신자와 수신자 및 도청자간의 정보량을 분석한다.

에러 정정을 위하여 일부 키를 공용 채널을 통해서 주고받게 되면 도청자도 이 정보를 수신할 수 있게 된다. 도청자가 이 정보를 추정할 수 없게 해야 보안성을 보장된다. 이 노출되는 정보량이 임계값을 넘지 않아야 한다. 오류 정정 전의 송신자와 수신자의 상호 정보 대 키 요소는 I_{AB} 이고 도청자와 수신자의 상호 정보 대 키 요소는 I_{EB}이다. 오류 정정 후의 I_{AB}, I_{EB}는 각각 $I_{AB}^{'}$, $I_{EB}^{'}$로 나타내고 게시된 에러 정정 정보 대 키 요소의 양은 R이다. 이론적으로 오류 정정 전에 생성할 수 있는 보안키의 양은 수식 3으로 표현할 수 있다.

$$\triangle I = I_{AB} - I_{EB}\,(bit). \tag{3}$$

오류 정정 완료 후에 정보의 변화는 식 4와 같다.

$$I_{AB}^{'} \le I_{AB} + R. \tag{4}$$

그리고 수신자와 도청자간의 정보량의 관계는 수식 5와 같이 된다.

$$I_{EB}^{'} = I_{EB} + R. \tag{5}$$

오류 정정 후의 송신자가 수신자가 정보를 교환한 비밀 키 비율은 다음 식 6과 같다.

$$\triangle I^{'} = \triangle I - \left(R - I_{AB}^{'} + I_{AB}\right). \tag{6}$$

이로부터 최종적으로 순수한 비밀 키를 생성해 낼 수 있다. 이 키는 식 7,8의 조건을 보장해야 한다.

$$\triangle I > R - (I_{AB}^{'} - I_{AB}). \tag{7}$$

$$R^{'} = I_{AB}^{'} - I_{AB}. \tag{8}$$

그러므로 실제에서는 오직 $R^{'}$bit 수정되어 질수 있는 에러를 정정하기 위해 키 요소당 $R^{'} + \triangle I$ bit 정보보다 적은 정보량을 사용한다. 전송 거리의 증가에 따라 $\triangle I / I_{AB}$ 는 지수적으로 감소하는 반면에 실제 에러 정정은 지수적으로 Shannon 한계에 도달해야 한다. 노이즈에 민감한 CV-QKD에서는 오류 정정을 위해서 더 많은 비트를 전송해야 하기 때문에 실제 키 생성 속도를 낮추는 요인이 된다. 기존에 연구된 예를 살펴보면 0.2dB/km의 감소가 있는 광통신 채널에서 100km 거리에서 연속 변수 키 교환을 실시한 결과 1bit의 키를 보내기 위해서 572bit를 소모하였다[8].

Ⅷ. 결론

양자 통신의 연속 변수 양자를 이용한 QKD 시스템의 키 교환 방식을 설명하였다. 연속 변수가 양자 역학의 성질을 이용하여 보안성을 보장하게 되는 원리를 설명하였다. 연속 변수를 사용하게 되는 장점과 DV-QKD시스템과의 차이점을 설명하였고 장거리 전송을 위하여 극복해야 되는 점을 살펴보았다. 양자 채널을 통한 양자 비트 교환을 끝낸 후에 공용 채널을 통하여 교환해야하는 일부 비트들의 정보량을 분석하였다.

참 고 문 헌

[1] D. Gottesman and J. Preskill, “Secure quantum key distribution using squeezed states,” *Phys. Rev.* A, vol. 63, p. 022309, 2001.

[2] C. Silberhorn, N. Korolkova, and G. Leuchs, “Quantum key distribution with bright entangled beams,” *Phys. Rev. Lett.,* vol. 88, p. 167902, 2002.

[3] R. Namiki and T. Hirano, “Practical limitations for continuous-variable quantum cryptography using coherent states,” *Phys. Rev. Lett.*, vol. 92, p. 117901, 2004.

[4] S. Y. Chung, G. D. Forney, T. J. Richardson, and R. Urbanke, “On the design of low-density parity-check codes within 0.0045 dB of the Shannon limit,” *IEEE Commun. Lett.*, vol. 5, no. 2, pp. 58 - 60, Feb. 2001.

[5] G. Van Assche, J. Cardinal, and N. J. Cerf, “Reconciliation of a quantum-distributed Gaussian key,” *IEEE Trans. Inf. Theory,* vol. 50, no. 2, pp. 394 - 400, Feb. 2004.

[6] M. Heid and N. Lükenhaus, “Efficiency of coherent state quantum cryptography in the presence of loss: Influence of realistic error correction,” *Phys. Rev.* A, vol. 73, pp. 052316-1 - 052316-7, 2006.

[7] U. M. Maurer and S. Wolf, “Secret-key agreement over unauthenticated public channels-Part III: Privacy amplification,” *IEEE Trans. Inf. Theory,* vol. 49, no. 4, pp. 839 - 851, Apr. 2003.

[8] F. Grosshans, G. Van Assche, J. Wenger, R. Brourl, N. J. Cerf, and P. Grangier, “Quantum key distribution using Gaussian-modulated coherent states,” *Nature,* vol. 421, pp. 238 - 241, Jan. 2003.

저자

이 선 의(Sun Yui Lee) **학생회원**

- 2013년 2월 : 광운대학교 전파공학과 졸업
- 2013년 2월 ~ 현재 : 광운대학교 전파공학과 석박사통합과정

<관심분야> : 가시광 통신, 협력통신, 인지무선통신, 양자통신

김 진 영(Jin Young Kim) **종신회원**

- 1998년 2월 : 서울대학교 전자공학과 공학박사
- 2001년 2월 : SK텔레콤 네트웍연구소 책임연구원
- 2001년 3월 ~ 현재 : 광운대학교 전자융합공학과 교수

<관심분야> : 디지털통신, 가시광통신, UWB, 부호화, 인지무선통신, 4G 이동통신