CV QKD 기술 발전 동향 연구

윤승호, 민건식, 김범일, 허준*

고려대학교, 고려대학교, 고려대학교, *고려대학교

seunghyoon@korea.ac.kr, mgs3351@korea.ac.kr, bik0118@korea.ac.kr, *junheo@korea.ac.kr

Development trends of CV QKD technology

Seungho Yoon, Min Gun Sik, Kim Bum Il, Heo Jun*

Korea Univ., Korea Univ., Korea Univ., *Korea Univ.

요 약

본 논문은 연속 변수 양자 암호키 분배(continuous variable quantum key distribution)의 최근 기술 연구 동향을 분석하는 논문이다. 처음 CV QKD가 제안되었을 때의 기술과 최근에 연구되고 있는 CV QKD기법을 비교 분석하여 어떤 관점에서 기술적 발전이 있었고, 추후 어떠한 방향성으로 기술 분석이 이루어져야 하는지에 대한 고찰을 하고자 한다.

Ⅰ. 서 론

본 논문에서는 CV QKD의 기술 발전 연구 동향 분석을 목표로 하고 있다. 양자 키 분배기법(QKD)는 도청자의 유무를 확인할 수 있으면서, public channel을 통해 송수신자에게 secret key를 공유하게 해주는 기법이다. 일반적으로, QKD 송신자(Alice)는 secret key 로 전송하고자 하는 정보를 encrypt 하고 수신자(Bob)에게 전송하면, 도청자(Eve)가 encrypt 된 정보를 탈취할 경우 송수신자는 도청자의 존재를 확인할 수 있게 된다.[1] CV QKD는 이산 변수 양자암호기 분배(discrete variable quantum key dsitribution)와는 다르게 신호를 생성한다. DV QKD는 단일 광자에 정보를 encoding하는 반면, CV QKD는 coherent state를 이용한 진폭과 위상 정보를 인코딩한다. 이러한 특징 때문에 기존 광 통신에서 사용하던 기법들을 적용할 수 있고, DV QKD보다 신호 생성이 수월하다는 장점이 있어 많은 연구가 진행중이다.

Ⅱ. 본론

CV QKD는 key 정보를 작은 신호의 beam, 즉 coherent state에 위상과 진폭을 사용해서 encoding을 진행한다. 이러한 기법은 1999년도에 제안되었다.[2] 이 프로토콜의 보안성은 신호 생성의 BER을 확인하는 것으로 도청자의 존재 유무를 확인하고자 고안된 프로토콜이다. 따라서 신호의 SNR을 아래와 같이 분석을 한다.

$$(\frac{S}{N})^{\pm} = \frac{V_s^{\pm}}{V_n^{\pm}} \quad (1)$$

신호의 두 quadrature들에 측정일 도청자가 시도를 하면 SNR은 아래 수식과 같이 원 신호의 SNR 보다 더 높은 SNR 값을 얻을 수 없는 특성을 사용한 프로토콜이다.

$$(\frac{S}{N})^{\pm}_{sim} = (\frac{\eta^{\pm} V_s^{\pm}}{\eta^{\pm} V_n^{\pm} + \eta^{\mp} V_m^{\mp}})(\frac{S}{N})^{\pm} \quad (2)$$

위 수식에서 η값은 도청자가 도청하고자 사용한 beam splitter의 splitting ratio이고, +는 진폭, -는 위상의 값들을 나타낸다. 전송자는 two independent random string을 만들어서 하나의 string은 amplitude modulator를 통해 신호의 진폭을 변조하고, 또 다른 string은 phase modulator를 통해 신호의 위상을 변조를 진행한다. 이때 two random string은 아래 와 같이 0,1 에 따라 phase 값은 임의의 continuous value θ, ϕ 로 mapping 되고, amplitude 값은 임의의 continuous value a,b 로 mapping 된다.

그러나 이러한 변조 방식으로 도청자를 감지를 하면, 송수신자가 도청자를 정확하게 확인하지 못하는 공격방법이 있다는 단점이 있다. 따라서 이러한 단점들을 극복하고자 squeezed state CV QKD 기법을 사용한다.

Squeezed state 의 경우 아래와 같이 I/Q plane에서의 신호의 한쪽 quadrature의 불확실성이 늘어나고 다른 하나의 quadrature의 불확실성을 매우 줄인 형태의 신호이다.

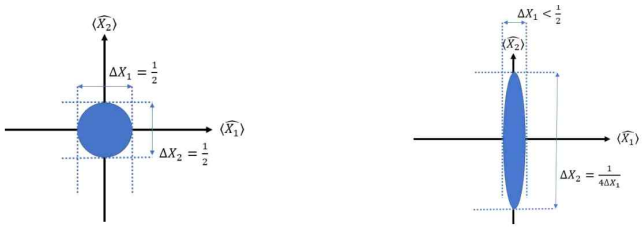

그림1. I/Q plane에서의 squeezed state 신호

Squeezed state 신호는 다음과 같은 절차를 따라 생성한다. 송신자는 자신의 number string을 digital로 encoding을 진행한다. 이후 amplitude squeezed beam A, B에 각각 두 개의 amplitude quadrature에 number string을 encoding을 진행한다. $\pi/2$ phase shift는 beam B에 impose를 하여 squeezed beam A는 amplitude qudrature에 encoding을 사용.

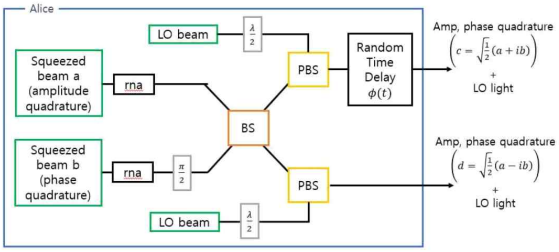

그림2. Squeezed state CV-QKD scheme

신호의 결과로 아래와 같은 두 개의 output C, D를 생성 후 수신자가 balanced homodyne detector에서 선택한 quadrature에 따른 신호를 얻을 수 있다

$$V^{+}=\left\langle \left|(\tilde{c}^{\dagger}+\tilde{c})+(\tilde{d}^{\dagger}+\tilde{d})\right|^{2}\right\rangle = V_{s,a}+V_{n,a}^{+} \quad (3)$$

$$V^{-}=\left\langle \left|(\tilde{c}^{\dagger}-\tilde{c})-(\tilde{d}^{\dagger}-\tilde{d})\right|^{2}\right\rangle = V_{s,b}+V_{n,b}^{+} \quad (4)$$

이후 Gaussian modulation을 활용한 GG02 프로토콜이 제안이 되었다.[3] GG02 프로토콜은 이전 프로토콜과는 다르게, 랜덤한 숫자열 x와 p가 가우시안 분포를 갖도록 준비한다. 송신자는 선택한 두 숫자열을 바탕으로 신호의 두 quadrature에 $|\ x+ip\ \rangle$와 같이 인코딩 후 수신자는 x와 p를 측정을 진행한다. 이때 측정의 방법은 I/Q plane 상에서 아래 사진과 같이 어느 사분면에 위치하는지 확인하는 방법으로 bit 검출을 진행. 이러한 Gaussian modulation 기법의 구현 관점에서 신호생성의 stability도 증가시키고, 구현 가격 절감의 기술이 제안이 되었다.[4] 이전에는 Gaussian modulated signal을 AM 과 PM을 사용해서 진행을 하였지만, 이 기법을 사용하면 한 개의 PM 만을 사용해 Gaussian modulated signal 생성이 가능하게 된다. 이는 회로 중간에 아래와 같은 ring 형태의 회로를 만들어서 clockwise, counter clockwise 신호에 각각 V_{PM}을 encoding 한 후 합쳐지게 만드는 것으로 가능하다.

$$V_{PM}=V_{\pi}\times[V_1(t_1),\ V_2(t_1),\ V_1(t_2),\ V_2(t_2),\ldots] \quad (5)$$

$$V_1=2\times U+\arccos(R)/\pi \quad (6)$$

$$V_2=2\times U-\arccos(R)/\pi \quad (7)$$

이후 Probabilistic constellation shaping 기법을 활용한 PCS CV QKD 기법이 제안이 되었다.[5] Probabilistic constellation shaping 기법은 기존 광통신에서 사용되던 기법이다. 간단한 예시로 16-QAM의 경우 16개의 constellation point로 symbol을 생성하게 된다. 이때 각 constellation point는 위상과 진폭을 encoding 하는 것으로 symbol 생성을 진행하게 된다. 이때 I/Q plane의 외곽에 위치한 constellation point의 경우 내부에 위치한 point보다 더욱 높은 에너지가 요구되기 때문에, 외곽의 point는 적게 생성하고, 내부의 point는 더욱 많이 생성되도록 확률을 조정하는 것이 PCS 기법이다. 또한, 이 PCS가 Gaussian distribution을 따르도록 encoding 하여 신호의 security를 보장 받을 수 있다. PCS CV QKD에서의 신호 생성은 아래 수식을 따라 각 constellation point들의 선택 확률이 결정된다

$$P_X(p+iq)=\frac{e^{-v(p^2+q^2)}}{\sum_{p,q}e^{-v(p^2+q^2)}} \quad (7)$$

이 수식의 p,q는 I/Q plane에서의 constellation point의 I축의 값, Q축의 값을 의미하고, 외곽의 constellation point의 확률을 결정하는 free parameter v를 포함한다. 이 수식을 활용하면 아래와 같은 확률로 constellation point들을 생성하여 전송하게 되는 기법이다.

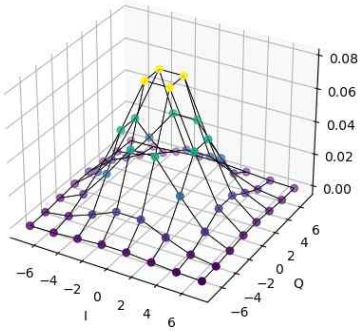

그림3. PCS 64-QAM probability, v=0.08

이러한 기술발전의 배경에는 기존 광통신에서 사용되던 기법들을 적용하며 발전되어왔다.

Ⅲ. 결론

본 논문에서는 CV QKD의 기술의 발전 동향을 확인하였다. CV QKD는 구현이 비교적 쉽다는 특징과 신호 생성의 용이성 때문에 연구가 활발하게 진행되고 있다. 특히 기존 광통신과의 유사성으로, 광통신에서 사용하던 기법들을 CV QKD에 적극적으로 활용되고 있는 모습을 보이고 있다. 따라서 추후 CV QKD 연구에 기존 광통신 기법을 적용하는 방향으로 연구가 진행될 것으로 보인다.

ACKNOWLEDGMENT

이 논문은 정부(과학기술정보통신부)의 재원으로 한국연구재단 양자정보과학 인적기반 조성사업의 지원을 받아 수행된 연구임 (Grant No. 2022M3H3A106307411).

본 연구는 고려대 암호기술 특화연구센터(UD170109ED)를 통한 방위사업청과 국방과학연구소의 연구비 지원으로 수행되었습니다.

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. RS-2023-00242396)

참 고 문 헌

[1] Jain, Nitin, et al. "Practical continuous-variable quantum key distribution with composable security." Nature communications 13.1 (2022): 4740.

[2] Ralph, Timothy C. "Continuous variable quantum cryptography." Physical Review A 61.1 (1999): 010303.

[3] Grosshans, Frédéric, and Philippe Grangier. "Continuous variable quantum cryptography using coherent states." Physical review letters 88.5 (2002): 057902.

[4] Zhao, Huanxi, et al. "Simple continuous-variable quantum key distribution scheme using a Sagnac-based Gaussian modulator." Optics Letters 47.12 (2022): 2939-2942.\

[5] Roumestan, François, et al. "Demonstration of probabilistic constellation shaping for continuous variable quantum key distribution." Optical Fiber Communication Conference. Optica Publishing Group, 2021.