연속 변수 측정기기독립 양자키분배의 postselection 적용을 통한 이산변조 연구

정지희, 허준*
고려대학교, *고려대학교

dpdk774@korea.ac.kr, *junheo@korea.ac.kr

A Study on discrete modulation of CV-MDI QKD by acting postselection

Jung Ji Hee, Heo Jun*

Korea Univ., *Korea Univ.

요 약

본 논문은 표준 CV-MDI-QKD(가우시안 변조·코히런트 전송, CV Bell 측정)를 유지한 채, **후처리 포스트셀렉션(PS)**만으로 **QPSK 결정**을 구현하는 소프트웨어적 이산화 기법을 제안한다. 결정 부채꼴의 중심각 $D = \{\Delta, \Delta + \frac{\pi}{2}, \Delta + \pi, \Delta + \frac{3\pi}{2}\}$영역을 도입하고, 공개값 r에 조건화한 **복소 AWGN 등가 모델**에서 통과확률 p_{pass}과 혼동행렬을 통해 채택 조건 상호정보를 산출한다. 보안 평가는 **truncated CM** 을 이용해 $\chi(E;Y \mid \text{pass})$를 상계하며, 무한장 키율은 $K_{\text{PS}}^{\text{MDI}} = p_{\text{pass}}[\beta I - \chi]$로 귀결된다. PS 는 표본을 줄이지만 축·경계 인접의 고오류 샘플을 배제해 저 SNR/장거리에서 순이득을 제공하며, 결과적으로, 변조기 변경 없이 **후처리만으로** 키율·도달거리 향상을 달성하는 경량 구현 경로를 제시한다.

Ⅰ. 서 론

CV QKD 는 전기장의 사분면 q, p 에 해당하는 연속변수(CV)에 정보를 실어 coherent 혹은 squeezed 상태를 전송하고, 수신 측에서 homodyne 측정으로 실수값 샘플을 얻어 키를 형성하는 QKD 방식이다. 기존의 광통신 상용 부품과의 높은 호환성, 상온 동작, 고속 수집 등이 장점이며, 주로 공분산 행렬(CM) 추정과 가우시안 최적성에 기대서 보안 분석이 이루어진다. 관행적으로는 가우시안 변조(GM)가 채널이 이상적인 AWGN 일 때 상호정보를 극대화하지만, 낮은 SNR 혹은 장거리에서 오류정정 (IR) 비용이 커지거나 실패확률이 높다는 한계가 있다. 이를 완화하기 위해 이산변조(DM)가 제안되었다. 실제 구현에서 코드 설계가 쉽고, 낮은 SNR 에서도 안정적인 LLR 계산이 가능하다는 장점이 있다. 하지만 비가우시안 상태가 되어 분석이 복잡해지기 때문에, 보안 증명은 선형 채널 매개변수 기반의 상계나 수치적 기법을 병행한다.

측정기기독립(MDI) QKD 는 수신 측 검출기의 취약점을 구조적으로 제거하기 위한 프로토콜로, CV-MDI QKD 에서는 Alice 와 Bob 이 각각 상태를 신뢰할 수 없는 중계자, Charlie 에게 보내고 중계자가 CV Bell 측정 결과 r 을 공개한다. 양측 사용자는 r 에 조건화된 통계로 correlation 을 복원하므로, 설령 중계자가 완전히 신뢰할 수 없더라도 키 생성이 가능하다.

본 논문은 전송 단계는 표준 CV-MDI(GM 사용, coherenet state 전송)[1]를 유지하되, 측정 이후 단계에서 postselection 을 적용해 QPSK 심볼을 형성하는 방식이 key rate 에 어떤 영향을 미칠지 분석한다.

Ⅱ. 본론

프로토콜 과정을 설명하기에 앞서 시스템 모델은 다음을 가정한다. 첫째, Alice 와 Bob 은 평균 V_A, V_B 의 가우시안 변조된 coherent states 를 각각 전송한다. Alice-Charlie, Bob-Charlie 링크의 전송률과 초과잡음을 $(T_A, \xi_A), (T_B, \xi_B)$ 로 둔다. 둘째, Charlie 는 균형 빔스플리터(BBS)와 heterodyne 검출로 구성된 CV Bell 측정을 수행하고, 결과 $r \in \mathbb{C}$ 를 공개한다. 마지막으로, 공개값 r에 조건화하면, 양단의 유효 통계는 복소 AWGN 채널로 모델링된다.

프로토콜은 다음과 같이 진행된다.

1. 표준 CV-MDI 절차를 수행하고 r을 공개한다.
2. 랜덤 샘플을 공개해 전송률과 초과잡음, 분산 등의 파라미터를 추정한다.
3. Alice 는 자신의 복소 샘플 $y \in \mathbb{C}$에 대해 선택영역, 예를 들어 QPSK 를 만드는 경우 영역을 $D = \{\theta_k(\Delta)\}_{k=0}^{3}$로 두되,

$$\theta_k(\Delta) = \Delta + \frac{k\pi}{2}, k = 0,1,2,3 \quad (1)$$

로 정의한다. 이 영역에 속하는 신호는 QPSK 심볼로 modulation 을 정의하고, 그 외에는 폐기한다.

이 경우 통과확률은[2]

$$p_{pass} = \sum_{k=0}^{3} \int_{\mathcal{R}_k(\Delta,\Delta\theta;r_c)} \frac{1}{\pi\sigma^2} \exp\left(-\frac{|y-\mu_l|^2}{\sigma^2}\right) d^2y \quad (2)$$

이다. 송신 심볼이 l일 때 k로 결정될 확률은 $P(k|l)$으로, 이로 인해 상호정보는

$$I(postselection|pass) = \sum_{l,k} \frac{p_l P(k|l)}{p_{pass}} \log_2 \frac{P(k|l)}{\sum_{l'} P(k|l')} \quad (3)$$

으로 변화하게 된다. 또한 holevo bound 도 이에 맞춰 상계가 변화하여, $\chi(E:Y|pass) \le \chi_G(\gamma_{BE|pass})$ 가 된다. 따라서 무한한 길이의(Devetak-Winte)r key rate[는

$$K_{PS}^{MDI} = p_{pass}[\beta I(PS|pass) - \chi(E:Y|pass)] \quad (4)$$

으로 바뀌게 된다. PS 는 샘플 손실을 유발하지만, 축·경계 인접의 오류가 높은 샘플을 제거함으로써 I 를 유의미하게 증가시키므로 낮은 SNR 에서 이득을 볼 수 있다. Finite-size key rate 관점에서, 블록 길이 $N = n + m$에서 PS 는 $n \approx p_{pass}N$으로 만들고 매개변수 추정 분산 증가 및 보안 보정항 Δ_{sec} 상승을 유발한다. 따라서 키 길이는

$$l \ge n[\beta I(PS|pass) - \chi(E:Y|pass)] - \Delta_{sec} - \Delta_{IR} \quad (5)$$

이며, 마지막항은 오류정정(information reconciliation)로 인한 보정항이다.

Ⅲ. 결론

본 연구는 표준 CV-MDI-QKD(가우시안 변조·코히런트 전송, 릴레이 Bell 측정)를 유지한 채, 후처리 단계에서 포스트셀렉션(PS)으로 QPSK 결정을 수행하는 소프트웨어적 이산화 방법을 정식화하였다. 구체적으로, 결정 부채꼴의 중심각을 $D = \left\{\Delta, \Delta + \frac{\pi}{2}, \Delta + \pi, \Delta + \frac{3\pi}{2}\right\}$ 로 정의하여서 영역을 결정하는 경우를 분석하였다. 결정 영역 외의 신호를 폐기하는 것에 대한 손실에도 불구하고, PS 는 상호정보를 유의미하게 증가시키기에 이러한 구조에 이점이 존재한다. 그래서 이를 바탕으로 조건부 확률을 구해 상호정보의 변화를 계산하였으며, 무한 길이인 경우, 유한 길이인 경우에 대해서 key rate 수식을 계산하였다. 구체적인 파라미터 최적화는 필요하겠지만, 이는 CV-MDI QKD 의 성능을 높일 수 있는 유의미한 프로토콜이라고 볼 수 있다.

ACKNOWLEDGMENT

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

본 연구는 한국과학기술정보연구원(KISTI)의 위탁연구개발과제로 수행한 것입니다

참 고 문 헌

[1] Fletcher, Alasdair, et al. "An Overview of CV-MDI-QKD." Reports on Progress in Physics (2025).

[2] Kanitschar, Florian, and Christoph Pacher. "Optimizing continuous-variable quantum key distribution with phase-shift keying modulation and postselection." Physical Review Applied 18.3 (2022): 034073.