SDP 기반 PCS-16-QAM 연속변수 양자 키 분배의 점근적 비밀키율 하계

김성욱° 허준

고려대학교 전기전자공학과

SDP-Based Asymptotic Secret-Key Rate Lower Bound for PCS-16-QAM CV-QKD

Seonguk Kim° Jun Heo

Dept. of Electrical Engineering

Korea University

djm06145@korea.ac.kr° junheo@korea.ac.kr

요 약

본 논문은 Semidefine program(SDP)를 활용하여 16-QAM(Quadrature Amplitude Modulation)을 기반으로 한 CV-QKD(Continuous Variable Quantum key distribution) 시스템에서의 key rate 하한을 도출하는 과정을 다룬다. SDP 과정은 covariance matrix 에서 alice 와 bob 의 correlation Z 값의 최솟값을 찾는 방식으로 이는 eve 에게 가장 유리한 상황을 가정해서 key rate 를 계산하는 것으로 다양한 modulation 상황에서 엄밀하게 값을 구할 수 있다.

1. 서론

CV-QKD 는 코히런트 상태의 퀴드러처를 이용하므로 표준 광통신과의 호환성이 높지만, 보안 증명은 주로 Gaussian modulation 을 전제로 발전해 왔다. 하지만 실제 변조기는 분해능이 유한하여 constellation 가 이산적인 한계가 있다. 그렇기 때문에, Discrete modulation 에 대한 key rate 하한이 필요하다.[1] 보안 증명이 다양한 방법으로 연구되고 있는데 본 논문에서는 semidefine program(SDP)를 활용하여 최적화 기반 수치해로 하한을 구하고자 한다. [2]

2. 본론

프로토콜을 Entangle based 로 등가화하고 관측 가능한 1,2 차 통계와 물리적 제약을 바탕으로 alice, bob 의 correlation 을 최소화하는 SDP 로 Devetak Winter 경계의 하한을 도출하는 방식이 제안되었다. 이러한 맥락에서 선행 결과를 바탕으로 16 QAM 에 SDP 를 적용하여 점근적 SKR 하한을 산출한다. [2]

[3]에 따르면, Gaussian modulation에서의 Alice, Bob covariance matrix는 $\sum_{AB}$로 표현된다. 파라미터는 다음과 같다. $V = V_A + 1$, V_A 는 alice의 평균 modulation variance (SNU기준), $Z_{GM} = \sqrt{V^2 - 1}$ 은 Gaussian modulation에서의 Alice와 Bob의 correlation이다. T는 전송 효율이며, I_2는 2×2 identity matrix, σ_z 는 Pauli Z matrix: $diag\ (1, -1)$, ϵ is excess noise, χ_{line} = 1/T-1+ϵ 이다.

$$\sum_{AB} = \begin{pmatrix} VI_2 & \sqrt{T}Z_{GM}\sigma_z \\ \sqrt{T}Z_{GM}\sigma_z & T(V + \chi_{line})\mathbb{I}_2 \end{pmatrix}$$

과거의 연구들은 $Z_{DM} \approx Z_{GM}$인 조건에서 기존 보안 증명이 많이 이루어진 Gaussian modulation 기반 key rate 수식을 근사해서 활용한다. [4][5] 하지만 SDP 기법을 활용하여 식을 전개하면 Z_{DM}의 최솟값을 얻어 더 정확하게 key rate 값을 얻을 수 있다.

SDP 의 기법은 다음과 같다.$Z = tr\ (\rho C)$ 수식을 바탕으로 minimal 한 Z 값을 구하며 조건들은 아래와 같다.

$Z = tr\ (\rho C)$:

$$\begin{cases} tr_B(\rho) = \tau \\ tr\ (\rho C_1) = 2c_1 \\ tr\ (\rho C_2) = 2c_2 \\ tr\ \left(\rho(\Pi \otimes b^\dagger b)\right) = n_B \\ \rho \succcurlyeq 0 \end{cases}$$

$C \coloneqq \hat{a}\hat{b} + \hat{a}^\dagger\hat{b}^\dagger$이고 이는 $\langle C \rangle = \langle x_A x_B \rangle - \langle p_A p_B \rangle$이며 곧 $tr\ (\rho C)$를 최소화하는 것은 Z 의 최솟값을 찾는 것과 동일하며 이는 key rate 의 하한을 제공한다. 첫

번째 조건에서 τ는 alice 가 보내는 state 의 평균상태이다. 이는 PM 프로토콜이 EM 프로토콜과 동치임을 보이는 것으로 alice 쪽의 상태가 laser source 의 modulation 으로 인한 상태와 동일해야 함을 의미한다. 두번째 조건은 $c_1 = \frac{1}{2}\langle x_A x_B \rangle$로 alice 와 bob 의 관계가 관측된 데이터 c_1에 해당한다는 것이며 세번째 조건도 이와 유사하게 $c_2 = \frac{1}{2}(-\langle p_A p_B \rangle)$로 표현되며 관측된 데이터 c_2에 선형적 상관성을 가진다는 의미이다. 네번째 조건은 2 차 모멘트 제약으로 bob 쪽의 분산을 실험에서 측정한 값으로 고정한 것이다. 다섯번째 조건은 ρ값이 positive semidefinite 라는 의미로 측정 확률이 양수인 양자 상태를 의미함. 이러한 조건들 속에서 SDP 를 이용하여 Z의 최솟값을 구할 수 있다.

16QAM 에 적용해 보자면 우선, coherent state 를 다음과 같이 기술 가능하다. [6]

$$\alpha_{k,l} = \alpha\sqrt{\frac{2}{3}}\left(k - \frac{3}{2}\right) + i\alpha\sqrt{\frac{2}{3}}\,(l - \frac{3}{2})$$
$$k = l = 0,1,2,3$$

이후 PCS 에 해당하는 Gaussian distribution 확률을 기술하면 다음과 같다.

$$p_{k,l} \sim \exp\left(-v(x^2 + p^2)\right)$$
$$\left(x = \alpha\sqrt{\frac{2}{3}}\left(k - \frac{3}{2}\right), p = \alpha\sqrt{\frac{2}{3}}\left(l - \frac{3}{2}\right)\right)$$

v를 조정해서 key rate 가 최대가 되는 지점을 얻을 수 있다. Asymptotic limit SKR 수식은 $SKR = \beta I_{AB} - S_{BE}$로 동일하며 mutual information, holevo information 은 다음과 같이 정의된다.

$$I_{AB,hom} = \frac{1}{2}\log_2(1 + \frac{TV_A}{2 + T\epsilon})$$
$$I_{AB,het} = \log_2\left(1 + \frac{TV_A}{2 + T\epsilon}\right)$$

Covariance matrix 는 다음과 같이 정의되며 symplectic eigenvalue 를 구하면 다음과 같다.

$$\Gamma_{\mathrm{AB}} = \begin{bmatrix} (V_A + 1)I_2 & Z^*\sigma_z \\ Z^*\sigma_z & (1 + TV_A + T\epsilon)I_2 \end{bmatrix}$$
$$\lambda_{3,hom} = \sqrt{(V_A + 1)(V_A + 1 - \frac{Z^{*2}}{1 + TV_A + T\epsilon})}$$
$$\lambda_{3,het} = V_A + 1 - \frac{Z^{*2}}{1 + TV_A + T\epsilon}$$

Correlation coefficient Z^*는 다음과 같이 계산된다. $\hat{a}, \hat{a}^\dagger$은 annihilation 과 creation operator 이고 ϵ는 total excess noise, τ 는 modulation 의 density matrix 이다.

$$Z^*(T,\epsilon) = 2\sqrt{T}tr\left(\tau^{\frac{1}{2}}\hat{a}\tau^{\frac{1}{2}}\hat{a}^\dagger\right) - \sqrt{2T\epsilon w}$$
$$w = \sum_k p_k\left(|\alpha_k\rangle\hat{a}_\tau^\dagger\hat{a}_\tau|\alpha_k\rangle - |\langle\alpha_k|\hat{a}_\tau|\alpha_k\rangle|^2\right)$$

위 수식들을 계산하여 key rate 하한을 얻을 수 있다.

3. 결론

SDP 를 활용한 DM 프로토콜의 key rate 도출과정을 전반적으로 살펴보았다. 전체적인 진행과정은 다음과 같다. 1. Modulation 방식에 따른 coherent state 도출, 2. Entangle based 로 옮기고 실험 값들을 조건으로 SDP 를 계산 후 Z_{16QAM}의 최솟값을 얻음, 3. EB 모델에서 얻는 Z_{EB}를 비교해 $Z_* = \min(Z_{DM}, Z_{EB})$를 사용하여 Holevo 값을 산출, 이후 key rate 공식에 적용하여 key rate 하한을 계산한다. 이 방식은 Z_{DM}, Z_{GM}이 근사할 때 Gaussian modulation 을 바탕으로 한 key rate 수식을 사용하는 것보다 더 엄밀하게 값을 얻을 수 있다. 또한 몇 개의 실험적 값들을 바탕으로 eve 가 가장 유리한 상황을 가정해서 보수적으로 key rate 를 얻을 수 있다.

4. Acknowledgments

본 연구는 한국과학기술정보연구원(KISTI)의 위탁연구개발과제로 수행한 것입니다.(50%) 이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. RS-2023-00242396, 50%)

5. 참고 문헌

[1] A. Leverrier and P. Grangier, “Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation“Phys. Rev. Lett. 102, 180504 (2009).

[2] A. Leverrier and P. Grangier, “Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation“Phys. Rev. Lett. 102, 180504 (2009).

[3] Fossier, Simon, et al. "Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers." Journal of Physics B: Atomic, Molecular and Optical Physics 42.11 (2009).

[4] Djordjevic, Ivan B. "Optimized-eight-state CV-QKD protocol outperforming Gaussian modulation based protocols." IEEE Photonics Journal 11.4 (2019)

[5] A. Becir et al., “Continuous-variable quantum key distribution protocols with eight-state discrete modulation,” Int. J. Quantum Inf., vol. 10 (2012)

[6] Sayat, Mikhael T., et al. "Satellite-to-ground continuous variable quantum key distribution: The Gaussian and discrete modulated protocols in low earth orbit." *IEEE Transactions on Communications* 72.6 (2024)