010-3694-0003

연속 변수 측정기기독립 양자키분배의 postselection 적용을 통한 이산변조의 SDP 기반 보안 증명

정지희, 곽혜린*, 허준**
고려대학교, *고려대학교, **고려대학교

dpdk774@korea.ac.kr, *lynkwak12@korea.ac.kr, *junheo@korea.ac.kr

SDP-based security proof on discrete modulation of CV-MDI QKD by acting postselection

Jung Ji Hee, Heo Jun*

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

요 약

본 논문은 passive MDI CV-QKD 구조를 유지하면서, 로컬 heterodyne 결과에 region operator(결정영역 POVM)를 적용하는 postselection 으로 연속 변수를 이산 심볼로 사상하는 프로토콜의 보안증명을 정리한다. Postselection 은 키에 사용되는 표본을 조건부로 선택하므로 통계가 일반적으로 비가우시안이 되며, 분삼만으로 가우시안 최적성(가우시안 상계 χ_E^{GM})을 적용하면 과도하게 보수적인 상계를 얻게 되므로 이를 해결하기 위해 SDP 증명을 본 프로토콜에 적용할 수 있는 방법에 대해 연구한다. 이를 통해 χ_E^{SDP}를 계산 가능한 형태로 상계하여 최종 키율에 반영할 수 있도록 한다.

Ⅰ. 서 론

CV QKD 에서 가우시안 변조 및 가우시안 측정은 보안분석이 공분산행렬(CM)에 의해 상계되는 장점이 있다. 반면, 본 연구의 프로토콜은 passive MDI CV-QKD 의 광학적 절차(열광원 및 BS 를 통과하여 전송을 하면 중계자가 이를 받아 relay 측정을 하는 것)를 유지하면서, 로컬 측정 이후 결정영역 기반 postselection 을 수행하여 이산 변조(심볼)을 생성한다. 이때 키에 사용되는 데이터는 조건부로 선택되므로 통계가 비가우시안으로 변하고, 분산만을 조건으로 하는 가우시안 최적성을 그대로 적용하면 χ_E가 과도하게 커져 키율이 과소평가될 수 있다.

본 논문은 이 문제를 일반적인 이산 변조 CV QKD 의 보안 증명 방식인 SDP(semidefinite propramming) 방법으로 처리한다. 핵심 아이디어는 postselection 이 만들어내는 통계를 비선형 표본 선택으로 다루지 않고, 통과 사건을 서브정규화 상태의 trace 및 선형 관측자 제약으로 흡수하여, 관측 통계를 만족하는 모든 양자상태에 대해 도청자 정보 상계를 최적화하는 형태로 바꾸는 것이다. 또한 MDI 구조의 특성상 Charlie 의 CV-Bell 측정 결과 γ가 공개되므로, γ로 조건화된 상태의 CM 갱신(조건부 가우시안 업데이트)을 명시적으로 포함한다.

Ⅱ. 본론

우선 프로토콜에 대해 간단히 요약하면 하면 다음과 같다. 각 사용자 $X \in \{A, B\}$는 평균 광자수 n_0의 thermal source 를 사용한다. 각 소스 출력은 50:50 BS 로 분할되어 전송 모드 T_X와 로컬 모든 K_X를 생성한다. T_X는 감쇠 후 양자채널(전송률 τ_X, excess noise ϵ_X)을 거쳐 Charlie 로 전송되고, K_X 는 로컬에서 heterodyne 측정에 사용된다. Charlie 는 두 전송 모드 T_A, T_B를 BS 로 간섭시켜 CV-Bell 결과 $\gamma = (q_-, p_+)$ 를 얻어 공개 채널로 전송한다. 로컬 측정 결과 $y = (q, p)$에 대해 결정 영역 D_K 를 정의하고, heterodyne POVM E_y 로부터 region operator $R_k \coloneqq \int_{D_k} E_y d^2y$ 를 구성한다. Postselection 통과 사건을 S_X 로

두고, 통과확률을 $p_{pass}^{X} = \Pr(S_X)$, 전체 통과확률을 $p_{pass} = \Pr(S_A \cap S_B)$ 로 둔다. 통과한 표본은 심볼 k 로 사상되어 키 생성에 사용되며, 이후 오류 정정과 비밀성 증폭 과정을 수행한다.

일반적인 SDP 방식은 이산 심볼을 전송하는 것을 전제로 증명되지만, 본 프로토콜은 전송 이후에 이산 심볼로 postselection 하는 방식이다. SDP 방식을 적용하기 위해서 우선 이 문제를 해결해야 한다. Postselection 측정 결과로부터 조건부 심볼로 만드는 비선형 절차처럼 보이나, Hughston-Jozsa-Wootters(HJW) 정리[1]를 통해 entaglement basis 관점에서 통계가 동일한 선형 제약 문제로 바꿀 수 있다. 또한 Naimark dilation[1]으로 POVM $\{R_k\}$ 는 다음과 같이 더 큰 공간에서의 직교측정으로 구현된다.

$$R_k = V^{\dagger}(\mathbb{I} \otimes |k\rangle\langle k|)V \tag{1}$$

따라서 심볼 레지스터 L_X 에 $|k\rangle$ 를 coherenet 하게 저장하는 형태의 EB 모델이 가능하며, deferred measurement 원리[2]에 의해 측정 시점 이동은 확률 분포를 바꾸지 않는다. 이로써 postselection 은 표본 선택이 아니라 조건부 사건에 대한 서브정규화 상태로 다룰 수 있다.

SDP 방법으로 보안 증명을 하기 위해, region operator 통과 사건 S_X에 해당하는 서브 정규화 상태를 SDP 변수로 둔다.

$$Y_X \succeq 0, Y_X \in \mathcal{H}_{L_X} \otimes \mathcal{H}_{K_X} \otimes \mathcal{H}_{T_X}, tr(Y_X) = p_{pass}^{X} \tag{2}$$

그러면 관측 및 계산 통계는 선형 제약으로 표현되어, 심볼 빈도는,

$$tr[(|k\rangle\langle k| \otimes \mathbb{I} \otimes \mathbb{I})Y_X] = p_{pass}^{X}\pi_k^{S,X} \tag{3}$$

심볼 overlap(정규화 Gram)은,

$$tr[(|k\rangle\langle k| \otimes \mathbb{I} \otimes \mathbb{I})Y_X] = p_{pass}^{X}\sqrt{\pi_k^{S,X}\pi_l^{S,X}}\tilde{G}_{k,l} \tag{4}$$

이며 $\tilde{G}_{k,l} = \frac{G_{kl}}{\sqrt{G_{kk}G_{ll}}}, G_{kl} = Tr\left[\sqrt{R_k}\sigma\sqrt{R_l}\right]$ 이다.

에너지(분산)은,

$$tr\left[\left(\mathbb{I} \otimes \left(N_{k_X} + 1\right) \otimes \mathbb{I}\right)Y_X\right] = p_{pass}^{X}V_{K_X},$$
$$tr\left[\left(\mathbb{I} \otimes \left(N_{T_X} + 1\right) \otimes \mathbb{I}\right)Y_X\right] = p_{pass}^{X}V_{T_X} \tag{5}$$

이다. SDP 변수에 대한 가능집합을 위 선형 제약을 고려할 때, $\mathcal{F}_X := \left\{Y_X \succeq 0 : \textit{제약만족}\right\}$으로 둔다.

그러면 SDP 로 최악 교차상관을 구해 유효 CM 을 구성할 수 있다. 소멸연산자 $\hat{k}_X, \hat{t}_X$ 에 대해 통과 사건 조건부 교차 상관을

$$f_X(Y_X) = \frac{1}{p_{pass}^{X}} tr\left[\left(\mathbb{I}_2 \otimes \left(\hat{k}_X\hat{t}_X + \hat{k}_X^{\dagger}\,\hat{t}_X^{\dagger}\right)\right)Y_X\right] \tag{6}$$

으로 정의하고,

$$Z_{X,+}^{*} = \max_{Y_X \in \mathcal{F}_X} f_X(Y_X), Z_{X,-}^{*} = \min_{Y_X \in \mathcal{F}_X} f_X(Y_X),$$
$$|Z_X^{*}| = \max\left\{\left|Z_{X,+}^{*}\right|, \left|Z_{X,-}^{*}\right|\right\} \tag{7}$$

를 SDP 로 계산한다. 이를 이용해 링크별 유효 CM 을

$$\Gamma_X^{*} = \begin{pmatrix} V_{K_X}\mathbb{I}_2 & Z_X^{*}\sigma_z \\ Z_X^{*}\sigma_z & V_{T_X}\mathbb{I}_2 \end{pmatrix} \tag{8}$$

로 둔다. $\mathcal{F}_X$는 분산만 제약하는 가우시안 집합보다 작은 집합이므로, 일반적으로 $\chi_{real} \le \chi_E^{SDP} \le \chi_E^{GM}$ 이 된다. CV QKD 의 key rate 로 정리하면,

$$K \ge p_{pass}\{\beta I_{AB} - \chi_E^{SDP}\} \tag{9}$$

이므로 가우시안 상계를 활용할때보다 더 높은 키율을 얻을 수 있다.

Ⅲ. 결론

본 논문은 passive MDI CV-QKD 구조를 유지하면서, 로컬 heterodyne 결과에 region operator(결정영역 POVM)를 적용하는 postselection 으로 연속 변수를 이산 심볼로 사상하는 프로토콜의 보안증명을 SDP 방식을 적용하여 보였다. Postselection 을 하는 경우에도 SDP 를 사용하기 위해 HJW 정리, Naimark dilation, deferred measurement 원리를 사용하여 등가 EB 표현이 생성 가능함을 보였다. 이를 통해 region operator 통과 사건에 해당하는 서브 정규화 상태를 SDP 변수로 두고 통계를 선형 제약으로 표현해 변수에 대한 가능집합을 구하였으며, 이를 만족하는 유효 CM 을 계산할 수 있었다. 결정 영역을 키 생성 데이터로 추정하면 postselection 이 공격자 교란에 의해 편향될 수 있어, SDP 제약 입력이 공격에 종속될 위험이 생긴다. 따라서 결정영역은 프로토콜 이전 별도 라운드로 합의하여 고정하여야 하고, 이후 무작위 샘플링으로 채널 파라미터를 추정해야 SDP 상계의 정당성이 유지될 것이다.

ACKNOWLEDGMENT

이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원-대학 ICT 연구센터(ITRC)의 지원(IITP-2026-RS-2021-II211810, 50%)과 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. RS-2023-00242396, 50%)

참 고 문 헌

[1] Watrous, John. The theory of quantum information. Cambridge university press, 2018.

[2] Nielsen, Michael A., and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.