수동적 이산변조 연속 변수 양자 키 분배의 reverse reconciliation softing 적용 연구

정지희, 허준
고려대학교

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

A Study on application reverse reconciliation softing of passive discrete modulation continuous variable quantum key distribution

Jung Ji Hee, Heo Jun
Korea Univ.

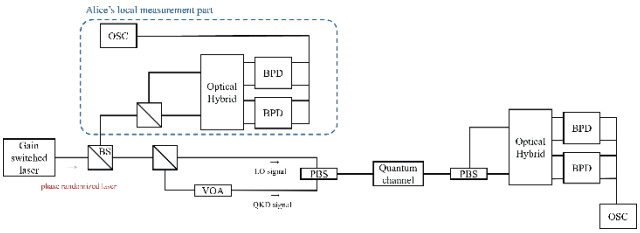
요 약

본 논문은 passive DMCV QKD 에서 RRS 기법의 적용 가능성을 분석하였다. Alice 의 사후 symbol 결정과 Bob 의 회전 측정값 기반 soft information 생성이 기존 RRS 와 차이점을 만든다는 것을 보였으며, 이를 통해 어떻게 passive 환경에서도 효율적인 RRS 이 가능한지를 보였다.

Ⅰ. 서 론

Continuous variable quantum key distribution(CV-QKD)는 구현의 효율성과 보안성 측면에서 주목받고 있다. 초창기에는 Gaussian modulation 을 이용하여 encoding 을 진행하였으나, 실험적 구현에서 discrete modulation 이 더 쉽고, reconciliation 효율 좋아 DMCV-QKD 가 많이 연구되고 있다. Reconciliation 은 인증된 공개 채널로 Alice 와 Bob 사이 일부 정보를 공유하여 같은 key 를 갖도록 하는 절차이다. 이때 높은 key rate 를 위해서 reverse reconciliation(RR)이 많이 이용되는데, 이는 Bob 이 공개한 정보를 바탕으로 Alice 가 자신의 key 를 수정하는 방식이다. GM 기반 RR 은 Bob 이 선택한 symbol 의 정보는 없고, 수신한 symbol 정보만 가지는 soft information 을 만들어 Alice 에게 보내는 soft RR 이 쉽게 가능했다. 하지만 DM 기반은 이런 soft information 을 만드는 것이 어려웠는데, 이를 해결한 것이 참고 문헌[1]의 reverse reconciliation softing(RRS)이다. 본 논문에서는 Alice 가 직접 encoding(ative)을 진행하는 것이 아닌 수동적으로 symbol 을 결정(passive)하는 passive DMCV QKD[2]에 대해서 RRS 의 적용 가능성을 살펴보고, 효율 측면에서 이점을 분석한다.

Ⅱ. 본론



[그림 1] passive DMCV QKD 구조도. 위상이 무작위인 광원을 BS 로 분할해 Alice 의 local measurement 와 Bob 에게 신호 전송을 위해 사용한다. 이때 voltage optical attenuator(VOA)를 통과하는 쪽이 QKD 신호로 사용되며, PBS 를 통해 time-multiplexing 되어 Bob 에게 전달된다.

Passive DMCV QKD 는 [그림 1]에서처럼 광원을 BS 로 분할해서 Alice 의 local measurement 를 통해 phase θ_k를 측정하고 이를 phase remapping scheme 를 통해 수동적으로 encoding 한다. 여기서 RRS 를 적용시키기 위해서는 2 가지가 중요하다. 첫째, Alice 가 symbol 정보를 온전히 알고 있어야 한다. 둘째, Bob 이 추정한 symbol $\hat{X}$에 대해 $I(N;\hat{X}) = 0$이 되도록 soft information random variable N 을 결정해야 한다. 이를 위해서는 조건을 만족하는 함수를 정할 필요가 있다. 본 논문에선 앞선 내용을 토대로 간단한 QPSK encoding 과정을 passive 방식으로 하면서 RRS 를 적용하겠다.

광원에서 나온 빛은 한 쪽은 신호로서 Bob 에게 보내지고 다른 한쪽은 Alice 가 passive encoding 을 위해서 θ_k 를 자신의 부분에서 측정한다. Encoding 한 Symbol $x_k = \left\lfloor \theta_k, \frac{\pi}{2} \right\rfloor = \{0,1,2,3\}$ 정보는 Alice 가 가지고 있고, $\varphi_k = mod\left(\theta_k, \frac{\pi}{2}\right)$를 공개 채널로 Bob 에게 전달해 phase remapping 을 할 수 있도록 한다. Bob 은 양자 채널을 통과한 후 노이즈가 섞인 신호 출력 $Y = \theta + W$를 받아 측정한다. 채널 노이즈는 간단한 AWGN 형태라 하면, $W \sim \mathcal{N}\left(0, \frac{N_0}{2}\right)$이다. 측정 결과에 φ_k를 이용한 회전 행렬 M_{φ_k}를 연산해 결과 $y' = M_{\varphi_k} y$를 얻는다. 이제 이를 토대로 symbol 추정치 $\hat{x}_k$와 추정 영역 D_i를 결정한다.

$$\hat{x} = \begin{cases} a_1 = 0, & y' \in D_1 \\ a_2 = 1, & y' \in D_2 \\ a_3 = 2, & y' \in D_3 \\ a_4 = 3, & y' \in D_4 \end{cases} \quad (1)$$

이렇게 해서 충분한 $\hat{X}$ 가 모이면 결과 sequence $\mathbb{X}$ 를 비트열 $\mathbb{B}$로 demapping 해야 하며, 미리 합의한 code 를 따라 syndrome 을 계산하여 Alice 에게 보낸다. 이때 Alice 는 decoder 를 통해 $\hat{\mathbb{B}}$를 decoding 하게 되는데, 이를 돕기 위해 Bob 은 공개 채널로 soft information random varible N을 보낸다. 이는 Y'에만 의존하고 $\hat{X}$에는 무관하여야 한다. 즉 정확한 symbol X 를 아는 Alice 에게만 유용한 정보가 된다. 그러면 Y', N 에 대한 전송을 다음과 같은 함수로 표현할 수 있다.

$$n = g(y') = \begin{cases} g_1(y'), & y' \in D_1 \\ g_2(y'), & y' \in D_2 \\ g_3(y'), & y' \in D_3 \\ g_4(y'), & y' \in D_4 \end{cases} \quad (2)$$

기존의 RRS 와는 다르게, symbol 에 대한 정보는 회전 행렬 연산을 진행해야 알기 때문에 Y 가 아니라 Y' 를 이용하여 함수를 만들어야 한다. Y' 은 Y 에 회전 행렬을 가해서 만든 결과이기 때문에, Y에 선형적이므로 기존의 RRS 와 같이 채널 분포를 이용하여 밀도 행렬 함수를 결정할 수 있다.

$$f_{Y'}(y') = \frac{1}{\sqrt{2\pi}\sigma} \sum_{a_i \in \{0,1,2,3\}} P(X = a_j) e^{-\frac{(y' - a_j)^2}{2\sigma^2}} \quad (3)$$

그럼 RRS 의 함수 조건에 의해, 다음과 같은 함수를 만들 수 있다.

$$g_i(y') = \frac{F_{Y'}(y') - F_{Y'}(\inf D_i)}{\Delta F_{Y_i'}} \quad (4)$$

$$g^{-1}(n) = F_{Y'}^{-1}\left(n \cdot \Delta F_{Y'} + F_{Y'}(\inf D_i)\right) \quad (5)$$

$$g_i'(y') = \frac{f_{Y'}(y')}{\Delta F_{Y_i'}} \quad (6)$$

Ⅲ. 결론

본 논문에서는 passive DMCV QKD 에 RRS 기법을 적용할 수 있을지, 적용한다면 어떤 부분에 유의해야 하는지를 분석했다. 수동적인 방법으로 encoding 을 하더라도, Alice 가 symbol 에 대한 정보를 가지고 있는 것은 분명하며 Bob 또한 symbol 에 대한 정보가 담긴 결과를 얻을 수 있으므로 RRS 를 적용하는데 문제가 없었다. 추후 연구에서는 이를 실제 실험 환경에 적용하여 같은 key rate 를 얻을 수 있는지를 확인하거나, security 가 여전히 같은 지를 분석할 수 있을 것이다.

ACKNOWLEDGMENT

이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원-대학 ICT 연구센터(ITRC)의 지원(RS-2021-II211810, 50%)을 받아 수행된 연구임

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. RS-2023-00242396, 50%)

참 고 문 헌

[1] Origlia, Marco, and Marco Secondini. "Soft Reverse Reconciliation for Discrete Modulations." *2025 14th International ITG Conference on Systems, Communications and Coding (SCC)*. IEEE, 2025.

[2] Li, Chenyang, et al. "Passive continuous variable quantum key distribution." *arXiv preprint arXiv:2212.01876* (2022).