CV-QKD에서 PCS-16QAM기반 MDR reconciliation 시뮬레이션

김성욱, 허준*
고려대학교, *고려대학교
djm06145@korea.ac.kr, *junheo@korea.ac.kr

Simulation of MDR Reconciiliation in PCS-16QAM based CV-QKD

Seonguk Kim, Heo Jun*
Korea Univ., *Korea Univ.

요 약

본 논문은 CV-QKD(continuous variable quantum key distribution)의 후처리 단계 중 reconciliation에 대해서 다룬다. 기존 reconciliation은 가우시안 변조에 맞춰 slice reconciliation, multidimensional reconciliation이 존재한다. 이에 대해 많은 연구가 이루어지지만 가우시안 변조가 아닌 이산 변조에 따른 reconciliation에 대한 연구가 필요한 시점이다. 본 논문에서는 가우시안 변조에서 이루어지는 MDR(multidimensional reconciliation)을 이산 변조에 적용해 보고자 한다. 다양한 이산 변조 종류 중 가우시안과 비슷한 PCS(probabilistic constellation shaping) 변조 방식을 활용할 것이며 SNR(signal to noise raio)를 기준으로 시뮬레이션 하여 reconciliation 결과를 분석할 것이다.

Ⅰ. 서 론

QKD는 alice와 bob이 양자 상태를 나눠가진 후, 후처리를 통해 고전 정보로 변환하여 최종적으로 안전한 공유키를 생성한다. 후처리의 단계는 프로토콜에 따라 차이는 있지만 대부분 parameter estimation, sifting, information reconciliation, privacy amplification 순으로 이루어진다.[1] CV-QKD의 reconciliation 단계에서는 대표적으로 slice reconciliation[2], multidimensional reconciliation[3]이 있다. 이는 DV-QKD에는 없는 CV-QKD에서의 방법으로 연속 확률 변수로 들어오는 정보를 양자화 하는 단계이다. 일반적으로 전송 거리가 짧은(약 30km까지), SNR이 0dB보다 높은 경우에는 slice가 효과적이고 전송 거리가 길어서 SNR이 0dB보다 낮은 경우에는 multidimensional이 유용하다.[4][5] 연속적인 정보를 양자화 한 이후 LDPC, turbo 코드 등을 활용하여 오류를 정정하는 과정을 거치게 된다. 이 두 방식은 가우시안 변조에 대한 reconciliation 방식으로 제안되었다. 이산 변조 방식의 CV-QKD는 또 다른 방식의 reconciliation이 요구되는데 측정 결과의 부호만을 활용하는지 더 나아가서 절댓값도 활용하는지에 따라 다르다. 부호만을 활용하는 경우는 general attack에 대한 증명이 되어있는 반면 절댓값활용에 대해서는 보안성이 증명되지 않았다.[6] 본 논문에서는 PCS 변조 방식을 활용하여 이산 변조 방식이지만 가우시안 모양의 형태로 변조하여 기존의 reconciliation을 활용하고자 한다.

Ⅱ. 본론

CV-QKD에서의 성능 평가는 key rate로 결정된다. 가우시안 변조에서 collective attacks을 가정하고 reverse reconciliation을 바탕으로 계산했을 때, secret key rate는 다음과 같이 결정된다.

$$K = \beta I(a:b) - \chi(b:E) \quad (1)$$

Alice와 Bob이 서로 공유하는 정보에 도청자가 Bob으로 부터 얻은 정보를 뺀 수식이다. 이때, Alice가 보낸 정보가 그대로 Bob에게 전송되지 않음으로 이를 나타내기 위해 β로 정보 비율을 결정한다. 이 값이 reconciliation으로 결정된다. reverse reconciliation의 시나리오는 다음과 같이 진행된다. 첫째, Raw key generation단계로 QRNG(quantum random number generator)를 활용하여 Bob이 무작위적인 bit를 생성하고 이는 raw key의 기본이 된다. 둘째, MDR단계로 Alice, Bob이 받은 양자 상태에 대해 MDR을 수행한다. 이는 연속 변수 양자 채널을 BI-AWGN(binary additive white gaussian noise)로 변환하는 과정이다. 셋째, LLR(log likelihood ratio) 과정으로 MDR 결과를 바탕으로 Alice가 조건부 확률을 계산한다. 넷째, Syndrome calculation 단계로 Bob은 알고 있는 parity check matrix를 이용하여 raw key의 syndrome을 계산하여 Alice에게 전송한다. 다섯째, 계산 및 CRC전송 단계로 Alice는 LLR와 Bob에게 받은 syndrome을 바탕으로 decoder를 진행한다. 이후 CRC(cyclic redundancy check)을 Bob에게 전송한다. 여섯째, Bob은 받은 CRC를 바탕으로 raw key를 사용할 것인지 폐기할 것인지를 결정한다.[7] 본 논문에서는 전체적인 reconciliation을 다루지 않고 MDR 과정까지만 진행하였다.

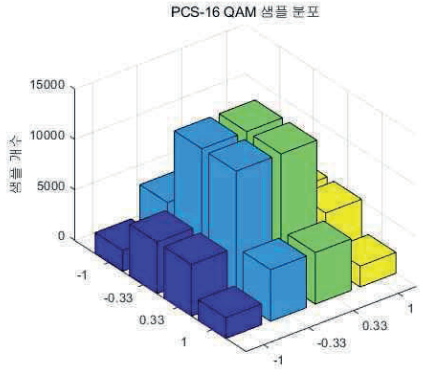

그림 2 PCS-16 QAM 샘플 분포

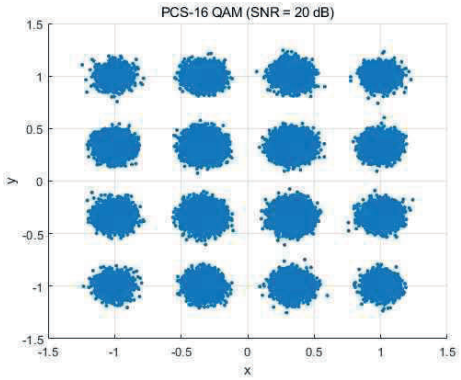

그림 3 PSC-16 QAM constellation point

다음과 같이 가우시안 형태의 16 QAM 샘플을 생성하고 Bob 쪽에서 QRNG를 대신하여 무작위한 비트를 생성 후 MDR을 진행해 주었다. MDR은 연속적인 분포를 이산적인 분포로 변환시켜주는 과정인데 벡터들을 고차원 공간에서 회전시켜 고르게 분포하도록 퍼지도록 하는 과정이다. 이를 위해서 회전 벡터가 필요한데 Cayley Dickson construction [8]를 활용하면 구할 수 있다.

$$(a,b)(c,d) = (ac - db^*, a^*d + cb) \quad (2)$$

이는 고차원 공간(dim:1,2,4,8)에서 norm preserving rotation의 특징을 가지고 있어 필수적 요소를 포함하고 있으며 계산도 간결하여 빠르게 구할 수 있다. 계산 방식은 A, B벡터가 있을 때 A를 a, b로 나누고 B를 c, d로 나누고 계산을 한다. 이때, 벡터의 요소가 1개 될 때 까지 절반으로 나누는 작업을 반복한다. 즉, 8개의 요소로 한 벡터가 구성되어 있으면 계속해서 절반으로 나누어서 1개의 요소가 남을 때까지 반복한 후 그 요소에 대해서 계산을 진행한다. 이런 과정을 거치기 때문에 dim: 1,2,4,8 에서만 만족한다.

MDR 연산을 거친 후 Alice는 Bob에서의 받은 MDR 결과 값을 바탕으로 LLR을 연산한다. 이때, channel noise의 분산, alice의 norm 값 등으로 계산되어 크기가 보정된다. LLR 값을 바탕으로 양수, 음수에 따라 hard decision을 진행한다.

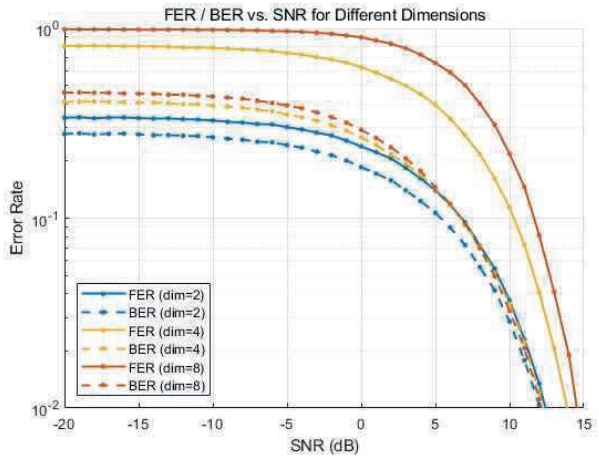

그림 5 차원 수에 따른 MDR 시뮬레이션

dim: 2, 4, 8일 때를 기준으로 MDR을 시뮬레이션 하였다. 낮은 SNR에서 dimension이 높은 MDR의 성능이 좋다는 연구결과들과 상반되는 결과가 나왔다. 본 결과는 MDR 계산 이후의 LDPC 기반 오류 정정 절차가 생략된 실험 설정에 따른 것으로 추정된다. 따라서 보다 정밀한 성능 평가를 위해서는 오류 정정 코드를 포함한 이후의 단계의 적용이 필요하다.

Ⅲ. 결론

PCS 변조 기법이 가우시안 형태로 나타낼 수 있음을 활용하여 기존 가우시안 변조 CV-QKD에서 활용되던 Multidimensional reconciliation을 적용해 보았다. 16-QAM 변조를 PCS를 이용하여 gaussian형태로 만들었고 샘플 수는 10^5개, SNR은 -20dB~15dB, MDR차원은 2,4,8을 조건으로 시뮬레이션을 진행하였다. 결과는 예상과 다르게 SNR이 안 좋은 상황에서 낮은 차원의 MDR이 더 좋은 성능을 나타내었다. 이는 생략된 오류 정정 부분이 원인으로 유추되며 LDPC, CRC를 적용하여 정정을 하면 다른 것과가 나올 것으로 기대된다. 향후에는 128-QAM, 256-QAM과 같은 고차원 이산변조 방식과[9] 다양한 후처리 단계들을 결합하여, MDR이 어떤 분포에서 적합한지에 대한 추가적인 분석이 가능할 것이다. 본 연구의 시뮬레이션 시나리오 및 코드는 [6]의 논문과 제공된 소스코드를 기반으로 수정 및 재구성하여 사용하였다.

ACKNOWLEDGMENT

본 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원(No. 2020-0-00014, 결함허용 논리양자큐빗 환경을 제공하는 양자운영체제 원천기술 개발, 50)과 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. RS-2023-00242396, 50)

참 고 문 헌

[1] Luo, Yi, et al. "An Overview of Postprocessing in Quantum Key Distribution." Mathematics (2227-7390) 12.14 (2024).

[2] Van Assche, Gilles, Jean Cardinal, and Nicolas J. Cerf. "Reconciliation of a quantum-distributed Gaussian key." IEEE Transactions on Information Theory 50.2: 394-400 (2004).

[3] Leverrier, Anthony, et al. "Multidimensional reconcilia tion for a continuous-variable quantum key distribution." Physical Review A—Atomic, Molecular, and Optical Physics 77.4 : 42325(2008).

[4] Usenko, Vladyslav C., et al. "Continuous-variable quantum communication." arXiv preprint arXiv:2501.12801 (2025).

[5] Zhang, Yichen, et al. "Continuous-variable quantum key distribution system: Past, present, and future." Applied Physics Reviews 11.1 (2024).

[6] Leverrier, Anthony. "Information reconciliation for discretely-modulated continuous-variable quantum key distribution." arXiv preprint arXiv:2310.17548 (2023).

[7] Cil, Erdem Eray, and Laurent Schmalen. "An Open-Source Library for Information Reconciliation in Continuous-Variable QKD." arXiv preprint arXiv:2408.00569 (2024).

[8] Baez, John. "The octonions." Bulletin of the american mathematical society 39.2 : 145-205 (2002).

[9] Almeida, Margarida, et al. "Reconciliation Efficiency Impact on Discrete Modulated CV-QKD Systems Key Rates." Journal of Lightwave Technology 41.19 : 6134-6141 (2023).