CV-QKD의 Gaussian Modulation의 성능 검정 방법 분석과 동향에 관한 연구

이상규, 허준*

고려대학교, *고려대학교

{2023020754, ksuwer, cherishiz, *junheo}@korea.ac.kr,

A Study on Performance Verification Mathods and Trends of Gaussian Modulation in CV-QKD

Lee Sang Gyu, Ha Jin Youn, Seo Youngjin, Heo Jun*

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

요 약

본 논문은 CV-QKD에서 사용되는 변조 기술인 가우시안 변조(Gaussian Modulation) 과정을 통해 생성된 신호가 가우시안 분포(gaussian distribution)와의 유사성을 평가하는 기법들을 분석하고 최근에 사용되는 기법들의 동향을 분석하는 것이 목표이다. 가우시안 변조에서 가우시안성(gaussianity)이 높을수록 통신의 안전성과 보안성을 향상시키며, 양자 통신 시스템에서 신뢰성 있는 정보 전송을 보장하는 데 중요한 역할을 한다. 가우시안성이 높을수록 양자 비트는 외부 잡음과 간섭에 강한 특성을 갖게 되고 외부의 도청으로부터 보호할 수 있다. 또한 가우시안성이 높을수록 오류 보정 알고리즘을 효과적으로 적용하여 전송 중 발생하는 에러를 보다 정확하게 수정할 수 있다. 따라서 가우시안 변조가 얼마나 정확하게 가우시안 분포를 따르는지를 확인하는 데 사용되는 다양한 통계적 검정 기법들 중 Anderson - Darling(AD), Jarque - Bera (JB), Shapiro-Wilk (SW), Linear regression test를 탐구하고 최근 사용되는 기법들의 동향을 분석하였다.

Ⅰ. 서 론

본 논문에서는 Continuous Variables Quantum Key Distribution (CV-QKD)에서 사용되는 핵심 변조 기술인 가우시안 변조(Gaussian Modulation)의 가우시안성 검정 기법에 초점을 맞추고 있다. CV-QKD에서 가우시안 변조는 양자 정보의 안전한 전송과 통신의 보안성을 향상시키는 데 중요한 역할을 한다.[1]

가우시안 변조는 신호의 가우시안성을 높이는 데 기여한다. 이것은 외부의 잡음과 간섭에 강하며 도청으로부터 정보를 보호하는 데 도움이 된다. 예를 들어, 외부에서의 도청을 막기 위해 양자 비트는 무작위한 외부 잡음과 간섭에 강한 특성을 갖는데 가우시안 변조에서 신호가 가우시안성을 잘 따르면, 이러한 잡음이나 간섭을 마스킹(masking)하거나 제거하는데 효과적일 수 있다. 이는 정보가 제3자에 의해 감지되거나 해독되는 것을 방지하여 데이터의 기밀성과 보안성을 강화시켜준다. 이와 함께, 높은 가우시안성은 전송 중 발생하는 오류를 보다 정확하게 수정하는데도 중요한 역할을 한다. 예를들어, 외부 잡음이나 간섭이 증가하더라도 가우시안 분포를 따르는 신호는 오류 정정 알고리즘을 적용하여 데이터를 보다 정확하게 복구할 수 있다. 이는 데이터의 손실을 줄이고 신뢰성 있는 정보를 전송하는 데 기여한다. CV-QKD에서 사용되는 가우시안 변조의 가우시안성을 평가하기 위한 통계적 검정 기법을 조사하고, 최근 사용되고 있는 기법들의 동향을 분석한다. 특히 Anderson - Darling(AD), Jarque - Bera (JB), Shapiro-Wilk (SW), Linear regression test 등의 통계적 검정 기법들에 초점을 맞춰 설명한다.

본 논문에서는 가우시안 변조의 정확성을 평가하는데 사용되는 다양한 평가 방법들을 살펴보고 기법들의 최근 동향을 분석한다.

Ⅱ. 본론

통계적 검정 기법은 주어진 데이터를 사용하여 특정 가설을 평가하거나 결론을 도출하는 데 사용되는 방법이다. 이러한 기법들은 데이터를 분석하여 특정 가설이나 가정이 사실인지 아니면 우연히 발생한 것인지를 판단한다. 통계적 가설 검정은 p-value(유의확률)이라는 값을 반환한다. 이 값은 귀무가설(H_0)을 기각하거나 기각 하지 않을지를 판단하는 데 사용된다. 이를 위해 미리 설정된 유의수준(α)이라 불리는 임계값과 p-value를 비교하고 만약, p-value가 α보다 작으면 귀무가설을 기각할 수 있다. 이에 따라 검정의 신뢰 수준을 1-α로 설정된다. 예를 들어, 유의수준(α)를 5%로 설정하고 p-value가 95%보다 크다면, 5% 유의수준에서 데이터가 정규분포를 따른다는 귀무가설을 기각할 수 없다는 결론을 내릴 수 있다. 이러한 통계적 검정 기법 중에서 분포 적합 검정 기법에는 Anderson-Darling(AD), Jarque-Bera(JB), Shapiro-Wilk(SW)등이 있다.[2]

먼저 Anderson-Darling(AD) 검정은 특정한 확률 분포를 따르는 모집단에서 추출된 데이터 샘플인지를 판단하는 데 사용된다. 데이터가 기대되

는 분포와 얼마나 일치하는지를 평가하며, 주로 꼬리 부분에서의 일치도를 살펴보는데 유용하다.

$$A^2 = -N - S \tag{1}$$

$$S = \sum_{i=1}^{N} \frac{(2i-1)}{N} [\ln(F(Y_i) + \ln(1 - F(Y_{N+1-i})] \tag{2}$$

A^2은 Anderson-Darling 검정 통계량을 의미하며 N은 표준 정규 분포를 따르는 값들의 집합, F는 주어진 특정 분포의 누적 분포 함수, Y_i는 검정하려는 값들의 집합을 의미한다.

Jarque-Bera(JB) 검정은 데이터의 왜도(skewness)와 첨도(kurtosis)가 정규분포와 일치하는지를 판단하는 검정 방법이다. n개의 통계데이터 $x_1, x_2, \ldots x_n$에 대하여

$$JB = \frac{n}{6}(S^2 + \frac{1}{4}(K-3)^2) \tag{3}$$

$$S = \frac{\hat{\mu}_3}{\hat{\mu}_2^{3/2}}, K = \frac{\hat{\mu}_4}{\hat{\mu}_2^2} \tag{4}$$

$$\hat{\mu}_j = \frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})^j \tag{5}$$

여기서 $\bar{x}$는 n개 데이터의 표본평균이고 S는 sample skewness이고 K는 sample kurtosis이다.

Shapiro-Wilk(SW) W값이 작을수록 데이터가 정규 분포에서 벗어난 정도가 크다는 증거가 된다.

$$W = \frac{(\sum_{i=1}^{n}\alpha_i x_{(i)})^2}{\sum_{i=1}^{n} x_i - \bar{x}^2} \tag{6}$$

Sagnac 기반 가우시안 변조기를 이용한 CV-QKD 연구에서는 이들을 이용하여 Table 1과 같이 가우시안성을 검증했다.[3]

Table 1. Success Rates at Different Values of n under α=0.05

	Modulated Data			Received Data		
n	AD	JB	SW	AD	JB	SW
512	0.940	0.944	0.940	0.934	0.942	0.930
1024	0.952	0.944	0.936	0.936	0.926	0.940
2048	0.956	0.948	0.948	0.936	0.928	0.904
4096	0.936	0.952	0.952	0.864	0.872	0.888

최근 CV-QKD 연구에서는 Linear feedback shift registers를 순환적으로 회전시키는 방식으로 가우시안 변조로 활용하는 연구(2020)가 진행되었고 Anderson-Darling Test와 Shapiro-Wilk Test 가 이용되었다.[2] CV-QKD를 위한 가우시안 변조기를 설계하는 연구(2021)에서는 Jarque-Bera Test를 사용했다.[4]

Ⅲ. 결론

본 논문에서는 CV-QKD에서 사용되는 가우시안 변조를 통해 얻어낸 신호의 가우시안성을 검증하는 통계적 검정 기법인 Anderson-Darling(AD), Jarque-Bera(JB), Shapiro-Wilk(SW)에 대해 분석했고 반환되는 p-value와 유의수준(α)와의 값을 비교함에 따라 귀무가설을 기각할지 말지를 판단하는 기준이 됨을 살펴보았다. 그리고 최근 CV-QKD 관련 연구중 가우시안 변조에 대한 가우시안성을 검정하는 기법들이 어떤 것들이 있는지 동향을 알아보았다. 이러한 가우시안성 검정 기법들을 통해 정밀한 가우시안 변조를 할 수 있게 되면 CV-QKD의 안정성과 신뢰성을 더욱 향상시킬 수 있을 것으로 보인다.

ACKNOWLEDGMENT

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

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음(IITP-2024-2021-0-01810).

이 논문은 2024년도 4단계 BK21 사업에 의하여 지원되었음.

참 고 문 헌

[1]Zhengwen Cao, “Continuous-Variable Quantum Secure Direct Communication Based on Gaussian Mapping”,PHYSICAL REVIEW APPLIED,August 2021.

[2]Guillermo Cotrina ,“Gaussian Pseudorandom Number Generator Baesed on Cyclic Rotations of Linear Feedback Shift Registers”,sensors, April 2020.

[3]Huanxi Zhao,“Simple continuous-variable quantum key distribution scheme using a Sagnac-based Gaussian modulator“,Optics Letters,June 2022.

[4]Xiunan Sun, Liang Hao,“Design of Gaussian modulator for continuous-variable quantum key distribution”, SPIE, December 2021.