연속 변수 양자 통신 연구 동향

김영준, *고영채
고려대학교
mkeeper@korea.ac.kr, *koyc@korea.ac.kr

Research Trend on Continuous Variable Quantum Communication

YoungJun Kim, *Young-chia Ko
Korea University

요 약

본 논문에서는 양자 통신을 실제적인 환경에서 구현하고자 하는 노력의 일환으로 개발된 연속 변수 양자 통신 기법에 대해 소개한다. 연속 변수 양자 통신 전반에 대한 설명에 이어 이를 이용한 최신 응용 기술들을 소개한다. 연속 변수 환경에서 구현된 다중 접속 채널, 최소 제곱 예측법, 그리고 다중 반송파 기법을 소개하고 그 효과와 한계를 서술한다.

1. 서론

신호는 디지털화 과정을 거치면 필연적으로 정보의 일부가 사라진다. 하지만 오류 정정 부호와 다양한 후처리 기법의 발전, 그리고 이를 뒷받침하는 반도체 기술의 발전을 통해 현재 아날로그 통신은 대부분 디지털 통신으로 대체되었다. 이제 통신은 양자 통신이라는 새로운 패러다임 변화에 직면해 있다.

큰 수를 인수분해 하는 것은 수가 커짐에 따라 지수적으로 증가하는 복잡도를 갖는다. 이 원리를 이용해 큰 수를 공개키로 사용하고 그 인수를 비밀키로 사용하는 비대칭 암호화 기술이 산업계에서 널리 이용되고 있다. 하지만 Shor 의 인수분해 알고리즘[1,4]에 의해 양자 컴퓨터를 이용하여 큰 수의 인수분해 문제를 선형적 복잡도 이하로 풀 수 있는 가능성이 열렸다. 이는 현존하는 대부분의 암호화 원리를 무력화시킬 수 있는 파괴력을 지녔다.

반면 양자 암호는 인수분해의 계산 복잡성이나 도청자의 연산능력 등의 외부적인 요인과 관계없이 무조건적으로 안전성을 보장하는 기술로 알려져 있다. 이는 양자의 고유 특성인 중첩, 붕괴를 수반하는 측정, 복제불가능성 등을 이용하는 기술로, 1984 년 C. Bennett 에 의해 실제 실험실에서 구현된[2] 이후 많은 연구가 진행되고 있다.

Bennett 이 제시한 초기 양자 암호화 기법은 단일광자의 양자적 특성을 이용한다. 단일 광자를 이용하기 위해서는 단일 광자 생성기, 단일 광자 측정기 등의 고가의 장비가 필요하며, 이를 구동하기 위해 절대온도 근방의 낮은 온도를 유지해야 한다.

양자 통신의 획기적인 발전은 연속변수를 이용한 양자 정보 기술을 통해 이루어지고 있다. 극저온 상태에서 단일 광자를 주로 이용하는 이산 변수 양자 정보 기술과 달리 연속 변수 양자 정보 기술은 약화시킨 레이저를 이용하여 구현한다[3]. 기존에 상용 통신에서 사용하고 있는 광통신망을 사용할 수 있고, 레이저 기술이 상당히 발전되어 있어 상대적으로 가격이 저렴한 것이 가장 큰 장점이다. 실제로 상업화에 성공한 양자 통신 기술은 대부분 연속변수 양자를 이용한 것이다.

많은 연구를 통해 이산 변수로 구현된 양자 통신 시스템은 동일한 기능을 하는 연속 변수 양자 통신 시스템으로도 구현되었다. 가장 기본적인 양자 상태 생성에서부터, 얽힘, 유니버셜 양자 게이트, 측정 등 각 요소기술에 대한 연속 양자 버전이 연구되고 있다[6]. 또한 이산 변수에서 제안된 암호키 분배 기법들도 연속 변수를 이용하여 구현하기 위한 연구가 계속되고 있다.

연속 변수 양자 통신 시스템은 가장 빠르게 상용화를 이룩한 양자 정보 기술이다. 또한 고전적인 방송통신공학과의 접점이 가장 많은 양자 정보 기술이다. 본 논문을 통해 양자 통신을 실현하기 위한 최근의 연구들을 소개하고자 한다.

2. 연속 변수 양자 통신

연속 변수 양자 통신은 전자기파의 양자화된(quantized) 모드가 단일 조화 진동자(single harmonic oscillator, SHO)의 위치와 운동량에 대응한다[6]. 위치와 운동량은 연속 변수로 정의된 양자 상태를 나타내는 두 기저로써 사용되며, 이는 고전 통신에서 사용되는 신호 공간의 동상위상(in phase)과 직교위상(quadrature phase)과 여러 면에서 유사하다.

논문 [6]에서는 양자의 기본 특성인 얽힘(entanglement), 전이(teleportation), 측정(measurement)이 연속 변수에서 어떻게 구현되는지에 대해 수학적인 표현을 제공한다. 또한 양자 역학을 토대로 구현된 기초적인 어플리케이션인 양자 암호, 덴스 코딩, 양자 오류 정정 부호, 기초적인 양자 암호화 등에 대한 프로토콜을 제공하고 있다.

3. 연속 변수 다중 접속 채널의 사용자 검출

연속 변수 양자 통신은 순수한 양자 상태(pure

state)[4]를 전송하지만 채널의 잡음이 더해져서 수신자는 섞인 상태(mixed state)를 수신한다. 논문 [7]은 채널 잡음이 더해지는 다중 접속 채널 환경에서 사용자를 검출하는 문제를 이산 결맞음 상태(Discrete coherent state, DCS) 근사 검출 기법을 이용하여 풀었다.

수신 신호를 측정하기 위하여 POVM[4]을 이용하였고, Bayes 의 검파 기법을 적용하여 가장 확률이 높은 가설을 선택하였다. 가산 가우시안 잡음 상태에서 다중 사용자의 검출 성능을 분석하였다. 또한 다중 사용자간의 간섭 효과를 설정하고 그에 따른 검출 오류 확률을 분석하였다.

다만 검출 가능한 사용자 숫자가 2 명에 그쳤고, 각 사용자의 부호화 기법도 BPSK 로 한정된 한계가 있다. 다양한 부호화 기법과, 3 명 이상의 사용자에 대한 검출 기법에 대한 연구로의 확장이 기대된다.

4. 연속 변수 양자 상태의 최소 제곱 예측법

연속 변수 양자 상태는 서로 직교하지 않은 코히런트 상태(coherent state)로 구현된다. 서로 직교하지 않는 상태를 검출하는 과정에서 필연적으로 오류가 발생한다[4]. 따라서 오류율을 줄이기 위해서 측정기를 설계하는 연구[9, 10]나 코히런트 상태 집합을 설계하는 연구[11, 12]가 진행되고 있다.

논문 [8]은 POVM[4]을 측정기로 사용하는 연속 변수 양자 통신 시스템에 최소 제곱 예측법을 적용하여 연속 변수 양자 상태의 검출 오류율을 줄이는 방법을 제안하였다. 제안한 기법 성능의 상한과 하한을 분석하여, POVM 을 단독으로 활용한 측정 기법 대비 0.001 의 오류율을 얻기 위한 평균 광자 개수[11]에서 최소 4, 최대 5 개의 이득을 얻었다.

논문 [8]의 검출 기법에는 선행(a priori)확률을 0.5 로 하여 Bayes 의 검출 기법만 사용되었다. 따라서 선행확률이 0.5 가 아닐 때의 리스크를 최소화 할 수 있는 최소최대(miniMax) 검출 기법이나, 주어진 오탐 확률 제한을 만족시키되 탐지 확률을 최대화하는 네이만-피어슨(Neyman-Pearson) 검출 기법으로의 확장을 고려해 볼 수 있다.

5. 다중 반송파 연속 변수 양자 통신 기법

연속 변수를 이용한 양자 통신의 가장 큰 장점은 실제적 구현이 쉬운 데에 있다. 상용 광통신망을 이용하기 때문에 여러 개의 채널을 동시 사용하는 데에 큰 어려움이 없기 때문에 다중 반송파를 이용한 다양한 기법이 연구되고 있다.

L. Gyongyosi 는 논문 [13-17]을 통해 다중 반송파를 이용한 다양한 기법을 연구하고 있다. 다중 사용자를 지원하고[14], 절대적 안전성을 보장하기 위한 QBER 의 임계점[5]을 구하고[15], 다차원 결합 추출기법을 개발[16]하여 반송파 차원[17]으로 확장 가능성을 열었다.

Gyongyosi 의 다중 반송파 기법은 역 고속 퓨리에 변환(IFFT)을 이용한 변조, 채널 상태에 따른 적응적 변조 기법 등 고전 통신의 직교주파수다중분할 기법(OFDM)과 상당히 유사하다. 채널 상황이 좋지 않은 반송파를 적게 사용하여 전체 전송 속도를 높이고 잡음에 대한 저항력을 높인다. 이에 추가하여 양자 암호화 기법에서 논의되는 도청 기법의 일종인 가우스 수집 공격에 대한 내구성을 높이는 효과도 얻는다.

6. 결론

본 논문에서는 양자 통신의 가장 큰 이슈인 연속 변수 양자 통신 기법에 대해 소개하였다. 특히 방송 통신 공학을 하고 있는 공학도가 익숙한 개념인 다중 접속 채널, 최소 제곱 예측법, 다중 반송파 기법 등이 적용된 최신 기법들을 소개하였다.

Acknowledgement

본 연구는 미래창조과학부 및 정보통신기술연구진흥센터의 정보통신 · 방송연구개발사업의 일환으로 수행하였음.
[12-911-04-003, 양자 통신 및 양자 정보 처리를 위한 기반 기술 개발]

Reference

[1] P. W. Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”, SIAM J. Comput. 26 (5): 1484–1509, 1997
[2] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography" Journal of cryptology, vol. 5, no. 1, pp.3-28, 1992.
[3] F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, “Quantum Key Distribution Using Gaussian modulated Coherent States”, Nature, Vol.412, p.238, 2003
[4] M. A. Nielsen, & I. L. Chuang, “*Quantum Computation and Quantum Information*”, Cambridge University Press, 2000.
[5] N. Lütkenhaus, “Estimates for practical quantum cryptography”, Phys. Rev. A 59, 3301, 1999
[6] S. L. Braunstein, P. V. Loock, “Quantum Information with Continuous Variables”, Rev. Mod. Phys. 77, 513, 2005
[7] S. Zhao, F. Gao, X. –L. Dong, and B. Zheng, “Detection Scheme for Quantum Multiple Access Channel with Noisy Coherent State”, IEEE WCSP, International Conference on, 2010
[8] W. Yu, B. Zheng, and S. Zhao, "Quantum detection of coherent-state signal using least-square estimation", IEEE ICCT, International Conference on, 2010
[9] M. Ban, K. Kurokawa, R. Momose, and O. Hirota, “Optimum measurements for discrimination among symmetric quantum states and parameter estimation,” International Journal of Theoretical Physics, vol. 36, no. 6, pp. 1269–1288, 1997.
[10] P. Hausladen and W. K. Wootters, “A pretty goodmeasurement for distinguishing quantum states,” Journal of Modern Optics, vol. 41, no. 12, pp. 2385–2390, 1994.
[11] K. Kato, M. Osaki, M. Sasaki, and O. Hirota, “Quantum detection and mutual information for qam and psk signals,” Communications, IEEE Transactions on, vol. 47, no. 2, pp. 248–254, 1999.
[12] Y. Kim and Y. C. Ko, “Detection of quantum circular QAM signals,” IEEE ICTC, International Conference on, 2013
[13] L. Gyongyosi and S. Imre, “Adaptive multicarrier quadrature division modulation for long-distance continuous-variable quantum key distribution", Proc. SPIE 9123, Quantum Information and Computation XII, 912307 (May 22, 2014)
[14] L. Gyongyosi, “Multiuser Quadrature Allocation for Continuous-Variable Quantum Key Distribution”, arXiv:1312.3614, 2013
[15] L. Gyongyosi, “Security Thresholds of Multicarrier Continuous-Variable Quantum Key Distribution”, arXiv:1404.7109, 2014
[16] L. Gyongyosi, “Multidimensional Manifold Extraction for Multicarrier Continuous-Variable Quantum Key Distribution”, arXiv:1405.6948, 2014
[17] L. Gyongyosi, “Subcarrier Domain of Multicarrier Continuous-Variable Quantum Key Distribution”, arXiv:1406.6949, 2014