연속변수 양자 정보를 활용한 양자 보안 기술

Quantum Secure Technologies Based on Continuous-Variable Quantum Information

김갑중 (K.-J. Kim, k.j.kim@etri.re.kr) 양자통신연구실 선임연구원
오준상 (J. Oh, js.oh@etri.re.kr) 양자통신연구실 연구원

ABSTRACT

This paper reviews recent advances in continuous-variable quantum technologies, with a focus on quantum random number generation and quantum key distribution. Continuous-variable approaches enable the development of practical, high-speed quantum systems that utilize room-temperature and telecom-compatible optical components. Continuous-variable quantum random number generation provides secure, high-throughput randomness by measuring vacuum fluctuations, with recent implementations achieving rates of up to 100 Gbps. Continuous-variable quantum key distribution employs coherent states, homodyne detection, and advanced error reconciliation techniques to enable long-distance, scalable secret key distribution. These advancements underscore the strong potential for the real-world deployment of quantum secure communication systems.

KEYWORDS continuous-variable quantum information, continuous-variable quantum random number generation, continuous-variable quantum key distribution, 연속변수 양자 정보, 연속변수 양자 난수 생성, 연속변수 양자 키 분배

I. 서론

연속변수(CV: Continuous-Variable) 양자 정보는 양자화된 전자기장 모드의 진폭 쿼드러처처럼, 고윳값(Eigenvalue)이 연속적으로 분포하는 물리량을 기반으로 표현되는 양자 정보 형태다[1,2]. 이러한 특

* DOI: https://doi.org/10.22648/ETRI.2025.J.400508
* 공동 제1저자 김갑중, 오준상 (공동 제1저자 오준상 추가, 2025. 10. 29. 수정)
* 본 보고서는 2024년도 ETRI 내부 연구 사업의 지원을 받아 수행된 연구임[24YS1400, 양자 난수 생성기를 위한 능동 정렬 이종 집적 실리콘 포토닉스 기반 광학 엔진 기술개발], 2025년 과학기술정보통신부의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임[2019-0-00005, 근거리 저속 이동형 양자암호통신을 위한 편광기반 무선 양자키분배 송수신부 직접화 모듈 기술 개발], [2022-0-01014, 경량형 무선 양자 중계 플랫폼 기술 개발], [RS-2024-00398716, 위성 양자 보안 통신을 위한 30km급 장거리 무선 양자 암호키 분배 전송 기술 및 위성 양자 암호키 분배(QKD) 핵심 요소기술개발], [RS-2025-02218080, 양자키분배 광집적화 모듈기반 소형 신뢰 중계기 및 핵심 전자 회로의 집적화 기술 개발]. 본 보고서는 2025년 과학기술정보통신부의 재원으로 한국연구재단(NRF)의 지원을 받아 수행된 연구임[RS-2024-00439005, 양자 기술용 반도체 레이저 다이오드 광원 및 모듈 개발].

성을 활용한 CV 양자 기술은 양자컴퓨팅, 양자 암호 통신, 양자 센싱 등 다양한 분야에서의 응용 가능성이 주목받으며, 최근 빠르게 연구가 확산되고 있다.

본고에서는 양자 정보 기술 중에서도 특히 양자 보안 기술에 초점을 맞추어, CV 양자 정보 기반의 양자 난수 생성(QRNG: Quantum Random Number Generation)과 양자 키 분배(QKD: Quantum Key Distribution) 기술의 연구 동향을 살펴본다.

일반적으로 사용되는 이산변수(DV: Discrete-Variable) 기반 양자 보안 기술은 여전히 구현상의 한계를 안고 있다. 예를 들어, 광원 기술의 경우 결정론적 단일광자 광원(Deterministic Single-Photon Source)은 여전히 실험실 수준에 머물러 있기 때문에, 실질적으로는 확률적 단일광자 광원(Probabilistic Single-Photon Source)에 의존하고 있다. 이는 시스템의 복잡성을 증가시킬 뿐만 아니라, 다광자(Multi-Photon) 발생 확률의 증가로 보안에 취약해진다. 또한, DV 기반 기술에서 필수적으로 사용되는 단일광자 검출기(Single-Photon Detector)는 암계수(Dark Count), 낮은 검출 효율(Detection Efficiency), Afterpulse, Dead Time 등의 기술적 한계로 인해 고속 양자 통신 및 암호 시스템 구현에 어려움을 겪는다. 물론, 초전도 기반 단일광자 검출기는 이러한 문제를 상당 부분 해소하였지만, 극저온 냉각 장치와 높은 장비 비용으로 인해 실용화에는 여전히 제약이 따른다.

이러한 한계를 극복하는 현실적인 대안으로 등장한 CV 양자 기술은 상온 환경에서 동작 가능하며, 범용 광학 소자를 활용하므로 경제적이고 실용적이다. 또한, 기존 DV 방식보다 현저히 빠른 속도와 높은 확장성을 제공하여, 실질적인 양자 보안 시스템 구현에 매우 적합하다. 특히 진공 상태(Vacuum State) 또는 결맞음 상태(Coherent State)를 사용하는 CV 기술은 상용 연속파(CW: Continuous-Wave) 레이저와 호모다인 검출기(Homodyne Detector)를 사용하므로 기존 광통신 인프라와 융합이 용이하다는 중요한 장점을 갖는다. 이러한 장점으로 인해 CV 기반의 양자 기술은 실질적인 양자 보안 시스템 구현을 위한 새로운 접근 방식으로 주목받고 있으며, 대표적인 예가 바로 QRNG 기술이다.

QRNG 기술의 최종 목표는 완벽히 예측할 수 없는 진정한 무작위성(True Randomness)을 제공하는 데 있다[3]. 기존의 의사 난수 생성(Pseudo-Random Number Generation)은 알고리즘에 기반하기 때문에 본질적으로 결정론적이며, 이는 보안상 근본적인 한계를 지닌다. 반면, QRNG는 양자역학적 불확정성을 기반으로 하기 때문에 생성된 난수를 예측하거나 복제 및 역추적할 수 없다. 따라서 QRNG에서 얻은 난수는 인증, 프로토콜 설정 등 보안 시스템의 핵심 요소로써 활용이 가능하며, 특히 QKD의 비트열 무결성과 절대적 보안성을 보장하는데 핵심적인 역할을 한다.

QRNG 구현 방식으로는 크게 방사성 붕괴 기반, 양자광학 기반으로 구분된다. 방사성 붕괴 기반 QRNG는 최초로 구현된 QRNG로 상용화까지 이르렀으나, 낮은 난수 생성 속도와 방사성 물질의 안전성 문제라는 한계를 지닌다. 이에 따라 단일 광자 기반, 광자 도착 시간 기반, 레이저 위상 확산 기반, 진공 요동 기반과 같은 양자광학 기반의 QRNG가 활발히 연구되고 있다. 이러한 여러 방식 중에서도 최근 연속변수 양자 정보를 활용하는 CV-QRNG (Continuous-Variable Quantum Random Number Generation) 기술이 주목받고 있다. 특히, CV-QRNG 기술 중 하나인 진공 요동 기반의 QRNG가 초고속, 초소형 QRNG 구현을 위한 유력한 방식으로 평가받고 있다.

진공 요동 기반 QRNG는 진공 상태(Vacuum State)의 연속적인 진폭 쿼드러처 고유상태(Amplitude Quadrature Eigenstate)를 측정하여 난수를 생성하는

방식이다. 이 방식은 상용 레이저와 광분배기, 상온에서 작동 가능한 호모다인 검출기를 이용해 간단히 구현할 수 있으며, 높은 속도로 난수를 생성할 수 있다. 따라서 단일광자 광원과 검출기를 사용하는 기존의 DV-QRNG 방식에 비해 구현의 용이성 및 속도 측면에서 큰 장점이 있다.

이러한 CV-QRNG 기술은 실험실 수준의 연구 단계를 넘어, 실제 응용이 가능한 고속 난수 생성 장치로 발전하고 있다. 대표적인 사례로, 광집적회로(PIC: Photonic Integrated Circuit)를 이용한 칩 기반 CV-QRNG가 보고되었으며, 이는 크기 · 무게 · 소비전력을 효과적으로 줄이는 동시에 초고속 난수 생성도 가능하게 하였다. 또 다른 연구에서는 단일 칩 내에서 여러 채널을 병렬로 운용하여 난수 생성 속도를 크게 향상시킨 엔트로피 소스(Entropy Source)도 보고되었다. 또한, 디지털화 장치의 보정과 검출기의 디지털 등화(Digital Equalization) 기술을 결합하여 고전적 잡음을 효과적으로 억제하였으며, 이를 통해 최대 100Gbps의 초고속 난수 생성 속도를 달성 하였다.

QRNG와 마찬가지로, CV 기반 기술이 적용 가능한 또 다른 양자 보안 핵심 기술로 QKD가 주목받고 있다. 현재 대부분의 암호화 기술은 수학적으로 복잡한 연산 문제를 기반으로 보안을 유지하고 있으나, 양자 컴퓨터와 같은 월등한 계산 능력을 지닌 장치가 등장할 경우, 기존의 암호 체계는 근본적인 위협에 직면하게 될 것으로 예상된다.

특히 양자컴퓨터는 피터 쇼어(Peter Shor)가 제안한 알고리즘[4]을 활용하여 기존의 암호 체계에서 사용되는 소인수분해 문제를 고전 컴퓨터보다 훨씬 빠르고 효율적으로 해결할 수 있어, 현재 가장 널리 사용되고 있는 RSA와 같은 기존 공개 키 암호 방식은 더 이상 안전하지 않게 될 것이다. 이에 따라 기존 암호 기술을 대체할 수 있는 근본적으로 새로운 접근 방법이 요구되고 있으며, 대표적인 해결책이 QKD 기술이다.

QKD 기술 중에서도 특히 CV 기반 방식은 실용성과 구현 용이성 측면에서 주목받고 있다. CV-QKD는 CV-QRNG와 유사하게 CW 레이저 광원과 호모다인 검출기와 같이 상온에서 동작하는 범용 광학 소자를 사용하기 때문에, 기존 광통신 인프라와의 높은 호환성, 빠른 키 생성 속도, 시스템 확장성 등에서 유리한 특성을 보인다. 특히 파장 분할 다중화(WDM: Wavelength-Division Multiplexing) 기술에 적합한 특징은 상용 광통신 기술과의 융합을 더욱 쉽게 만든다.

CV-QKD 기술은 현재 실험실 단계를 넘어, 실제 운용 환경(Field Environment)에서의 검증과 프로토타입 개발 단계에 진입하고 있다. 특히 기존 결맞음 광통신에서 활용된 디지털 신호 처리(DSP: Digital Signal Processing) 기반 고속 신호 처리 기술이 양자 통신에도 도입되면서, 신호 및 시스템 보정을 위해 요구되던 복잡한 구성이 크게 간소화되고 있다. 이러한 단순화는 상용 부품의 집적화와 결합되면서, 소형 PIC 기반 양자 통신 모듈 개발에서 의미 있는 성과로 이어지고 있다.

II. 연속변수 양자 난수 생성

1. CV-QRNG 개요

진공 상태를 측정하여 난수를 생성하는 방식은 CV-QRNG의 대표적인 예이다. 진공 상태는 위상공간 (x, p) 위에서 정의된 양자계의 상태를 나타내는 준확률 분포 함수인 위그너 함수(Wigner Function)로 나타낼 수 있다[5].

$$W_0(x,p)=\frac{1}{\pi}\exp(-x^2-p^2)$$

진공 상태는 위상공간에서 등방성을 가지므로,

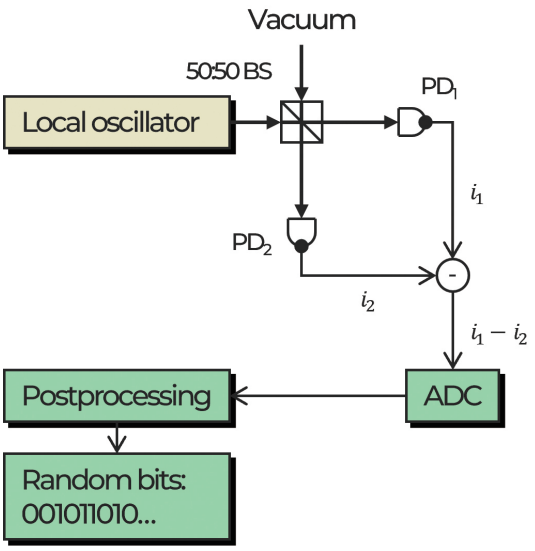


그림 1 진공 요동 기반 난수 비트열(Random Bits) 생성 과정. 진공(Vacuum) 상태와 로컬 오실레이터(Local Oscillator)는 50:50 광분배기(BS: Beam splitter)에서 간섭하며, 간섭된 출력광은 광검출기(PDs: Photodectors)로 측정되고, ADC(Analog-to-Digital Converter)와 후처리(Postprocessing)를 거쳐 난수 비트열이 출력됨

일반성을 해치지 않고 진폭 쿼드러처(X Quadrature)를 측정한다고 가정할 수 있다. 따라서, 진공 상태 진폭의 확률 밀도 함수는 위그너 함수의 적분을 통해 구할 수 있다[5].

$$|\psi_0(x)|^2 = \int_{-\infty}^{\infty} W_0(x,p)dp = \frac{1}{\sqrt{\pi}} \cdot e^{-x^2}$$

여기서 $\psi_0(x)$는 진공 상태의 파동 함수이며, 확률 밀도 함수는 $x=0$을 중심으로 한 가우시안 형태이다.

호모다인 측정은 진폭 쿼드러처를 측정하는 대표적인 방법으로, M.J. Collett 등(1987)이 그 구체적인 방법을 제안하였다[6]. 그림 1은 호모다인 측정을 통해 진공 상태의 진폭 쿼드러처를 측정하여 난수를 생성하는 원리를 보여준다. 이 과정을 보다 구체적으로 살펴보면, 진공 상태와 결맞음 상태의 로컬 오실레이터(LO: Local Oscillator)가 50:50 광분배기(BS: Beam Splitter)에서 간섭하고 출력된다. 이 출력은 두 광검출기에 의해 측정되고, 각 광검출기에서 발생한 전류(i_1, i_2)는 차동 방식($i_1 - i_2$)으로 출력된다. 이렇게 얻어진 아날로그 전기 신호는 ADC(Analog-to-Digital Converter)를 통해 디지털화되며, 적절한 후처리(Postprocessing)를 거치면 진공 상태의 양자 요동에 기인한 난수 비트열(Random Bits)을 최종적으로 생성할 수 있다. 여기서, 난수 생성률은 LO의 특성, 검출기의 대역폭, ADC의 분해능 및 시스템 잡음 등 다양한 요소에 의해 영향을 받는다.

2. 광학 부품 기반 CV-QRNG

Y. Shen 등(2010)은 상용 레이저(LO 광원), 50:50 광분배기와 균형 광검출기(Balanced Photodetector)의 개별 광학 부품들을 조합하여 진공 상태의 진폭 쿼드러처를 측정함으로써 양자 난수를 생성하였다[7]. 필터링된 진공 요동 신호를 주기적으로 샘플링하고, 디지털화된 진폭 값의 최하위 비트(Least Significant Bit)를 추출하는 방법으로 12Mbps의 난수 생성

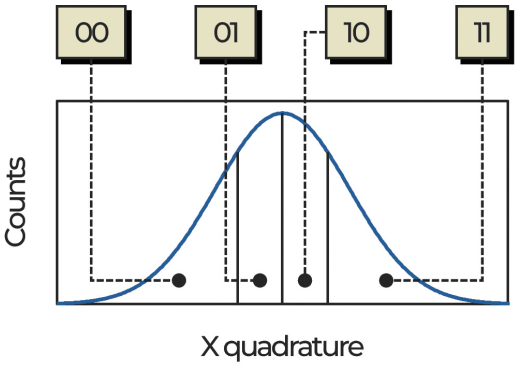


그림 2 진공 상태의 진폭 쿼드러처(X Quadrature)의 확률 분포가 2^n개의 동일한 면적의 구간으로 나뉘며, 난수는 특정 구간에 할당하여 생성. 여기서는 n=2일 때의 예임

속도를 달성하였다.

진폭 쿼드러처의 측정 결과는 예측 불가능하지만, 그 확률 분포는 가우시안 분포로 편향되어 있다. 그러나 그림 2와 같이 측정 결과를 적절히 구간(Bin)으로 나누어 각 구간에 속할 확률을 동일하게 만들 수 있다. 이때 측정값이 구간 i에 속할 확률은 다음과 같다[8].

$$\int_{x_i}^{x_{i+1}} |\psi_0(x)|^2 dx$$

C. Gabriel 등(2010)은 이 방식을 활용하여 최대 5비트(32개 구간)를 추출함으로써 6.5Mbps의 난수를 생성하였으며, 해시 함수를 사용해 연속된 난수열들 간에 남아 있는 잔여 상관관계를 제거하였다[8].

Gbps급 속도의 고속 동작은 고속 광검출기의 사용과 난수 생성용 전자 회로 최적화를 통해 실현될 수 있다. T. Symul 등(2011)은 기술적 잡음을 최소화하는 시스템을 설계하여 실시간으로 2Gbps의 난수를 생성하였다[9]. ADC 출력의 상위 비트(Most Significant Bit)를 제거하고 양자 잡음이 주로 포함된 하위 비트만 활용함으로써 환경 잡음에 대한 높은 내성을 가진 무작위성을 확보하였다.

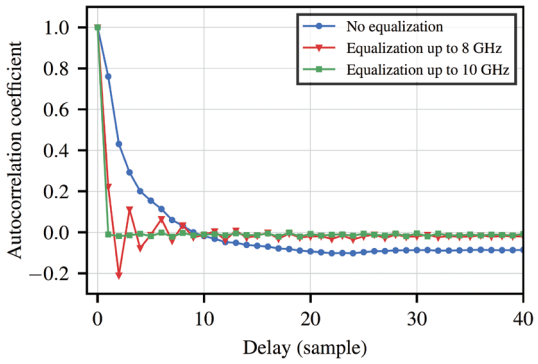
3. 집적화칩 기반 CV-QRNG

상용 광학 부품을 조합하여 QRNG 광학 시스템을 구현할 경우 각 부품의 우수한 개별 성능을 활용할 수 있다는 장점이 있다. 그러나 시스템 크기가 커지고 복잡해져 대량 생산 및 상용화에 제약이 따른다. 이러한 한계를 극복하기 위해 일부 또는 전체 기능을 하나의 PIC 상에 집적화하여 소형화하는 접근법이 주목받고 있다[10]. 웨이퍼 수준 공정으로 PIC 기반 QRNG를 구현하면 장치의 크기, 무게, 복잡성, 소비전력 및 비용을 크게 줄일 수 있으며, 집적광학 기술로 QRNG의 신뢰성과 성능도 향상시킬 수 있다.

F. Raffaelli 등(2018)은 실리콘 포토닉스 기반으로 세계 최초의 단일 집적형 호모다인 검출기 칩을 구현하였으며, 진공 상태를 측정하여 1.2Gbps의 속도로 양자 난수를 생성하였다[11]. 또한, 빠른 속도와 소형화를 동시에 달성하여 QRNG의 실용적 구현 가능성을 입증하였다.

그러나 실리콘 포토닉스 플랫폼에서 단일 칩에 모든 기능을 모놀리식 집적(Monolithic Integration)으로 구현하면서 동시에 높은 성능을 달성하는 방법에는 기술적 한계가 존재한다. 특히 광검출기(PD: Photodiode)의 암전류(Dark Current), 감도(Responsivity), 대역폭(Bandwidth) 특성은 QRNG의 난수 생성 속도에 큰 영향을 미친다. 실리콘 포토닉스 플랫폼에서는 단일 소자 집적을 위해 종종 게르마늄(Ge) PD를 사용하는데, Ge PD의 암전류는 InGaAs PD보다 수십 배 이상 높다. 이러한 한계를 보완하기 위해 이종 소재를 단일 칩 위에 집적하는 하이브리드 집적 방식이 제안되었다. 성능과 기술적 복잡성을 모두 고려할 때, 이 방식은 전기-광 통합 소자 응용, 특히 집적형 QRNG 구현에서 높은 성능을 달성하기 위한 효과적인 접근법이다[12]. B. Bai 등(2021)은 실리콘 포토닉스 칩과 III-V족 화합물 광검출기, 고대역폭 트랜스임피던스 증폭기를 하이브리드 집적한 QRNG를 제안하였다[13]. 이 장치를 통해 양자 엔트로피 소스의 주파수 응답 특성을 크게 향상시키고 실시간 난수 생성 속도를 18.8Gbps까지 높였다.

더 빠른 난수 생성을 위해 광대역 엔트로피 소스와 실시간 고속 난수 추출기(Randomness Extractor)에 관한 연구가 활발히 진행되어 왔다. 일반적으로 난수 추출기에는 해시 함수가 사용되며, 이 과정에서 대규모 행렬-벡터 곱셈 연산이 필요하다. 따라서 실시간으로 대량의 난수를 추출하기 위해서는 상당한



출처 Reprinted from C. Bruynsteen et al., "100-Gbit/s Integrated Quantum Random Number Generator Based on Vacuum Fluctuations," PRX Quantum, vol. 4, 2023, p. 010330. doi: 10.1103/PRXQuantum.4.010330

그림 3 등화(Equalization)가 자기상관(Autocorrelation)에 미치는 영향. 등화 이후 연속 샘플 간 상관성이 개선됨

수준의 디지털 회로 자원이 요구된다. 이러한 문제를 해결하기 위해 후처리 과정을 병렬화하고 채널당 처리 속도를 낮추는 방식이 제안되었으며, 이를 통해 고속 난수 추출이 가능하다[14]. K. Tanizawa 등(2024)은 기존에 오프라인으로만 구현되었던 병렬 후처리 방식을 발전시켜 4채널 병렬 실시간 난수 생성을 달성하였다[15]. 실리카 기반 광 회로를 사용하여 네 개의 진공 요동 신호를 병렬 엔트로피 소스로 디지털화하였고, 병렬 후처리를 통해 난수를 추출하였다. 그 결과 채널당 12.5Gbps, 총 50Gbps의 난수를 생성하였다.

한편, 양자 난수 생성 과정에서 전자 장치의 열잡음이나 레이저 출력 요동과 같은 고전적 잡음이 양자 신호에 섞여 들어올 수 있으며, 이는 난수의 예측 불가능성을 저하할 뿐만 아니라 생성 속도의 제한 요인으로 작용한다. 아울러, 시스템 내 전자 부품들의 유한한 대역폭으로 인해 연속된 측정값들 사이에 상관관계가 발생하여 난수성이 감소한다. 더 나아가, ADC의 비선형 동작은 측정 과정에서 추가적인 오차를 유발하여 난수 생성 성능을 저하시키며, 그 결과 생성 속도가 실제보다 과소 또는 과대 평가될 위험이 존재한다. C. Bruynsteen 등(2023)은 맞춤형 집적 전자 회로를 설계 및 적용함으로써 측정 과정에서 발생하는 고전적 잡음을 크게 줄여, 고전적 잡음으로 인한 성능 제한을 효과적으로 완화하였다. 또한, 그림 3에서와 같이 전자 부품의 대역폭 한계를 보상하기 위해 디지털 등화(Equalization) 필터를 적용하여 연속 샘플 간 상관성을 현저히 감소시켰으며, ADC의 정적 비선형성을 정량적으로 측정하여 그 영향을 모델에 반영함으로써 디지털화 과정에서 발생하는 왜곡을 보정하였다. 그 결과 진공 요동 기반 QRNG에서 100Gbps의 난수 생성 속도를 실험적으로 달성하였다[16].

III. 연속변수 양자 키 분배

1. 초기 프로토콜 발전 동향

1999년, T.C. Ralph는 기존의 단일광자 기반 양자 키 분배 방식이 가진 한계를 고려하여 다광자를 활용하는 새로운 프로토콜을 제안하였다[17]. 그가 제안한 최초의 연속변수 양자 키 분배 방식은 결맞음 상태 또는 스퀴즈드 상태의 위상 및 진폭 변조를 통해 비밀키(Secret Key)를 분배하는 방식이었다. 이 변조 방식은 고전역학에서 조화 진동자의 위치와 운동량에 대응하는 빛 모드의 켤레 변수(Conjugate Variables)인 X와 P(진폭 쿼드러처)에 정보를 인코딩하는 것이다.

이 암호화 방식은 양자역학의 불확정성 원리에 기반하며, 고전적 변수 X와 P는 양자역학적으로는 각각 연산자 $\hat{X}$와 $\hat{P}$로 표현된다. $\hat{X}$와 $\hat{P}$는 비가환 연산자(Non-Cmmutative Operators)이므로, $[\hat{X}, \hat{P}] = i\hbar$의 교환 관계를 만족한다. 따라서 두 물리량을 동시에 정밀하게 측정하려는 시도는 필연적으로 추가 잡음(Excess Noise)을 발생시킨다. 이로 인

해 도청자(Eve)가 정보를 빼내려는 시도는 송신자(Alice)와 수신자(Bob)가 공유하는 비밀키 정보의 상관관계에 불가피하게 잡음을 유발하며, 이를 바탕으로 도청 여부를 감지하고 보안성을 확보할 수 있다. 이러한 접근법은 단일광자 광원과 검출기 문제를 완화할 수 있는 실용적 대안으로 주목받았다. 그러나 T.C. Ralph의 분석에서 따르면, 더 높은 보안을 달성하기 위해서는 스퀴즈드 상태를 사용해야 했으며, 스퀴즈드 상태의 생성과 안정화는 여전히 기술적 난제로 남아 있었다.

이러한 기술적 한계는 2002년 F. Grosshans와 P. Grangier에 의해 제안된 GG02 또는 GMCS(Gaussian-Modulated Coherent States) 프로토콜로 인해 크게 완화되었다[18]. GG02 프로토콜은 결맞음 상태와 호모다인 검출만으로 키를 분배하는 방식으로, 결맞음 상태를 이용하면서도 스퀴즈드 상태 기반 방식과 동등한 보안성을 확보했다는 점에서 CV-QKD 발전의 결정적인 전환점이 되었다. Alice가 결맞음 빔의 수직한 두 진폭 쿼드러처가 각 각 가우시안 분포를 갖도록 변조하고, Bob이 호모다인 검출을 통해 두 켤레 변수 (X, P) 중 하나를 임의로 측정하는 과정은, Alice가 가상의 양자 얽힘 상태를 공유한 뒤 하나의 모드는 직접 측정하고 다른 모드를 Bob에게 보내는 형태와 수학적으로 등가임이 증명되었다. 이 등가성 덕분에 스퀴즈드 광원을 사용하지 않고도 동일한 정보 이론적 보안을 달성할 수 있게 되어 실험적 구현의 난이도가 크게 낮아졌다.

그러나 실제 암호키를 만들기 위해서는 송신자와 수신자가 가진 아날로그 데이터를 비트 정보로 완전히 일치시키는, 정보 재조정(Information Reconciliation) 과정에서의 문제가 여전히 남아 있었다. 초기 CV-QKD의 정보 재조정은 송신자가 가지고 있는 원본값을 수신자가 추정하는 Forward Reconciliation 방식에 기반했으나, 이 방식은 채널 손실이 3dB(약 15km의 광섬유에 해당)를 초과하면 키 생성이 불가능한 문제가 있었다. 이를 해결하기 위해 Post-Selection 기법[19] 등이 제안되었으나 큰 개선을 보이지 못했다. 2003년 F. Grosshans와 P. Grangier는 최초의 CV-QKD 실험 결과를 발표하면서 정보 재조정의 기준을 송신자 데이터에서 수신자 데이터로 바꾸는 Reverse Reconciliation[20]을 도입하여 3dB 손실의 전송 한계를 제거했다. 이를 통해 CV-QKD가 장거리 광섬유 환경에서도 암호키를 생성할 수 있었다. 이후 CV-QKD의 장점을 살리고 한계를 극복하기 위해 다양한 프로토콜이 제안되었다. 대표적으로 2004년 C. Weedbrook 등이 제안한 No-Switching 프로토콜[21]은 측정 기저 전환 없이 두 쿼드러처(X, P)를 동시에 측정함으로써 비밀키 생성률을 높일 수 있는 방식을 제시했으나, 당시에는 구현 복잡성과 보안 분석의 미비로 인해 실험적 구현으로 이어지지 못했다.

한편, 2008년 도입된 다차원 재조정(MDR: Multi-Dimensional Reconciliation)[22]의 도입으로 낮

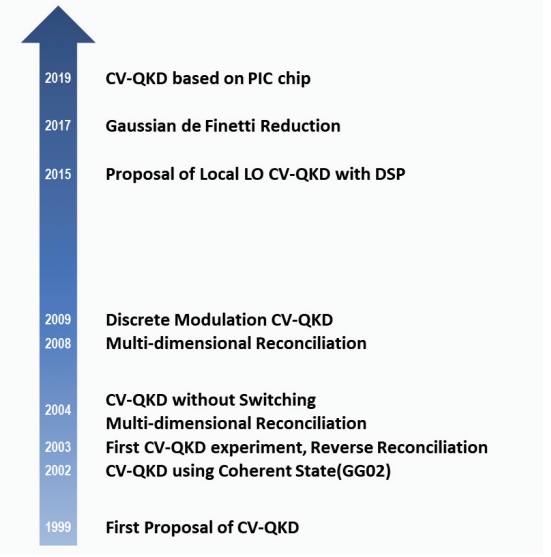


그림 4 연속변수 양자 키 분배 주요 프로토콜 및 시스템 동향

은 신호대잡음비(SNR: Signal-to-Noise Ratio) 환경에서도 LDPC(Low-Density Parity-Check)나 Polar 코드와 같은 오류정정 기법을 효과적으로 적용할 수 있게 되었고, 후처리 단계의 재조정 효율(Reconciliation Efficiency)은 0.9 이상으로 크게 향상되었다. 정보 재조정 기술이 성숙 단계에 접어들면서 CV-QKD의 기본 시스템 틀이 정립되었고, 이를 바탕으로 최근 연구는 기존 광통신 인프라와의 호환성 강화, 시스템 간소화, 그리고 상용화에 초점을 맞추어 진행되고 있다(그림 4).

2. 시스템 동향 및 방향성

2.1 초기 시스템 연구 동향

실용성 측면에서 결맞음 상태를 이용한 CV-QKD 프로토콜은 시스템 구성이 단순하고 단일광자 광원이나 검출기와 같은 전용 부품이 필요 없다는 점에서 큰 장점이 있다. 최초의 CV-QKD 실험은 파장 780nm의 레이저와 호모다인 검출기를 사용하여 자유공간 채널에서 구현되었다[23]. 송신부 레이저에서 분기한 빛 일부에 세기(Intensity)와 위상(Phase) 변조를 가해 결맞음 상태의 양자 신호로 사용하고, 나머지는 LO로 활용하였다. 또한, Reverse Reconciliation을 도입하여 전통적인 3dB 한계를 돌파하였으며, 손실이 없는 채널에서는 1.7Mbps, 손실 3.1dB의 채널에서는 75kbps의 비밀키 생성률을 달성하였다.

그러나 당시 재조정 효율은 여전히 0.7~0.8 수준에 머물러, 전송 거리가 늘어날수록 비밀키를 충분히 생성하지 못했다. 이후, MDR은 낮은 SNR 영역에서 고차원 회전 사상(Mapping)을 통해 연속 값을 비트 영역으로 효과적으로 변환함으로써 재조정 효율을 크게 향상시켰다. 이러한 발전을 기반으로 시간 · 편광 다중화를 활용한 신호-LO 동시 전송 기술과 위상/주파수 잠금, 클록 동기 등과 같은 시스템 안정화 기술이 실험적으로 정착되었다. 그 결과 2009년에는 최초의 광섬유 기반 CV-QKD 시스템이 구현되어 25km 링크에서 약 2kbps의 비밀키 생성률을 기록하였다[23]. 이후 MDR과 결합한 다중 엣지 타입 LDPC(Multi-Edge Type LDPC) 코드[24]와 Polar 코드[25] 등과 같은 고효율 오류정정 알고리즘의 도입으로 재조정 효율이 지속적으로 개선되었다. 그 결과 2013년, 80km를 초과하는 CV-QKD 장거리 전송이 실험적으로 입증되었으며[26], 2020년에는 초저손실 광섬유를 통해 202.91km의 장거리에서도 암호키 분배에 성공하였다[27].

2.2 고속 호환 시스템을 위한 연구 방향

시스템 안정화 기술이 발전함에 따라, CV-QKD의 실험적 구현 방향은 비밀키 생성률을 높이고 시스템을 단순화하여 상용화 가능성을 높이는 데 중점을 두고 있다. 비밀키 생성률을 높이려면 시스템 클럭 속도를 끌어올릴 수 있는 고속 균형 광검출기가 필요하다. 수 GHz 대역폭을 갖는 상용 검출기가 존재하나, 일반 광통신용으로 설계되어 노이즈 특성이 최적화되어 있지 않아 CV-QKD에서 요구하는 샷노이즈 한계(Shot-Noise Limited) 검출에는 적합하지 않다. 이 때문에 CV-QKD에 특화된 검출기를 개발하기 위한 연구가 활발히 진행되었으며[28-32], 2020년에는 1GHz 대역폭 검출기를 이용한 실험에서 250MHz 시스템 전송 속도를 달성하였다[33]. 최근에는 실리콘 포토닉스 수신기를 사용한 Local LO CV-QKD에서, 집적형 칩을 활용한 호모다인 검출기 대역폭을 약 1.5GHz까지 확장한 연구가 보고되었다[34]. 또한, 10GHz급 균형 광검출기에 위상 민감 증폭기(Phase Sensitive Amplifier)를 결합하여 10GHz 이상의 검출 대역폭을 구현한 실험 결과도 보고되었다[35]. 이에 따라, 수 GHz부터 10GHz까

지의 검출 대역 확장이 빠르게 지속되고 있다.

CV-QKD에서 사용되는 호모다인 검출에서는 LO가 사실상 스펙트럼 필터로 작용하여 채널 간 누화(Crosstalk)를 억제할 수 있다. 이로 인해 CV-QKD는 기존 광통신 환경과의 호환성이 높으며, 비밀키 생성률을 더 끌어올리기 위한 파장 분할 다중화(WDM: Wavelength-Division Multiplexing) 기술에도 적합하다. 최근 연구에서는 100개의 WDM 채널을 활용하여 10km 전송에서 27.2kbps의 비밀키 생성률을 달성하였으며, 이를 통해 양자 신호와 대용량 결맞음 WDM 트래픽이 하나의 광섬유에 공존하는 환경에서도 안정적인 비밀키 생성이 가능함을 실험적으로 입증하였다[36-43].

2.3 시스템 간소화를 위한 연구 방향

시스템 간소화를 위해 이산 변조 CV-QKD는 그림 5(a)의 가우시안 변조 대신 그림 5(b)의 위상공간에 소수의 점으로 구성된 상태 앙상블을 사용한다.

이산 변조 기반 CV-QKD 프로토콜은 초기 바이너리 변조로 출발하여, 두 개 이상의 인코딩 상태를 활용하는 다양한 형태로 확장되었다[44-48]. 이러한 프로토콜은 낮은 SNR 환경에서 오류정정 복잡성을 줄이고 실용적 구현에 적합하다는 장점이 있다. 하지만 이산 변조 프로토콜의 보안성 증명은 오랫동안 미해결 과제로 남아 있었다. 최근에는 일반 결맞음 공격에 대한 유한 키(Finite-Key) 영역의 보안성 증명[49]이 제시되면서, 이산 변조 프로토콜 관련 연구가 활발히 진행되고 있다.

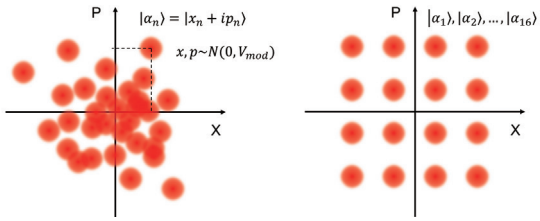


그림 5 (a) 가우시안 변조 방식의 양자 상태 앙상블, 위상 변조와 진폭 변조를 통해 각 쿼드러처의 분포는 가우시안 분포를 따른다. (b) 이상 변조 방식의 양자 상태 앙상블, 16-QAM(Quadrature Amplitude Modulation) 예시로 4×4 격자의 등확률 상태 집합을 나타낸다.

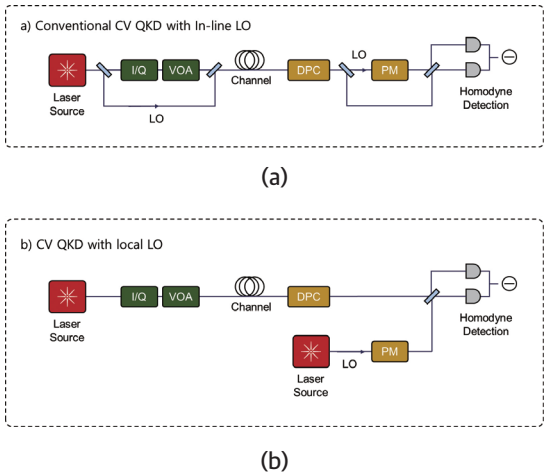


그림 6 (a) in-line LO 전송 방식 (b) Local LO 전송 방식 시스템 구성, 동상/직교 성분 변조기(I/Q: I/Q Modulator), 가변 광 감쇠기(VOA: Variable Optical Attenuator), 동적 편광 보상기(DPC: Dynamic Polarization Compensator), 위상 변조기(PM: Phase Modulator).

이어서, 시스템 간소화를 위한 또 다른 접근으로 Local LO를 사용하는 CV-QKD 시스템 구현 방식이 있다[50]. 그림 6은 기존의 In-Line LO 전송 방식과 Local LO 구성을 나란히 비교한다. 그림 6(a)는 송신부에서 레이저 광원으로부터 결맞음 광신호를 생성하고 I/Q 변조기로 두 진폭 쿼드러처가 가우시안 분포를 가지도록 변조한다. 수신부에서는 전송된 양자 신호와 LO로 결맞음 검출을 수행해 비트열을 얻는다. 이때 기저 선택은 수신부에서 LO의 위상을 변조하여 수행된다. 기존 In-Line LO 전송 방식은 송신자가 수신자에게 LO를 직접 전송한 반면, 그림 6(b)의 Local LO 전송 방식에서는 수신자가 별도의 레이저 광원을 이용해 결맞음 검출을 수행한다.

Local LO 기반 결맞음 검출을 안정적으로 구현하기 위해, 두 광원 간 위상 및 주파수 동기화와 위상 노이즈 완화를 위한 연구가 활발히 수행되고 있다. 한편, Local LO의 도입을 통해 수신기 구조를 단순화할 수 있으며, 기존에는 구현이 어려웠던 No-Switching 검출 시스템도 실현할 수 있다. 최근에는 이러한 Local LO를 이용해 0.154dB/km 손실을 가지는 초저손실 광섬유를 통해 100km 거리에서 비밀 키 분배를 성공적으로 달성하였다[51].

하지만 여전히 Local LO 구성을 안정적으로 구현하기 위해서는 송신자와 수신자의 광원 간 위상 및 주파수 동기화가 필수이며, 동기화 오차로 인한 위상 노이즈 억제가 중요한 과제이다. 최근 Local LO 기반 시스템에서는 기존 고속 광통신에서 활용되는 DSP를 적용하여 이러한 문제들을 해결하고 성능을 향상시키는 연구가 활발히 진행되고 있다. 그 결과 DSP 기반 위상 보정과 주파수 오프셋 보정을 통해 안정적인 복조를 구현할 수 있으며, 낮은 SNR 환경에서도 견고한 샘플링과 실시간 처리가 가능해졌다.

보안성 증명에 대해서도 A.G. Mountogiannakis와 S. Pirandola 등이 DSP 기반 CV-QKD를 고려한 유한키 보안 분석 및 Composable 보안 체계를 제시하여 시스템 안정성과 이론적 타당성을 강화하였다[52]. 이러한 결과를 바탕으로, 최근 다중 반송파(Multicarrier) 및 OFDM(Orthogonal Frequency-Division Multiplexing) 기반 CV-QKD에서는 DSP를 활용하여 Subcarrier 주파수 분해 · 채널 보정 · 잡음 억제 등을 수행하였으며 단거리에서는 수 Gbps, 100km 거리에서 수 Mbps 수준의 비밀키 생성률을 달성한 결과가 보고되었다[53].

2.4 시스템 상용화를 위한 연구 방향

QKD의 저비용 상용화를 위해서는 PIC 기반 QKD 시스템 구현이 필수적이다. DV-QKD는 단일광자 광원과 저온 단일광자 검출기가 필요해 칩 집적이 까다롭지만, CV-QKD는 모든 소자가 실온에서 동작하고 광통신 대역 파장과 완벽히 호환돼 집적화에 유리하다. 실제로 실리콘 포토닉스 기반의 송 · 수신부 통합 회로를 포함한 16GBaud CV-QKD 칩이 20km 광섬유에서 0.25Gbps 이상의 비밀키 생성률을 달성하며 대량 생산형 플랫폼으로서의 가능성을 입증하였다[54]. 여기에 InP 기반 송신기 PIC, 온칩 파장 가변 레이저, 집적 수신기 등이 잇따라 시연돼 10Gbps급 변조 속도와 수백 Mbps의 초고속 비밀키 생성률을 달성하고, 칩 하나로 GMCS 프로토콜 전 과정을 수행하는 단계까지 발전하고 있다[55].

IV. 결론

연속변수 기반 양자 기술은 기존 이산변수 방식이 지닌 구현상의 제약을 극복할 수 있는 실용적 대안으로 자리매김하고 있다. 특히 CV-QRNG는 고속 난수 생성과 시스템 통합 측면에서 우수한 성능을 보이며, 100Gbps에 달하는 속도가 실험적으로 달성됨으로써 클라우드 보안, 암호키 생성, 인증 시스템 등 다양한 보안 응용에 적합한 기반 기술로 진화하고 있다. 또한, 칩 기반 집적 기술, 병렬 처리, 잡음 억제 등의 융합을 통해 소형화와 대량 생산 가능성도 함께 확보하고 있다.

CV-QKD 역시 GG02 프로토콜과 Reverse Reconciliation의 도입 이후 장거리 전송이 가능해졌고, 기존 광통신 인프라와의 높은 호환성, 실온 동작, 저비용 구현 등에서 기존 QKD 기술 대비 뚜렷한 우위를 점하고 있다. 고속 균형 광검출기, DSP 기반 후처리, Local LO 전송 구조와 같은 기술적 진보는 키 생성률을 향상시키는 동시에 시스템을 단순화하고 안정성을 강화하고 있으며, PIC 기반의 송수신기 개발은 대규모 네트워크 구축과 상용 제품화에 실

질적인 기반을 제공하고 있다.

따라서 연속변수 양자 기술은 향후 양자 보안 통신의 핵심 플랫폼으로 자리할 뿐만 아니라, 양자 암호 네트워크, 위성 QKD, 양자 인터넷 등 차세대 보안 인프라와의 연계 가능성을 통해 기술적 · 산업적 응용 범위를 크게 확장할 수 있을 것으로 전망된다. 이러한 기술은 양자 정보 과학의 발전에 기여할 뿐만 아니라, 국가 사이버 안보와 민간 통신 산업 전반에 걸쳐 중장기적으로 큰 파급 효과를 가져올 것으로 기대한다.

용어해설

자기상관(Autocorrelation) 원본 신호와 시간 지연된 복사본 간의 상관성을 측정. 또한, 자기상관 분석은 잡음에 의해 가려진 신호 속 반복 패턴이나 숨겨진 주기성을 찾아내기 위한 수학적 도구

재조정(Reconciliation) 송신자가 보낸 연속값 신호와 수신자가 수신한 신호 사이에 남아 있는 작은 차이를 오류정정 코드로 보완해, 두 사람이 완전히 동일한 비트열(비밀키의 전 단계)을 갖도록 만드는 단계. 이때 "누구의 값을 기준으로 맞출 것인가"에 따라 순방향(Forward)과 역방향(Reverse) 재조정의 두 가지 방법으로 나뉨

참고문헌

[1] S.L. Braunstein and P. van Loock, "Quantum information with continuous variables," Rev. Mod. Phys., vol. 77, 2005, pp. 513-577.

[2] C. Weedbrook et al., "Gaussian quantum information," Rev. Mod. Phys., vol. 84, 2012, pp. 621-669.

[3] M. Herrero-Collantes and J.C. Garcia-Escartin, "Quantum random number generators," Rev. Mod. Phys., vol. 89, 2017, p. 015004.

[4] P.W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," in Proc. Annu. Symp. Found. Comput. Sci., (Santa Fe, NM, USA), Nov. 1994, pp. 124-134.

[5] U. Leonhardt and H. Paul, "Measuring the quantum state of light," Prog. Quantum Electron., vol. 19, 1995, pp. 89-130.

[6] M.J. Collett et al., "Quantum theory of optical homodyne and heterodyne detection," J. Mod. Opt., vol. 34, 1987, pp. 881-902.

[7] Y. Shen et al., "Practical quantum random number generator based on measuring the shot noise of vacuum states," Phys. Rev. A, vol. 81, 2010, p. 063814.

[8] C. Gabriel et al., "A generator for unique quantum random numbers based on vacuum states," Nat. Photon., vol. 4, 2010, pp. 711-715.

[9] T. Symul et al., "Real time demonstration of high bitrate quantum random number generation with coherent laser light," Appl. Phys. Lett., vol. 98, 2011, p. 231103.

[10] J. Wang et al., "Integrated photonic quantum technologies," Nat. Photon., vol. 14, 2020, pp. 273-284.

[11] F. Raffaelli et al., "A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers," Quantum Sci. Technol., vol. 3, 2018, p. 025003.

[12] E. Pelucchi et al., "The potential and global outlook of integrated photonics for quantum technologies," Nat. Rev. Phys., vol. 4, 2022, pp. 194-208.

[13] B. Bai et al., "18.8 gbps real-time quantum random number generator with a photonic integrated chip," Appl. Phys. Lett., vol. 118, 2021, p. 264001.

[14] K. Tanizawa et al., "Spatially multiplexed quantum entropy source with single LD for 100-Gbps random numbers and beyond," IEEE Photon. Technol. Lett., vol. 35, no. 5, 2023, pp. 229-232.

[15] K. Tanizawa et al., "Real-Time 50-Gbit/s Spatially Multiplexed Quantum Random Number Generator Based on Vacuum Fluctuation," J. Lightwave Technol., vol. 42, 2024, pp. 1-7.

[16] C. Bruynsteen et al., "100-Gbit/s Integrated Quantum Random Number Generator Based on Vacuum Fluctuations," PRX Quantum, vol. 4, 2023, p. 010330. doi: 10.1103/PRXQuantum.4.010330

[17] T.C. Ralph, "Continuous variable quantum cryptography," in Proc. Aust. Conf. Opt. Fibre Technol., 1999, pp. 123-126.

[18] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," Phys. Rev. Lett., vol. 88, no. 5, 2002, p. 057902.

[19] C. Silberhorn et al., "Continuous variable quantum cryptography: Beating the 3 dB loss limit," Phys. Rev. Lett., vol. 88, no. 5, 2002, p. 167901.

[20] F. Grosshans et al., "Quantum key distribution using Gaussian-modulated coherent states," Nature, vol. 421, no. 6920, 2003, pp. 238-241.

[21] C. Weedbrook et al., “Quantum cryptography without switching,” Phys. Rev. Lett., vol. 93, no. 17, 2004, p. 170504.

[22] A. Leverrier et al., “Multidimensional reconciliation for a continuous-variable quantum key distribution,” Phys. Rev. A, vol. 77, no. 4, 2008, p. 042325.

[23] J. Lodewyck et al., “Quantum key distribution over 25 km with an all-fiber continuous-variable system,” Phys. Rev. A, vol. 76, no. 4, 2007, p. 042305.

[24] H. Mani et al., “Multiedge-type low-density parity-check codes for continuous-variable quantum key distribution,” Phys. Rev. A, vol. 103, no. 6, 2021, p. 062419.

[25] P. Jouguet and S. Kunz-Jacques, “High performance error correction for quantum key distribution using polar codes,” Quantum Inf. Comput. vol. 14, no. 3-4, 2014, pp. 329-338.

[26] P. Jouguet et al., “Experimental demonstration of long-distance continuous-variable quantum key distribution,” Nat. Photon., vol. 7, 2013, pp. 378-381.

[27] Y. Zhang et al., “Long-Distance Continuous-Variable Quantum Key Distribution over 202.81 km of Fiber,” Phys. Rev. Lett., vol. 125, 2020, p. 010502.

[28] Y.M. Chi et al., “A balanced homodyne detector for high-rate Gaussian-modulated coherent-state quantum key distribution,” New Journal of Physics, vol. 13, no. 1, 2011, p. 013003.

[29] R. Kumar et al., “Versatile wideband balanced detector for quantum optical homodyne tomography,” Optics Communications, vol. 285, no. 24, 2012, pp. 5259-5267.

[30] Y. Wang et al., “High-speed balanced homodyne detector for quantum information applications,” in Proc. J. Phys.: Conf. Ser., vol. 844, (Nanjing, China), Apr. 2017, p. 012010.

[31] F. Raffaelli et al., “A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers,” Quantum Sci. Technol., vol. 3, no. 2, 2018, p. 025003.

[32] S. Du et al., “High-speed time-domain balanced homodyne detector for nanosecond optical field applications,” J. Opt. Soc. Am. B, vol. 35, no. 2, 2018, pp. 481-486.

[33] X. Tang et al., “Performance of continuous variable quantum key distribution system at different detector bandwidth,” Opt. Commun., vol. 471, 2020, p. 126034.

[34] Y. Bian et al., “Continuous-variable quantum key distribution over 28.6 km fiber with an integrated silicon photonic receiver chip,” Appl. Phys. Lett., vol. 124, no. 17, 2024, p. 174001.

[35] J. Liao et al., “Experimental demonstration of high-speed continuous variable quantum key distribution enhanced by phase-sensitive amplifier,” npj Quantum Inf., vol. 11, 2025, p. 105.

[36] T.A. Eriksson et al., “Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 Tbit/s data channels,” Commun. Phys., vol. 2, no. 1, 2019, p. 9.

[37] Y. Mao et al., “Integrating quantum key distribution with classical communications in backbone fiber network,” Opt. Express, vol. 26, no. 5, 2018, pp. 6010-6020.

[38] L.J. Wang et al., “Long-distance copropagation of quantum key distribution and terabit classical optical data channels,” Phys. Rev. A, vol. 95, no. 1, 2017, p. 012301.

[39] J.F. Dynes et al., “Ultra-high bandwidth quantum secured data transmission,” Sci. Rep., vol. 6, no. 1, 2016, p. 35149.

[40] R. Kumar et al., “Coexistence of continuous variable QKD with intense DWDM classical channels,” New J. Phys., vol. 17, no. 4, 2015, p. 043027.

[41] D. Huang et al., “Field demonstration of a continuous-variable quantum key distribution network,” Opt. Lett., vol. 41, no. 15, 2016, pp. 3511-3514.

[42] T.A. Eriksson et al., “Coexistence of continuous variable quantum key distribution and 7×12.5 Gbit/s classical channels,” in Proc. IEEE Photonics Soc. Summer Topical Meet. Ser., (Waikoloa, HI, USA), Jul. 2018, pp. 71-72.

[43] T.A. Eriksson et al., “Joint propagation of continuous variable quantum key distribution and 18×24.5 Gbaud PM-16QAM channels,” in Proc. Eur. Conf. Opt. Commun., (Rome, Italy), Sep. 2018, pp. 1-3.

[44] A. Leverrier and P. Philippe Grangier, “Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation,” Phys. Rev. Lett., vol. 102, no. 18, 2009, p. 180504.

[45] K. Bradler and C. Weedbrook, “A security proof of continuous-variable quantum key distribution using three coherent states,” Phys. Rev. A, vol. 97, no. 2, 2018, p. 022310.

[46] D. Sych and G. Leuchs, “Coherent state quantum key distribution with multi-letter phase-shift keying,” New J. Phys., vol. 12, no. 5, 2010, p. 053019.

[47] P. Papanastasiou et al., “Quantum key distribution with phase-encoded coherent states: Asymptotic security analysis in thermal-loss channels,” Phys. Rev. A, vol. 98, no. 1, 2018, p. 012340.

[48] M. Almeida et al., “Secret key rate of multi-ring M-APSK continuous-variable quantum key distribution,” Opt. Express, vol. 29, no. 23, 2021, pp. 38669-38682.

[49] T. Matsuura et al., “Finite-size security of continuous-variable quantum key distribution with digital signal processing,” Nat. Commun., vol. 12, 2021, p. 252.

[50] B. Qi et al., “Generating the Local Oscillator ‘Locally’ in Continuous-Variable Quantum Key Distribution Based on Coherent Detection,” Phys. Rev. X, vol. 5, 2015, p. 041009.

[51] A.A.E. Hajomer et al., “Long-distance continuous-variable quantum key distribution over 100-km fiber with local local oscillator,” Sci. Adv., vol. 10, no. 1, 2024, p. eadi9474.

[52] A.G. Mountogiannakis et al., “Composably secure data processing for Gaussian-modulated continuous variable quantum key distribution,” Phys. Rev. Research, vol. 4, 2022, p. 013099.

[53] H. Wang et al., “High-rate continuous-variable quantum key distribution over 100 km fiber with composable security,” arXiv preprint, 2025. doi: 10.48550/arXiv.2503.14843

[54] A.A.E. Hajomer et al., “Chip-Based 16 GBaud Continuous-Variable Quantum Key Distribution,” arXiv preprint, 2025. doi: 10.48550/arXiv.2504.09308

[55] J. Aldama et al., “Integrated InP-based transmitter for continuous-variable quantum key distribution,” Opt. Express, vol. 33, no. 4, 2025, pp. 8139-8149.