논문 18-43-01-21 The Journal of Korean Institute of Communications and Information Sciences '18-01 Vol.43 No.01
https://doi.org/10.7840/kics.2018.43.1.152

CVQKD 기술동향

임 경 천◆, 오 준 상*, 김 용 신*, 박 일 환*, 이 준 구°

A Review of Continuous Variable Quantum Key Distribution

Kyongchun Lim◆, Junsang Oh*, Yongseen Kim*, Ilhwan Park*, June-Koo Kevin Rhee°

요 약

연속 변수 양자 암호키 분배 (CVQKD – continuous variable quantum key distribution)는 기존 광통신 물리 계층을 활용하여 완벽한 보안채널을 제공하는 기술로 저가화가 가능하여 세계적으로 활발히 연구가 진행되고 있다. CVQKD연구에 관한 많은 연구 결과들이 있음에도 불구하고, CVQKD의 현재 기술수준을 판단하기에는 해당 연구들의 결과들에 대한 정리 및 분석이 부족한 상황이다. 본 리뷰논문은 CVQKD에 대한 최신 연구 결과들을 정리하고, 이를 토대로 CVQKD의 최고 기술수준에 대해 논한다. 기술수준을 파악하기 위해 최근 연구 결과들을 분석하고 해당 결과들을 이산 변수 양자 암호키 분배 (DVQKD – discrete variable quantum key distribution)의 연구 결과와 비교 분석 한다. 이를 기반으로 현재 기술수준의 CVQKD가 가질 수 있는 응용에 대한 논의 후, CVQKD의 앞으로의 발전 가능성에 대한 논하고자 한다.

Key Words : Quantum key distribution, Continuous variable quantum key distribution, Phase compensation, Reconciliation, Quantum information theory

ABSTRACT

Continuous variable quantum key distribution (CVQKD) has been actively researched as it provides an unconditionally secure channel utilizing conventional optical communication techniques enabling low-cost implementation. Although there are plenty of related researches, their review and analysis are not enough to judge current CVQKD technology level. This paper organize recent results of the related researches, then discuss about the state of the art of CVQKD technologies. In order to validate technical strength, we analyze the recent developments and compare them with discrete variable quantum key distribution (DVQKD). Based on this, we discuss possible applications of CVQKD as well as the future potential of CVQKD.

Ⅰ. 서 론

현대 인터넷 또는 그 외 정보시스템 보안 기술은 다항식 기반의 암호 (encryption) 체계를 활용하여 보안성이 높은 정보시스템을 구축하도록 하고 있다. 그러나 양자컴퓨터 시대의 도래가 기대됨에 따라 이러

※ 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 정보통신·방송 연구개발사업의 일환으로 수행되었습니다. (1711057505, 양자암호통신망 구축을 통한 신뢰성 검증기술 및 QKD 고도화를 위한 핵심요소기술 개발)
※ 본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터육성지원사업의 연구결과로 수행되었습니다. (IITP-2017-2015-0-00385)
◆ First Author : Korea Advanced Institute of Science and Technology School of Electrical Engineering, lim.kc@kast.ac.kr, 학생회원
° Corresponding Author : Korea Advanced Institute of Science and Technology School of Electrical Engineering, rhee.jk@kaist.ac.kr, 정회원
* Korea Advanced Institute of Science and Technology School of Electrical Engineering, js.oh@kaist.ac.kr, chunday2@kaist.ac.kr, tom0713@kaist.ac.kr
논문번호 : KICS2017-10-289, Received October 1, 2017; Revised December 26, 2017; Accepted December 28, 2017

한 암호체계가 쉽게 복호될 수 있는 가능성이 제기되어 양자후보안기술 (post-quantum cryptography) 의 개발이 요구되고[1], 양자 암호키 분배 (QKD – quantum key distribution) 는 이러한 문제점을 해결하는 데 있어 하나의 중요한 솔루션으로 인식되어 국내외에서 활발한 연구개발이 진행되고 있다. QKD는 광채널의 양자 특성을 기반으로 무조건적인 절대 보안성을 제공하는 암호키 분배 방법으로써 보안 통신 연구 분야에서는 양자컴퓨터를 이용한 공격에도 안전한 보안 기술로서 각광을 받고 있다. 초기에는 이산 변수를 활용한 양자 암호키 분배 (DVQKD – discrete variable QKD) 연구가 활발히 진행되었으나, 고가 부품이 많이 요구되는 점과 기존 광통신 시스템과의 호환성 문제가 대두되었다. 이를 해결하기 위해 상대적으로 기존의 광통신 시스템을 응용하여 저가 상용화가 가능한 CVQKD (CVQKD – continuous variable QKD)가 관심을 받게 됨에 따라 해당 연구가 국내외에서 활발히 진행되었다. 그러나 해당 연구결과들에 대한 정리 및 분석은 부족한 상황이다. 본 리뷰 논문은 CVQKD 연구 결과들을 정리해서 기술 요소별 핵심을 소개하고, 현재 CVQKD의 기술수준을 논한다. 구체적으로, 2장에서는 CVQKD의 원리 및 실험 결과들에 대한 리뷰를 다룬다. 3장 및 4장은 양자 암호키 분배의 오류정정을 담당하는 후처리와 양자 암호키 생성 용량에 관한 이론적 분석에 관한 연구 결과들의 리뷰를 다룬다. 5장에서는 최근까지의 이산 변수 양자 암호키 분배 기술에 대한 비교분석과 견주어 CVQKD가 갖는 장·단점을 논한다. 이를 기반으로 향후 통신시스템과의 응용이 6장에서 다루어진다. 마지막으로, CVQKD 연구 현황 및 기술수준을 총평하고, 향후 발전성에 대한 결론을 끝으로 본 논문을 마무리 한다.

Ⅱ. CVQKD

1999년 T.C Ralph가 제안한 다광자를 이용한 CVQKD (CVQKD – continuous variable QKD) 방법은 기존의 단일 광자 전송에 기반을 둔 양자 암호키 분배 방식이 갖는 비용 문제와 전송률 문제를 해결하는데 도움이 된다[2]. 기존 이산 변수 양자 암호키 분배 방식의 경우 송신자(Alice)는 하나의 펄스에 평균 0.5개 수준의 광자를 전송하고[3,4] 20% 수준의 검출 효율을 갖는 값 비싼 단일 광자 검출기[4,5]를 사용하기 때문에 실제로 이를 실용화하는데 있어 고비용의 어려움이 있었다. 한편, CVQKD의 경우 전송되는 하나의 펄스가 수 개의 평균 광자수를 갖고 60% 이상의 검출 효율을 갖는 호모다인 검출기[6-9]를 이용하기 때문에 높은 양자 암호키 전송률을 얻을 수 있고 비용 효율도 좋다.

CVQKD는 일반적으로, Alice가 결맞음 상태 (coherent state)의 직교하는 두 위상을 Gaussian 분포에 따라 변조하여 전송하고, 수신자 (Bob)는 호모다인 검출을 통해 값을 측정한다. 이후, 송수신자는 조정 (reconciliation)및 비밀성 증폭 (privacy amplification)을 하는 후처리 단계를 통해 암호키를 공유한다.

CVQKD가 갖는 이점으로 인해 연구가 많이 진행되어왔다. 한 연구는 2011년 개발된 다차원 조정 (multidimensional reconciliation) 방식[10]을 바탕으로 후처리 효율을 약 96%까지 올리고 시스템에서 발생하는 추가적인 잡음을 줄임으로써 실험적으로 100km에서 약 1kbps 암호키 전송률을 달성했다[8]. 암호키 생성률에 초점을 맞춘 방법으로는 50km에서 52kbps의 키 전송률을 달성한 실험 결과도 있다[7]. 이러한 실험 결과를 도출하는데 있어서 가장 중요한 역할 중 하나가 안정화다.

CVQKD 시스템의 성능을 좌우하는 것 중 하나가 검출기의 안정화다. 호모다인 검출 방식은 두 개의 신호를 입력으로 한다. 암호키를 생성하는 데이터 신호와 Alice와 Bob의 기준 위상 정보를 제공하는 로컬 오실레이터 신호다. 이 두 신호 사이의 간섭에 의한 신호 검출에 있어 로컬오실레이터 위상 불안정은 부정확한 검출 결과를 얻게 한다. 이를 해결하기 위한 방법으로써 편광분할다중화, 시분할다중화 및 파장분할다중화를 이용한 송신방법들이 제안되었다[6,11-15]. 제안되었던 방법들은 두 신호를Alice에서 모두 생성해서 전송하는 방법이다. 이 경우, 여전히 두 신호 사이의 간섭이 존재하며, 같이 전송되는 로컬 오실레이터를 이용한 공격이 가능하다[16,17]. 해당 문제를 근본적으로 해결하기 위한 방법으로써 Bob에서 로컬 오실레이터를 생성하고, 후처리 과정에서 위상을 보정하는 방법이 제안되고 있다[18-20]. 이러한 위상 보정 기술들은 광 간섭계의 안정화가 필요 없으며 일반적인 통신에서 사용하는 레이저로도 통신이 가능하다. 제안되었던 방법들이 두 개의 검출기를 사용하는 헤테로다인 검출이 사용되는 반면, 최근 하나의 검출기만 사용하는 호모다인 검출만으로 위상 보정이 가능한 것을 보인 연구결과가 제안되고 있다[21].

Ⅲ. 후처리

양자 암호키 시스템에서 양자 채널의 상태를 예측하고, 양자 채널을 통해 주고 받은 양자 상태에서 추출한 암호키의 오류를 정정하며, Eve가 갖는 암호키에 대한 정보를 제거하는 일련의 과정들을 후처리라고 부른다. 이산 변수 시스템의 양자 채널은 양자 비트 오류율 (quantum bit error rate, QBER)로 표현될 수 있는 반면, 양자 변수 시스템의 경우에는 과잉 잡음 (excess noise)이 양자 채널의 상태를 표현한다. 연속 변수 시스템의 경우 일반적으로 수신 신호 파워가 shot noise 파워 대비 같거나 작은 영역의 채널을 사용하고 있어 주어진 양자 채널을 양자 비트 오류율로 표현할 수 있지만, 이는 연속 변수 시스템에서 사용하는 양자 상태의 변복조 방식과 암호키를 추출하는 양자화 방식 등에 따라 달라진다. 따라서 연속 변수 시스템의 후처리에서는 양자화 방식에 무관한 과잉 잡음을 양자 채널의 상태 지표로 이용한다. 따라서 Alice와 Bob 양자 키 전송 후에, 채널추정 (Channel estimation)을 통해 예상 QBER 또는 과잉 잡음을 계산하고 양자 채널의 상태를 예측한다.

후처리 중에서 조정 (Reconciliation)은 Alice와 Bob의 암호키 정보를 일치하게 만드는 과정이다. 이산 변수 기반의 시스템과 다르게, CVQKD에서 정의되는 채널에서는 오류 정정이 상대적으로 어렵다. 따라서 CVQKD 시스템의 성능은 후처리에 많은 영향을 받는다. 이산 변수 암호키 시스템의 대표적인 조정 방식인 Cascade[22]는 Alice와 Bob이 채널을 통해 생성한 암호키의 패리티를 주고받음으로써 오류를 고치는 방식이다. Cascade 방식은 간단하면서도 효과적이어서 표 1.에서 볼 수 있듯이 최근 실험에서도[4,5] 이를 이용하고 있다. 하지만, 연속 변수 양자 암호키 시스템에서 결맞음 상태와 호모다인 검출기를 통해 주고 받은 정보는 연속 변수이기 때문에, Alice와 Bob은 Cascade 방식으로 효율적인 조정이 불가능하다. 이런 문제는 암호키 생성율과 전송 거리에 그대로 반영되고 다른 방식의 조정을 필요로 한다.

초기에는 Bob이 Alice가 보낸 정보를 추정하는 순방향 (Direct) 조정을 기반으로 연구가 진행되었다. 순방향 조정의 문제점 손실률이 3dB보다 큰 채널에서는 암호키를 생성할 수 없었다[23]. 이 문제점을 해결하기 위해, post selection[24]과 같은 다양한 방법들이 등장했지만 극적인 개선은 이루어지지 않았다[24-26]. 이후, Alice가 Bob의 정보를 유추하는 역방향 (Reverse) 조정은 3dB 제한을 이론적으로 해결했다[27].

역방향 조정으로 3dB 제한을 극복할 수 있었지만, 일반적으로 실제 조정 시스템에서 Alice와 Bob은 Eve와 다르게 채널 용량 한계만큼의 상호정보 (mutual information) I_{AB}를 달성할 수 없다. 이러한 한계도 암호키 시스템의 성능에 큰 영향을 준다. 이를 반영하고 분석하기 위해 실제 조정 성능을 일반적으로 조정 효율인 β로 표기한다. 이는 실제 시스템에서 사용되는 조정의 성능이 이론과 얼마나 근접한 지를 나타내는 성능 지표이다. 높은 조정 효율 β를 얻기 위해 Sliced Error Correction (SEC)이 제안되었다[28]. SEC는 Gaussian 변조된 연속 변수를 양자화 함으로써, 특정 신호대잡음비 (SNR - Signal to Noise Ratio)에서 90% 이상의 높은 조정 효율을 달성했다. 그러나 SEC의 문제는 SNR이 낮아지면, 조정 효율 β도 작아져 암호키의 장거리 전송이 힘들다는 것이다.

연속 변수 암호키의 장거리 전송을 위해 가장 널리 사용하는 방법으로 다차원 (Multidimensional reconciliation) 조정이 있다[10]. 다차원 조정은 SNR이 낮은 이진 입력 (binary-input) 부가 백색 가우스 잡음 (AWGN - additive white Gaussian noise) 채널에서 효율적인 순방향 오류 정정 (forward error correction) 부호들을 활용한다. 다차원 조정과 함께 가장 많이 사용하는 순방향 오류 정정 부호는 다중 모서리 저밀도 패리티 체크 (ME LDPC - multi-edge-type low density parity check)부호이다[29]. 다중 모서리 저밀도 패리티 체크 부호는 매우 낮은 부호율 (code rate)을 가질 수 있는 오류 정정 부호로서, SNR이 굉장히 낮은 곳에서 I_{AB} 한계치에 근접하는 키 용량을 얻을 수 있다. 여러 실험에서 다차원 조정과 다중 모서리 저밀도 패리티 체크 부호를 이용해 장거리 전송에 성공했다[6-8,30]. 다중 모서리 저밀도 패리티 체크 부호 외에도, 극 부호 (polar codes)[31]와 다차원 조정을 통해 낮은 SNR 영역에서 높은 조정 효율을 얻을 수 있다는 가능성을 보인 결과도 있다[32,33].

Ⅳ. 암호키 생성 용량

양자 암호키 분배 연구에 있어서 근본적인 연구 주제 중에 하나는 주어진 채널에서의 암호키 생성 용량을 규명하는 것이다. 이에 관한 연구는 수년 전부터 진행되어 왔고, 암호키 생성 용량의 하계 (lower bound)가 2009년에 제시되었다[34]. 해당 연구에서는 압착 상태 (squeezed state)와 호모다인 검출을 사용하는 역방향 조정 CVQKD 프로토콜이 암호키 생성 용

량의 하계임을 보였다. 상계 (upper bound)에 관한 연구로써, 기존 암호 통신 분야의 개념인 고유 정보 (intrinsic information)에 기반한 압착 얽힘 (squashed entanglement) 개념을 제시하고 압착 얽힘이 상계가 됨을 보인 연구 결과가 있다[35]. 그러나 압착 얽힘에 기반을 둔 상계가 2009년에 제안된 하계와 일치하지 않았다. 따라서 이를 줄이기 위한 연구들이 진행되었고, 압착 얽힘을 기반으로 한 더 정교한 상계가 제시되었다[36]. 그러나 여전히 상계와 하계 사이의 격차는 존재했고, 이후 더 정교한 상계가 제시된다[37]. 새로운 상계는 상대 얽힘 엔트로피 (relative entanglement of entropy)를 이용하며, 이는 현재 제일 정교한 상계이다. 또한 채널의 잡음을 진공 잡음만으로 가정한 순수 손실 채널 (pure-loss channel)에서 해당 상계가 2009년의 하계와 일치함을 보임으로써 순수 손실 채널에서의 암호키 생성 용량을 규명했다. 그러나 채널 잡음을 진공과 더불어 자연 발생하는 열에 의한 잡음도 고려하는 더 현실적인 열 손실 채널 (thermal-loss channel)에서는 제안한 결과들이 암호키 생성 용량을 규명하지 못했다. 이후 2009년의 프로토콜에서 수신단에 잡음을 추가하는 프로토콜을 제안함으로써 열 손실 채널에서 더 정교한 하계를 제시했으나[38], 그 정교함은 암호키 생성 용량을 규명하는데 부족한 상황이다.

V. 이산 변수 양자 암호키 분배와의 비교

본 장에서는 연속 변수와 이산 변수 양자 암호키 분배 사이의 차이점을 살펴보고, 이에 따라 CVQKD가 갖는 특징에 대해 논하고자 한다. 표 1.은 DVQKD와 CVQKD의 연구 결과들을 파라미터에 따라 정리해놓은 표이다.

DVQKD 경우에는 세밀한 방법론의 차이를 제외하고는 주로 BB84와 decoy를 결합한 형태의 프로토콜이 사용되고 있다[3,4,39]. Coherent one way (COW) 프로토콜의 경우에는 307km의 긴 전송 거리를 보였으나, 가장 강력한 공격 모델인 coherent 공격에 대한 보안성 분석의 부재로 보안성이 변할 가능성이 있다[5]. 평균 광자수의 경우, 유사 단일 광자 소스를 구현하기 위해 모두 1 미만의 평균 광자 수를 사용한다. 따라서 DVQKD의 경우 광 소스의 세밀한 조정이 요구된다. DVQKD의 주요 성능 파라미터로써 QBER은 모두 3% 정도 수준을 유지하고 있으며, 오류 정정은 양방향 오류 정정인 cascade방식을 주로 채용하고 있다. 양방향 오류 정정은 오류 정정 효율이 뛰어나지만, 오류 정정을 위해 주고받는 데이터가 많은 방법으로써 기존 통신 채널에 부담을 줄이기 위한 대안을 함께 고려해야하는 방법이다. 측정 장치의 경우, 모두 고가의 단일 광자 검출기를 사용하고 있다. 검출기의 검출 효율은 사용 소자에 따라 다르지만, 높은 효율의 시스템일수록 구현이 힘들어진다. 예를 들어, 초전도체를 이용한 검출기는 극저온 상태 유지등과 같은 고난이도 환경 조성이 요구된다. 암호 키 전송률은 약 41km에서 최대 5.3Mbps의 성능을 보이나 이 또한 coherent 공격 모델 분석에 따라 변화될 것으로 예상한다[3].

CVQKD의 경우 사용되는 프로토콜은 모두 Gaussian 변조를 사용하는 Gaussian modulated coherent states (GMCS)가 사용되고 있으며, coherent 공격에 대한 분석은 아직 완성되지 않아서 보안성 분석 측면에서 DVQKD보다 연구가 더 필요한 상황이다[6-9]. 단일 광자를 사용하지 않고 코히어런트 펄스를 사용하는 프로토콜로써 평균 광자 수는 상대적으로 DVQKD보다 높고 기존 광통신 장비 활용이 가능하다. QBER의 경우, 전반적으로 DVQKD보다 높은 경향성을 보이며, 많게는 약 40% 가까이 보이는 결과도 있다. 그러나 CVQKD에서 QBER이 주요 성능 파라미터로써 사용되지 않는다. QBER은 CVQKD 프로토콜에서 사용되는 양자화 방식에 따라 달라질 수 있기 때문에, 양자화 방식에 무관하게 표현 가능한 과잉 잡음을 주요 성능 파라미터로써 사용한다. 과잉 잡음은 주로 시스템 구현에서 발생하는 잡음의 파워를 나타내는 지표로써, 연구 결과들이 대체로 소수 둘째자리 정도 수준을 보이고 있다. 오류 정정은 단방향의 LDPC가 주로 사용되기 때문에 DVQKD의 양방향 오류 정정 보다 높은 채널 효율을 가질 수 있다. 검출기에 있어서, 단일 광자 검출기 대비 상대적으로 저가인 호모다인 검출기 사용하며, 이 또한 기존 광통신 장비와의 호환이 가능함을 의미한다. 암호 키 전송률은 약 50km 52kbps정도 수준이지만[7], 이는 이론적 결과와 차이가 있으므로 해당 연구가 진행됨에 따라 개선될 것으로 기대한다[37].

앞서 정리한 표 1.의 내용을 기반으로 CVQKD 시스템이 DVQKD 시스템보다 상대적으로 저가화가 가능할 것을 기대할 수 있으며, 저가화에 기여하는 것은 사용 신호, 오류정정, 검출기의 세 가지로 볼 수 있다. CVQKD의 경우 단일 광자 대신 코히어런트 펄스의 사용으로 인해 기존 광통신 장비와 호환이 가능하다. 또한, 상대적으로 높은 평균 광자 수는 광 소스의 구현 용이성을 보장한다. 오류정정에 있어서는 양방향

표 1. DVQKD와 CVQKD 성능 비교표
Table 1. Performance comparisons between DVQKD and CVQKD

	Ref.	Protocol	Attack	Mean photon number	Noise factor		Reconciliation	Detector (efficiency)	Secure key rate
Discrete variable QKD	[5]	COW	Collective	0.075	3.5% (QBER)		Cascade	InGaAs (20~22 %)	3.18bps at 307km
	[39]	Loss-tolerant (three-state + decoy)	Coherent	-	< 3.0 % (QBER)		Hash function	Unspecified SPD (4.99~5.05 %)	107bps at 50km
	[3]	Dispersive-optics-QKD + decoy	Collective	0.5	-		-	NbN SNSPD (68 %)	5.3Mbps at 41km
	[4]	BB84+decoy	Coherent	0.4	3.47 % (QBER)		Cascade	InGaAs (20 %)	210kbps at 45 km (Field trial)
Continuous variable QKD	[6]	GMCS	Collective	0.5~5	0.015 SNU (excess noise)	25.3 % (QBER)	LDPC + MDR	Homodyne detector (55.2 %)	200bps at 80.5km
	[7]	GMCS	Collective	7.5	0.07 SNU (excess noise)	0.3 % (QBER)	LDPC + MDR	Homodyne detector (60 %)	52kbps at 50km
	[8]	GMCS	Collective	2	0.05 SNU (excess noise)	38.2 % (QBER)	LDPC + MDR	Homodyne detector (60 %)	500bps at 100km
	[9]	GMCS	Collective	1	0.02 SNU (excess noise)	-	Irregular LDPC + slice reconciliation technique based on multi-level coding and multistage decoding	PBHD (65 %)	700bps at 50km

COW: Coherent one way, GMCS: Gaussian-Modulated Coherent States, SNU: Shot noise unit, LDPC: Low density parity check, MDR: Multidimensional reconciliation, SNSPD: Superconducting nanowire single-photon detector, PBHD: Pulsed balanced homodyne detector

대신 단방향 오류정정 사용으로 인한 네트워크 자원 절약 효과가 있다. 마지막으로, 기존 광통신 장비와 호환 가능한 호모다인 검출기의 사용이 있다. 따라서 향후에는 저가화가 가능한 솔루션인 CVQKD 시스템이 저가 상용화될 것으로 기대한다.

Ⅵ. 연속 변수 양자 암호키 분배 응용

본 장에서는 앞서 언급한 CVQKD 기술의 응용을 살펴보고자 한다. 연속 변수 양자 암호 키 분배의 주요 장점은 저비용 시스템 구현이다. 이산 변수 양자 암호 키 분배에서 고가의 단일 광자 소스와 단일 광자 검출기가 필요한 반면, 연속 변수 양자 암호 키 분배는 현재 광통신에서 사용하고 있는 코히어런트 펄스와 호모다인 검출기 혹은 헤테로다인 검출기를 이용한 구현이 가능하다는 이점이 있다. 또한 최근 연구되고 있는 수신단의 로컬 오실레이터를 사용하는 연속 변수 양자 암호 키 분배 시스템의 경우 수신단의 간섭계 안정화가 필요하지 않기 때문에 더욱 저비용화가 될 전망이다[18-21].

성능측면에서는 이론적으로는 CVQKD가 DVQKD보다 우수하나, 현재 기술 수준은 CVQKD가 DVQKD보다 장거리 전송에 불리함을 보이고 있다. 따라서 현재 기술 수준의 CVQKD는 단거리 전송에 적합하다고 판단한다. 약 20km 정도의 단거리에서 수 Mbps정도의 암호키 전송률을 보이는 결과를 통해 단거리에서 나쁘지 않은 성능을 보임을 알 수 있다[7].

현재 기술 수준의 CVQKD 응용이 가능한 네트워크 모델로써 수동 광 네트워크 (Passive Optical Network, PON)를 생각할 수 있다. PON은 OLT (Optical Line Terminal)와 ONU (Optical Network Unit) 사이의 거리가 약 20km 정도로 비교적 단거리 전송 네트워크에 속하며, 실생활에 많이 배치되어 있다. 이미 많이 배치되어 있는 PON에서 QKD 구현을 위해서는 저비용화가 주요 이슈일 것으로 기대한다. 이처럼 저비용 시스템 구축 및 단거리 전송이 필요한 네트워크의 QKD구현은 현재 연구 결과들을 볼 때, CVQKD로 구현하는 것이 적합하다는 판단을 할 수 있다. 관련 연구들도 이미 진행되고 있으며[40-44], 해당 연구 성과들을 기반으로 현재 광섬유 기반으로 전국적으로 깔려있는 Fiber-To-The-x (FTTx) 형태의 광 액세스 네트워크에 CVQKD 기술이 상용화될 수 있을것으로 전망한다.

Ⅶ. 결 론

본 논문에서는 CVQKD 연구 동향 및 이산 변수 양자 암호키 분배와의 차이점에 대해 살펴봤다. 이를 통해 CVQKD에 관한 이론 및 실험적 연구가 세계적으로 활발히 일어나 왔음을 확인할 수 있다. 또한, 이산 변수 양자 암호키 분배와의 비교를 통해 CVQKD의 현 연구 수준 및 특징을 살펴보았다. 비용 측면에서 CVQKD는 기존 광통신 장비 활용 가능성 및 DVQKD 대비 저비용 장비의 사용이 가능하기 때문에 저비용 시스템 구축이 가능하다. 성능 측면에서는 CVQKD 기술은 이론적 한계는 DVQKD보다 우수하지만 현재 기술 수준은 이에 대응하지 못하고 있다. 이에 대한 개선 가능성은 충분히 존재 하지만 현재 기술 수준은 단거리 전송에 적용 가능한 수준으로 파악한다. 이러한 특징을 기반으로 CVQKD는 수동 광 네트워크에 적합할 것으로 기대한다. 따라서, CVQKD는 이론과의 차이를 줄이기 위한 연구뿐만 아니라 현재 기술 수준의 기술을 기존 통신망에 구현하는 연구도 요구되는 상황이다. 이러한 관점에서 해당 연구 분야가 앞으로도 세계적 관심을 받을 것으로 기대한다.

References

[1] D. Bernstein and T. Lange, “Post-quantum cryptography,” *Nature*, vol. 549, no. 7671, pp. 188-194, Sept. 2017.

[2] T. Ralph, “Continuous variable quantum cryptography,” *Phys. Rev. A*, vol. 61, no. 1, 1999.

[3] C. Lee, D. Bunandar, Z. Zhang, G. Steinbrecher, P. Dixon, F. Wong, J. Shapiro, S. Hamilton, and D. Englund, “High-rate field demonstration of large-alphabet quantum key distribution,” *arXiv preprint arXiv:1611.01139*, Dec. 2016.

[4] A. Dixon, J. Dynes, M. Lucamarini, B. Fröhlich, A. Sharpe, A. Plews, W. Tam, Z. Yuan, Y. Tanizawa, H. Sato, S. Kawamura, M. Fujiwara, M. Sasaki, and A. Shields, “Quantum key distribution with hacking countermeasures and long term field trial,” *Sci. Rep.*, vol. 7, no. 1, May 2017.

[5] B. Korzh, C. Lim, R. Houlmann, N. Gisin, M. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, “Provably secure and practical quantum key distribution over 307 km of optical fibre,” *Nat. Photonics*, vol. 9, no. 3, pp. 163-168, Feb. 2015.

[6] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, “Experimental demonstration of long-distance continuous-variable quantum key distribution,” *Nat. Photonics*, vol. 7, no. 5, pp. 378-381, Apr. 2013.

[7] C. Wang, D. Huang, P. Huang, D. Lin, J. Peng, and G. Zeng, “25 MHz clock continuous-variable quantum key distribution system over 50 km fiber channel,” *Sci. Rep.*, vol. 5, no. 1, Sept. 2015.

[8] D. Huang, P. Huang, D. Lin, and G. Zeng, “Long-distance continuous-variable quantum key distribution by controlling excess noise,” *Sci. Rep.*, vol. 6, no. 1, Jan. 2016.

[9] X. Wang, W. Liu, P. Wang, and Y. Li, “Experimental study on all-fiber-based unidimensional continuous-variable quantum

key distribution," *Phys. Rev. A*, vol. 95, no. 6, Jun. 2017.

[10] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, "Multidimensional reconciliation for a continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 77, no. 4, Apr. 2008.

[11] P. Jouguet, D. Elkouss, and S. Kunz-Jacques, "High-bit-rate continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 90, no. 4, Oct. 2014.

[12] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. Scholz, M. Tomamichel, and R. Werner, "Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks," *Phys. Rev. Lett.*, vol. 109, no. 10, Sept. 2012.

[13] F. Furrer, "Reverse-reconciliation continuous-variable quantum key distribution based on the uncertainty principle," *Phys. Rev. A*, vol. 90, no. 4, Oct. 2014.

[14] A. Leverrier, "Composable security proof for continuous-variable quantum key distribution with coherent states," *Phys. Rev. Lett.*, vol. 114, no. 7, Feb. 2015.

[15] B. Qi, L. Huang, L. Qian, and H. Lo, "Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers," *Phys. Rev. A*, vol. 76, no. 5, Nov. 2007.

[16] X. Ma, S. Sun, M. Jiang and L. Liang, "Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol," *Phys. Rev. A*, vol. 87, no. 5, May 2013.

[17] J. Huang, C. Weedbrook, Z. Yin, S. Wang, H. Li, W. Chen, G. Guo, and Z. Han, "Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack," *Phys. Rev. A*, vol. 87, no. 6, Jun. 2013.

[18] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, "Generating the local oscillator "Locally" in continuous-variable quantum key distribution based on coherent detection," *Phys. Rev. X*, vol. 5, no. 4, Oct. 2015.

[19] D. Soh, C. Brif, P. Coles, N. Lütkenhaus, R. Camacho, J. Urayama, and M. Sarovar, "Self-Referenced continuous-variable quantum key distribution protocol," *Phys. Rev. X*, vol. 5, no. 4, Oct. 2015.

[20] D. Huang, P. Huang, D. Lin, C. Wang, and G. Zeng, "High-speed continuous-variable quantum key distribution without sending a local oscillator," *Opt. Lett.*, vol. 40, no. 16, pp. 3695-3698, Aug. 2015.

[21] I. Park, K. Lim, J. Oh, Y. Kim, and J. Rhee, "Continuous variable quantum key distribution with local oscillator phase compensation," in *Proc. ICSSUR 2017*, Jeju Island, Korea, Aug. 2017.

[22] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Wksp. of Theory and Appl. Cryptog. Techniques*, pp. 410-423, Lofthus, Norway, May 1993.

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

[24] C. Silberhorn, T. Ralph, N. Lütkenhaus, and G. Leuchs, "Continuous variable quantum cryptography: Beating the 3 dB loss limit," *Phys. Rev. Lett.*, vol. 89, no. 16, Sept. 2002.

[25] N. Walk, T. Ralph, T. Symul, and P. Lam, "Security of continuous-variable quantum cryptography with Gaussian postselection," *Phys. Rev. A*, vol. 87, no. 2, Feb. 2013.

[26] Y. Zhang, M. Xu, S. Han, T. Wang, S. Yu, and W. Gu "Beating 3-dB loss limit of direct reconciliation continuous-variable quantum key distribution by using a noiseless linear amplifier," in *Proc. ACPC 2013*, Beijing, China, Nov. 2013.

[27] F. Grosshans and P. Grangier, "Reverse reconciliation protocols for quantum cryptography with continuous variables," *arXiv preprint quant-ph/0204127*, Apr. 2002.

[28] G. VanAssche, J. Cardinal, and N. Cerf, "Reconciliation of a quantum-distributed

gaussian key," *IEEE Trans. Inf. Theory*, vol. 50, no. 2, pp. 394-400, Feb. 2004.

[29] T. Richardson, R. Urbanke, et al., "Multi-edge type LDPC codes," in *Wksp. Honoring Prof. Bob McEliece on his 60th birthday*, pp. 24-25, California, USA, Jan. 2002.

[30] D. Lin, D. Huang, P. Huang, J. Peng, and G. Zeng, "High performance reconciliation for continuous-variable quantum key distribution with LDPC code," *Int. J. Quantum Inf.*, vol. 13, no. 02, p. 1550010, Mar. 2015.

[31] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051-3073, Jun. 2009.

[32] P. Jouguet and S. Kunz-Jacques, "High performance error correction for quantum key distribution using polar codes," *Quantum Inf. and Computation*, vol. 14, no. 3&4, pp. 329-338, Mar. 2013.

[33] Y. Kim, C. Suh, and J. Rhee, "Reconciliation with polar codes constructed using Gaussian approximation for long-distance continuous-variable quantum key distribution," in *Proc. Int. Conf. ICT Convergence*, Sept. 2017.

[34] S. Pirandola, R. García-Patrón, S. Braunstein, and S. Lloyd, "Direct and reverse secret-key capacities of a quantum channel," *Phys. Rev. Lett.*, vol. 102, no. 5, Feb. 2009.

[35] M. Takeoka, S. Guha, and M. Wilde, "Fundamental rate-loss tradeoff for optical quantum key distribution," *Nat. Commun.*, vol. 5, p. 5235, Oct. 2014.

[36] K. Goodenough, D. Elkouss, and S. Wehner, "Assessing the performance of quantum repeaters for all phase-insensitive Gaussian bosonic channels," *New J. Phys.*, vol. 18, no. 6, p. 063005, Jun. 2016.

[37] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nat. Commun.*, vol. 8, p. 15043, Apr. 2017.

[38] C. Ottaviani, R. Laurenza, T. Cope, G. Spedalieri, S. Braunstein, and S. Pirandola, "Secret key capacity of the thermal-loss channel: improving the lower bound," *Quantum Inf. Sci. Technol. II*, vol. 9996, Oct. 2016.

[39] F. Xu, K. Wei, S. Sajeed, S. Kaiser, S. Sun, Z. Tang, L. Qian, V. Makarov, and H. Lo, "Experimental quantum key distribution with source flaws," *Phys. Rev. A*, vol. 92, no. 3, Sept. 2015.

[40] R. Asif and W. Buchanan, "Quantum-to-the-home: Achieving gbits/s secure key rates via commercial off-the-shelf telecommunication equipment," *Secur. and Commun. Netw.*, vol. 2017, pp. 1-10, Jun. 2017.

[41] S. Aleksic, D. Winkler, G. Franzl, A. Poppe, B. Schrenk, and F. Hipp, "Quantum key distribution over optical access networks," in *Proc. NOC-OC&I 2013*, Aug. 2013.

[42] B. Fröhlich, J. Dynes, M. Lucamarini, A. Sharpe, S. Tam, Z. Yuan, and A. Shields, "Quantum secured gigabit optical access networks," *Sci. Rep.*, vol. 5, no. 1, Dec. 2015.

[43] K. Lim, H. Ko, C. Suh, and J. Rhee, "Security analysis of quantum key distribution on passive optical networks," *Opt. Express*, vol. 25, no. 10, pp. 11894-11909, 2017.

[44] J. Rhee, K. Lim, H. Ko, J. Oh, and C. Suh, "Security analysis for quantum key distribution system on passive optical network," in *Proc. Photonics Conf. 2015*, pp. 51, Pyeongchang, Korea, Dec. 2015.

임 경 천 (Kyongchun Lim)

2012년 2월 : 성균관대학교 전자전기컴퓨터공학과 학사

2014년 2월 : 한국과학기술원 전기및전자공학부 석사

2014년 3월~현재 : 한국과학기술원 전기및전자공학부 박사과정

<관심분야> 양자통신, 양자 암호키 분배, 양자 정보 이론

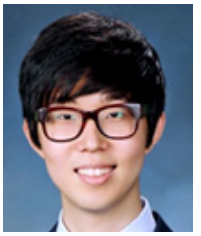
오 준 상 (Junsang Oh)

2014년 8월 : 한국과학기술원 전기및전자공학부 학사
2016년 8월 : 한국과학기술원 전기및전자공학부 석사
2016년 9월~현재 : 한국과학기술원 전기및전자공학부 박사과정
<관심분야> 양자암호통신, 양자컴퓨팅, 양자기계학습

김 용 신 (Yongseen Kim)

2016년 2월 : 충남대학교 전자공학과 학사
2016년 3월~현재 : 한국과학기술원 전기및전자공학과 석사과정
<관심분야> 양자암호통신, 양자 암호키 분배, 양자 정보 이론

박 일 환 (Ilhwan Park)



2016년 2월 : 한국과학기술원 전기및전자공학부 학사
2016년 3월~현재 : 한국과학기술원 전기및전자공학부 석사과정
<관심분야> 양자암호통신, 광통신, 양자 암호키 분배, 양자 정보 이론

이 준 구 (June-Koo Kevin Rhee)

1988년 2월 : 서울대학교 전기공학과 공학석사
1990년 8월 : 서울대학교 전기공학과 이학석사
1995년 8월 : Univ. of Michigan Electrical Engineering, 박사
2005년 3월~현재 : KAIST 전기및전자공학부 부교수, 정교수
<관심분야> 양자통신, 양자기계학습, 광통신