# 양자 네트워크 연구개발 동향 분석

배광일, 이은주, 심규석, 이원혁*
*한국과학기술정보연구원
kibae@kisti.re.kr, saranha@kisti.re.kr, kusuk007@kisti.re.kr, *livezone@kisti.re.kr

# Analysis on quantum network research and development trends

Kwangil Bae, Eunjoo Lee, Kyu-Seok Shim, Wonhyuk Lee*
*Korea Institute of Science and Technology Information

요 약

본 논문을 통하여 최근 활발히 연구되고 있는 양자 네트워크 분야를 소개하고 해당 분야 연구개발 단계를 설명한다. 이를 바탕으로 각 개발 단계에서 필요한 기술 항목을 정리하고 현재 양자 네트워크 연구 수준을 점검한다. 양자 네트워크를 넘어 양자 인터넷 개발을 목표로 관련 프로젝트를 진행 중인 기술 선도국의 연구 동향을 최신 연구 결과를 중심으로 정리한다. 최근 중국과 유럽 그룹에서 양자 네트워크 분야 높은 수준의 연구 성과를 보고하고 있다. 중국의 위성을 사용한 QKD 구현 사례와 유럽 QIA(Quantum In ternet Alliance)의 양자 인터넷 연구사례가 향후 양자 네트워크 연구에 대하여 갖는 시사점을 도출하여 정리한다.

## Ⅰ. 서 론

양자 네트워크는 향후 대단히 높은 중요성을 가질 것으로 예상되는 연구 분야 중 하나이다. 양자 암호키 분배(QKD; Quantum Key Distribution)는 양자 네트워크 상에서 구현되는 가장 대표적인 양자정보 프로토콜 중 하나이다. QKD 방식은 그 안전성이 물리 법칙에 근거한다는 점에서 기존의 계산 복잡도에 의해 안전성이 보장되는 고전 암호키 분배 방식에 대하여 이점이 있다. 이러한 이점은 계산 복잡도에 기반하는 현행 암호체계에 잠재적 위협이 되는 높은 계산 성능을 가진 양자 컴퓨터 개발이 점차 진행되는 상황에서 큰 중요성을 갖는다. [1] QKD 네트워크는 2002년 12월 미 국방부 산하 DARPA에서 최초로 구현한 이래, 다양한 형태와 기능으로 발전되어 왔다. [2-6] (‘표 1’ 참고) J. W. Pan 그룹에서는 최근 광섬유로 연결한 대륙 규모의 QKD 네트워크와 위성을 활용한 QKD 방식을 접목한 네트워크 구현을 보고한 바 있다. [7] 이는 현재 가장 복잡하고 높은 수준의 QKD 네트워크 구현 실험 중 하나라 할 수 있다.

양자 네트워크 상에서는 양자 암호키 분배 외에 다양한 양자 암호 프로토콜이 구현 가능할 것으로 예상된다. 양자 비밀 공유(Quantum Secret Sharing) 양자 비트 위임(Quantum Bit Commitment), 동전 뒤집기(Coin Flipping), BQC(Blind Quantum Computation), 분산 양자 연산(Distributed Quantum Computation) 등에 양자 네트워크가 활용 가능할 것으로 기대된다. EU가 주도하는 QIA(Quantum Internet Alliance)는 양자 네트워크를 궁극적으로 양자 인터넷 수준으로 발전시키는 것을 목표로 관련 연구를 수행하고 있다. [8] 최근 3체 양자 메모리 간 얽힘을 구현한 연구, [9] 양자 네트워크 구현 문제를 다양한 최적화 문제로 모델링한 연구 등은 향후 양자 네트워크 구현 방향에 시사하는 바가 크다. [11,12] 본 논문을 통하여 양자 네트워크 개발 단계를 구분하고, 이를 바탕으로 현재 기술 단계에 대하여 논한다. 또한 최신 동향을 중심으로 기술 선도국의 연구 동향을 분석하고, 현재 연구 흐름이 향후 양자 네트워크 분야 연구에 대하여 시사하는 바에 대하여 논의한다.

## Ⅱ. 본론

### Ⅱ-1. 양자 네트워크 기본 단위 및 현 개발 단계

양자 네트워크를 구성하는 기본 단위 장치들은 ‘그림 1’에 나타나 있다. 노드단(End Node)은 큐비트, 양자 컴퓨터 등 양자 시스템으로 주어진다. 각 노드에서 광자 상태에 정보를 인코딩하여 양자 채널(Quantum Channel)을 통하여 전송할 수 있다. 양자 채널로는 광섬유가 주로 활용되며, 자유 공간을 이용하여 통신 할 수도 있다. 중국 USTC J. W. Pan 그룹에서 위성을 활용한 자유 공간 QKD 실험을 최초로 수행한 바 있다. [10] 양자 중계기(Quantum Repeater)는 얽힘 스와핑(Entanglement Swapping)을 이용하여 상태 정보를 멀리 떨어진 지점으로 전송하는 장치이다. 양자 중계기를 활용하면 양자 상태를 전달하는 문제에서 기존 거리 한계를 극복할 수 있으나, 아직까지 완전한 형태의 양자 중계기는 개발되지 않았다. 양자 메모리(Quantum Memory)는 노드단에서 양자 상태를 저장하는 데 활용될 수 있으며, 중계기를 구현하는데도 활용될 수 있다. S. Wehner의 분류에 따르면, 양자 네트워크의 발전 단계는 크게 Trusted Repeater, Prepare and Measure, Entanglement Distribution, Quantum Memory, Fault-tolerant Quantum Computation 단계로 나눌 수 있다. [8]

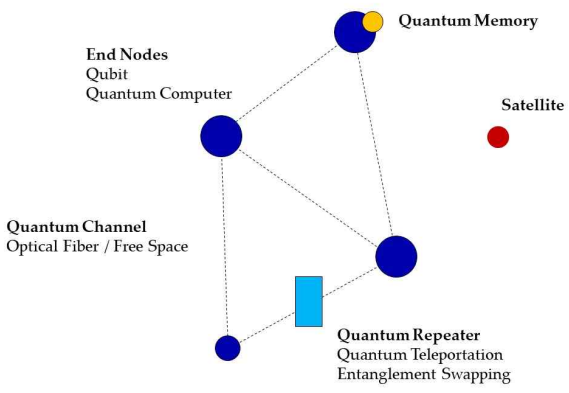


그림 1. 양자 네트워크 구성 장치 개요도

| Network | Project Year | Nodes | Distance (km) | Achieved Key Rate | Protocols |
|---|---|---|---|---|---|
| DARPA (US) | 2003 | 10 | 29+α | 400bps(10km) | BB84 |
| SECOQC (EU) | 2004 | 6 | 200 | 3.1kbps(33km) | BB84, BBM92, COW |
| Wuhu (CH) | 2009 | 7 | 36.8 | 3.15kbps(10km) | BB84 |
| SwissQuantum (EU) | 2009 | 3 | 35.2 | ≃2kbps(3km) | BB84, COW |
| Tokyo QKD (JP) | 2010 | 6 | 218 | 304kbps(45km) | BB84, BBM92, DPS |
| Beijing-Shanghai (CH) | 2017 | 32 | 2000 | 250kbps(43km) | BB84 |

표 1. 기존 QKD 네트워크 성능 (노드 수, 거리, 키 생성률 등)

각 단계는 구현 난이도가 쉬운 순서로 분류되었다. 각 네트워크 단계 구현을 위해 필요한 핵심 기술로는 신뢰할 수 있는 중계기(trusted repeater), 단대단 양자 얽힘 상태 및 생성, 높은 확률의 얽힘 상태 생성/측정, 양자 메모리, 오류-허용 양자 연산이 고려된다. 현 기술 수준은 신뢰할 수 있는 중계기를 활용한 양자 네트워크 단계에 있다고 할 수 있다. 이 단계에서는 통신 거리를 늘리기 위해 통신자 사이에 신뢰할 수 있는 제 3자를 활용한다. QKD의 경우를 예로 들면, 발신자와 중간의 제3자가 암호키를 나누어 갖고, 중간의 제 3자와 수신자가 독립적인 QKD 수행을 통하여 암호키를 나누어 갖는 방식이다. 신뢰할 수 있는 중계기를 활용하면, 현재 기술 수준의 단대단 암호키 분배 거리 한계를 극복할 수 있는 반면, 제3자를 신뢰해야 한다는 문제가 발생한다.

### Ⅱ-2. 최신 연구 동향

현재 기능상 가장 대표적인 연구 성과 중 하나는, 3개 단일 광자 간섭을 통하여 3개 메모리 간 얽힘을 구현한 결과이다. [9] 해당 연구에서는 레이저-쿨링된 원자 앙상블(atomic ensemble)과 링 공진기(ring cavity)를 활용하여, 기존의 2개 메모리간 얽힘을 구현한 연구보다 얽힘 생성의 효율을 높였다. 해당 연구 결과는 다양한 형태의 양자 네트워크 구현에 응용될 가능성이 있는 한편, 양자 네트워크 구현에 있어 매우 중요한 장치인 양자 중계기 개발의 기반이 될 것으로 기대된다.

양자 네트워크를 현 기술 단계에서 대규모로 구현하는 연구도 꾸준히 이루어져 오고 있다. 중국 J. W. Pan 그룹에서 위성을 활용한 QKD 구현에 성공한 이래, [10] 2020년 1,120km 규모의 얽힘 기반 QKD 프로토콜 구현 결과를 보고하였다. 이 결과에서는 위성을 활용하여 단순히 암호키가 분배되는 지점 간 거리를 늘렸을 뿐 아니라, 얽힘 기반 QKD 프로토콜을 활용함으로써 암호키 분배의 안전성을 소스-독립적(Source-Independent) 수준으로 보였다. 2021년에는 광섬유 기반 양자 네트워크와 위성을 결합한 형태의 네트워크 구현 결과가 처음 보고되었다. [7] 해당 네트워크를 활용하면 총 거리 4,600km 네트워크 상에서 임의 유저가 다른 노드의 유저와 암호키 교환이 가능하다. 상기 연구들은 이전에 없던 수준의 복잡한 형태의 양자 네트워크를 구현하였다는 점에서 큰 의미가 있는 한편, 신뢰할 수 있는 중계기를 활용해야 하는 기술 한계를 노출한다. 대규모로 양자 네트워크를 구현할수록 신뢰 노드의 수는 매우 많아지며, 이는 전체 암호 프로토콜의 안전성에 큰 위협이 될 수 있다. 안전한 네트워크를 구현하기 위해서는 신뢰 노드 수를 줄이는 문제 외에 다수 유저를 효율적으로 인증해야 할 필요 또한 중요하다. 다체 간 양자 디지털 인증이나 PQC(Post Quantum Cryptography) 활용방법이 인증 문제를 해결하기 위해 제안되어 왔다.

양자 네트워크 최적화는 양자 네트워크 분야에서 새롭게 연구되고 있는 연구 주제 중 하나이다. 최근 TU Delft 그룹에서는 기존의 광섬유 인프라에 양자 네트워크를 구현하기 위하여 최소 개수의 양자 중계기를 활용하기 위한 방법론을 제안한 바 있다. [11] 또한, 주어진 중계기 성능 아래에서 얽힘 생성/분배를 최적화하는 연구가 진행되었다. [12]

### Ⅲ. 결론

본 논문에서는 양자 네트워크를 구현하기 위한 기술 단계를 바탕으로 현재 기술 단계와 최신 연구 동향에 대하여 정리하였다. 현재 장거리 양자 네트워크 구현을 위해서는 신뢰할 수 있는 중계기가 주로 활용된다. 신뢰 노드의 도입이 필요 없는 안전성이 높은 네트워크 구축을 위해서는 양자 중계기, 안전성 높은 양자 암호 프로토콜 관련 연구가 필요하다. 최근 양자 네트워크 연구는 기능상 3체 메모리 간 얽힘 구현 연구가 가능한 수준으로 발전하였으며, 자유공간과 광섬유를 활용한 대규모 양자 네트워크 구현도 보고된 바 있다. 기존 광섬유 망에 기반하여 양자 네트워크를 구현하기 위해 양자 중계기 수, 얽힘 등의 자원을 최적화하는 연구가 새롭게 진행되고 있는 점을 특기한다.

## ACKNOWLEDGMENT

본 연구는 2021년도 한국과학기술정보연구원(KISTI) 주요 사업 과제로 수행한 것입니다.

## 참 고 문 헌

[1] Arute, F. "Quantum supremacy using a programmable superconducting processor," Nature 574, pp. 505 - 510, Oct. 2019.

[2] Peev, M. "The SECOQC quantum key distribution network in Vienna" New Journal of Physics 11, 075001 Jul. 2009

[3] Xu, F. et al. "Field experiment on a robust hierarchical metropolitan quantum cryptography network" Chinese Science Bulletin 54, pp. 2991 - 2997, Aug. 2009.

[4] Stucki, D. et al. "Long-term performance of the SwissQuantum quantum key distribution network in a field environment" New Journal of Physics, 13, 123001 Dec. 2011.

[5] Sasaki, M. et al. "Field test of quantum key distribution in the Tokyo QKD Network" Optics Express 19, 11, pp. 10387-10409, May, 2011.

[6] Courtland, R. "China's 2,000-km quantum link is almost complete [News]" IEEE Spectrum, 53, 11, Nov. 2016.

[7] Chen, Y.-A. et al. "An integrated space-to-ground quantum communication network over 4,600 kilometres" Nature 589, pp. 214 - 219, Jan. 2021.

[8] Wehner, S. and Hanson, R. "Quantum internet: A vision for the road ahead" Science 362, 303, Oct. 2018.

[9] Jing, B. et al. "Entanglement of three quantum memories via interference of three single photons" Nature Photonics, 13, pp. 210 - 213 Jan. 2019.

[10] S.-K. et al. "Satellite-to-ground quantum key distribution," Nature 549, pp. 43 - 47 Aug. 2017.

[11] Rabbie, Julian, et al. "Designing quantum networks using preexisting infrastructure." arXiv preprint arXiv:2005.14715, 2020.

[12] da Silva, Francisco Ferreira, et al. "Optimizing entanglement generation and distribution using genetic algorithms," Quantum Science and Technology, 2021.