양자통신의 현황과 표준화 동향

윤춘석 (주)KT 융합기술원 선임연구원

1. 양자물리학과 정보이론의 만남

작년 여름 인기를 모은 영화 '오펜하이머'에는 아인슈타인, 하이젠베르크, 닐스 보어, 리처드 파인만 등 유명한 물리학자들이 많이 나온다. 양자 관련 분야에 종사하는 사람이라면 그 이름을 보는 것만으로도 아주 반가우면서도, 나를 힘들게 만든 사람들이란 원망 아닌 원망도 즐겁게 할 수 있었을 것이다. 바로 이 분들이 활약하던 시기가 오늘 이야기의 시작점이다.

19세기 후반~20세기 초반 원자/전자/양성자/중성자 같은 미시세계 입자와 관련된 물리학 실험들은 이전까지 물리학의 핵심이던 뉴턴의 고전역학으로는 설명할 수 없는 결과들을 보여주었다. 과학자들은 이를 해결하기 위해 깊은 고민에 빠졌고, 물리학계는 이 실험 결과들을 담을 수 있는 새로운 역학 체계가 필요해졌다. 이렇게 20세기에 새롭게 만들어진 것이 양자역학(Quantum Mechanics)이다.

양자(Quantum)라는 단어는 양/구체적인 양/크기 등과 같은 의미로 사용되는 고대 프랑스어(quantite)와 라틴어(quantitatem)에서 유래된 영어단어 quantity를 그 어원으로 한다. 즉, 어떤 불연속적인 값들을 가리키거나 헤아리는 것들을 나타내는 단어로, 입자의 에너지 레벨이 불연속적인 값을 가지거나, 원자의 전자궤도가 불연속적으로 존재한다는 것처럼 고등학교 이상 수준에서 이야기하는 과학 이야기가 다 이것과 연관되어 있다.

양자 역학은 미시세계에서 보이는 이런 불연속적인 값을 통해 이루어지는 입자 간 힘의 영향과 운동을 설명한다. 물리량의 연속적인 개념에 의존해 설명하는 기존의 뉴턴 역학과는 다르게, 미시세계의 이런 현상들을 설명하는 양자역학은 20세기 이후 수많은 과학기술들의 발전과 함께 현재 우리가 사용하고 있는 전자를 사용하는 기술들에 대한 발전도 가져올 수 있었다.

한편, 정보이론은 20세기 중반 클로드 섀넌(Claude Shannon)에 의해 정립된 분야로, 데이터의 전송, 처리 및 해석과 관련된 수학적 연구를 포함한다. 정보이론은 정보의 불확실성을 수학적으로 다루는 방법을 제공함으로써, 메시지가 가진 정보의 양을 정량화하는 데 중요한 역할을 했다. 이를 통해 데이터 압축, 오류 수정 코드, 통신채널의 용량 계산, 효율적인 데이터 전송 방식 등을 다루며 현대 디지털 통신과 컴퓨팅의 기반이 되었다.

이 두 분야의 만남, 즉 양자물리학과 정보이론의 결합은 과학계에 혁명적인 발전을 가져왔다. 양자역학은 기본적으로 확률론적인 개념을 가지고 있으며, 이는 정보이론에서 다루는 불확실성과 잘 맞아떨어진다. 양자역학의 핵심 원리들, 특히 얽힘(Entanglement)과 중첩(Superposition) 상태는 정보이론의 전통적인 관점을 확장하고, 정보 처리와 전송의 새로운 가능성을 열었다.

이러한 양자역학의 개념을 정보 전송과 처리에 적용함으로써, 훨씬 더 효율적이고 안전한 정보 처리 방식을 개발할 수 있었다. 그 결과, 양자 컴퓨팅, 양자 통신, 양자 센싱과 같은 새로운 기술들을 탄생시켰다.
이렇게 양자물리학의 원리들이 정보이론과 결합되어 정보의 정의와 전송 방식을 재해석하고, 좀 더 효율적이고 안전한 통신 기술의 발전을 이끌고 있다. 양자통신은 이러한 혁신적인 결합의 가장 대표적인 예로, 세계적으로 많은 관심을 받으며 빠르게 발전하고 있다.

2. 양자 통신과 표준화

2.1 양자 통신

양자 통신은 양자역학의 원리를 이용하여 정보를 전송하는 통신 방식이다. 이는 기존의 고전적 통신 방식과 다르게, 양자 중첩 및 얽힘 상태를 활용하여 정보를 전달한다.
이런 양자통신의 가장 큰 특징은 보안성에 있다. 물리학적 특성에 기반하여 전송하는 정보를 안전하게 보호할 수 있으며, 이는 기존의 수학적 어려움에 기반한 보안 방식에 비해 안전한 기술로 평가받고 있다. 통신을 위해 양자 기술을 사용하는 것만으로도 보안성을 가질 수 있는 특징 덕분에 양자 통신과 양자 암호통신 두 개의 단어를 같거나 유사한 의미로 사용하기도 한다.
양자 통신은 사용하는 큐비트(Qubit)에 담기는 정보의 종류에 따라 대칭키 암호 알고리즘에 사용되는 비밀키를 나누어 가질 수 있는 양자 키 분배(QKD, Quantum Key Distribution), 메시지를 큐비트를 이용해 직접 주고 받는 양자 직접 통신(QDC, Quantum Direct Communication), 개체(Entity) / 메시지(Message) 인증(Authentication) 기능을 제공하는 양자 인증(Quantum Authentication), 전자 서명(Digital Signature) 기능을 위한 양자 서명(Quantum Signature), 양자 비밀 공유(Quantum Secret Sharing) 등으로 나눌 수 있다.
이 중 실생활에 가장 근접해 있는 대표적인 기술이 바로 양자 키 분배(QKD) 기술이다. 이 기술은 통신에 참여하는 당사자들 간에 암호통신을 위한 비밀키를 나뉘어 가질 수 있도록 한다. 이렇게 나뉘어진 키는 데이터를 암/복호화 하는데 사용되며 물리적으로 복제하거나 도청하는 것이 불가능하다.
이런 특징 때문에, 기존의 RSA 알고리즘이 양자 컴퓨터의 쇼어 알고리즘(Shor's algorithm)에 의해 공격받게 되면서, RSA 알고리즘의 중요한 기능 중 하나인 암호키 교환 기능을 대체하기 위한 방법으로 주목받고 있다.
하지만, 기술의 안전성과 미래 가능성에도 불구하고 실생활에서 사용하기 위해서는 아직 넘어야 할 어려움들이 많다. 양자 키 분배 기술은 장비의 구조와 성능에 대한 기준도 세워야 하고, 보안 장비로써 안전성을 검증받아야 하며, E2E 구조를 벗어난 현대의 인터넷 같은 대규모 네트워크화 작업도 필수이다.

2.2 양자키 분배망

기존의 양자통신은 실험실 또는 상용환경에서 1:1 구조의 실험 장비를 설치하고 장비의 성능을 테스트하는 구조였다. 이는 학문적 관점에서는 중요한 결과를 도출하며 관련 분야가 발전하는 듯이 보였다. 하지만 장비가 발전하고 실제 사용자의 관점을 고려하기 시작하면서 통신서비스를

제공하는 사업자 사이에서 먼저 이슈가 제기되였다. 약 5~80km 내외의 짧은 구간을 1:1 구조로 통신할 수 있는 장비만을 가지고는 어떤 상용화도 불가능하다는 것이었다. 이 문제를 극복하기 위해 양자키분배 기술이 아닌 양자키분배망(QKD Network)라는 개념이 나오고 관련 기술과 표준들이 등장하기 시작했다.

양자키분배망에 대한 첫 번째 국제 표준은 ITU-T SG13에서 만들어진 Y.3800(Overview on networks suppor ting quantum key distribution)이다. 이 문서에서 양자키분배 장비 계층, 생성된 암호키를 관리하는 키 관리 계층, 양자키분배망을 제어 및 관리하는 계층, 사용자 네트워크에서 키를 사용하는 서비스 계층 등 각각의 계층들을 나누고 각각의 계층들의 역할을 처음 정의했다.

이를 통해 양자 통신 기술이 진정한 대규모 통신 네트워크로 발전하기 위한 기반이 처음 마련되었다. 또한 한국의 7개 기업이 처음 제안한 이 표준을 통해 양자기술을 가지고 있는 세계 몇 안 되는 기업뿐만 아니라, 기존의 ICT 기술을 가지고 있는 국내외 다양한 기업들의 양자통신산업 참여를 유도하는 계기도 마련되었다.

2.3 표준화 현황

양자키분배 기술의 상용화와 산업의 발전을 위해서는 다양한 분야에 걸친 노력이 필요하다. 특히, 세계를 이어줄 미래 보안통신으로서 역할을 다하려면 표준화된 기술 정립을 위한 노력이 필수이다. 다양한 국가들이 참여하여 국제 표준을 만들고 그 표준을 기준 삼아 관련 산업의 투자와 함께 발전을 위한 노력이 요구되는 시점이다.

2.3.1 유럽전기통신표준기구(ETSI)

ETSI는 2008년부터 양자키분배 기술 관련된 그룹(ISG QKD)을 만들어 운영하고 있다. 이는 양자키분배 기술관련 표준을 만들기 위한 국제사회의 첫 번째 시도였다. 현재까지 약 28건의 표준규격 및 연구보고서/가이드를 발행하고 있으며, 계속해서 새로운 표준들을 만들고 있다. ETSI의 주요 작업은 양자키분배 장비의 인터페이스, 구성 요소 특성, 표준 인터페이스 등 양자키분배 기술의 상용화를 촉진하는 데 집중되어 있다.

2.3.2 국제전기통신연합 전기통신표준화부문(ITU-T)

ITU-T는 2018년 SG13에서 첫 번째 표준을 개발하기 시작한 이후로 다양한 표준들을 약 50여 건 가까이 개발했거나 개발하고 있다. 특히 ITU의 장점을 최대한 살려 양자키분배 기술을 네트워크화하는 데 중점을 두고 있으며, 양자키분배 네트워크의 안전성을 확보하는 표준도 동시에 개발하고 있다.

ITU-T에서는 3개의 연구반(SG)이 관련 표준들을 역할을 나누어 개발하고 있다. SG13(Future Networks)에서는 양자키분배 네트워크 구조와 기능, 네트워크 QoS를 측정하고 보장하기 위한 기준, 네트워크간 연동을 위한 구조, 네트워크 제어 및 관리 등의 표준을 개발하고 있다. SG17(Security)는 이렇게 만들어진 양자키분배 네트워크와 관련된 보안 기술 표준들을 개발하고 있다. SG11(Signalling req, Protocols, Test spec)에서는 양자키분배 네트워크 레이어들을 연결하

는 각각의 인터페이스들에 대한 프로토콜들을 개발하고 있다.

2.3.3 ISO/IEC 합동기술위원회 JTC1

ISO와 IEC가 공동으로 설립한 JTC1은 정보기술에 대한 국제 표준을 개발한다. JTC1은 양자 컴퓨팅 및 양자통신 기술에 관한 표준을 개발하고 있으며, 이를 통해 양자 기술의 상호 운용성과 보안을 강화하고자 한다. 특히 JTC1의 SC27 WG3은 기존 암호기술의 안전성 평가와 관련 장비들의 보안 인증과 관련된 표준을 개발하는 곳으로, 이곳에서 양자키분배 장비의 보안 인증/평가를 위한 기반 표준이 개발되고 있다. 현재 개발 중인 2개의 표준이 마무리 단계에 있으며, 각각 양자키분배 장비의 보안 인증을 위한 요구사항을 정의하는 표준과 테스트/평가 방법을 정의하는 표준으로 나뉘어 개발되고 있다.

2.3.4 인터넷연구태스크포스(IRTF)

IRTF는 미래 인터넷 기술의 발전을 위한 연구 작업을 수행하는 기구이다. 이곳에서 연구하는 14개의 연구그룹 중 하나인 QIRG(Quantum Internet Research Group)에서는 장기적인 관점에서 양자 인터넷이라는 주제를 가지고 기초연구를 시작하는 단계에 있다. 특히 양자 인터넷의 구조를 정의하기 위한 기반 기술 원리 문서와 양자 인터넷의 응용 시나리오 문서 초안을 개발하고 연구를 이어가고 있다. 이를 통해 양자키분배 기술을 넘어선 양자 기술로 세계가 이어지는 양자 인터넷 세상에 대한 준비를 시작하고 있다.

3. 맺음말

양자통신과 그 표준화는 정보통신 기술의 미래를 형성하는 핵심 요소 중 하나이다. 양자키분배와 같은 기술들은 정보를 전송하고 보호하는 방식을 근본적으로 변화시킬 잠재력을 가지고 있다. 이는 단순히 보안도 강화할 뿐만 아니라, 정보통신 기술의 새로운 패러다임을 제시하고 있다 하겠다.

특히, 국제 표준화 기구들의 노력은 양자통신 기술의 발전과 보급에 필수적인 활동이다. ETSI, ITU-T, JTC1, IRTF와 같은 기구들이 수립하는 표준들은 기술의 상호 호환성, 안정성, 그리고 신뢰성을 보장할 것이다. 이러한 국제적 협력은 양자통신이 세계적으로 일관되고 효율적으로 구현될 수 있는 기반을 마련하는 데 큰 도움이 될 것이다.

양자통신의 미래는 밝다. 이 기술은 급속히 발전하고 있으며, 앞으로도 계속해서 우리의 통신방식을 혁신할 것이다. 이미 세계가 앞다투어 시범망을 구축하고 상용환경에서 테스트하는 등 상용화 준비에 박차를 가하고 있으며, 앞으로 수년 내에 상업적으로 적용될 가능성이 매우 큰 분야이다. 이는 우리 사회와 경제에도 중대한 영향을 미칠 것이다.

우리는 이 새로운 기술의 발전을 주목하고, 그 가능성을 최대한 활용하기 위해 노력해야 한다. 양자통신은 단순히 정보를 보호하는 수단이 아닌, 우리의 미래를 형성하는 핵심 기술로 자리매김할 것이기 때문이다.

[참고문헌]
[1] ITU-T Y.3800, https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13990
[2] ETSI ISG QKD, https://www.etsi.org/technologies/quantum-key-distribution
[3] ITU-T SG13, https://www.itu.int/en/ITU-T/studygroups/2022-2024/13/Pages/default.aspx
[4] ITU-T SG17, https://www.itu.int/en/ITU-T/studygroups/2022-2024/17/Pages/default.aspx
[5] ITU-T SG11, https://www.itu.int/en/ITU-T/studygroups/2022-2024/11/Pages/default.aspx
[6] 정보보호학회 – 양자암호통신 글로벌 표준화 현황,
https://public.thinkonweb.com/journals/kiisc/digital-library/25945
[7] 한국통신학회 - [Vol.39 No.5] 주제1 : 양자정보통신,
https://www.kics.or.kr/html/?pmode=Bpublication&page=2&smode=view&seq=3535&searchValue=&searchTitle=strTitle
[8] ISO/IEC 23837-1, https://www.iso.org/standard/77097.html
[9] ISO/IEC 23837-2, https://www.iso.org/standard/77309.html
[10] Quantum Internet Research Group, https://www.irtf.org/qirg.html

※ 출처: TTA 저널 제210호