보안 통신에서 양자 얽힘 사용 방법

(2023.03.12., 양자정보연구지원센터)

□ 보안 통신에서 양자 얽힘을 어떻게 사용할 것인가

○ 빛보다 빠르게(Faster Than Light)

- 광속보다 빠른 이동 및 통신은 물질(정보)이 빛의 속도보다 빠르게 이동할 수 있다는 이론(FTL)
- 아인슈타인 특수 상대성 이론에 따르면, 정지 질량이 0인 광자를 제외하고 자연계의 어떤 것도 빛의 속도보다 빠르게 이동할 수 없음
- “빛보다 빠른 입자의 가능성 “ 논문에서 명명한 타키온(tachyon), 가상의 입자는 빛의 속도를 초과(이론화), 그러나 인과 관계에 위배, 시간 여행이 가능하다는 가설로 실현 불가능함(현대 과학)
- FTL 난제의 기본 이론과 함께, 양자 얽힘 통신이 무엇이며 FTL 이론이 양자 통신과 어떻게 연결되는지 설명

○ **양자 얽힘 통신**이란

- ” spooky action at a distance “로 알려진 얽힘은 통신이 즉시 발생하는 현상, 두 입자가 그들 사이 물리적 거리에 관계없이 함께 묶인 경우임
- 얽힌 양자 입자는 거리에 관계없이 빛의 속도로 이동함에 따라 순간 상호작용하는 것처럼 보이지만, 양자 얽힘을 사용하여 데이터 전송은 불가능한 것으로 해석됨
- 정보를 전송, 통신하려면 데이터를 보내야 하는데, 양자 얽힘 사용하면 불가능, 양자 얽힘 통신이 가능해지면 응용 프로그램은 감지 기술 및 안전한 정보 전송에 광범위한 영향을 미칠 수 있음
- 얽힘 광자 사용한 실험, 벨 부등식 위반 확립 및 양자 정보과학 개척, 양자 통신의 의미
- 특정 연속 변수 기반에서 광자 얽힘이 광자가 소스에서 멀리 전

파함에 따라 스스로 부활한다는 사실 입증(올해 1월 인도 연구팀), 장거리에 걸쳐 양자 정보를 안전하게 전송하는 데 적용 가능

○ **사이버 보안**에서 **양자 통신**의 의미

- 이미 전 세계 정부는 양자 컴퓨터가 Shor 알고리즘 사용하여 정수 분해 기반 암호화를 사용하는 모든 공개 키 시스템을 깨뜨릴 수 있는 "Q-day" 준비 중
- 양자 통신은 보안을 보장하기 위해 양자 상태의 특수 속성을 활용, 큐비트라는 양자 상태에서 정보를 인코딩(일반적으로 광자 사용됨)

- QKD(Quantum Key Distribution)는 미래 대비할 수 있지만, 장거리에서는 신뢰할 수 있는 노드가 필요함(이론적 보안), 현재 단일 QKD 링크는 약 100km로 제한됨, 범위 확장을 위한 양자 중계기 및 위성-QKD 작업 진행 중, 하드웨어 통합 비용 증가의 단점

- PQC(post-quantum cryptography)는 양자 얽힘 활용하지 않는 미래 보안 문제의 다른 접근방식, 격자 기반, 코드 기반, 해시 기반, 초특이 등질성, 다변량-2차, PQC 보안은 아직 의심스러움, 그러나 알고리즘이 소프트웨어 계층에서 작동하므로 장거리 제공
- 소프트웨어가 메모리 및/또는 시간 요구 사항을 증가시킴, PQC 알고리즘은 양자 보안 기술에 대한 칩 기반 접근 방식으로 비용이 계속 감소하는 이점이 있음

○ 양자 얽힘 기반 통신이 현실이 되어 통신과 사이버 보안을 지원할 새로운 기술 시대의 가능성을 높이는 양자 기술 및 연구에 진전이 이루어지고 있음

- 2022년 노벨상 수상한 양자 얽힘에 대한 물리학자들의 지속적 연구가 수행되고 있음

(원문)

1. https://thequantuminsider.com/2023/02/20/quantum-entanglement-communication/