양자암호기반 통신망과 양자얽힘 기반 양자네트워크에 관한 연구

박포일
한국원자력통제기술원
poepark50@gmail.com

A Study on the network using quantum key distribution and quantum network based on quantum entanglement

Park Poe Il
Korea Institute of Nuclear non-proliferation And Control

요 약

본 논문은 세계 각국에서 실제로 테스트베드 형태로 구축하였던 양자키분배 방식(Quantum Key Distribution, QKD)의 양자암호기반 통신망과 양자얽힘을 기반으로 한 양자네트워크(Quantum Network)에 대해 살펴보고 각 방식의 한계와 발전 방향에 대해 연구하였다.

Ⅰ. 서 론

세계적으로 양자기술에 대한 다양한 연구가 활발히 진행되고 있으며, 세계 각국은 양자기술에 대한 다양한 이론들을 실제로 구현하여 양자기술을 현실화 하고 있다. 양자기술은 양자가 가지는 그 물리학적 특성을 활용하여 현재 전자를 기반으로 구현되어 있는 시스템을 대체하여 전자 기반의 체계에서 발생하는 보안 및 연산의 한계를 극복하고자 하는 것이다. 양자기술은 일반적으로 양자통신, 양자컴퓨팅 및 양자센서분야로 분류되며, 국가별로 분류되는 방식은 다양하나 우리나라의 경우 양자통신을 양자암호, 양자전송, 양자네트워크 3개로 세분류하고 있다.[1]

본 논문에서는 양자암호를 기반으로 하는 통신망과 양자얽힘을 기반으로 하는 양자네트워크에 대해 알아보고 각 방식의 한계와 발전 방향에 대해 논하고자 한다.

Ⅱ. 본론

미국, 유럽, 영국 등 세계 각국에서는 QKD방식의 양자암호를 기반으로 하는 통신망의 실험망, 시험망, 시험서비스 실증망 및 상용서비스망 등을 구축하고 있으며, 우리나라 역시 '초연결 지능형 연구개발망(KOREN)'에 양자암호기반 통신망의 실험망, 시험망 등을 구축하고 있다.

양자암호기반 통신망은 기존 통신망에 QKD장비를 추가하여 QKD에서 생성된 양자키를 통해 암호화를 하는 방식이다. 기존 RSA 암호방식의 경우 소인수분해 복잡도를 기반으로 하고 있으나, 양자컴퓨팅을 통해 구현될 Shor 알고리즘을 통해 기존 소인수분해의 복잡도를 $O(e^{(\log N)^{\frac{1}{3}}})$에서 $O((\log^N)^2)$ 수준으로 비약적으로 줄여 RSA 암호방식을 파훼할 수 있다.[2] 하지만 양자암호 방식은 기존 RSA 암호방식과 달리 연산의 복잡성을 통해 암호 수준을 결정하고 있지 않으며, 양자 그 자체의 특성을 사용하여 암호 수준을 높이는 방법이다. 따라서 기존컴퓨팅 또는 양자컴퓨팅의 수준이 향상 되더라도 양자 암호가 연산을 통해 해독되는 일이 발생하지 않는 장점이 있다.

양자암호의 해독을 위해서는 양자키를 확보하여야 한지만 양자는 그 물리학적 특성상 복제가 불가능하여 양자키를 복제를 통한 양자키 확보를 할 수 없고, 코펜하겐 해석에 따라 한번 측정한 양자는 붕괴하여 재사용할 수 없어 패킷 스니핑과 같은 형태의 양자키 확보 방식을 사용할 경우 수신자가 양자키를 수신할 수 없게 되어 양자키를 사실상 해킹할 수 없게 된다.

QKD의 경우 BB84프로토콜이 가장 대표적인 방식으로 오랫동안 연구되어 가장 확실하게 사용할 수 있는 방식의 프로토콜이라고 볼 수 있으며, 이외에도 BB84의 단순화 버전인 B92과 얽힘 양자를 사용한 E91 등이 있다. BB84프로토콜은 QKD장비를 통해 편광필터를 통한 측정신호를 상호 확인하여 비밀키를 생성하는 형태를 의미한다.

생성 비트	0	1	1	0
편광 필터	+	+	×	+
편광 신호	↑	→	↘	↑
측정 필터	+	×	×	×
측정 신호	↑	↗	↘	↗
필터 일치여부	일치	불일치	일치	불일치
비밀키	0	-	1	-

Table 1 : BB84 프로토콜 예시

다만, QKD의 경우 인증형태를 거치지 않기 때문에 중간자 공격 방식을 통해 비밀키를 획득 할 수 있고 이 경우에 취약[3]하며 QKD장비 자체가 부채널공격인 트로이목마[4], 수신기효율부조화[5], 위상재매핑[6], 블라인딩 공격[7]등에 취약하여 이에 대한 많은 연구가 필요하며 현재 다양한 연구가 진행되고 있다.

양자암호기반 통신망이 기존 통신망에 QKD장비를 추가하여 암호화 방식을

양자암호로 변경하여 양자를 암호체계에 사용하였다고 한다면, 양자얽힘을 기반으로 하는 양자네트워크는 기존 전자에 정보를 실어서 주고받던 방식에서 양자에 정보를 실어서 주고받는 형태로 양자를 통신 그 자체에 적용한 방식이다.

이는 얽힘을 통해 연결된 두 개의 양자(EPR pair라고 부른다)가 거리와 무관하게 같은 상태 값을 가지는 양자 얽힘의 특성을 바탕으로 하고 있다. EPR pair를 통해 양자 텔레포테이션을 수행하고 이를 통해 데이터를 전송할 수 있게 된다. 단, 발신지에서 생성된 양자 메시지는 측정과 동시에 파괴되며 파괴 시 생성된 2비트의 BSM(Bell-State Measurement) 결과를 기존 통신방식으로 발송시켜 이를 바탕으로 양자 메시지를 재구성하여야 한다.[8]

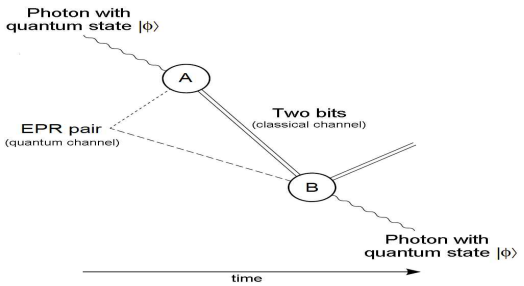

Figure 1 : 양자 텔레포테이션 구성도[9]

아직까지 양자얽힘을 기반으로 양자네트워크 구축에 성공한 사례는 Delft University of Technology의 Link Layer 프로토콜이 유일[10]하며, Delft는 세계 최초로 2미터 양자얽힘 기반 양자네트워크 구축에 성공하였다.

양자암호기반 통신망에서 양자역학에 기초한 양자키의 보안성에 대해 논한 바와 같이, 양자얽힘 기반 양자네트워크의 경우에도 양자는 복제되거나 도청할 수 없어 양자얽힘 기반 양자네트워크로 통신된 양자 메시지의 경우 이론적으로 해킹이 불가능하다는 큰 장점을 가진다. 또한 양자얽힘이 거리와 무관하게 즉각적으로 같은 값을 나타내기 때문에 양자 텔레포테이션만 지속적으로 연결하여 구현 할 수 있게 되면 통신 속도 또한 기하급수적으로 상승 할 것으로 기대된다. 아쉽게도 양자얽힘을 기반으로 양자네트워크를 구축의 최대 단점은 그 실제 구현이 극히 어렵다는 점이다.

Ⅲ. 결론

본 논문을 통해 양자암호기반 통신망과 양자얽힘기반 양자네트워크에 대해서 알아보았다. 양자암호기반 통신망의 경우 QKD장비를 기존 통신망에 사용하여 양자를 암호화 강화에 활용한 사례이다. 기존 RSA 암호체계가 양자컴퓨팅 발전에 따라 파훼될 수 있는 만큼 양자 암호키를 활용한 통신망의 보안 강화에 확실한 도움이 될 것으로 보인다. 다만 인증부재, QKD장비의 부채널공격 취약점 등 아직 추가적인 연구를 통한 보완이 필요하다.

또한, 양자얽힘기반 양자네트워크의 경우 실제 양자에 데이터를 실어 기존 전자의 역할을 대체하는 방식으로 EPR pair를 통항 양자 텔레포테이션을 수행하고 2-bit BSM값을 기반으로 양자 메시지를 재구성하는 방식으로 구현된다. 양자얽힘기반 양자네트워크를 통해 네트워크의 비약적 속도 증가와 해킹에서부터 자유로운 네트워크가 구축 될 것으로 기대된다. 다만 아직 실제 구현사례가 1개 밖에 없을 정도로 기술적 어려움이 많은 네트워크 구축 방식이다.

참 고 문 헌

[1] IITP, “ICT R&D 기술로드맵 2023 발표”, 2018 (https://www.iitp.kr/kr/1/notice/reportAndClarify/view.it?ArticleIdx=3437&count=true)

[2] Shor, P.W. "Algorithms for quantum computation: discrete logarithms and factoring". Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE Comput. Soc. Press: 124 - 134

[3] National Cyber Security Centre, “Whitepaper-Quantum Security Technologies”, 2020 (https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies)

[4] N. Gisin et al., “Trojan-horse attacks on quantum-key-distribution systems,” Phys. Rev. A, vol. 73, 2006, 022320.

[5] C.-H. Fung et al., “Security proof of quantum key distribution with detection efficiency mismatch,” Quant. Inf. Comp., vol. 9, 2009, 131-165.

[6] Marøy et al., “Security of quantum key distribution with arbitrary individual imperfections,” Phys. Rev. A, vol. 82, 2010, 032337.

[7] Z. Yuan et al., “Avoiding the blinding attack in QKD,” Nature Photonics, vol. 4, 2010, 800-801.

[8] Angela Sara Cacciapuoti and Marcello Caleffi. “The Quantum Internet: Networking Challenges in Distributed Quantum Computing”, Feb 2019.

[9] C. H. Bennett, “Teleporting an Unknown Quantum Stat via Dual Classical and Einstein-Podolsky-Rosen Channels”, 1993.

[10] Axel Dahlberg, Matthew Skrzypczyk, Tim Coopmans, Leon Wubbben, Filip Rozpedek, Matteo Pompili, Arian Stolk, Przemyslaw Pawelczak, Robert Knegjens, Julio de Oliveira Filho, Ronaldo Hanson, Stephanie Wehner, “A Link Layer Protocol for Quantum Networks”, Mar 2019.