양자기술의 가용성에 관한 연구

박포일*

한국원자력통제기술원

Study on availability of quantum technology

Poe-il Park

Korea Institute of Nuclear nonproliferation And Control(KINAC)

E-mail : poepark50@gmail.com

요 약

본 논문은 미래 양자 기술(Quantum technology)로 구현된 사회에서 양자 기술이 가지는 가용성에 대해 알아보고 그 가용성에 영향을 미치는 다양한 공격기법에 대해 연구하였다.

ABSTRACT

On this paper, the availability of quantum technologies are studied and various attack methods to damage the availability of quantum technologies are studied.

키워드

양자기술, 양자컴퓨팅, 가용성, 양자공격, Quantum Technology, Quantum computing, Availability, Quantum Attack

Ⅰ. 서 론

양자 기술은 현재 세계적으로 큰 관심을 받고 있는 주요한 미래 기술 중 하나이다. 양자 기술은 아주 긴 시간동안 전세계에서 활발히 연구되고 있으며 최근 양자 컴퓨팅, 양자 통신, 양자 인터넷 등 다양한 실증사례들이 나오고 있다.

양자 컴퓨팅의 경우 양자CPU 개발이 다수 진행중에 있다. 특히 IBM의 경우 현재 65큐비트 수준의 양자컴퓨터를 클라우드 형태로 서비스 중이며, 향후 2023년까지 1000큐비트 수준의 컴퓨팅 파워를 확보하는 목표를 가지고 있다.[1].

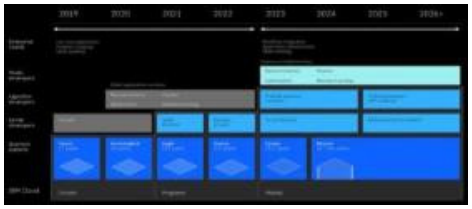

그림 1. IBM의 양자 컴퓨팅 로드맵[1]

양자 통신의 경우 Delft University의 QuTech에서 Link Layer 프로토콜을 사용하여 2019년 실제 양자 통신에 성공한바 있으며 이론적으로 얽힘을 연속적으로 하여 통신이 가능함을 입증하였다.[2]

양자를 구현하는 방식에는 여러 가지 방식이 있으나 다이아몬드 질소공동센터 방식을 제외하고는 아직까지 극도로 제한된 물리적 환경을 요구하고 있다.[3] 이토록 구현되기 힘든 양자를 활용한 양자기술의 가용성은 어느 정도이며, 이 가용성을 침해할 수 있는 공격방식은 무엇이 있는지 논하고자 한다.

양자 기술은 양자의 중첩과 얽힘이라는 특성을 활용하여 기존 전자를 대체하는 기술을 개발하는 것이다. 보안관점에서 가장 중요한 양지의 특성은 양자가 결잃음에 따라 정보가 사라진다는 점[4]과 양자는 no cloning theorm에 따라 복제가 안된다는 특성[5]이라고 할 수 있다. 이는 공격자가 의도적으로 양자의 결잃음을 유도하여 정보를 유실 시킬 수 있으며, 복제가 안 되는 양자의 특성 상 유실된 정보가 아주 중요도가 높다면 그만큼 양자기술의 가용성에 치명적인 영향을 주게 된다는 것을 의미한다.

* corresponding author

II. 양자기술의 가용성

양자 기술의 현재 개발 단계로서 가지는 가용성은 높지 않다고 할 수 있다. 이는 양자가 구현 될 수 있는 물리적 환경(온도 등)이 상당히 제한적이기 때문이다. 다만, 양자 기술이 상용화되는 수준에 이르게 된다면 현재 상용화된 전자 기술(electron technology)에 준하는 수준의 가용성을 가진다고 가정해야 할 것이다.

양자 기술의 가용성에 영향을 줄 수 있는 공격기법은 다양하지만 본 논문에서는 양자 기술에 적용될 수 있는 몇가지 공격기법에 대해 알아보았다.[6]

첫 번째는 공격자의 악의적인 얽힘(malicious entanglement)을 통한 공격이다. 이는 공격자가 의도적으로 양자에 얽힘을 연결하여 다중 얽힘을 통해 정보를 탈취해가는 방식을 말한다. 기존 패킷 스누핑과 유사한 방식으로 데이터를 탈취해가는 것으로 양자 기술에서는 복제 불가성(no cloning)에 따라 기존 패킷 스누핑보다 큰 영향을 받게 된다.

두 번째는 공격자가 의도적으로 결함이 있는 양자를 주입(fault injection)하는 것이다. 이를 통해 사용 중인 양자 중에 어떤 것이 진짜인지 판단하기 어렵도록 유도하여 시스템의 가용성을 해치는 방식이다. 기존 서비스 거부 공격(denial-of-service attack)과 유사한 방식의 공격 기법으로 기존 서비스 거부 공격과 같이 시스템에 부하를 발생 시켜 가용성을 해칠 수 있다. 다만 양자 기술에서는 이러한 의도적인 공격에 대한 방어책으로 다양한 양자필터를 활용 할 수 있으며, 이를 통해 시스템의 가용성을 확보 할 수 있다.

세 번째는 측정자 공격(blinding of detector) 방법으로 데이터를 운반하는 양자(qubit)가 아닌 단순 광자(pulse)를 주입하는 공격이다. 양자 기술의 특성상 최종 측정자(end-user)는 양자의 파동을 감지하여 데이터를 측정하여야 하는데 공격자가 양자가 아닌 광자를 섞어서 송신하여 사용자의 측정 장비의 가용성을 해칠 수 있다. 이러한 방식의 공격은 기존 전자를 통한 기술에서는 보기 어려운 방식으로 측정 장비에서 어느 정도 방어할 수 있는 능력을 갖춰야 할 것으로 보인다.

네 번째는 시스템 외부 공격(out-of-system attack)으로 외부 환경에 민감한 양자 기술의 취약성을 조준한 공격이다. 외부에서 강한 RF노이즈를 통해 양자를 파괴하거나 양자 기술에서 사용되는 장비에 물리적인 온도 변화와 같이 양자가 구현될 수 있는 환경을 훼손하여 구현된 양자가 해당 시점에 파괴도록 유도하는 공격 방법이다. 외부의 강한 노이즈를 통한 공격은 기존 전자를 통한 기술에도 다양하게 적용 될 수 있으나 양자의 복제 불가성에 따라 그 치명도가 훨씬 높다고 할 수 있다.

아직 완전히 구현되지 않은 양자 기술들에 대한 다양한 공격기법들이 연구되고 있으나, 아직 양자 기술이 완전한 구현단계에 이르지 못하였기 때문에 이러한 공격 기법들의 가능성에 대한 것들은 미지수이다. 다만, 기존 전자를 통한 기술에서와 유사한 형태의 공격이 양자기술에도 적용될 것으로 보이며, 양자의 물리적 취약성에 따라 양자기술에 대한 공격 기법들의 영향이 더욱 치명적일 것으로 예상된다.

III. 결 론

본 논문을 통해 4가지 양자 기술의 공격 기법을 통한 양자 기술의 가용성에 대한 영향을 알아보았다.

공격자의 악의적 얽힘(malicious entanglement), 결함 있는 양자 주입(fault injection), 측정자 공격(blinding of detector), 시스템 외부 공격(out-of-system attack)의 방식은 기존 패킷 스누핑, 서비스 거부 공격과 같이 기존 전자를 통한 기술에서 활용되던 공격 기법도 있으며, 양자 기술에만 특수하게 적용되는 공격 기법도 있음을 확인하였다.

양자 기술이 실제로 상용화되기 까지 상당한 시간이 더 필요 할 것으로 보이며, 양자 기술이 상용화되어 사용 된다면 이러한 공격 기법 이외에도 다양한 공격 기법들에 대한 방어 방안을 철저히 마련하여 양자 시스템의 가용성을 확보하도록 노력하여야 할 것이다.

References

[1] IBM, IBM’s roadmap for building an open quantum software ecosystem [Internet]. Available : https://ibm.com/blogs/research/2021/02/quantum-development-roadmap

[2] Delft Univerity of Technology. World’s first link layer protocol brings quantum interent closer to a reality [Internet]. Available : https:www.delta.tudelft.nl/article/first-version-quantum-internet-making

[3] 이준, ”양자컴퓨터 R&D 현황과 전망“, 정보통신기획평가원 주간기술동향 1915호, p.14-32, 2019.

[4] Lucia Hackermuller, Klaus Hornberer, Bjorn Brezger, Anton Zeilinger, and Markus Arndt, “ Decoherence of matter waves by thermal emission of radiation”, Nature 427, 711-714, 2004

[5] James Park, “The concept of transition in quantum mechanics”, Foundations of Physics 1, p23-33, 1970

[6] Takahiko Satoh, Shota Nagayama, Shigeya Suzuki, Takaaki Matsuo, and Rodney Van Meter, “Attacking the Quantum Internet”, IEEE, 2020