양자 키 분배의 개념과 과제

고민혁 · 김도현 · 이대성*

부산가톨릭대학교

Concepts and Challenges of Quantum Key Distribution

Min-hyuk Ko · Do-hyun Kim · Daesung Lee*

Catholic University of Pusan

E-mail : gomin2480@gmail.com / dohyun@cup.ac.kr / dslee@cup.ac.kr

요 약

본 논문에서는 지금까지의 양자 키 분배 기술에 대한 기본적인 개념과 기술적으로 발전해야 할 문제들을 소개하려 한다. 양자 키 분배 기술은 더이상 쪼갤 수 없는 물리량의 최소 단위인 양자(Quantum)의 특성을 이용해 도청 불가능한 암호키를 생성, 송신자와 수신자 양쪽에 나눠주는 기술이다. 이 기술의 대표적인 프로토콜인 BB84 프로토콜을 소개하고 현실적인 어려움과 앞으로의 과제를 살펴보고자 한다.

ABSTRACT

In this paper, we would like to introduce the basic concepts of quantum key distribution techniques so far and the problems that need to be technically advanced. Quantum key distribution technology is a technology that generates non-tapable encryption keys and distributes them to both sender and receiver using the characteristics of Quantum, which is the minimum unit of physical quantity that can no longer be split. We would like to introduce BB84 protocol, a representative protocol of this technology, to explore realistic difficulties and future challenges.

키워드

Quantum, Quantum key distribution, Encryption key, Quantum Communication

Ⅰ. 서 론

최근 여러 다국적 기업들이 양자컴퓨터 연구개발 경쟁을 치열하게 진행하면서 관련 기술이 비약적으로 발전하고 있다. 양자컴퓨터 기술의 발전은 많은 분야에서 큰 발전을 꾀할 수 있다는 긍정적인 관점도 있다. 그에 반해 수학적 복합성을 기반으로 하는 현대암호의 안전성이 크게 위협받는 상황이 되었다. 이를 해결하기 위해서 수학적 계산 복잡성이 아닌 물리 법칙에 안전성을 기반하는 차세대 보안 통신 기술인 양자 키 분배 시스템이 1984년에 처음 제안되었고 지속해서 연구가 진행중에 있다. 하지만 양자 키 분배 시스템도 이론적으로는 완전한 안전성을 보장하지만, 아직은 실질적인 장비의 결함 등으로 인한 외부로부터의 양자 공격이 존재하고, 현대암호 인프라에 더욱 실용적으로 적용하기 위해 풀어야 하는 기술적 이슈들이 존재한다. 본 논문에서는 양자컴퓨터의 위협으로부터 보호할 수 있는 양자 키 분배 시스템과 국내 · 외의 기술개발 동향을 살펴본다.

Ⅱ. 양자 키 분배

동일한 양자 키를 나누어 가지기 위한 대표적인 프로토콜로 BB84 프로토콜이 있다. BB84 프로토콜은 1984년 C. H. Bennett과 G. Brassard가 제안한 프로토콜로 양자역학의 관측이론과 OTP(One Time Password) 암호 방식을 결합하여 해독이 불가능하게 만든 암호 방식이다[1]. 큐빗의 양자상태 중 광자의 편광을 이용한 양자 키 분배 과정은 다음과 같다. 송 · 수신자는 가로와 세로 기저의

* corresponding author

두 편광상태 ↕, ↔을 각각 bit 0과 1로 정의하고, 마찬가지로 두 대각 기저의 편광상태 ↘,↙을 마찬가지로 bit 0과 1로 한다. 송신자는 앞의 4개의 양자상태를 무작위로 큐빗 열을 만들고 양자채널을 통해 수신부로 전송한다. 수신자는 전송받은 큐빗 열 각각을 가로나 세로 또는 대각 기저를 무작위로 선택하여 측정한다. 만약 큐빗의 편광과 같은 기저로 측정할 경우 측정한 정보는 전송했던 정보와 같게 측정이 되지만, 다른 기저로 측정을 할 경우에는 측정한 정보가 전송한 정보와 같을 확률과 다를 확률이 각각 50%가 된다[2]. 따라서 수신자는 측정한 결과와 사용한 기저를 전부 기록하고 모든 큐빗의 측정이 끝난 후, 송 · 수신자는 송신한 큐빗의 기저와 측정한 기저가 같은 것만 추려내는 sifting 과정을 거쳐 정보를 나누어 가진다. 나누어 가진 정보 중 일부를 비교하여 오류확률을 측정하고 도청자의 유무를 판단한다[3].

III. 양자 키 분배의 한계

양자 키 분배 시스템을 구현하기 위해선 큐빗 생성을 위한 단일광자 광원이 필요하다. 하지만 아직 고순도의 단일광자 광원을 구현해 내는 것은 현실적으로 불가능하다. 그래서 지금까지의 양자 키 분배 시스템은 실용성과 경제성을 고려하여 단일광자 광원을 감쇄된 레이저로 대체하여 사용하고 있다. 하지만 레이저는 단일광자 광원과는 달리 광자의 개수는 Poisson 분포를 따르고 있어 하나가 아닌 두 개 이상의 광자가 출력될 확률이 있다. 이를 이용해 도청자가 두 개의 광자 중 한 개를 탈취하여 측정하는 것으로 손쉽게 도청을 할 수 있게 된다. 이러한 큰 단점 때문에 2000년대 초반 양자암호통신은 큰 어려움을 겪었으나, Decoy 프로토콜의 등장과 다양한 이론적 · 실험적 고찰로 현재까지 다양한 연구가 이어져 올 수 있게 되었다. 그러므로 Decoy 프로토콜은 현재 필수적으로 수행되어야 할 기술이 되었다[3].

현실적으로 양자 키 분배 시스템은 전송 과정에서 양자채널과 수신부 광학계에서의 손실률, 단일광자 검출기의 검출 효율의 부족함으로 인한 손실률이 존재한다. 실제로 일반 광케이블의 손실률은 0.2 dB/km이고, 단일광자 검출기의 효율은 통신 파장 대역에 따른 물질 특성에 따라 10~90% 정도로 측정된다. 또한 송신 측에서는 반드시 단일광자 수준의 큐빗이 전송돼야만 하므로 통신거리에도 한계가 있다[3].

IV. 결 론

양자 키 분배 시스템의 기본적인 개념과 향후 해결해 나가야 할 과제들을 기술했다. 양자 키 분배와 같은 양자 관련 연구들은 지금까지 계속 발전되고 분야가 점점 다양해지고 있다. 그럼에도 불구하고 아직까지 현실적으로 해결하지 못하고 있는 문제와 더욱 개선이 필요한 기술적 문제들이 존재한다. 미국과 같은 여러 나라들이 양자 통신 및 양자 기술들에 많은 투자를 하고 있지만, 현재는 중국이 위성을 통한 대륙 간 양자 통신, 도시 간 신뢰연계점을 통한 유선 장거리 양자 통신 등으로 양자 통신 강국으로 올라가고 있다[4]. 우리나라도 뛰어난 통신 인프라 및 반도체 기술이 있기에 양자 키 분배 및 양자 통신 분야에서 두각을 비출 수 있는 환경을 가지고 있다. 앞으로는 이러한 기술적 문제들을 해결하고 핵심기술의 연구를 통해서 양자 통신 시대를 맞이해야 할 것이다.

References

[1] PW Shor, J Preskill, “Simple proof of security of the BB84 quantum key distribution protocol,” Physical review letters, Vol. 85, Iss. 2, 2000

[2] HY Lee, KH Cho, HJ Yang “Quantum Key Distribution Protocol,” KIISC review, Vol.12 No.5, pp. 1-7 , 2002

[3] BG Park, SU Han, “Trends in Technology Development of Quantum Key Distribution Systems,” Electrical & Electronic Materials, Vol. 33 Iss. 4, Pages.26-35, 2020

[4] China successfully communicates quantum cryptography over 4,600 kilometers...Evaluate Technology Aggregation [Internet]. Available : http://dongascience.donga.com/news.php?idx=42981