시뮬레이션을 이용한 decoy state 기법 분석

김범일, 허준*
고려대학교, *고려대학교

bik0118@korea.ac.kr, *junheo@korea.ac.kr

Analysis of decoy state method using simulation

Kim Bum Il, *Heo Jun(Korea Univ.)

요 약

본 논문에서는 시뮬레이션을 통해 decoy state 기법에 대해 분석한다. 양자 키 분배 기술은 이론적으로 무조건적인 보안을 보장하는 기술이다. 그러나, 기술적 한계로 인한 항상 완벽한 단일 광자를 생성하지 못하고 다중 광자 또한 발생한다. Photon Number Splitting attack(PNS attack)은 이와 같은 허점을 노려서 송수신자 사이 공유하는 키를 도청하는 방법이다. 이를 방어하기 위해 decoy state 기법이 제안되었다. 따라서, 시뮬레이션을 통해 PNS attack 을 확인할 수 있는 Y_1의 lower bound 를 구하고 PNS attack 을 모사하여 공격이 발생했을 때의 Y_1의 lower bound 와 비교하여 본다.

Ⅰ. 서 론

양자 키 분배 기술은 양자 역학적 성질을 이용하기 때문에 무조건적인 보안을 보장하게 된다. 그러나, 기술적 한계로 인해 이론적으로 가정한 상황을 현실적으로 구현할 수 없다. 대표적으로 양자 키 분배에 이용되는 레이저는 이론적으로는 항상 단일 광자를 생성해야 한다. 하지만, 기술적인 한계로 인해 포아송 분포를 가지는 레이저에 감쇠를 이용하여 단일 광자 수준으로 낮추어 이용한다. 단일 광자 수준은 완벽히 단일 광자를 생성하는 것이 아니기 때문에 다중 광자가 발생할 위험이 항상 존재한다. PNS attack 은 이러한 허점을 노려 키를 얻어낸다. PNS attack 은 양자 비트 오류율에 변화를 주지 않기 때문에 양자 비트 오류율로 도청자를 파악하는 방법으로는 도청자를 확인할 수 없다. 이를 극복하기 위해 제시된 방법이 decoy state 기법이다[1]. 본 논문에서는 PNS attack 을 시뮬레이션을 통해 모사하여 decoy state 기법의 효과를 확인한다.

Ⅱ. 본 론

A. Photon Number Splitting attack

그림 1. PNS attack 개요도

양자 키 분배에 사용되는 Laser 는 식(1)과 같은 확률로 광자가 발생하는 포아송 분포를 따른다.

$$p(i,\mu)=\frac{\mu^i}{i!}e^{-\mu} \quad (1)$$

이때, μ 는 평균광자수이고 i 는 생성광자수이다. 이 때문에 단일 광자 수준으로 감쇠시켜 사용하여도 다중 광자가 전송되는 경우가 발생한다.

PNS attack 은 도청자가 양자채널을 관찰하여 단일 광자가 지나가는 경우는 제거하고 2 개이상의 광자는 광자를 한 개는 도청자가 저장하고 나머지는 수신자에게 전송되도록 한다. 이후, 송수신자가 key sifting 과정을 진행할 때, 포획 과정에서 포획된 광자와 동시에 생성된 다른 광자에 영향을 끼치지 않기 때문에 양자 비트 오류율에 영향을 주지 않으면서 송수신자와 동일한 키를 얻게 된다.

B. Decoy state method

레이저의 평균 광자수가 μ라고 할 때, 송신자가 광자를 수신할 확률을 gain(Q_μ)이라 한다. 식(2) 과 같이 나타난다.

$$Q_\mu=\sum_{i=0}^{\infty}Y_i\frac{\mu^i}{i!}e^{-\mu} \quad (2)$$

식(2)에서 Y_i (yield)는 i 개의 광자가 생성되었을 때, 수신자가 관측할 조건부 확률을 말한다. yield 는 광원의 평균 광자수와 상관없이 양자 채널과 detector 의 효율에 영향을 받는다. 이를 통해 PNS attack 에 가장 크게 영향을 받는 파라미터는 Y_1를 추론을 통해 PNS attack 의 발생여부를 확인할 수 있다. 이를 위해서는 평균 광자수가 0, 평균 광자수가 ν인 decoy state 를 사용하는 Vaccum+ weak decoy state 를 사용한다면 Y_1의 lower bound 를 구할 수 있다[2].이때의 평균 광자수는 식(3)과 같은 조건을 만족한다.

$$0<\nu<\mu \quad (3)$$

이때, Q_0은 식(4)과 같이 나타난다.

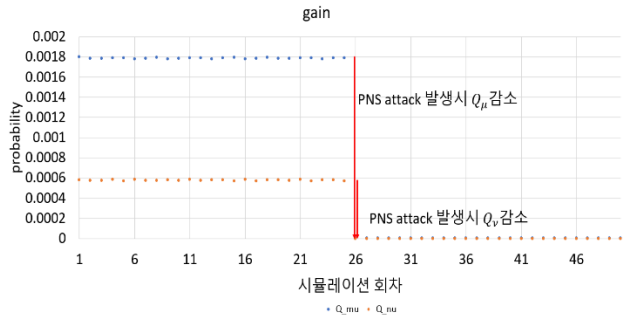
$$Q_0=Y_0 \quad (4)$$

Q_μ, Q_ν 값을 이용하여 Y_1 을 식(5)과 같이 추론할 수 있다.

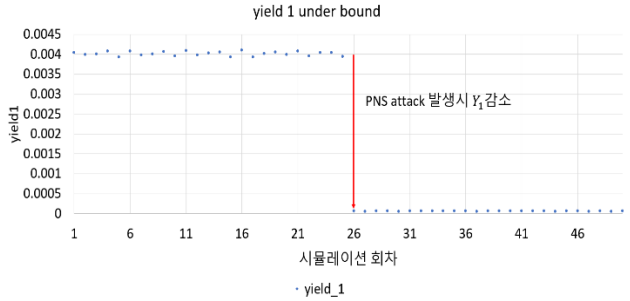
$$Y_1\geq Y_1^L=\frac{\mu}{\mu\nu-\nu^2}\left(Q_\nu e^\nu-Q_\mu e^\mu\frac{\nu^2}{\mu^2}-\frac{\mu^2-\nu^2}{\mu^2}Y_0\right) \quad (5)$$

C. 시뮬레이션

시뮬레이션의 변수는 [3]을 참조하여 진행하였다. 총 50 회를 진행시켰고 26 회부터는 PNS attack 을 모사하여 진행하였다.



Q_μ 의 평균은 $1.7872 * 10^{-3}$, Q_ν 의 평균은 $5.7717 * 10^{-4}$ 로 나타났다. PNS attack 이 발생한 경우, Q_μ 의 평균은 $1.1789 * 10^{-6}$, Q_ν의 평균은 $1.4086 * 10^{-7}$로 나타났다.



Y_1^L 의 평균은 $4.0157 * 10^{-3}$로 나타났다. PNS attack 이 발생한 경우, Y_1^L의 평균은 $5.8965 * 10^{-5}$, 로 나타나 PNS attack 이 발생하면 Y_1^L이 감소하여 Y_1^L을 PNS attack 이 발생여부를 확인할 수 있음을 확인할 수 있다.

Ⅲ. 결론

본 논문에서는 시뮬레이션을 통해 decoy 기법을 분석하였다. PNS attack 이 발생하지 않았던 상태의 Y_1^L을 구하고 PNS attack 이 발생한 상태에서의 Y_1^L 을 구해 비교하여 정상적인 상황에 비해 Y_1^L가 명확히 감소되는 것을 확인하여 decoy 기법의 효과를 확인하였다.

ACKNOWLEDGMENT

"본 연구는 과학기술정보통신부 및 정보통신기획 평가원의 대학 ICT 연구센터육성지원사업의 연구결과로 수행되었음" (IITP-2021-2018-0-01402*)

본 연구 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No. 2020-0-00014, 결함허용 논리양자큐빗 환경을 제공하는 양자운영체제 원천기술 개발)

참 고 문 헌

[1] W.-Y. Hwang "Quantum Key Distribution with High Loss: Toward Global Secure Communication", Phys. Rev. Lett. 91, 057901 (2003).

[2] Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo, "Practical decoy state for quantum key distribution", Phys. Rev. A 72, 012326 (2005)

[3] Y. Zhao, B. Qi, X. Ma, H. Lo and L. Qian, "Simulation and Implementation of Decoy State Quantum Key Distribution over 60km Telecom Fiber," 2006 IEEE International Symposium on Information Theory, Seattle, WA,USA,2006,pp.2094~2098,doi:10.1109/ISIT.2006.261920