Squeezed State를 기반으로 한 양자 키 분배 기법 분석

문현승, 허준
고려대학교

hsmoon1104@korea.ac.kr, junheo@korea.ac.kr

Analysis of Quantum Key Distribution Based on Squeezed States

Moon Hyun Seung, Heo Jun*
Korea Univ.

요 약

본 논문에서는 기존의 광자 기반의 양자 키 분배 기술에서 모델링하는 결맞음 상태를 변형한 squeezed state에 대해 분석하고, 이를 기반으로 한 양자 키 분배 기법에서의 secret key rate에 대해 분석한다 .

.

Ⅰ. 서론

양자 키 분배 기법은 광자를 신호로 사용하여 비밀 키를 나누어 가지는 키 분배 기법으로, 비가역적인 자연 현상을 기반으로 한다는 특징이 있다. [1] 이러한 양자 키 분배 기법은 양자역학의 기초적인 현상 중 하나인 복제 불가능성 원리에 의해, 단 한번의 측정만 가능하기 때문에 광자의 복사가 불가능하여 단일 광자가 완전한 경우 이론적으로 무결점 보안을 가질 수 있음이 증명되었다. [2]

본 논문에서는 양자 키 분배 기법의 현실적 한계로 지적되는 양자 채널에서의 신호 왜곡 또는 잡음에 의한 효과를 보완할 수 있도록 결맞음 상태를 변형하여 squeezed state 기반의 양자 키 분배 기법을 소개하고, 이를 통해 분배되는 비밀 키의 key rate에 대해 분석한다.

Ⅱ. 본론

전자기장에서 결맞음 상태는 소멸 연산자의 eigenstate로서, 수식적으로 다음과 같이 표현된다.

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle, where\ \hat{a}\ is\ the\ annihilation\ operator$$

이 때, 결맞음 상태를 number state를 기저로 가지도록 normalization condition을 고려하여 확장해주면 다음과 같다.

$$|\alpha\rangle = \exp\left(\frac{-|\alpha|^2}{2}\right)\sum_n \frac{\alpha^n}{\sqrt{n!}}|n\rangle$$

또한, squeezed coherent state는 vacuum state($|0\rangle$)에 대해 displacement operator $D(\alpha)$ 를 취해주고 squeezing operator $S(\xi)$를 곱해주어서 얻을 수 있다.

$$|\alpha,\xi\rangle = S(\xi)D(\alpha)|0\rangle,$$
$$where\ S(\xi) = \exp\left(\frac{1}{2}\xi^*\hat{a}^2 - \frac{1}{2}\xi\hat{a}^{\dagger 2}\right),$$
$$\xi = r\exp(i\varphi)\ and\ r\ is\ the\ squeezing\ parameter$$

이를 바탕으로 squeezed coherent state를 number state로 확장해 photon-number probability(p_n)에 대한 다음과 같은 식을 얻을 수 있다.

$$p_n = \frac{1}{n!\,\mu}\left(\frac{|\nu|}{2\mu}\right)^n\left[H_n\left(\frac{|\alpha|}{\sqrt{2\mu|\nu|}}\right)\right]^2\exp\left(-|\alpha|^2\left(1-\frac{|\nu|}{\mu}\right)\right),$$
$$where\ \mu = \cosh(r)\ and\ \nu = \sinh(r)$$

양자 키 분배 상황에서, 최종 키에 대한 도청자의 Shannon information은 지수적으로 작아야 하기 때문에, sifted key에 대한 오류 정정 및 비밀성 증폭 과정을

거치게 된다. 이러한 일련의 과정들을 거친 뒤의 individual attack에 대한 gained secret key는 [3]에서 제시되었으며, 이를 squeezed coherent state에 맞게 변형하면 다음과 같은 수식을 얻을 수 있다.

$$R = \frac{1}{2}p_{exp}\{\frac{p_{exp}-S_m}{p_{exp}}\times$$
$$\left(1-\log\left[1+4e\frac{p_{exp}}{p_{exp}-S_m}-4\left(e\frac{p_{exp}}{p_{exp}-S_m}\right)^2\right]\right)$$
$$+f(e)[elog(e)+(1-e)\log(1-e)]\}$$

이 때의 p_{exp} 는 expected photon-counting probability로, 신호에 의해 수신자의 detector가 측정할 확률(p_{exp}^{sig})에 dark count probability(d_B)를 더해서 얻을 수 있으며, S_m 은 multiphoton state probability, e 는 error rate로서 다음과 같이 표현된다.

$$e = \frac{cp_{exp}^{sig}+d_B}{p_{exp}}$$

분자에서 첫 항은 검출된 신호에 의한 오류이고, 두번째 항은 dark count에 의한 오류를 나타낸다. $f(e)$는 bidirectional error correction을 하기 위해 필요한 중복되는 비트로서, 실험적으로 얻을 수 있는 값이다. 앞서 구한 p_n을 기반으로 하여 gained secret key rate를 1500nm 대역에 대해 그래프를 그리면 다음과 같다.[4]

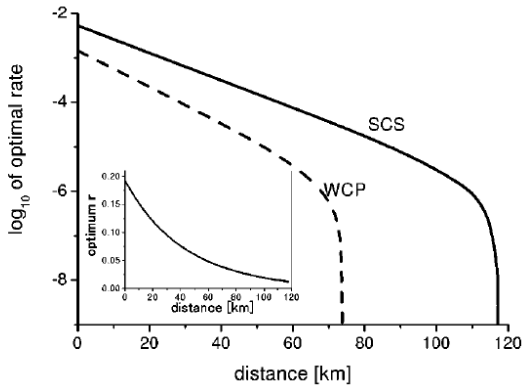

그림 1. Transimission distance 에 따른 secret key rate. 내부에 삽입된 inset graph 는 거리에 따른 optimal squeezing parameter r 을 나타냄. WCP 는 일반적인 weak coherent pulse, SCS 는 본 논문에서 분석한 squeezed coherent state.

그림 1의 결과를 통해, 기존의 WCP를 사용하는 프로토콜에 비해 secret key rate 및 통신 거리가 모두 개선되었음을 알 수 있다. 만약 실험 환경에서 이러한 squeezed state를 생성해주는 장비, 예를 들어 parametric down converter 등이 있을 경우 더 효율적인 양자 키 분배 프로토콜으로써 squeezed state protocol이 사용될 수 있을 것으로 생각된다.

Ⅲ. 결론

본 논문에서는 레이저(광자) 기반의 photon source에 대한 광학적 모델링인 결맞음 상태를 변형한 squeezed coherent state를 수식적으로 표현하고, 이를 기반으로 한 양자 키 분배 기법에 대한 secret key rate를 분석하였다. 분석한 결과, 기존의 프로토콜에서 사용되는 WCP를 통한 양자 키 분배 대비 성능이 뛰어남을 확인하였다. 추후 연구를 통해 다양한 squeezed state에 대해 양자 키 분배 기법으로의 응용을 분석할 수 있을 것으로 생각된다.

.

ACKNOWLEDGMENT

본 연구는 고려대 암호기술 특화연구센터(UD170109ED)를 통한 방위사업청과 국방과학연구소의 연구비 지원으로 수행되었습니다

참 고 문 헌

[1] Bennett, C. et al. Quantum Cryptography: “Public key distribution and coin tossing”, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 175-179, 1984.

[2] Shor, P. et al. “Simple proof of security of the BB84 quantum key distribution protocol”, Phys. Rev. Lett. 85, 2000.

[3] Lutkenhaus. N. “Security against individual attacks for realistic quantum key distribution”, Phys. Rev. A 61, 2000.

[4] Matsuoka, M. et al., “Quantum key distribution with a single photon from a squeezed coherent state”, Phys. Rev. A 67, 2000.