김일성종합대학학보
물리학

주체107(2018)년
제64권 제4호

량자얽힘상태를 리용한 량자안전직접통신의 한가지 규약

장철정, 김남철

1984년에 벤네트와 브라싸드가 최초의 량자열쇠분배규약을 제안한 후 각이한 량자열쇠분배규약들에 대한 연구[1, 2]과정에 량자력학의 많은 특성들 실례로 클론불가능성정리, 불확정성원리, 량자얽힘, 비직교량자상태들의 구별불가능성원리 및 비국부성 등과 같은 량자력학적성질들을 리용하면 전통적인 정보처리분야에서는 실현불가능하거나 실현하기 힘든 정보처리과제들을 수행할수 있다는것이 밝혀졌다. 그러나 량자열쇠분배와 관련하여 량자열쇠의 생성률이 높지 못한 문제가 발생하였다. 일단 량자열쇠를 준비하는 과정에 도청자가 도청한다면 모든 량자열쇠들은 버려야 하며 따라서 시간랑비와 함께 자원도 소모되게 된다. 이러한 리유로 하여 량자열쇠분배에 기초한 량자암호통신의 개발응용과 함께 새로운 량자통신방안들을 탐색하기 시작하였는데 그 대표적실례가 바로 량자안전직접통신(QSDC)방안이다.[3, 4] 량자안전직접통신방안은 최근시기에 제안되여 그 리론적연구가 매우 활발히 진행되고있다. 량자통신의 관점에서 볼 때 량자안전직접통신에서는 통신쌍방이 량자상태를 정보나르개로 리용하고 량자력학의 원리와 각종 량자특성을 리용하며 량자정보의 전송을 통하여 통신쌍방사이에 정보루실이 없이 안전하게 직접 정보를 효과적으로 전송할수 있다. 량자안전직접통신과 량자열쇠분배의 차이점은 그것을 리용하는 직접전송과정에 비밀정보를 변화시키지 않는다는것이다.

2002년에 량자조밀부호의 착상에 기초하여 량자얽힘쌍(또는 간단히 EPR쌍)을 리용하는 량자안전직접통신규약[3]과 EPR쌍에 기초한 수값자료형식으로 하는 두단계 규약과 비직교편극된 단일포톤에 기초한 량자안전직접통신규약이 제안되였다. 최근에는 인증에 기초한 QSDC규약이 제안되였다.[4] 현재까지 제안된 대다수의 QSDC규약들은 모두 얽힘상태에 기초하여 설계된것들로서 실례로 벨상태를 리용하여 비밀정보를 직접 전송한다.

우리는 얽힘상태를 리용한 새로운 한가지 량자안전직접통신방안을 제안하고 그 통신규약을 설명하였으며 도청전략에 대한 안전성을 분석하였다.

1. 량자얽힘상태를 리용하는 량자안전직접통신의 한가지 규약

다음과 같은 4가지 얽힘상태를 리용하기로 한다.

$$|\Phi^-\rangle=\frac{1}{\sqrt{2}}(|\phi^-\rangle-|\psi^+\rangle)_{AB}=\frac{1}{\sqrt{2}}(|-0\rangle-|+1\rangle)_{AB}=\frac{1}{\sqrt{2}}(|0-\rangle-|1+\rangle)_{AB} \quad (1)$$

$$|\Phi^+\rangle=\frac{1}{\sqrt{2}}(|\phi^+\rangle+|\psi^-\rangle)_{AB}=\frac{1}{\sqrt{2}}(|0+\rangle-|1-\rangle)_{AB}=\frac{1}{\sqrt{2}}(|+1\rangle-|-0\rangle)_{AB} \quad (2)$$

$$|\Psi^-\rangle=\frac{1}{\sqrt{2}}(|\phi^+\rangle-|\psi^-\rangle)_{AB}=\frac{1}{\sqrt{2}}(|0-\rangle+|1+\rangle)_{AB}=\frac{1}{\sqrt{2}}(|+0\rangle-|-1\rangle)_{AB} \quad (3)$$

$$|\Psi^+\rangle=\frac{1}{\sqrt{2}}(|\phi^-\rangle+|\psi^+\rangle)_{AB}=\frac{1}{\sqrt{2}}(|+0\rangle+|-1\rangle)_{AB}=\frac{1}{\sqrt{2}}(|0+\rangle+|1-\rangle)_{AB} \quad (4)$$

여기서 $|0\rangle$, $|1\rangle$ 은 파울리연산자 σ_z 의 2개 고유상태들이며 $|+\rangle$, $|-\rangle$ 는 σ_x 의 고유상태들이다. 밑첨자 A, B 는 매개의 얽힘포톤쌍에서 2개의 상관된 포톤들을 각각 나타낸다. 그리고 $|\phi^+\rangle=(|00\rangle+|11\rangle)_{AB}/\sqrt{2}$, $|\phi^-\rangle=(|00\rangle-|11\rangle)_{AB}/\sqrt{2}$, $|\psi^+\rangle=(|01\rangle+|10\rangle)_{AB}/\sqrt{2}$, $|\psi^-\rangle=(|01\rangle-|10\rangle)_{AB}/\sqrt{2}$ 들은 벨토대상태들이다.

4개의 국부우니따르연산자 $U_{00}, U_{01}, U_{10}, U_{11}$ 은 다음과 같이 정의한다. 즉 $U_{00}=I$, $U_{01}=\sigma_Z$, $U_{10}=\sigma_x$, $U_{11}=i\sigma_y$. 여기서 I 는 2×2 단위행렬이고 $\sigma_i(i=x,\ y,\ z)$ 는 파울리행렬이다. 이와 같은 국부우니따르변환을 리용하면 4개의 얽힘상태 식 (1)－(4)의 변환을 다음과 같이 실현할수 있다. 즉

$$\left.\begin{aligned} &U_{01}\otimes I\,|\Phi^{\pm}\rangle=|\Psi^{\pm}\rangle,\ U_{10}\otimes I\,|\Phi^{\pm}\rangle=-|\Phi^{\mp}\rangle,\ U_{11}\otimes I\,|\Phi^{\pm}\rangle=-|\Psi^{\mp}\rangle\\ &U_{01}\otimes I\,|\Psi^{\pm}\rangle=|\Phi^{\pm}\rangle,\ U_{10}\otimes I\,|\Psi^{\pm}\rangle=|\Psi^{\mp}\rangle,\ U_{11}\otimes I\,|\Psi^{\pm}\rangle=-|\Phi^{\mp}\rangle \end{aligned}\right\}. \tag{5}$$

이와 같은 4가지 얽힘상태들 $\{|\Phi^{\pm}\rangle,\ |\Psi^{\pm}\rangle\}$ 을 리용하여 송신자와 수신자사이에 비밀정보를 안전하게 공유해가지기 위한 량자안전직접통신규약을 다음과 같이 설정한다.

송신자와 수신자는 우선 다음과 같이 약속한다. 즉 송신자는 매 얽힘포톤쌍에 4가지 국부조작 $U_{ii}(i=0,\ 1)$ 의 작용을 통하여 정보를 부호화하며 다음과 같은 방안을 통하여 두 비트의 정보에 대하여 제3자가 모르게 부호화조작을 진행한다.

$$U_{00}\rightarrow 00,\ U_{01}\rightarrow 01,\ U_{10}\rightarrow 10,\ U_{11}\rightarrow 11 \tag{6}$$

송신자는 자기의 수중에 있는 포톤에 대하여 국부변환을 진행한 후 만일 얽힘포톤쌍이 상태 $|\Phi^+\rangle$ 또는 $|\Psi^-\rangle$ 에 있다면 토대 $\{|+\rangle,\ |-\rangle\}$ 에서 자기의 포톤에 대하여 국부측정을 진행한다. 만일 얽힘포톤쌍이 상태 $|\Phi^-\rangle$ 또는 $|\Psi^+\rangle$ 에 있다면 토대 $\{|0\rangle,\ |1\rangle\}$ 에서 국부측정을 진행한다.

통신로의 안전성을 담보한 후에 송신자는 얽힘포톤쌍에 대하여 자기의 비밀정보를 부호화한다. 즉 송신자는 자기의 비밀정보에 기초하여 매 얽힘포톤쌍들에서 자기의 1개 포톤에 대하여 미리 확정한 국부우니따르변환을 진행한다.

국부변환을 진행한 후 얽힘포톤쌍의 상태에 기초하여 송신자는 토대 $\{|+\rangle,\ |-\rangle\}$ 또는 $\{|0\rangle,\ |1\rangle\}$ 에서 자기의 포톤들에 대하여 국부측정을 진행하며 고전통신로를 통하여 수신자에게 자기의 측정결과를 알려준다.

실례로 송신자와 수신자가 사전에 공유한 얽힘포톤쌍렬들이 모두 상태 $|\Phi^-\rangle$ 에 놓이고 송신자가 수신자에게 보내려는 비밀정보가 01110010이라고 하자. 비밀정보에 기초하여 송신자는 자기자신의 매개 포톤들에 대하여 순서대로 국부변환 U_{01}, U_{11}, U_{00}, U_{10} 을 실시한다. 이리하여 포톤쌍의 상태는 초기상태로부터 차례로 각각 상태 $|\Psi^-\rangle$, $|\Psi^+\rangle$, $|\Phi^-\rangle$, $|\Phi^+\rangle$ 로 변화된다. 그후 송신자는 차례로 토대상태 $\{|+\rangle,\ |-\rangle\}$, $\{|0\rangle,\ |1\rangle\}$, $\{|0\rangle,\ |1\rangle\}$, $\{|+\rangle,\ |-\rangle\}$ 에서 자기의 포톤에 대하여 국부측정을 진행한다. 송신자의 측정결과를 받은 후 수신자는 대응한 토대에서 자기의 포톤에 대하여 측정을 진행한다. 만일 송신자의 측정결과가 + 또는 –라면 수신자는 자기의 포톤에 대하여 토대 $\{|0\rangle,\ |1\rangle\}$ 에서 측정을 진행하며 만일 송신자의 측정결과가 0 또는 1이라면 토대 $\{|+\rangle,\ |-\rangle\}$ 에서 측정을 진행한다.

얽힘포톤쌍의 초기상태를 알고 송신자와 자기사이의 측정결과에 기초하여 수신자는 송신자의 비밀정보를 효과적으로 읽어낼수 있다.

만일 송신자의 측정결과가 +, 1, 0, −라면 수신자의 측정결과는 반드시 0, −, −, 0으로 된다. 이러한 두조의 측정결과에 기초하여 수신자는 전체적으로 축소되면서 압축된 얽힘포톤쌍의 상태가 $|\Psi^-\rangle$, $|\Psi^+\rangle$, $|\Phi^-\rangle$, $|\Phi^+\rangle$ 임을 판단해낼수 있게 된다. 얽힘포톤쌍의 초기상태가 모두 $|\Phi^-\rangle$임을 알고있기때문에 수신자는 즉시 송신자가 완성한 조작이 U_{01}, U_{11}, U_{00}, U_{10} 임을 판단해낼수 있게 된다. 식 (1)−(6)에 기초하여 수신자는 송신자의 비밀정보가 01110010 임을 알아낼수 있다. 따라서 통신쌍방은 안전한 비밀통신을 실현할수 있게 된다.

이상에서 설명한 방안에 기초하여 송신자와 수신자는 얽힘포톤쌍을 리용한 비밀정보의 안전한 통신을 진행할수 있다. 이 방안의 우점은 다음과 같다.

첫째로, 비밀정보를 나르는 포톤을 공개통신로로 전송하지 않기때문에 도청자는 전송과정에 임의의 유용한 정보를 얻을수 없다는것이다.

둘째로, 부호화률이 높다는것이다. 이 제안에서는 매 얽힘포톤쌍에서 두 비트의 정보를 부호화할수 있다.

셋째로, 정보를 해득하기 위하여 이 제안에서는 국부측정을 완성할뿐 벨토대측정을 진행할 필요는 없다는것이다. 때문에 이 제안을 실험적으로 실현하기가 쉽다.

2. 규약의 안전성분석

우리의 제안에서 비밀정보를 나르는 포톤이 공개통신로로 전송되지 않으므로 도청자는 전송중의 포톤을 가로채거나 통신을 중단시킬수 없다. 이 단계에서 도청자가 유용한 정보를 획득하는 유일한 방도는 추측이다. 송신자가 공개한 측정결과에 토대하여 도청자는 1/4의 확률로 얽힘포톤쌍의 수축전의 상태를 추측한다. 또한 도청자는 얽힘포톤쌍의 초기상태와 부호화방안을 전혀 모르기때문에 이 단계에서 그 어떤 방법으로도 정확한 고전비트를 얻을수 없다. 따라서 도청자는 얽힘포톤쌍을 제조하거나 배포할 때 공격을 진행할수 있다. 론문에서는 도청자의 가로챔−재송신공격방법을 분석한다.

도청자는 송신자가 수신자에게 보내는 얽힘포톤을 가로챈 후 다른 1개의 포톤을 수신자에게 송신한다. 그러나 얽힘포톤쌍의 매 포톤들은 모두 최대혼합상태에 있으므로 즉

$$\rho_A = \rho_B = \mathrm{tr}_A(\rho_{AB}) = \mathrm{tr}_B(\rho_{AB}) = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \frac{1}{2}(|+\rangle\langle +| + |-\rangle\langle -|) \qquad (7)$$

이므로 오직 얽힘포톤쌍의 1개 포톤만을 획득하여서는 얽힘포톤쌍의 초기상태를 추측해낼수 없다. 그러므로 도청자는 그 어떤 방법으로도 얽힘포톤쌍의 초기상태와 관련된 정보를 얻을수 없다. 초기상태와 관련된 정보를 모르면 송신자가 얽힘포톤쌍에 대하여 실시하는 우니따르변환을 추측해낼수 없으므로 송신자가 수신자에게 전송하는 비밀정보를 알아낼수 없다.

맺 는 말

벨토대와는 다른 량자얽힘상태를 리용하는 한가지 새로운 량자안전직접통신방안을 리용하면 비밀정보를 나르는 포톤을 공개통신로로 전송하지 않기때문에 도청자는 전송과정에 임의의 유용한 정보를 얻을수 없다. 또한 매 얽힘포톤쌍에서 두 비트의 정보를 부호화할수 있으므로 통신로용량을 높일수 있으며 벨토대측정을 진행할 필요가 없으므로 실험적으로 실현하기가 쉽다.

참 고 문 헌

[1] C. H. Bennett; Phys. Rev. Lett., 68, 3121, 1992.
[2] Zhiyuan Tang et al.; Phys. Rev. Lett., 112, 190503, 2014.
[3] K. Bostrom et al.; Phys. Rev. Lett., 89, 187902, 2002.
[4] Hwayean Lee et al.; Phys. Rev., A 73, 04230, 2006.

주체107(2018)년 6월 5일 원고접수

A Quantum Secure Direct Communication Protocol Using Quantum Entanglement States

Jang Chol Jong, Kim Nam Chol

We proposed a quantum secure direct communication protocol based on quantum entanglement and analyzed the security of the protocol. In the quantum secure direct communication protocol based on quantum entanglement proposed in this paper, the Bell's base measurement isn't needed, resulting in the easiness of realization experimentally and the increase of channel capacity.

Key words: quantum entanglement, quantum secure direct communication, Bell's state, local measurement