情報保護學會論文誌
第16卷 第1號, 2006. 2

Entanglement Swapping을 이용한 안전한 직접 통신 프로토콜*

홍 창 호,[1†] 이 화 연,[1] 김 지 인,[2] 임 종 인,[1] 양 형 진[1,3‡]

[1]고려대학교 정보보호대학원, [2]고려대학교 일반대학원, [3]고려대학교 디스플레이 반도체물리학과

Secure Direct Communication protocol Using Entanglement Swapping*

Chang-ho Hong,[1†] Hwa-yean Lee,[1] Ji-in Kim,[2] Jong-in Lim,[1] Hyung-jin Yang[1,3‡]

[1]Graduate School of Information Security(GSIS), Korea University

[2]Department of Physics, Korea University

[3]Department of Display Semiconductor, Korea University

요 약

본 논문에서는 entanglement swapping을 이용하여 직접적인 통신이 가능한 통신 프로토콜을 제안한다. 이 프로토콜은 암호화된 메시지가 공개 채널 상으로 전달되지 않음으로 도청자로부터의 안전성을 높였다. 효율성에 있어서도 한 세션에 두 비트의 고전 정보가 전달되므로 Bostrom 과 Felbinger에 의해 제시된 ping-pong 프로토콜 보다 두배의 효율성 향상을 가져왔다. 본 프로토콜에서 사용하고 있는 검증 모드는 75%의 확률로 도청자의 존재를 확인할 수 있기 때문에 충분한 검증 절차를 거치면 이론적으로 도청자로부터 거의 완벽한 안전성을 보장 받을 수 있다.

ABSTRACT

We propose a direct communication protocol using entanglement swapping. The safety of this protocol is guaranteed by the basic properties of entanglement swapping. This protocol is efficient to transmit two classical bits of information per one session. This efficiency is better than that of ping-pong protocol suggested by Bostrom and Felbinger. Even if an eavesdropper intervenes in midway, the eavesdropper will be detected with the probability of 75% in the verification process of one bit. Therefore the perfect security is guaranteed if we use enough amount of bits for the verification process.

Keywords : *Entanglement Swapping, Quantum Direct Communication*

Ⅰ. 서 론

현재 널리 이용되고 있는 고전 암호의 안전성은 계산의 어려움에 근거하고 있다. 따라서 연산 능력이 뛰어난 기술이 개발되면 현재 암호는 더 이상 안전성을 보장할 수 없다. 연산 능력의 향상 기술로 거론 되는 것이 양자역학을 이용한 양자 연산 기술

접수일 : 2005년 5월 13일 ; 채택일 : 2005년 11월 28일
* 본 연구는 과학기술부의 연구과제(NC33520)지원 아래 수행되었습니다.
† 주저자 : hchc1@paran.com
‡ 교신저자 : yangh@korea.ac.kr

이다. 양자 연산 능력이 현재 암호의 안전성에 심각한 영향을 끼친다는 것은 양자역학을 이용한 암호 시스템이 가지는 무조건적인 안전성을 높게 평가할 수 있는 반증이라 할 수 있다.

지금까지 양자암호학의 연구는 양자전송[1-4], 양자키분배[5-7,15], 양자비밀공유[8,12], 그리고 양자통신[9]에 이르기까지 폭넓은 분야에서 성과를 거두었다. 특히 양자역학에서 다루는 측정에 따른 양자 상태의 붕괴가 확률적이고 비결정론적(non-deterministic)이라는 특징은 양자 키 분배 프로토콜에서 사용자 중 한 명에 의해 일방적으로 키가 생성되지 않게 하는 큰 장점이 된다[5,9,10]. 그러나 결정된 정보의 전송을 목적으로 하는 양자 직접 통신 분야에서 양자 상태 측정에 의한 확률적인 붕괴는 적지 않은 장애물로 작용한다. 이러한 양자역학적 특징을 극복하여 직접적인 메시지 전달을 가능하게 하는 양자 프로토콜이 개발 되었거나 개발 되고 있는데 그 중 하나가 2002년 Bostrmo 과 Felbinger가 제안한 ping-pong 프로토콜이다[11]. 이것은 두 사용자인 Alice와 Bob이 키뿐만 아니라 메시지까지 직접 전달할 수 있는 방법으로 키 없이 직접통신이 가능하다는 면에서 주목을 받았다. 이 프로토콜은 크게 키나 평문을 전달하는 message 모드와 도청자를 검출하는 control 모드로 이루어져 있으며 두 모드간의 전환은 일정한 확률을 가지고 임의적으로 일어난다. 정보가 전달되는 message 모드에 대해 간단히 설명해 보면 다음과 같다. Bob이 초기에 두 개의 큐빗이 최대로 얽혀진 상태, 즉 네 개의 벨 상태 중 하나를 준비한다. 여기서 네 개의 벨 상태는 서로 직교한 관계에 있으며 자세한 형태는 II 장에서 다룰 것이다. Bob이 준비한 얽힘상태를 이루고 있는 두 큐빗 중 한 큐빗은 자신이 간직하고 나머지 한 큐빗은 Alice에게 전송한다. 이를 받은 Alice는 Bob에게 보낼 고전 한 비트 정보를 고려하여 받은 큐빗에 σ_z연산을 적용(1)하거나 적용하지 않고(0) Bob에게 다시 전송한다. Bob은 Alice로부터 받은 큐빗과 자신이 보관하고 있던 큐빗에 벨 측정을 수행하여 어떤 벨 상태인지를 알아낸다. 최종적으로 Bob은 이 측정 결과와 초기에 자신이 준비했던 벨 상태 정보를 이용하여 Alice가 연산을 취했는지(1) 안취했는지(0)를 알아낸다. 큐빗을 주고받음으로 하나의 세션을 이루는 이 프로토콜은 결과적으로 한 세션에 한 비트의 정보를 전송하는 효율을 가진다.

본 논문에서는 양자얽힘교환(quantum entanglement swapping)과 고전통신(classical communication)을 이용한 양자직접통신프로토콜을 제안한다. 이 프로토콜은 ping-pong 프로토콜에 비해 높은 안전성과 효율성을 제공한다. 또한 프로토콜의 진행 중에 암호화된 정보가 공개 채널 상에 공개되지 않음으로 일반적인 도청자 뿐만 아니라 도청자중간공격(man-in-the-middle attack)에 대해서도 강한 특성을 가진다.

II. 얽힘교환(entanglement swapping)

얽힘상태란 두 양자상태가 얽혀서 독립적으로 분리될 수 없는 상태를 말한다. 두 큐빗으로 이루어진 하나의 양자상태 ψ는 일반적으로 $(\alpha|0>+\beta|1>)$의 형태를 가진다. 여기서 $|0>$과 $|1>$은 큐빗의 두 상태를 나타내며 α와 β는 복소수이다. $|\alpha|^2+|\beta|^2=1$의 관계식을 만족 한다. 양자상태 ψ의 형태는 0과 1을 동시에 표현할 수 없는 고전적인 비트와 달리 $|0>$과 $|1>$이 중첩을 이룰 수 있음을 나타낸다. 양자상태의 개념을 가지고 $|0>\otimes|0> + |1>\otimes|1>$식을 생각해 보자. 이 상태는 두 양자상태가 텐서 곱(tensor product)된 $\psi\otimes\phi'$ 형태로 나타낼 수 없다. 즉, $(|0>\otimes|0> + |1>\otimes|1>) \neq (|0>+|1>)\otimes(|0>+|1>)$관계로 양자상태를 분리 할 수 없다. 이러한 상태를 우리는 얽힘상태라 정의 한다. 그리고 얽힘교환은 두 시스템이 각자 생성한 각각의 얽힘상태 중 한 큐빗씩을 나누어 가진 다음 한 시스템에서 벨 측정을 수행하면 이 측정을 통해 이전에는 얽혀있지 않던 큐빗들이 얽힘상태를 이루는 현상이다.[15-18] 자세한 설명을 위해 두 큐빗이 얽혀 있는 얽힘상태 네 개를 생각해 보자. 이 상태는 양자역학에서 잘 알려진 벨 상태로써 각각이 얽힘상태에 있을 뿐만 아니라 서로 직교 관계에 있다.

$$|\Phi^+>_{ij} \equiv (00)_{ij} \equiv \frac{1}{\sqrt{2}}(|0>_i\otimes|0>_j + |1>_i\otimes|1>_j) \quad (1)$$

$$|\Phi^->_{ij} \equiv (01)_{ij} \equiv \frac{1}{\sqrt{2}}(|0>_i\otimes|0>_j - |1>_i\otimes|1>_j) \quad (2)$$

$$|\Psi^+>_{ij} \equiv (10)_{ij} \equiv \frac{1}{\sqrt{2}}(|0>_i\otimes|1>_j + |1>_i\otimes|0>_j) \quad (3)$$

$$|\Psi^->_{ij} \equiv (11)_{ij} \equiv \frac{1}{\sqrt{2}}(|0>_i\otimes|1>_j - |1>_i\otimes|0>_j) \quad (4)$$

표 1. 얽힘교환에 따른 상관관계. 여기서 ID++ 가 의미하는 바는 Alice와 Bob의 측정 결과가 $\{(00)_{14}, (00)_{23}\}$, $\{(01)_{14}, (01)_{23}\}$, $\{(10)_{14}, (10)_{23}\}$, $\{(11)_{14}, (11)_{23}\}$각각 1/4의 동일 확률로 나타남을 의미한다. 마찬가지로 ID+- 는 $\{(10)_{14}, (11)_{23}\}$, $\{(01)_{14}, (00)_{23}\}$, $\{(00)_{14}, (01)_{23}\}$, 그리고 $\{(11)_{14}, (10)_{23}\}$, Rev++는 $\{(00)_{14}, (10)_{23}\}$, $\{(01)_{14}, (11)_{23}\}$, $\{(10)_{14}, (00)_{23}\}$, 그리고 $\{(11)_{14}, (01)_{23}\}$, Rev+-는 $\{(00)_{14}, (11)_{23}\}$, $\{(01)_{14}, (10)_{23}\}$, $\{(10)_{14}, (01)_{23}\}$, 그리고 $\{(11)_{14}, (00)_{23}\}$로 결과 값이 나타남을 의미한다.

	$(00)_{34}$	$(01)_{34}$	$(10)_{34}$	$(11)_{34}$
$(00)_{12}$	ID++	ID+-	Rev++	Rev+-
$(01)_{12}$	ID+-	ID++	Rev+-	Rev++
$(10)_{12}$	Rev++	Rev+-	ID++	ID+-
$(11)_{12}$	Rev+-	Rev++	ID+-	ID++

여기서 i와 j는 큐빗들을 구분하는 큐빗 번호를 나타낸다. $|\Phi^{\pm}>_{ij}$와 $|\Psi^{\pm}>_{ij}$를 다시 $(00)_{ij}, (01)_{ij}, (10)_{ij}$ 그리고 $(11)_{ij}$로 정의한 것은 본 논문에서 고전 비트 정보를 나타내는데 필요하기 때문이다.

충분한 거리에 있는 Alice와 Bob은 위의 벨 상태 중 하나씩을 임의로 준비한다. 예를 들어 Alice가 $(00)_{12}$, Bob이 $(11)_{34}$를 준비하였다고 가정하자. Alice는 2번 큐빗을 Bob에게 전송하고 Bob은 4번 큐빗을 Alice에게 전송한다. Alice가 자신이 가진 1과 4번 큐빗에 벨 측정을 수행하게 되면 네 개의 벨 상태 중 하나의 벨 상태를 결과 값으로 얻게 되는데 이 결과 값은 Bob이 2와 3번 큐빗에 벨 측정을 수행하여 얻게 되는 벨 상태와 강한 양자상관관계를 가진다. 즉, Alice의 벨 측정치가 $(10)_{14}$라면 Bob의 벨 측정치는 "반드시" $(01)_{23}$이어야 한다. 각 벨 상태에 따르는 측정값의 상관관계를 표 1과 같이 정리할 수 있다.

즉, 두 개의 벨 상태 각각에서 한 큐빗씩을 취하여 이 두 큐빗에 국소적인 벨 측정을 수행하면 나머지 두 큐빗들도 벨 상태를 이루게 되는데 새로 생성된 벨 상태 사이에는 강한 상관관계가 나타난다. 이는 그림 1과 같은 도식으로 표현 할 수 있다.[16]

III. 직접 통신 프로토콜

본 논문에서 제안하는 통신 기법은 식(1)~식(4)를 기저로 하는 벨 측정을 사용하며 표 1의 벨 측정

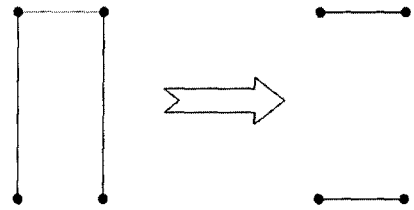

그림 1. 얽힘교환. 여기서 1,2,3 그리고 4는 큐빗 번호를 나타내면 선으로 연결된 큐빗은 서로 얽혀있는 얽힘상태를 나타낸 것이다. 점선은 벨 측정이 수행될 큐빗을 연결한 것이다. 초기에 1-2와 3-4 의 벨 상태가 국소적인 2-3벨 측정(혹은 1-4 벨 측정)을 통해 2-3과 1-4의 벨 상태로 변환된다[16].

결과에 따른 얽힘교환의 결과를 이용한다. 이 프로토콜은 크게 메시지가 전달되는 전송 모드와 안전성 확인을 위한 검증 모드로 나누어 진행되며 두 모드의 전환은 Alice에 의해 확률 p로 전환 된다.

프로토콜은 다음과 같다.

1) Alice와 Bob은 각각 벨 상태 두 개와 한 개를 준비한다. 즉, Alice는 식(1)과 (4)중에서 선택하여 큐빗 번호 1 과 2 (이하 1-2라 표기) 그리고 3과 5(이하 3-5)가 얽힌 두 개의 벨 상태를 준비하고, Bob 역시 식(1)~(4)중 임의로 선택하여 큐빗 번호 4와 6이 얽힌 벨 상태를 준비한다.

이 때, Alice의 1-2 벨 상태가 Bob에게 전송되는 고전 비트를 결정한다. 예를 들어, Alice가 $(01)_{12}$ 상태를 준비하였다면 Bob에게 전송되는 고전 비트 값은 "01"이다. 단, 검증 모드를 위해 준비되는 1-2 벨 상태는 Alice가 Bob에게 보내는 정보와 전혀 무관하게 선택되어야 한다.

2) Alice는 2번 큐빗을 Bob에게 전송하고, Bob은 6번 큐빗을 Alice에게 전송한다.
3) Alice와 Bob은 각각 1-3, 2-4에 Bell 측정을 수행한다.
4) Alice는 초기에 자신이 준비한 1-2 벨 상태가 전송 비트인지 검증 비트인지를 확인하고 전송 비트이면 (전,a) 단계로, 검증 비트이면 (검,a)단계로 이동한다. 이 두 모드의 선택은 Alice에 의해 확률 p로 일어나며 Alice만이 알고 있는 비밀 정보이다.

전,a) Alice는 초기 상태 중 3-5와 벨 측정 결과 값 1-3과 5-6을 Bob에게 알린다.

전,b) Bob은 Alice가 공개한 상태들과 자신의 초기 상태 4-6 및 최종 상태 2-4에 대한 벨 상태의 정보를 통해 Alice의 초기 벨 상태 1-2를 알아내어 Alice가 보낸 정보를 얻는다.

검,a) Alice는 Bob에게 초기 벨 상태 4-6 과 최종 벨 상태 2-4의 결과 값을 요구한다.

검,b) Bob은 자신의 초기 벨 상태 4-6 과 최종 벨 상태 2-4의 값을 Alice에게 전송 한다.

검,c) Alice는 Bob에게 받은 정보와 자신이 알고 있는 정보를 이용하여 도청자의 존재를 확인한다. 즉, Bob에게서 전송받은 정보가 자신의 정보와 올바르게 얽힘교환 쌍을 이루면 1) 단계로 이동하고 그렇지 않으면 채널 상에 공격자가 존재하는 것으로 판단하여 통신을 차단한다. 이는 얽힘교환이 어떤 특정한 연관성을 갖고 얽힘을 이루게 되는 특징을 이용한 것이며 공격자가 Bob의 초기 벨 상태를 모른 채 우연히 Bob과 동일한 상태를 준비하였을 때(1/4의 확률)를 제외하고는 도청자의 존재가 드러나게 된다.

예를 들어, Alice가 준비한 상태가 $(11)_{12}$와 $(10)_{35}$이고, Bob이 준비한 상태가 $(10)_{46}$이었다고 가정해 보자. 3)단계에서 각자 벨 측정을 통해 얻어진 결과가 Alice는 $(11)_{13}$과$(00)_{56}$, 그리고 Bob이 $(00)_{24}$인 경우 전,a) 단계에서 Bob에게 주어진 정보는 $(10)_{35}$, $(10)_{46}$,$(11)_{13}$,$(00)_{56}$, 그리고 $(00)_{24}$이다. 이를 통하여 Bob은 다음과 같은 세 단계의 얽힘교환 연관 관계를 비교하여 Alice가 보낸 정보는 11이라는 것을 알아내게 된다.

$$①\ (00)_{56}\otimes(00)_{24} \rightarrow (10)_{52} \otimes (10)_{46} \quad (5)$$

$$②(10)_{35} \otimes (00)_{24} \rightarrow (00)_{34} \otimes (10)_{52} \quad (6)$$

$$③(11)_{13} \otimes (00)_{24} \rightarrow (11)_{12} \otimes (00)_{34} \quad (7)$$

위 식에서 "→"은 얽힘교환을 나타낸다.

즉, Bob은 ①에서 Alice가 공개한 $(00)_{56}$, 자신의 초기 상태 $(10)_{46}$그리고 벨 측정 후의 최종 상태 $|00>_{24}$를 알고 있으므로 표 1을 통해 $(10)_{52}$의 정보를 알아낸다. ②에서는 $(10)_{35}$, $(00)_{24}$ 그리고 ①에서 구한 $(10)_{52}$를 알고 있으므로 $(00)_{34}$를 알아낸다. ③에서도 마찬가지로 $(11)_{13}$, $(00)_{24}$ 그리고 ②에서 구한 $(00)_{34}$를 토대로 마침내 $(11)_{12}$을 알아내게 된다. 따라서 Bob은 자신이 가진 정보와 Alice가 공개한 정보를 이용 표 1의 간단한 검색만으로 Alice의 초기 상태, 즉 고전 비트 "11"을 알아낼 수 있다.

Ⅳ. 안전성

본 프로토콜에서 공격자가 접근할 수 있는 정보는 전송되는 큐빗들에 한정된다. 얽혀있는 큐빗들 중 하나가 전송될 때에는 한 큐빗 정보가 완전히 무작위이기 때문에 도청자가 전송 큐빗들만을 가지고는 Alice가 생성한 1-2 벨 상태를 알아 낼 수 없다. 따라서 공격자는 전송 큐빗들 외의 다른 정보들을 알아내기 위해 채널 중간에 개입하여, 자신의 존재를 드러내지 않고 Alice가 생성한 1-2 벨 상태와 관련된 정보를 알아내야 한다. 그러나 공격자가 자신의 존재를 드러내지 않고 유용한 정보를 얻기 위해서는 프로토콜 전반에 걸쳐 Bob이 초기에 준비한 상태와 동일한 초기 상태를 준비하고 채널 중간에서 도청하는 방법 외에는 없는데, Bob의 초기 상태는 프로토콜 전반에 걸쳐 비밀 정보이므로 공격자가 같은 상태를 준비할 확률은 기껏해야 1/4에 불과하다.

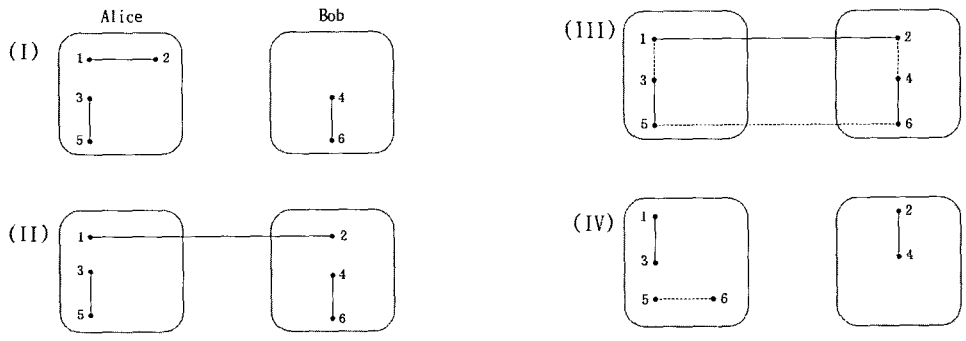

그림 2. 얽힘교환을 이용한 단계별 직접 통신 프로토콜

따라서 본 프로토콜의 검증 모드가 n번 수행되면 모든 검증 과정을 통과할 확률은 $(1/4)^n$이 되어 공격자가 자신의 존재를 드러내지 않고 공격을 성공할 확률이 지수적으로 감소하게 된다. 즉 n을 충분히 크게 하면 공격자의 도청에 대해 완벽한 안정성을 기대할 수 있다. 그런데, 한 회당 두 비트를 검증하게 되므로 결과적으로 비트당 Eve가 드러날 확률은 $1-(1/2)^n$ 이다. 이는 BB84의 $1-(3/4)^n$ 확률보다 개선된 것이다.

채널의 중간에 공격자가 있을 때 그 존재가 어떻게 드러나는지 알아보기 위하여 다음의 예를 살펴보자. 이는 고전 암호에서 다루는 중간자공격(man-in-the-middle attack)에 해당한다. 초기에 Alice가 준비한 상태는 $(11)_{12}$와 $(10)_{35}$이고, Bob이 준비한 상태는 $(10)_{46}$라고 가정하자. 공격자가 도청을 위해서는 Bob이 준비한 것과 마찬가지로 하나의 벨 상태를 준비하여야 하지만, Bob이 준비한 상태는 공개되지 않으므로 공격자는 Bob이 준비한 상태를 추측하여 4개의 벨 상태중 하나를 임의적으로 선택하여 준비하게 된다. 공격자가 취할 수 있는 가능한 도청 방법은 다음과 같다.

(1) Alice와 Bob, 그리고 공격자 Eve는 각각 초기 상태를 준비한다. 이 때, Alice가 준비한 상태는 $(11)_{12}$와 $(10)_{35}$, Bob이 준비한 상태는$(10)_{46}$, 그리고 공격자 Eve가 준비한 상태는 $(00)_{78}$이라고 가정하자. 즉, Alice가 Bob에게 보내려는 고전 비트는 "11"이다.

(2) Alice는 2번 큐빗을 Bob에게 전송하는데 공격자 Eve가 중간에서 이를 가로챈다.

(3) 공격자 Eve는 2번 큐빗을 자신이 준비한 8번 큐빗과 함께 벨 측정을 한다. 이때, 얽힘교환이 일어나게 되어 결과적으로 큐빗 1과 큐빗 7이 벨 상태를 형성하게 된다. 이후, 공격자 Eve는 2번 큐빗을 Bob에게 전송한다.

(4) Alice와 Bob은 큐빗 1과 큐빗 3, 큐빗 2와 큐빗 4에 벨 측정을 수행한다. 이로 인하여 큐빗 5와 큐빗 7 그리고 큐빗 8과 큐빗 6이 새로운 벨 상태를 형성하게 된다.

(5) Bob은 큐빗 6을 Alice에게 전송하는데 공격자 Eve가 이를 가로채고 큐빗 8과 큐빗 6에 벨 측정을 수행하여 결과 값을 얻는다.

(6) 공격자 Eve는 6번 큐빗을 Alice에게 전송하고 큐빗 7과 큐빗 8에 벨 측정을 수행한다.

(7) Alice는 큐빗 5와 큐빗 6에 벨 측정을 수행하고 큐빗 1과 큐빗 3, 큐빗 5와 큐빗 6의 벨 상태를 공개한다.

위와 같은 공격 시나리오는 공격자 Eve의 초기 상태가 Bob의 초기 상태와 같지 않은 경우, 검증 단계에서 도청자 Eve의 존재가 드러나게 된다. 예를 들어, Eve가 채널 상에 없을 때 위에서 제시한 초기 상태에서 예상 될 수 있는 얽힘교환의 결과를 정리하면,

$$
\begin{aligned}
&(11)_{12} \otimes (10)_{35} \otimes (10)_{46} \\
&\Rightarrow (|001011\rangle+|001110\rangle+|011001\rangle+|011100\rangle \\
&-|100011\rangle-|100110\rangle-|110001\rangle-|110100\rangle)_{13,24,56} \qquad (8)
\end{aligned}
$$

이 식은 얽힘교환을 취하기 전의 상태와 취한 후의 가능한 상태를 편의상 표준화(normalization)를 생략한 채 모두 나타낸 식이다.

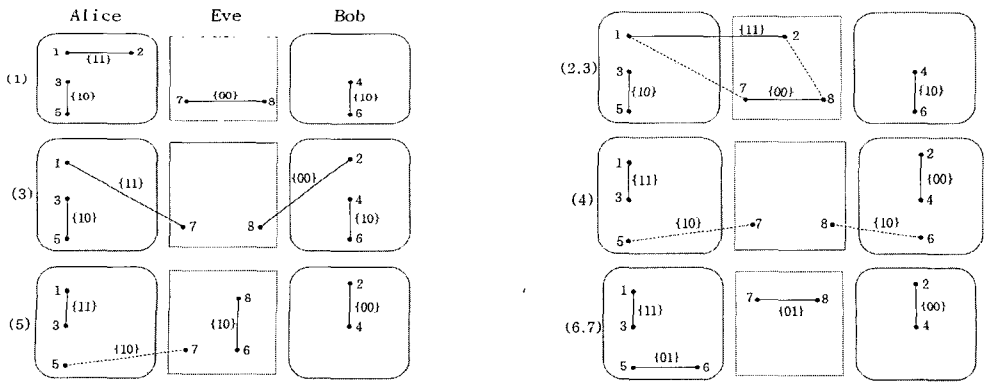

그림 3. 중간자공격(Man-in-the-middle attack)

한편, 공격자 Eve가 개입한 앞의 예에서 (6)단계 이후의 결과는 다음 식과 같다.

$$(11)_{13} \otimes (00)_{24} \otimes (01)_{56} \quad (9)$$

이 식은 식(8)과 비교하여 볼 때 나올 수 있는 결과 값이 아니다.

따라서 Alice는 검증 단계에서 Bob의 정보를 요구하여 위와 같은 얽힘교환의 잘못된 연관성을 확인함으로써 공격자 Eve의 존재를 확인 할 수 있다.

이 프로토콜은 요즘 주목받고 있는 강력한 공격 방법, PNS 공격에 대해서도 안전성을 제공한다. PNS(Photon-Number Splitting) 공격은 현실적으로 단일 큐빗 소스의 생성 중에 생기는 다중 큐빗을 이용한 공격 방법으로 양자상태는 복제되지 않는다는 양자역학의 기본 원리를 지키면서도 도청자에게 복제의 효과를 주는 공격 방법이다[22,23]. 그러나 본 프로토콜에서의 PNS 공격은 Bob의 얽힘상태를 완전히 알지 못한 채 진행되므로 채널 상에서 PNS 공격을 통해 전송되는 큐빗들을 가지고 있더라도 Alice의 초기 상태를 유추할 정보는 제공되지 않는다. 따라서 이 프로토콜은 중간자공격과 더불어 PNS 공격에 대해서도 안전 하다.

V. 유사 프로토콜과의 비교

본 논문과 같이 직접통신에 대한 여러 프로토콜들이 제안되어 있다. 서론에서 간단히 설명한 Bostrmo과 Felbinger의 ping-pong 프로토콜 외에도 본 논문에서 사용한 얽힘상태를 이용한 논문들도 있다[13,14]. 그 중에서 최근 Man과 Zhang이 개발한 직접통신프로토콜[13]과 그 장단점을 비교해 보자. Man과 Zhang의 대략적인 프로토콜은 다음과 같다.

(1) Bob은 $|\Psi^+>$상태를 여러 개 준비 한다. 각 큐빗은 큐빗 숫자로 표시되며 한 쌍씩 $|\Psi^+>$ 상태를 이룬다. (즉, 1-2, 3-4, 5-6,.. 여기서 "-"는 얽힘상태임을 나타낸다.) Bob은 각 얽힘상태에서 한 큐빗씩을 선택하여 Alice에게 전송하는데 큐빗의 숫자 순서를 유지하고 받도록 해야 한다. 다시 말해, Alice는 2468...의 연속적인 큐빗들을 흐트러짐 없이 시간의 순서대로 받아야 한다. (이 큐빗들을 C 배열이라 정의 한다.) 나머지 큐빗들은 Bob이 저장하고 있는데(이 큐빗들을 M 배열이라 저의 한다.) 두 큐빗씩 그룹을 지어 놓는다. 즉, 큐빗 1과 3은 그룹 1, 큐빗 5와 7은 그룹 2 등...

(2) Alice는 C 배열을 이루는 큐빗들을 받았는지 확인하고 Bob과 마찬가지로 두 큐빗씩 그룹을 짓는다. 일반적으로 받은 순서대로 2 큐빗씩 선택하여 그룹을 짓는다. 즉, 큐빗 2와 4는 그룹 1, 큐빗 6과 8은 그룹 2 등...

(3) Alice는 임의적으로 몇 개의 큐빗 그룹들을 선택하여 암호화-복호화 그룹으로 정의하고 나머지 그룹들을 점검 그룹으로 정의한 뒤 Bob에게 자신이 선택한 그룹들을 공개적으로 알린다.

(4) Alice는 점검 그룹 내의 각 그룹들을 측정하기 위해 필요한 측정기저로 σ_z와 σ_y 중 하나를 선택하여 측정 하고 큐빗의 순서, 선택한 측정기저 그리고 결과 치를 Bob에게 공개적으로 알린다.

(5) Bob은 Alice가 공개한 정보를 바탕으로 Alice가 선택한 검증 그룹에 대응하는 자신의 그룹들에 Alice가 선택한 것과 같은 측정기저로 측정을 수행 한다. 그리고 그 결과 치를 Alice의 결과 값과 비교하여 도청자의 존재를 확인한다. 즉, 도청자가 없는 상태에서 Alice와 Bob이 σ_z 측정기저로 측정을 수행한 경우 Bob의 결과가 0(1)이면 Alice의 결과는 1(0)이어야 한다. σ_y 측정기저로 측정을 수행한 경우는 Bob이 0(1)이면 Alice도 0(1)이어야 한다. 그렇지 않으면 도청자가 존재하는 것으로 판단하여 통신을 종료한다.

(6) 암호화-복호화 그룹이 Alice와 Bob에게 동일하게 인지되었다는 가정 하에 Alice는 Bob에게 보내려는 비트 열을 고려하여 자신의 암호화-복호화 그룹들 각각 중 한 큐빗에 단위연산자를 수행한다. 단위연산자는 다음과 같이 정의 된다.

$$u_0 \equiv |0><0| + |1><1|$$
$$u_1 \equiv |0><0| - |1><1|$$
$$u_2 \equiv |1><0| + |0><1|$$
$$u_3 \equiv |1><0| - |0><1|$$

u_0는 "00", u_1은 "01", u_2는 "10" 그리고 u_3는 "11"을 암호화 한다.

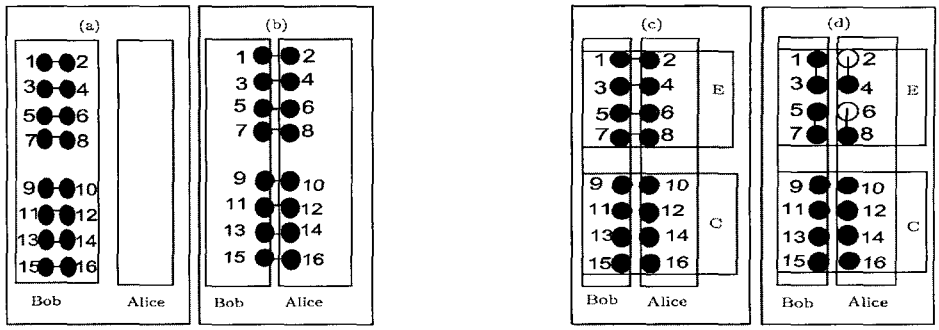

그림 4. Man과 Zhang의 양자얽힘상태와 단위연산자를 이용한 직접통신프로토콜[13] 흰 점은 Alice에 의해 연산자가 취해진 큐빗 부분을 나타내고 큐빗 사이의 선은 얽힘을 의미 한다.

이 연산적용 후에 각 암호화-복호화 그룹별로 벨 측정을 한다.

(7) Alice는 이 결과와 암호화-복호화 그룹의 순서를 Bob에게 공개 채널을 통해 알린다.

(8) Bob은 Alice의 측정 결과 치를 받은 후에 자신의 암호화-복호화 그룹을 순서에 맞추어 측정하고 비교하면 Alice가 취한 연산자의 종류를 알 수 있다. 즉, 고전 비트 정보를 알 수 있다.

예를 들어, (6)에서 Alice가 그룹 1에 u_1 연산을 취하면 "01"을 암호화 한 것이 되는데 이 때 초기 상태 $|\Psi^+>_{12}\otimes|\Psi^+>_{34}$는 $|\Psi^->_{12}\otimes|\Psi^+>_{34}$ 로 변하게 되어 Alice가 벨 측정을 통해 $|\Phi^+>_{24}$를 얻었다면 양자얽힘교환 효과에 의해 Bob이 같은 그룹 내에서 측정한 결과는 $|\Phi^->_{13}$이어야 한다. Bob은 자신의 벨 측정 결과, Alice가 보내 준 측정 결과 그리고 초기 상태를 알고 있으므로 Alice가 취한 연산자가 u_1임을 알고 "01" 비트를 복호화 해 낸다. Alice가 취하는 연산자에 따른 가능한 측정 결과들을 표 2와 같이 정리할 수 있다.

본 논문에서 제시하는 직접통신 프로토콜과 위에서 설명한 Man과 Zhang의 직접통신 프로토콜의 장단점을 비교해 보자. Man과 Zhang의 프로토콜은 메시지의 암호화 작업이 필요하다. 즉, Alice에 의해 u 연산자가 수행되어야 한다. 그러나 본 논문의 프로토콜은 암호화 작업이 필요하지 않고 초기에 Alice가 준비하는 벨 상태 자체가 메시지가 된다. 이는 암호화의 번거로움을 덜어 주는 효과 외에 연산중에 발생 할 수 있는 오류를 방지하는 장점이 있다. Man과 Zhang의 프로토콜은 한 번의 양자 채널 전송을 포함하여 총 네 번의 정보 전송을 필요로 한다. 그에 비해 본 논문의 프로토콜은 두 번의 양자 채널 전송을 포함하여 총 세 번의 정보 전송만을 필요로 한다. 따라서 도청자에게 드러나는 정보의 기회가 적고 비용 절감 효과도 기대할 수 있다. 도청자의 점검 방법에서 Man과 Zhang의 프로토콜은 Alice가 측정 기저를 선택하고 그에 대한 정보를 Bob에게 전달해야 하며, 점검 그룹에 대한 정보가 사전에 채널 상에 공개 되므로 도청자는 점검 그룹에 대한 정보를 알 수 있어 선택적인 공격에 대한 기회가 있다. 그러나 본 논문의 프로토콜은 측정기저의 선택이 필요 없고 점검 전까지는 점검 모드가 메시지 모드와 동일하게 진행되므로 점검 큐빗인지 전송 큐빗인지에 대한 정보가 도청자에게 공개되지 않아 선택적인 공격이 불가능하다. 프로토콜의 수행 과정에 있어 Man과 Zhang의 프로토콜은 송신자의 단위연산자(unitary operator) 수행이 전달 정보가 되므로 적어도 연산을 적용하는 시간과 측정의 시간동안 양자상태를 보관해야 하는 어려움이 있다. 그러나 본 프로토콜에서는 정보를 위한 다른 연산자가 필요하지 않고 큐빗이 전달되는 대로 측정을 수행하여 결과만을 저장하면 되므로 양자상태의 보관에 따른 어려움이나 번거로움이 없는 장점을 가진다. 효율적인 측면에서 Man과 Zhang의 프로토콜은 본 논문의 프로토콜보다 좋다. 즉, 이 프로토콜

표 2. 단위연산자 u(암호화 비트), 초기 상태 그리고 Bob과 Alice의 벨 측정 결과

연 산 자	$u_0\,(00)$	$u_1\,(01)$	$u_2\,(10)$	$u_3\,(11)$
초기 상태	$\Psi_{12}^+\otimes\Psi_{34}^+$	$\Psi_{12}^+\otimes\Psi_{34}^-$	$\Psi_{12}^+\otimes\Phi_{34}^+$	$\Psi_{12}^+\otimes\Phi_{34}^-$
얽힘교환 결과값	$\{\Phi_{13}^+,\Phi_{24}^+\}$	$\{\Psi_{13}^-,\Psi_{24}^+\}$	$\{\Psi_{13}^+,\Phi_{24}^+\}$	$\{\Psi_{13}^+,\Phi_{24}^-\}$
	$\{\Psi_{13}^-,\Psi_{24}^-\}$	$\{\Phi_{13}^+,\Phi_{24}^-\}$	$\{\Psi_{13}^-,\Phi_{24}^-\}$	$\{\Psi_{13}^-,\Phi_{24}^+\}$
	$\{\Psi_{13}^+,\Psi_{24}^+\}$	$\{\Phi_{13}^-,\Phi_{24}^+\}$	$\{\Phi_{13}^+,\Psi_{24}^+\}$	$\{\Phi_{13}^-,\Psi_{24}^-\}$
	$\{\Phi_{13}^-,\Phi_{24}^-\}$	$\{\Psi_{13}^+,\Psi_{24}^-\}$	$\{\Phi_{13}^-,\Psi_{24}^-\}$	$\{\Phi_{13}^-,\Psi_{24}^+\}$

이 한 세션에 두 개의 얽힘상태를 이용하여 두 비트의 정보가 전달되는데 비해 본 논문의 프로토콜 같은 두 비트를 전달하기 위해 세 개의 얽힘상태를 이용한다. 그럼에도 본 논문이 가지는 안전성과 비용적인 장점, 그리고 암호화의 용이성은 높은 가치를 부여 받는다.

Gao, Yan 그리고 Wang이 개발한 프로토콜은 GHZ 얽힘교환을 이용하여 동시에 두 채널 통신이 가능한 방법이다[14]. 그러나 이 프로토콜도 Man과 Zhang의 프로토콜처럼 암호화를 위해 단위연산자를 적용하여야 하며 안전성을 위해 단위연산자의 고전 정보에 대한 규약이 두 채널의 사용자들 간에 비밀 정보로 미리 공유하고 있어야 한다는 점에서 직접통신의 범주에서 생각하기 어렵다. 통신을 위해 비밀 정보를 미리 공유 한다는 것은 사전에 키 공유를 전제로 하는 고전 통신과 크게 다르지 않다.

Ⅵ. 결 론

얽힘교환을 이용하여 키 또는 메시지를 전송 할 수 있는 우리의 직접통신 프로토콜은 얽힘교환과 고전통신을 이용한다. 수신자는 송신자가 보낸 정보를 알아내기 위해 연산이 3 단계에 걸쳐 이루어져야 하지만 각 연산이 벨 상태에 대한 얽힘교환의 전 후 관계를 확인하는 것만으로 이루어지므로 빠른 시간 내에 수행된다. 또한, 세션 당 한 비트의 정보가 전달되는 ping-pong 프로토콜[4]과 비교하여도 한 세션에 두 비트의 정보가 전달되므로 효율성도 높다. 검증 모드를 이용하여 중간자공격(man-in-the-middle attack)에 대한 안전성을 제공하며 매 번 75%의 확률로 도청자의 존재를 확인 할 수 있으므로 충분한 검증 모드를 사용한다면 공유키가 없어도 완전한 안전성을 보장 받으며 통신이 가능하다. 그러나 메시지를 직접 보내는 메시지 모드 전에 충분한 검증 모드를 사용하여야 프로토콜 중간에 도청자가 존재하더라도 그에게 유출되는 정보의 양을 줄일 수 있다. 공격자의 입장에서는 자신의 존재를 감추고 도청에 성공하더라도 초기에 준비했던 상태가 Bob의 초기 상태와 같은지를 확인할 수 없으므로 도청한 정보에 대해 유용한 정보인지 아닌지를 구별할 수 없다. 이는 가로챈 정보가 유용한 비트인지 임의적인 비트인지를 구별 할 수 있는 능력이 도청자에게는 없음을 의미한다.

본 프로토콜은 대개의 통신 프로토콜들과 달리 정보의 암호화를 위한 연산자가 필요하지 않고 큐빗이 전달 되는대로 측정을 수행하여 결과만을 고전적으로 저장하면 되므로 양자상태의 보관에 따른 어려움이나 번거로움이 없다. 또한 이 프로토콜은 얽힘상태 중에서도 가장 기본적인 벨 상태만을 사용하고 있는데 이는 그 이상의 큐빗이 얽힌 GHZ 상태, 더 일반적으로는 캣 상태(cat states)보다 생성과 측정 등에서 용이하므로 실현적인 면에서도 장점이 될 수 있다.

임의 적인 거리에 있는 사용자 간 벨 상태의 신뢰적인 공유는 얽힘정화(entanglement purification)와 양자반복자(quantum repeater) 등을 이용하여 해결[21] 될 수 있으므로 본 프로토콜의 현실화에 힘을 실어 준다. 그러나 신뢰적인 벨 상태의 측정은 현재까지도 어려움이 많은 상태이다. 앞으로 계속 되는 연구에서 벨 측정의 신뢰적인 실험적 구축은 해결될 것으로 기대하며 그렇게 되면 본 프로토콜의 중간자공격 및 PNS공격에 대한 안전성, 간편성 그리고 비용적인 면뿐만 아니라 구현적인 측면에서도 많은 주목을 받을 것으로 기대하고 있다.

참 고 문 헌

[1] C. H. Benett, G. Brassard, C. Crepeau, R. Jozsa, A. Pres, and W. Wootters. "Teleporting an unknown quantum state via dual classical and EPR channels." *Phys. Rev. Lett.* 70:1895-1899, 1993

[2] D. Boschi, S. Branca, F. D. Martini, L. Hardy, and S. Popescu. "Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolski-Rosen channels." *Phys. Rev. Lett.*, 80:1121-1125, 1998

[3] D. Bouwmeester, J. W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger. "Experimental quantum teleportation." *Nature*, 390(6660):575-579, 1997

[4] M. A. Nielsen, E. Knill, and R. Laflamme. "Complete quantum teleportation using nuclear magnetic

resornance." *Nature*, 396(6706):52-55, 1998

[5] A. Ekert, "Quantum cryptography based on Bell's theorem." *Phys. Rev. Lett.* 67, 661, 1991

[6] A. Cabello, "Quantum key distribution without alternative measurements." *Phys. Rev. A* 61, 052312, 2000

[7] H. Bechmann-Pasquinucci and N. Gisin, "Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography." *Phys, Rev, A* 59, 4238, 1999

[8] M. Hillery, V. Buzek, and A. Berthiaume, "Quantum secret sharing." *Phys. Rev. A* 59, 1829, 1999

[9] A. Cabello, "Quantum key distribution without alternative measurements." *Phys. Rev. A* 61, 052312, 2000

[10] D. Bruss, "Optimal Eavesdropping in Quantum Cryptography with Six States." *Phys. Rev. Lett.* 81, 3018, 1998

[11] K. Bostrom and T. Felbinger, "Deterministic Secure Direct Communication Using Entanglement." *Phys. Rev. Lett.* 89, 187902, 2002

[12] S. Bandyopadhyay, "Teleportation and secret sharing with pure entangled states." *Phys. Rev. A* 62, 012308, 2000

[13] MAN Zhong-Xiao, ZHANG Zhan-Jun and LI Young, "Deterministic secure direct communication by using swapping quantum entanglement and local unitary operation." *Chin. Phys. Lett.* 22, No. 1, 2005

[14] T Gao, F L Yan and Z X Wang, "Deterministic secure direct communication using GHZ states and swapping quantum entanglement." *J. Phys. A* 38, 5761, 2005

[15] D. Song, "Secure key distribution by swapping quantum entanglement." *Phys. Rev. A* 69, 034301, 2004

[16] S. Bose, V. Vedral, and P. L. Knight, "Multiparticle generalization of entanglement swapping." *Phys. Rev. A* 57, 822, 1998

[17] B. Yurke and D. Stoler, "Bell's-inequality experiments using independent-particle sources." *Phys. Rev. A* 46, 2229, 1992

[18] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, "Event-ready-detectors Bell experiment via entanglement swapping." *Phys. Rev. Lett.* 71, 4287, 1993

[19] M. Koashi and N. Imoto, "Quantum Cryptography Based on Split Transmission of One-Bit Information in Two Steps." *Phys. Rev. Lett.* 79, 2383, 1997

[20] A. beige, B. G. Englert, C. Kursiefer and H. Weinfurter, *Acta Phys. Pol. A* 101 357

[21] Lo Hoi-Kwang Lo and H. F. Chau *Science* 283, 2050, 1999

[22] Won-Young Hwang, "Quantum key distribution with high loss." Phys. Rev. Lett. 91, 057901, 2003

[23] N. Lutkenhaus, "Security against individual attacks for realistic quantum key distribution." *Phys. Rev. A* 61, 052304, 2000

〈著者紹介〉

홍 창 호 (Chang-ho Hong) 정회원
2001년 2월 : 고려대학교 자연과학대학 물리학과 학사
2003년 2월 : 고려대학교 응용물리대학원 응집물리학과 석사
2005년 2월 : 고려대학교 정보보호대학원 박사과정 수료
〈관심분야〉 양자암호, 암호프로토콜

이 화 연 (Hwa-Yean Lee) 정회원
2001년 2월 : 고려대학교 수학과 학사
2003년 2월 : 고려대학교 정보보호대학원 석사
2005년 2월 : 고려대학교 정보보호대학원 박사과정 수료
〈관심분야〉 양자암호, 암호프로토콜

김 지 인 (Ji-in Kim)
1995년 2월 : 고려대학교 자연과학대학 물리학과 졸업
1997년 2월 : 고려대학교 이과대학 물리학과 석사 졸업
2005년 2월 : 고려대학교 이과대학 물리학과 대학원 박사과정 수료
〈관심분야〉 양자암호, 양자컴퓨터, 양자얽힘, 다체계에서의 양자얽힘

양 형 진 (영문이름) 정회원
1990년 8월~1990년 10월: 미국 Oak Ridge 국립 연구소, Computer Consultant
1990년 12월~1991년 12월: 미국 신시내티대학교 박사후 연구원
1999년 1월~1999년 12월: 미국 매릴랜드대학교 교환교수
1992년 3월~현재: 고려대학교 자연과학대학 디스플레이 반도체 물리학과 교수
2001년 3월~현재 : 고려대학교 정보보호대학원 겸임교수
〈관심분야〉 양자암호, 암호프로토콜

임 종 인 (Jongin Lim)
1986년 2월: 고려대학교 대학원 수학과 박사(암호학)
2000년 8월: 고려대학교 정보보호대학원/CIST 원장(센터장)
2004년 1월: 국가정보원 정보보호정책자문위원
2005년 7월: 대통령 자문 전자정부 특별위원
2005년 12월: 국회 과기정위원회 정보통신 정책 자문위원
〈관심분야〉 정보보호기술, 정보보호정책, PET, 컴퓨터 포렌식