情報保護學會論文誌
第18卷 第4號, 2008. 8

CHSH 부등식을 이용하여 양자 키 분배와 양자 인증의 안전성을 개선한 프로토콜*

허 진 오[1†], 홍 창 호[1], 임 종 인[1], 양 형 진[1,2‡]
[1]고려대학교 정보경영공학전문대학원, [2]고려대학교 디스플레이 반도체 물리학과

Improving The Security Of Quantum Key Distribution And Quantum Authentication By Using CHSH Inequality*

Jin o Heo[1†], Chang ho Hong[1], Jongin Lim[1], Hyoung jin Yang[1,2‡]
[1]Graduate School of Information Management and Security, Korea University,
[2]Department of Display Semiconductor, Korea University

요 약

본 논문에서는 Bao-sen Shi(2001년)에 의해 제안된 얽힘 상태(벨 상태)를 이용한 양자 키 분배와 양자 인증 프로토콜의 취약성을 분석하고 그것을 보완한 프로토콜을 제안한다. 기존의 프로토콜은 사용자들이 제 3자(중재자)를 인증하는 과정만 존재했기 때문에 도청자의 Impersonation 공격에 대해 취약성을 가지고 있었다. 본 논문이 제안하는 프로토콜은 CHSH 부등식을 이용한 체크 모드를 사용하여 중재자가 사용자들을 인증함으로써 안전성을 보완한 프로토콜이다.

ABSTRACT

We propose to analyze a weakness of quantum key distribution and quantum authentication which use entangled state were proposed by Bao-sen Shi(2001) and to improve the security of the protocol. The existing protocol had a weakness against an impersonation attack of an eavesdropper, because of a only process which authenticated a third party(Center) by users. In this paper, we propose improving the security of the protocol that authenticates users by a third party using check mode which applies CHSH inequality.

Keywords : Quantum key distribution, Quantum authentication, CHSH inequality

Ⅰ. 서 론

양자 암호는 1984년 Bennett과 Brassard에 의해서 처음 제안된 키 분배 프로토콜[1] 이후로 양자 직접 통신[2,3], 양자 전송[4,5], 양자 비밀 공유[6,7]에 이르기까지 많은 분야에서 연구가 이루어지고 있다. 특히 양자 키 분배 프로토콜은 고전적인 키 분배 프로토콜과 달리 양자 상태의 붕괴가 확률적이고 무작위적인 것[1,8]과 임의의 양자 상태가 복제 될 수 없는[9] 양자적 특징으

접수일 : 2008년 1월 31일; 채택일 : 2008년 5월 16일
* 본 연구는 지식경제부 및 정보통신 연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음 (IITA-2008-(C1090-0801-0025))
† 주저자, heojo80@yahoo.co.kr
‡ 교신저자, yangh@korea.ac.kr

로 안전성을 보장하고 있으며 다른 양자 통신 분야보다도 실험적 구현[10,11]이 활발히 진행 되고 있다. 최근에는 사용자의 인증 과정[12,13]을 추가함으로써 보다 높은 안전성을 보장하는 연구가 활발히 이루어지고 있다. 이 중에서 2001년에 Bao-sen Shi에 의해 제안된 얽힘 상태를 이용한 양자 키 분배와 양자 인증 프로토콜[16]은 두 가지 local unitary operation[17]과 벨 측정[17]을 통하여 양자 키 분배와 양자 인증을 수행하게 한다. 또한 양자정보저장장치[14,15]를 이용하여 제 3의 기관(이제부터 중재자)이 얽힘 상태 교환[18,19]으로 정당한 사용자에게 벨 상태[17]를 공유 시킨 후 양자 키 분배와 양자 인증을 수행하는 방법을 제시 하고 있다.

본 논문에서는 Bao-sen Shi가 제안한 프로토콜 [16]에서 중재자에 의해 벨 상태가 공유되는 과정에서 나타나는 도청자의 Impersonation 공격에 대한 취약성을 지적하고 이 문제를 해결하는 프로토콜을 제시한다.

Ⅱ. 양자 키 분배와 양자 인증에 필요한 기본 개념

이 장에서는 양자 키 분배와 양자 인증 프로토콜에서 필요한 얽힘 상태와 local unitary 연산자 그리고 새롭게 제시하는 프로토콜에서 인증 과정에 필요한 CHSH 부등식[20,21]을 살펴본다.

얽힘 상태[17]란 두 개의 양자 상태가 얽혀서 독립적으로 분리될 수 없는 상태를 말한다. 하나의 양자 상태 $|\psi>$는 일반적으로 $\alpha|0>+\beta|1>$으로 표현하는데 여기서 $|0>$과 $|1>$은 큐빗의 Z 기저에서의 두 고유상태를 나타내며, α와 β는 두 상태의 확률을 나타내는 복소수이고 측정 시 두 상태($|0>$과 $|1>$)가 나올 확률은 각각 $|\alpha|^2$와 $|\beta|^2$이다. 위의 양자 상태는 $|\alpha|^2+|\beta|^2=1$ 의 관계식을 만족한다. 그리고 양자상태 $|\psi>$는 $|0>$과 $|1>$이 중첩을 이루고 있는데 이는 0과 1을 동시에 표현할 수 없는 고전적인 비트와는 다르다. 큐빗 두 개가 얽힌 양자상태는 각각의 양자상태의 텐서 곱의 형태로 분리 할 수 없는 상태이다. 양자 역학에서 벨 상태라고 불리는 (식 1과 2)의 네 가지 상태는 두 큐빗이 얽혀 있을 뿐 아니라 서로 직교 관계에 있다.

$$|\Phi^{\pm}>=\frac{1}{\sqrt{2}}(|00>\pm|11>) \quad (1)$$

$$|\Psi^{\pm}>=\frac{1}{\sqrt{2}}(|01>\pm|10>) \quad (2)$$

local unitary 연산자[17]란 양자 상태를 변화시키는 연산자이며, $U^{+}U=UU^{+}=I$ 의 조건을 만족시킨다. (U는 unitary 연산자를 의미하며 U^{+}는 U의 hermitian conjugate이다.) 이러한 unitary 연산자의 대표적인 것이 네 개의 Pauli 연산자[17]이다.

$$I=\begin{pmatrix}1&0\\0&1\end{pmatrix}\ \sigma_X=\begin{pmatrix}0&1\\1&0\end{pmatrix}\ \sigma_Y=\begin{pmatrix}0&-i\\i&0\end{pmatrix}\ \sigma_Z=\begin{pmatrix}1&0\\0&-1\end{pmatrix} \quad (3)$$

네 개의 Pauli 연산자가 양자 상태에 적용 될 경우 I는 양자 상태를 그대로 유지시키고 σ_X는 비트플립의 역할을 σ_Y는 비트플립과 위상을 바꾸며 σ_Z는 $|1>$의 위상만 바꾸는 역할을 한다. 위의 네 가지 연산자들 $I^{+}I=\sigma_X^{+}\sigma_X\sigma_Y^{+}\sigma_Y=\sigma_Z^{+}\sigma_Z=I$ 의 관계식을 만족한다.

CHSH 부등식은 벨 정리[22]와 벨 부등식[22]에 기초한다. 1964년 John Bell은 시, 공간적으로 서로 떨어진 한 쌍의 입자들의 물리량을 측정할 때 고전 역학적인 결과인 실재성(Realism)과 국소성(Locality)[23] 그리고 양자 역학적인 결과인 기댓값(Expectation value)과 얽힘 상태의 비국소성(Nonlocality)인 상반된 4가지 개념을 기초로 측정에 대한 문제를 설명한 벨 정리와 한 쌍의 입자들의 물리량을 측정 할 때 그 결과가 고전 역학을 따르는지 양자 역학을 따르는지를 알 수 있는 벨의 부등식 고안하였다. 그 이후에 1969년에 John Clauser, Michael Horne, Abner Shimony 그리고 Richard Holt는 벨의 이론을 실험적으로 검증할 수 있는 형태의 실재성과 국소성의 가정 위에서 만든 부등식(CHSH 부등식)을 제안 하였다. 그래서 CHSH 부등식을 만족하는 계는 고전 역학의 물리법칙을 따르는 계이고 만족하지 않는 계는 양자 역학의 법칙을 따르는 계라는 결론을 내릴 수 있는 기준을 제시하였다.

예를 들어 Singlet 상태 $|\Psi^{-}>=\frac{1}{\sqrt{2}}(|01>-|10>)$를 생각해보면 A와 B가 자신의 큐빗에 A : $(a_1,a_2)=\{\sigma_X,\sigma_Y\}$, B : $(b_1,b_2)=\{(\sigma_X+\sigma_Y)/\sqrt{2},(-\sigma_X+\sigma_Y)/\sqrt{2}\}$ 와 같은 두 측정 기저 중에서 하나를 선택하여 측정을 수행 한다. 큐빗에 대한 측정 결과는 기본 단위를 $\frac{1}{2}\hbar$로 한 +1(up spin)과 -1(down spin) 둘 중 하나이다. 우리는 여기서 다음과 같은 값을 정의 한다.

$$E(a_i,b_j)=P_{++}(a_i,b_j)+P_{--}(a_i,b_j)-P_{+-}(a_i,b_j)-P_{-+}(a_i,b_j) \quad (4)$$

위의 값에서 $P_{\pm\pm}(a_i, b_j)$는 A와 B가 a_i와 b_j로 큐빗을 측정하여 그 결과가 ±1와 ±1이 나오는 확률을 의미한다. 그래서 A와 B가 같은 측정 기저로 측정 할 경우 $E(a_i, b_j) = E(\sigma_Z, \sigma_Z) = -1$이 된다. 이제 우리는 CHSH 부등식과 같은 측정 기저에 의한 측정 결과 통계인

$$S = E(a_1, b_1) - E(a_1, b_2) + E(a_2, b_1) + E(a_2, b_2) \quad (5)$$

를 볼 때 이 S를 양자 역학의 가정(기댓값)으로 계산한 결과는

$$E(a_1, b_1) = E(a_2, b_1) = E(a_2, b_2) = -\frac{1}{\sqrt{2}}$$
$$E(a_1, b_2) = +\frac{1}{\sqrt{2}} \quad (6)$$

$S = -2\sqrt{2}$ 이다. 그러나 고전 역학을 기초로 한 S 값은 이와 다르다.

$$\text{측정}(a_1, b_1)\text{-측정}(a_1, b_2)+\text{측정}(a_2, b_1)+\text{측정}(a_2, b_2) \quad (7)$$

여기서 $\text{측정}(a_i, b_j)$ = (a_i에 의한 측정 결과)×(b_j에 의한 측정 결과)이다. 즉 위의 식을 다시 정리 하면

$$\text{측정}[a_1, (b_1 - b_2)]+\text{측정}[a_2, (b_1 + b_2)] \quad (8)$$

이 된다. 만일 b_1과 b_2의 측정 결과가 같으면$(b_1 - b_2)$의 값은 0이 되고 결과가 다르면 $(b_1 + b_2)$의 값이 0이 된다. 그러므로 $(b_1 - b_2)$또는 $(b_1 + b_2)$은 측정 결과가 둘 중 하나는 반드시 0이 나오게 되며 전체 결과는a_1와 a_2에 의한 측정 결과에 따라 +2 또는 -2의 결과를 가지게 된다. 이에 대한 기대치 $[E(\bullet)]$을 구해보면

$$\begin{aligned} &E[\text{측정}(a_1, b_1)\text{-측정}(a_1, b_2)+\text{측정}(a_2, b_1)+\text{측정}(a_2, b_2)] \\ &= \sum P(a_1, a_2, b_1, a_2)\times[\text{측정}\{a_1, (b_1 - b_2)\} \\ &\qquad + \text{측정}\{a_2, (b_1 + b_2)\}] \\ &\le \sum P(a_1, a_2, b_1, a_2)\times(+2) = +2 \\ &\text{또는 } \ge \sum P(a_1, a_2, b_1, a_2)\times(-2) = -2 \end{aligned} \quad (9)$$

이다. 여기서 $P(a_1, a_2, b_1, a_2)$는 측정 실험에서 결과의 부정확성에 의한 확률 분포 이다. 그런데 전체 측정 실험에서 확률 분포의 합$(\sum P(a_1, a_2, b_1, a_2))$은 1 이므로 다음과 같이 식을 바꿀 경우 S는

$$\begin{aligned} &E[\text{측정}(a_1, b_1)\text{-측정}(a_1, b_2)+\text{측정}(a_2, b_1)+\text{측정}(a_2, b_2)] \\ &= \sum P(a_1, a_2, b_1, a_2)\times\{\text{측정}(a_1, b_1) - \text{측정}(a_1, b_2) \\ &\qquad + \text{측정}(a_2, b_1) + \text{측정}(a_2, b_2)\} \\ &= E(a_1, b_1) - E(a_1, b_2) + E(a_2, b_1) + E(a_2, b_2) \\ &= S \qquad \therefore -2 \le S \le +2 \end{aligned} \quad (10)$$

의 범위를 가지게 된다. 이와 같이 Singlet 상태에 대한 CHSH 부등식의 결과가 양자 역학과 고전 역학에서 서로 다르게 나타난다.

이후 Aspect[24,25]의 실제 실험 결과에 의하면 양자 역학의 가정이 통용되고, 고전 역학의 측정에 대한 가정인 실재성$(-2 \le S \le +2)$을 따르지 않는 것으로 밝혀졌다. 이것은 오히려 측정 행위 자체가 물리량의 특징을 규정짓는다는 것을 의미하며 이는 양자 역학에서 가정하는 측정 결과에 대한 기댓값으로 물리량을 기술하는 것이 정당하다는 것을 입증한다.

이러한 결과는 위에서 예를 든 Singlet 상태의 특징인 얽힘 상태의 비국소성과도 연결 된다. 예를 들어, A와 B가 서로 같은 측정 기저로 두 큐빗을 측정하면 그 결과는 항상 반대이다. 그렇다면 A와 B가 아주 멀리 떨어져 있을 때(광속으로도 상당한 시간이 걸리는 거리)도 측정결과가 동시에 결정 되는지가 의문이다. 만일 상대론을 받아들인다면 빛 보다 빠른 정보전달의 방법은 존재하지 않으므로 측정결과가 동시에 결정되는 것이 아니라 서로 반대되는 결과인 물리적 특징을 원래부터 지니고 있었다는 실재성의 결론을 내릴 수 있다. 그러나 Aspect등의 실험에서 물리적인 실재성의 가정이 틀리다는 것은 결국 얽혀있는 두 큐빗에 대한 측정 결과는 국소성의 개념으로는 설명할 수 없으며 이는 얽힘 상태가 비국소성의 특징을 가지고 있다고 할 수 밖에 없다. 그러므로 CHSH 부등식은 얽힘 상태와 그렇지 않은 상태를 구별하는 척도이며 이는 뒤에서 새롭게 제안 되는 프로토콜의 인증 과정에 사용될 것 이다.

Ⅲ. 얽힘 상태를 이용한 양자 키 분배와 양자 인증 프로토콜

Bao-sen Shi(2001년)는 양자정보저장장치가 없는 사용자간의 통신과 양자정보저장장치를 사용하는 중재자가 존재하는 통신을 제안 하였다. 이 절에서는 이 두 가지 프로토콜을 간략히 알아 볼 것이다.

3.1 사전에 사용자끼리 벨 상태를 공유한 프로토콜 (양자정보저장장치를 사용하지 않음)

키를 공유하려는 두 사용자 Alice(A)와 Bob(B)의 양자 키 분배와 양자 인증 프로토콜은 다음과 같다.

(a) A와 B는 사전에 벨 상태를 준비한 후 서로 큐빗을 나누어 가진다.
(b) B는 두 가지 local unitary 연산자인 I와 σ_X중 하나를 선택하여 자신이 가진 큐빗에 적용한다.
(c) B는 연산자가 적용된 큐빗을 A에게 전송한다.
(d) A는 두 큐빗을 벨 측정하고 결과에 따라 B가 적용한 연산자를 알아낸다.

프로토콜의 인증 과정은 다음과 같다.

(인증 과정) [표 1]은 (d)의 과정에서 A가 얻을 수 있는 측정 결과이다. 즉 정당한 B일 경우 위의 [표 1]과 다른 결과는 나올 수 없는 것으로 B의 신원을 인증한다. 반대로 B가 A를 인증하기 위해서는 (b),(c)는 A가 수행 하며 (d)에서 B가 벨 측정으로 인증을 확인 한다. 이러한 상호간에 신원 인증을 위해서 A와 B가 가진 큐빗에 unitary 연산자를 적용하고 전송하는 순서는 통신전에 약속하여 결정한다.
이 프로토콜은 키 공유와 사용자 인증을 하면서 하나의 큐빗 이외에 어떠한 고전적인 정보도 전송하지 않는다는 장점을 가지고 있다. 그래서 도청자(이하 Eve)가 공격을 수행할 경우 단지 하나의 큐빗만을 얻을 수 있다. 이때 도청자가 가져갈 수 있는 정보의 양, 즉 엔트로피는 다음과 같다.

$$\rho_B = Tr_A(\rho_\Psi) = \frac{1}{2}(|0><0| + |1><1|)$$
$$S(\rho_A) = S(\rho_B) = \log_2 2 = 1 \qquad (11)$$

$S(=-\sum_x \lambda_x \log \lambda_x)$는 Von Neumann entropy[17] 이고 엔트로피의 결과가 최대 (S=1)이다. 이는 양자 상태에 대한 불확정도가 최대이므로 Eve가 하나의 큐빗을 획득 한다 해도 키에 대한 정보를 전혀 얻어가지 못하며 중간에서 큐빗을 가로채는 도청에 대해서 이 프로토콜은 안전성이 보장된다.

[표 1] 벨 상태에 따라 취해주는 unitary 연산자에 의해 변환된 벨 상태

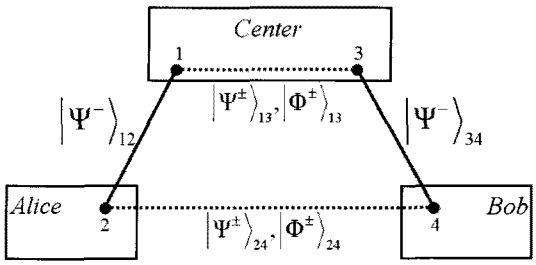
A와 B의 벨 상태	Unitary 연산자	operation 후의 벨 상태
$\Psi^{\pm}$	$(I$ or $\sigma_X)$	$(\Psi^{\pm}$ or $\Phi^{\pm})$
$\Phi^{\pm}$	$(I$ or $\sigma_X)$	$(\Phi^{\pm}$ or $\Psi^{\pm})$

3.2 중재자가 사용자에게 벨 상태를 공유하게 하는 프로토콜 (양자정보저장장치 사용)

(a) 중재자는 A와 B 사이에서 벨 상태를 하나씩 공유한다. 그리고 A와 B사이에 벨 상태를 공유시켜주기 전 까지 이 상태들을 저장하고 있기 위해 양자정보저장장치를 이용 한다.
(b) 중재자는 자신이 가진 두 큐빗에 벨 측정을 한다. 이 측정에 의해 서로 얽혀 있지 않았던 A와 B의 두 큐빗은 얽혀지게 되는 즉, 둘 사이에 벨 상태가 공유되게 된다.
예를 들어 초기에 A, B, 중재자가 공유하고 있는 상태를 $|\Psi^->_{12}|\Psi^->_{34}$ 가정 하면 [그림 1]에서 중재자가 가진 1과 3번 큐빗에 대해 벨 측정을 한 후의 상태는

$$|\Psi^->_{12}|\Psi^->_{34} \Rightarrow$$
$$\frac{1}{2}(|\Psi^->_{13}|\Psi^->_{24} - |\Psi^+>_{13}|\Psi^+>_{24} + |\Phi^+>_{13}|\Phi^+>_{24} - |\Phi^->_{13}|\Phi^->_{24}) \qquad (12)$$

의 상태가 된다. 이것은 중재자의 큐빗들 외에 다른 큐빗들이 서로 얽힘 상태가 되는 효과를 가져 오며 이를 얽힘 상태 교환(Entanglement swapping)이라고 한다.



[그림 1] 실선은 A와 중재자 사이의 벨 상태 $|\Psi^->_{12}$와 B와 중재자 사이의 벨 상태를 $|\Psi^->_{34}$를 나타내며 점선은 중재자의 1-3 큐빗의 벨 측정 후 나오게 되는 벨 상태이다.

(c) 얽힘 상태 교환이 끝난 후 중재자는 A와 B의 벨 상태를 공개 채널로 알려 준다.

(d) 이후 A와 B는 중재자에 의해서 공유된 벨 상태를 이용하여 3.1절에서와 같이 키 분배와 사용자 간의 인증을 수행한다. 그러나 3.1절에서의 인증과 다른 점은 [표 2]처럼 공유된 벨 상태가 $|\Psi^{\pm}>_{24}$일 경우 unitary 연산자(I, σ_X)을 사용하고 $|\Phi^{\pm}>_{24}$일 경우 $(I, i\sigma_Y)$을 사용 한다.(이후 측정 결과로 나올 수 있는 벨 상태의 확인으로 사용자끼리 인증)

(e) [표 2]와 같이 두 종류의 연산자를 사용하는 이유는 사용자들끼리의 인증은 물론 사용자들이 정당한 중재자에 의해 벨 상태를 공유 받은 것 인지까지 인증하기 위해서 이다. 이것은 [표 3]과 같이 공유 채널에서 사용자들이 받은 벨 상태의 정보가 잘 못 되었을 경우 큐빗에 unitary 연산자를 잘 못 적용하게 됨으로써 벨 측정에 의해서 나올 수 없는 결과 때문에 중재자의 신분을 인증 할 수 있게 한다.

[표 3]에서 예를 들면 A와 B사이에 공유된 벨 상태가 $|\Phi^{+}>$인 것으로 중재자가 잘못 된 정보를 알릴 경우 (실제로는 $|\Psi^{+}>$가 공유되어 있다.) A와 B는 $(I, i\sigma_Y)$를 선택 하여 통신을 수행 한다. 이때 벨 측정에 의해서 나와야 하는 결과는 $|\Psi^{-}>$와 $|\Phi^{+}>$이다. 그러나 표와 같이 실제 벨 상태는 $|\Psi^{+}>$이므로 실제 측정 결과는 $|\Psi^{+}>$와 $|\Phi^{-}>$이므로 사용자들은 중재자에 의한 벨 상태 공유에 이상이 있다는 것을 알게 되는 것으로 중재자의 인증이 가능 하게 한다.

〔표 2〕 벨 상태에 따라 취해주는 unitary 연산자와 큐빗에 적용한 후의 결과

A와 B의 벨 상태	Unitary 연산자	operation 후의 벨 상태
$\Psi^{\pm}$	$(I \text{ or } \sigma_X)$	$(\Psi^{\pm} \text{ or } \Phi^{\pm})$
$\Phi^{\pm}$	$(I \text{ or } i\sigma_Y)$	$(\Phi^{\pm} \text{ or } \Psi^{\pm})$

〔표 3〕 A와 B의 실제 공유된 벨 상태와 공개 채널에서 잘못된 정보로 인한 벨 상태에 대해서 unitary 연산자가 적용된 후 결과

벨 상태의 잘못된 정보	A와 B의 실제 벨 상태	잘못된 unitary 연산자	operation 후의 벨 상태
Φ^{+}	Ψ^{+}	$(I \text{ or } i\sigma_Y)$	$(\Psi^{+} \text{ or } \Phi^{-})$
Φ^{-}	Ψ^{-}	$(I \text{ or } i\sigma_Y)$	$(\Psi^{-} \text{ or } \Phi^{+})$
Ψ^{-}	Φ^{+}	$(I \text{ or } \sigma_X)$	$(\Phi^{+} \text{ or } \Psi^{+})$
Ψ^{+}	Φ^{-}	$(I \text{ or } \sigma_X)$	$(\Phi^{-} \text{ or } \Psi^{-})$

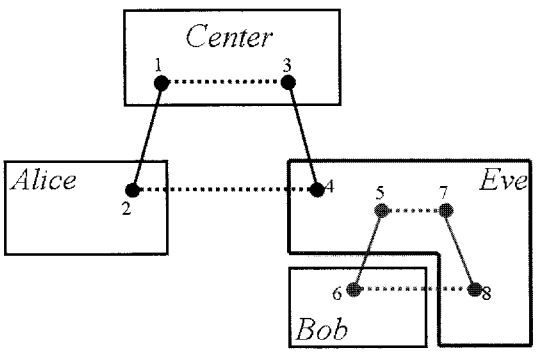
Ⅳ. 양자정보저장장치를 이용한 프로토콜의 취약성

이 장에서는 3.2절에서 제안된 중재자가 양자정보저장장치를 사용하여 키 분배와 인증을 수행하는 경우 벨 상태를 공유시키는 과정에서 Eve의 Impersonation 공격에 취약하다는 것을 보일 것이다.

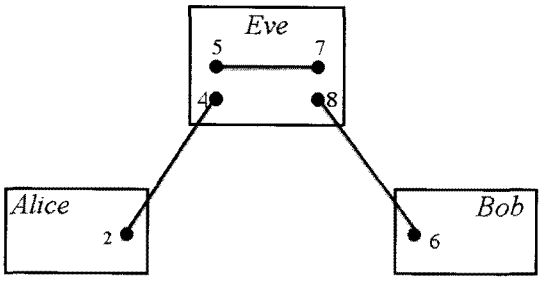
Eve의 Impersonation 공격은 [그림 2]의 실선과 같이 Eve가 B를 가장하여 중재자에게 벨 상태를 공유 받는다. 그리고 이후 Eve는 중재자를 가장하여 B에게 벨 상태를 공유시켜 준다. [그림 2]의 점선과 같이 중재자가 얽힘 상태 교환을 통해 A와 Eve에게 벨 상태를 공유시키면 Eve는 얽힘 상태 교환을 통해 자신과 B사이에 새로운 벨 상태를 공유 시킨다.

여기까지 Eve의 Impersonation 공격이 수행 되었다면 [그림 3]와 같이 A와 B사이의 통신에 Eve가 개입할 수 있는 Man in the middle 공격의 형태가 갖추어지게 된다. 이는 Eve가 중간에서 벨 측정을 통하여 키 값을 얻는 것은 물론 적절한 unitary 연산자를 적용하여 A와 B 사이의 인증, 사용자가 중재자를 인증하는 과정을 통과할 수 있다.

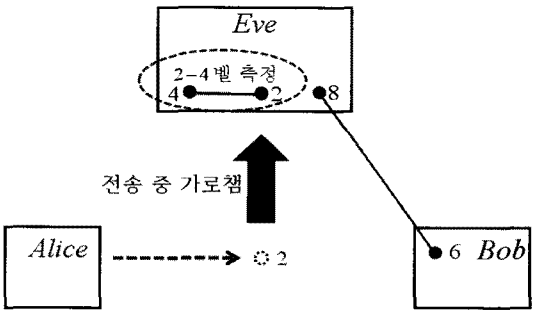
이러한 Eve의 Impersonation 공격에 기인하는 Man in the middle 공격을 예를 통해 자세히 보면 다음과 같다.



〔그림 2〕 실선은 Eve가 B와 중재자를 가장하여 공유 받고 (3-4) 공유 하는(5-6) 벨 상태 이다. 점선은 중재자와 Eve의 얽힘 상태 교환을 통해 공유된 벨 상태 (2-4, 6-8)이다. A와 B는 (2-6)가 서로 벨 상태로 공유 되었다고 생각 한다.



〔그림 3〕 2-4는 중재자에 의한 벨 상태이고 6-8은 Eve에 의한 벨 상태이다.(Man in the middle 공격)



〔그림 4〕 A는 자신의 큐빗(2번)에 unitary연산자를 적용하여 B에게 전송하지만 이를 Eve가 중간에서 가로채서 2-4에 대한 벨 측정 수행 후 A의 연산자 정보를 획득한다.

예를 들어 A와 Eve사이에 벨 상태는 중재자에 의한 얽힘 상태 교환에 의해서 $|\Psi^-\rangle_{AE}$가 공유 되었다고 가정한다.

(a) Eve와 B사이에 공유된 벨 상태는 $|\Phi^+\rangle_{EB}$이다.(Eve의 얽힘 상태 교환에 의한 결과) 그러나 B는 A와 마찬가지로 자신이 $|\Psi^-\rangle_{AB}$을 공유 한 것으로 알고 있다.

(b) 여기서 A와 B가 Eve의 Impersonation 공격을 알아차리지 못 하는 경우 [그림 4]와 같이 A는 자신의 큐빗에 키 분배와 인증을 위해서 unitary 연산자 적용하고 큐빗을 B에게 전송하게 된다.
이 과정을 자세히 본다면
A 와 Eve 사이의 벨 상태에 대해 A가 unitary 연산자 σ_X을 수행하면

$$(\sigma_X \otimes I)_{AE} \,|\Psi^-\rangle_{AE} \Rightarrow |\Phi^-\rangle_{A'E'} \qquad (13)$$

가 되고 A의 큐빗 전송 중간에 Eve는 큐빗을 가로채서 벨 측정을 한다. A와 Eve가 벨 상태를 공유했기 때문에 Eve는 벨 측정을 통해 A가 적용한 unitary 연산자가 σ_X임을 정확히 알 수 있다.

(c) 이후 Eve는 B가 벨 측정을 통한 키 공유 과정에서 인증 과정을 수행 할 경우 나타나는 오류를 없애기 위해 자신과 B사이에 공유한 벨 상태에 적절한 unitary 연산자를 적용해야 한다. 즉, Eve가 B에게 자신의 큐빗을 전송한다면 B가 벨 측정 결과를 통해서 A의 unitary 연산자가 σ_X임을 확인할 수 있어야 한다.(B의 인증 과정을 통과하기 위해) 이를 위해 Eve는 자신과 B가 공유한 $|\Phi^+\rangle_{EB}$을 $|\Phi^-\rangle_{E'B'}$로 바꾸는 적절한 unitary 연산자를 수행하여야 한다. 처음 가정대로 Eve와 B사이의 초기 벨 상태에서 Eve는 $|\Phi^+\rangle_{EB}$를 $|\Phi^-\rangle_{E'B'}$로 변화시키 위해서 Eve가 적용해야 하는 unitary 연산자는 σ_Z이다.

$$(\sigma_Z \otimes I)_{EB} \,|\Phi^-\rangle_{EB} \Rightarrow |\Phi^-\rangle_{E'B'} \qquad (14)$$

그 후 Eve는 큐빗을 B에게 보낸다.

(d) B는 받은 큐빗과 자신의 큐빗에 벨 측정을 수행한다. 측정 결과에 의해서 키 공유와 함께 A와 B가 3.2절의 (d)와 (e)에서 했던 것과 동일한 방법으로 서로 정당한 사용자 인지에 대한 인증이나 정당한 중재자에 의한 벨 상태를 공유 받은 것에 대한 인증 과정을 수행하더라도 중재자, A 그리고 B는 Eve의 존재를 눈치 채지 못 한다.

지금까지 프로토콜의 취약성은 앞에서 본바와 같이 중간에서 Eve가 신원(A또는 B)을 가장하여 중재자에게 벨 상태를 공유 받을수만 있다면 (중재자 입장에서는 Impersonation 공격) 이후 A와 B 사이에서 공유되는 키를 자신의 존재를 드러내지 않고 가져 갈 수 있는 Man in the middle 공격이 가능하다. 이러한 Eve의 공격을 방지하기 위해 사전에 Eve의 Impersonation 공격이 불가능한 프로토콜을 다음 장에서 제시 할 것이다.

V. Eve의 Impersonation 공격 방지를 위해 보완된 프로토콜

3.2절에서 A와 B는 벨 상태를 공유시켜주는 중재자를 인증한다. 그러나 반대로 중재자는 A와 B가 정당한 사용자인지를 인증하지 않기 때문에 4절에서 지적한 취약성이 나타난다. 그러므로 이 절에서는 Eve의 Imper-

sonation 공격을 방지하기 위해 중재자도 CHSH 부등식을 이용하여 A와 B를 인증하는 새로운 프로토콜을 제시할 것 이다.

앞 장에서 지적한 취약성을 보완한 프로토콜을 살펴보면, 새로이 제안되는 프로토콜의 처음 과정인 (a)와 (b)는 3.2절에서 소개한 (a)와 (b)의 과정과 동일하다.

(c) 얽힘 상태 교환이 끝난 후 중재자는 벨 측정을 통한 결과와 체크 모드 사용 여부를 공개 채널로 A 와 B에게 알려준다.

체크 모드를 사용하지 않는 경우는 (c-1)과정으로, 체크 모드를 사용하는 경우에는 (d-1)과정으로 서로 별도로 진행 되게 된다.

(c-1) 체크 모드를 사용하지 않을 경우 A와 B는 공유한 벨 상태를 가지고 3.2절의 (d)와 (e)과정을 수행한다.(키 공유와 인증 과정)

(d-1) [그림 5]과 같은 체크 모드는 중재자가 A와 B를 인증하는 과정이다.

(d-2) A의 측정 기저$(a_1,a_2)=[\sigma_X,\sigma_Y]$와 B의 측정 기저$(b_1,b_2)=[(\sigma_X+\sigma_Y)/\sqrt{2},(-\sigma_X+\sigma_Y)/\sqrt{2}]$ 중에서 무작위로 선택한 측정 기저로 큐빗을 측정한다. 그리고 A와 B 각각 자신의 측정 결과와 측정 기저를 중재자에게 전송한다. 위 과정은 중재자가 A와 B에게 벨 상태를 공유하게 할 때마다 공유된 벨 상태에 대해서 수행한다.

(d-3) 중재자는 공유 시킨 벨 상태에 따라서 측정 기저와 측정 결과 통계를 가지고 각각에 대한 CHSH 부등식(식 5)을 계산한다.

중재자가 공유시킨 벨 상태가 $|\Phi^{\pm}>$인 경우에는

$$|\Phi^{\pm}>:\ -E(a_1,b_1)+E(a_1,b_2)+E(a_2,b_1)+E(a_2,b_2)=\mp 2\sqrt{2} \quad (15)$$

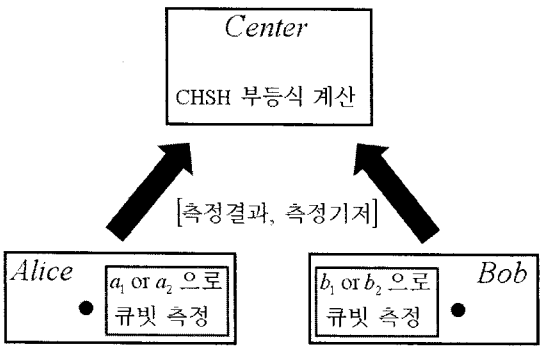
중재자가 공유 시킨 벨 상태가 $|\Psi^{\pm}>$인 경우에는

$$|\Psi^{\pm}>:\ +E(a_1,b_1)-E(a_1,b_2)+E(a_2,b_1)+E(a_2,b_2)=\pm 2\sqrt{2} \quad (16)$$

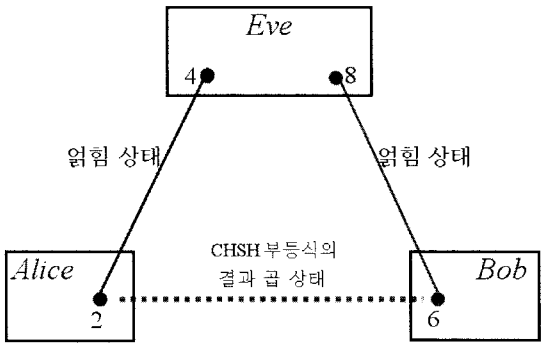
인 결과가 나와야 Eve의 Impersonation 공격이 없는 것으로 판단된다. 공격이 없다면 체크 모드를 제외하고 (c-1)에서 수행한 것이 A와 B가 공유하는 인증 키가 된다. 만일 위의 측정 결과 통계 값이 나오지 않는다면 Eve의 Impersonation 공격이 존재 한다는 것을 의미하며 전체 통신을 다시 시작해야 한다.

(d-3)에서 측정 결과의 통계로 CHSH 부등식의 계산한 결과가 Eve의 공격 여부에 대한 판단의 기준이 될 수 있는 이유는 얽힘 상태와 곱 상태(product 상태)[17]에서 CHSH 부등식의 결과가 다르기 때문이다. 곱 상태란 얽힘 상태와 달리 두 양자상태의 텐서 곱으로 인수분해 할 수 있는 상태이다. 그리고 이 두 상태는 같은 측정 기저로 측정할 경우 측정 결과 값이 서로 다르다. 즉 [그림 1]의 점선에서와 같이 A와 B사이에 Eve의 Impersonation 공격이 없다면 그들은 서로 정당한 벨 상태를 공유 하고 있으며 중재자의 측정 결과 통계는CHSH 부등식 특성에 따라 (식 15)과 (식 16)의 결과가 나오게 된다. 그러나 [그림 6]과 같이 Eve의 Impersonation 공격이 있었다면 A와 B가 공유한 상태는 벨 상태가 아니기 때문에 (식 15)이나 (식 16)의 값이 나타나지 않는다.

예를 들어, 2-4 큐빗의 상태가 $|\Psi^{-}>_{24}$ 이고 6-8 큐빗의 상태가 $|\Psi^{-}>_{68}$이면 2와 6 두 큐빗 상태는



〔그림 5〕 (중재자의 체크 모드)A와 B는 무작위적으로 선택된 측정 기저로 자신들의 큐빗 측정 후 결과와 기저의 종류를 중재자에게 공유 채널로 중재자에게 전송하고 중재자는 CHSH 부등식 계산으로 얽힘 상태인지 판단.



〔그림 6〕 Eve의 Impersonation 공격에 의해서 A와 B는 서로 얽힘 상태(벨 상태)를 공유하고 있지 않으며 CHSH 부등식의 결과로 이것을 확인 할 수 있다.

$$|\Psi^-\rangle_{24}\otimes|\Psi^-\rangle_{68} \Rightarrow$$
$$\frac{1}{2}(|\underline{0}1\rangle_{24}|\underline{0}1\rangle_{68}+|\underline{1}0\rangle_{24}|\underline{1}0\rangle_{68}$$
$$-|\underline{0}1\rangle_{24}|\underline{1}0\rangle_{68}-|\underline{1}0\rangle_{24}|\underline{1}0\rangle_{68}) \quad (17)$$

의 밑줄 친 상태이다. 만일 2와 6의 두 큐빗이 벨 상태 [$|\Psi^-\rangle_{26}=(|01\rangle-|10\rangle)_{26}/\sqrt{2}$]일 경우 A와 B가 큐빗을 Z 기저로 측정 할 때 나올 수 있는 결과는 (+1, -1) 또는 (-1, +1) 두 가지 뿐이다. 그러나 (식 17)처럼 A와 B 사이의 상태에서 측정하여 얻을 수 있는 결과는 (+1, +1), (-1, -1), (+1, -1), 그리고 (-1, +1)인 네 가지의 경우 중 하나의 결과가 나오게 된다. 이는 (식 17)에 대한 측정결과의 통계로 Eve의 공격에 의해 A와 B가 가진 큐빗이 $(|0\rangle+|1\rangle)_2/\sqrt{2}\otimes(|0\rangle+|1\rangle)_6/\sqrt{2}$ $=(|00\rangle+|11\rangle+|01\rangle+|10\rangle)_{26}/2$]의 형태인 곱 상태로 됐음을 의미한다. 그래서 CHSH 부등식을 이용하여 벨 상태와 곱 상태를 구별하는 방법으로 Eve의 공격 여부를 판단할 수 있다. 위에서와 같이 Z기저가 아닌 제안된 프로토콜에서 A와 B가 정한 측정 기저로 (식 17)을 측정한 결과 통계를 다시 계산 한다면 그 결과는

$$-E(a_1,b_1)+E(a_1,b_2)+E(a_2,b_1)+E(a_2,b_2)=0$$
$$+E(a_1,b_1)-E(a_1,b_2)+E(a_2,b_1)+E(a_2,b_2)=0 \quad (18)$$

이다. 그러므로 중재자는 (식 15)과 (식 16)에서의 결과와 (식 18)에서의 결과를 비교하여 A와 B사이에 공유한 상태가 벨 상태인지 곱 상태인지를 판단한다. 그래서 (식 18)의 결과가 나올 경우 중재자는 A와 B가 서로 공유한 상태가 곱 상태임을 알게 되며, 이것으로 Eve의 도청이 있었음을 알게 된다.

Ⅵ. 결 론

기존에 제안된 (Bao-sen Shi 2001년)[16] 양자정보저장장치를 이용하는 중재자에 의해서 사용자들이 사용할 벨 상태를 공유한다면, 이를 이용하여 두 사용자는 서로 어떠한 고전적인 정보 교환 없이 양자 키 분배와 양자 인증 과정을 수행할 수 있고 사용자들이 얽힘 상태(벨 상태)를 직접 공유해야하는 불편을 해소할 수 있었다. 그러나 기존 프로토콜의 경우 사용자들 간의 중재자 인증 과정(3.2절)만을 가지고 있기 때문에 Eve가 정당한 사용자의 신원으로 위장한 채 중재자에게 벨 상태를 공유 받는다면 [그림 2] 공격자는 키 공유와 인증 과정에서 오류 없이 모든 정보를 얻어 갈 수 있는 Man in the middle 공격 [그림 3,4]이 가능하게 되는 구조적인 문제를 지적하였다. 이 문제의 원인은 중재자가 사용자들에게 벨 상태를 공유 시켜준 후 정당한 사용자인지를 인증하지 않기 때문에 생기는 것이다. 그러므로 본 논문에서 제안된 프로토콜은 중재자에 의한 체크 모드 [그림 5]를 사용하여 사용자들에게 공유 해준 상태를 CHSH 부등식에 의해서 확인하는 [그림 6] 인증 과정을 추가 하여 사전에 도청자의 Impersonation 공격을 차단하는 방법을 사용 하였다. 만일 체크 모드의 사용 없이 기존의 프로토콜을 그대로 사용할 경우 Impersonation 공격에 의한 Man in the middle 공격으로 사용자 사이에 모든 정보가 100% 새어나가는 문제점이 있으므로 본 논문에서 이를 보완하기 위해 제시된 프로토콜은 체크 모드의 사용 [그림 5,6]으로 인해 공격의 유무만 확인 되면 체크 모드 외의 나머지 벨 상태를 가지고 키 분배를 할 수 있다. 특히 기존에 제안된 프로토콜의 장점인 통신 중간에 사용자들끼리의 고전적인 정보 교환 없이 양자 키 분배와 양자 인증을 수행하는 장점을 그대로 살리면서 CHSH 부등식에 의한 체크 모드만 추가하여 문제된 취약성을 보완한 프로토콜이다.

참고문헌

[1] C. H. Bennett and G. Brassard, in Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing (IEEE, New York, 1984), pp. 175.

[2] 홍창호, 이화연, 김지인, 임종인, 양형진, "Entanglement Swapping을 이용한 안전한 직접 통신 프로토콜.", *한국정보보호학회논문지*, 16(1), Feb 2005

[3] H. Y. Lee, J. I. Lim, H. J. Yang, "Quantum direct communication with authentication.", *Phys. Rev. A* 73, 042305, 2006.

[4] C. H. Bennett and G. Brassard, C. Crepeau, R. Jozsa, A. Pres, and W, Wooters, "Teleporting an Unknown quantum state via dual classical and EPR channels.", *Phys. Rev. Lett,* 70:1859 -1899, 1993.

[5] M. D. Barrett, J. Chiaverini, T. Schaetz, J. Britton, "Deterministic Quantum teleportation

of atomic qubits.", *Nature*, 429, 737, 2004.

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

[7] C. Schmid, P. Trojek, M. Brourennance, C. Kurtsiefer, "Experimental single Quantum secret sharing.", *Phys. Rev. Lett*, 95, 230505, 2005.

[8] A. Ekert, "Quantum cryptography based on Bell's Theorem.", *Phys. Rev. Lett*, 67,661, 1999

[9] W. K. Wooters, W. H. Zurek , "A Single Quantum cannot be cloned.", *Nature*, 299:802-803, 1982.

[10] R. J. Hughes, J. E. Nordholt, D. Derekcs, C. G. Peterson, "Practical free-space Quantum key distribution over 10Km in dayright and at night.", *New. Journal. of Phys*, 4, 43 2002.

[11] C. Krutsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Goran, P. R. Tapster, J. G. Rarity, "A step towards global key distribution.", *Nature*, 491:450, 2002.

[12] 이화연, 홍창호, 이덕진, 양형진, 임종인, "인증된 양자 키 분배 프로토콜.", *한국정보보호학회 논문지* 14(2), April 2004.

[13] J. Oppenheim, M. Horodecki, "How to reuse a one time pad other nites on authentication encryption and protection of Quantum information.", *Phys. Rev. A*, 72. 042309, 2005

[14] E. Dennis, A. Kitaev, A. Landahl, J. Preskill, "Topolgical Quantum memories.", *J. Math. Phys*, 43. 4452, 2002.

[15] V. Giovannetti, D. Burgarth, "Improved transfer of Quantum information using a local memory.", *Phys. Rev. Lett*, 96. 030501, 2006.

[16] Bao-sen Shi, Jian Li, Jin-Ming Liu, Xiao-Feng Fan, Guang-Can Guo, "Quantum key distribution and Quantum authentication based on entangled state.", *Phys. Lett, A*, 281:83-87, 2001.

[17] A. Nielsen, L. Chuang, "Quantum computation and Quantum information.", *CAMBRIDGE UNIVERSITY PRESS.*

[18] M. Zukowski, A. Zeilinger, M. A. Horne, A. K. Ekert, "Event-ready-detectors Bell experiment via Entaglement Swapping.", *Phys. Rev. Lett*, 71:4287-4290, 1993.

[19] H. De riedmatten. I. Marcikic, A. W. van Houwelingen, W. Tittel, H. Zbinden, N. Gisin, "Long distance entanglement swapping with photons from separated sources.", *Phys. Rev. A*, 71,050302, 2005.

[20] J. F. Clauser, M. A. Horne, A. Shimony, R. A. Holt, "Proposed experiment to test Local Hidden-Variable theories.", *Phys. Rev. Lett*, 23:880-884, 1969.

[21] J. F. Clauser, M. A. Horne, "Experimental consequences of objective local theories.", *Phys. Rev. D*, 10, 526, 1974.

[22] J. S. Bell, "Speakable and Unspeakable in Quantum Mechanics.", *CAMBRIDGE UNIVERSITY PRESS.*

[23] A. Einstein, B. Podolsky, N. Rosen, "Can Quantum Mechanical description of Physical Reality be considered complete?", *Phys. Rev. Lett*, 47:777-780, 1935.

[24] A. Aspect, P. Grangier, G. Roger, "Experimental tests of Realistic Local Theories via Bell's Theorem.", *Phys. Rev. Lett*, 47:460-463, 1981.

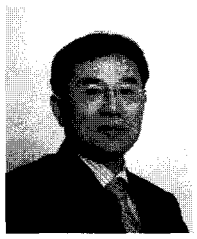
[25] A. Aspect, J. Dalibard, G. Roger, "Experimental tests of Bell's inequalites using time varying analyzers.", *Phys. Rev. Lett*, 49, 1804, 1982.

〈著者紹介〉

허 진 오 (Jin-o Heo) 학생회원
2006년 2월 : 고려대학교 물리학과 학사
2006년 3월~현재 : 고려대학교 정보경영공학전문대학원 석사 과정
<관심분야> 양자 암호, 양자 정보이론, 얽힘 상태

홍 창 호 (Chang-ho Hong) 정회원
2001년 2월 : 고려대학교 물리학과 학사
2003년 2월 : 고려대학교 응용물리대학원 응집물리학과 석사
2005년 2월 : 고려대학교 정보보호대학원 박사 과정 수료
<관심분야> 양자암호, 암호 프로토콜

양 형 진 (Hyoung-jin Yang) 정회원
1990년 8월~1990년 10월 : 미국 Oak Ridge 국립연구소. Computer Consultant
1990년 12월~1991년 12월 : 미국 신시내티 대학원 박사 후 연구원
1999년 1월~1991년 12월 : 미국 메릴랜드대학교 교환교수
1992년 3월~현재 : 고려대학교 디스플레이 반도체 물리학과 교수
2001년 3월~현재 : 고려대학교 정보보호대학원 겸임 교수
<관심분야> 양자 암호, 암호 프로토콜



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