情報保護學會論文誌
第16卷 第6號, 2006. 12

GHZ 상태 교환을 이용한 인증된 양자 비밀 공유

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

[1]고려대학교 정보보호대학원, [2]고려대학교 디스플레이 반도체 물리학과

Authenticated Quantum Secret Sharing using GHZ state swapping

Duk-jin Lee[1†], Hwa-yean Lee, Chang-ho Hong, Jong-in Lim, Hyoung-jin Yang[2‡]

[1]Center for Information Secu

[2]Department of Display Semiconductor, Korea University

요 약

본 논문에서는 GHZ swapping을 이용하여 구성원 수의 절반보다 많은 인증된 사용자가 모이면 비밀을 복원할 수 있는 양자 비밀 공유 프로토콜을 제안한다. 메시지를 분배하는 중재자와 복원하려는 구성원들 사이에 미리 공유된 ID를 이용하여 중재자는 각 구성원을 인증할 수 있으며, 인증 받은 구성원들은 GHZ swapping에 의해 양자비밀공유가 가능해진다. 또한 구성원의 수를 임의의 n명으로 확장하기가 용이하다는 측면에서 고전적인 비밀 공유에 근접한 양자 비밀 공유프로토콜이다.

ABSTRACT

We propose a quantum secret sharing protocol which can authenticate more than half of members using GHZ state swapping. The Trusted Third Party, Trent can authenticate all members using previously shared ID among Trent distributing his message and the members wanting to reconstruct the message. Authenticated members can reconstruct a secret message through GHZ swapping. Moreover, this protocol is efficient to expand the number of members to arbitrary number n, so it is a close quantum secret sharing protocol to classical secret sharing protocol.

Keywords : *GHZ state swapping, Quantum Secret Sharing*

Ⅰ. 서 론

양자 암호는 1984년 Bennett과 Brassard[1]에 의해 처음으로 제안된 키 분배 프로토콜[2-6]을 필두로 지금까지 양자전송[7-10], 양자 통신[11-12], 양자비밀공유[13-15]에 이르기까지 폭넓은 분야에서 연구가 이루어지고 있다. 가장 활발한 연구 성과를 보이는 양자 키 분배 프로토콜은 양자 상태의 붕괴가 확률적이고 무작위적이라는 특징[2,11,16]을 이용하여 완전한 안전성을 보장하고 있다. 이러한 양자 키 분배 프로토콜 분야의 연구는 실험적 구현[17-18]이 활발하게 진행되고 있으며, 보다 다자간의 프로토콜[7,10,12]로 확장되는 과정에서 GHZ[17-18] 상태를 이용한 프로토콜에 대한 연구들이 관심을 끌고 있다. 또한 이 GHZ 상태를 이용하여 키 분배 프로

접수일: 2006년 10월 18일 ; 채택일: 2006년 11월 28일
* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구 결과로 수행하였습니다.
† 주저자, dj325@nate.com
‡ 교신저자, yangh@korea.ac.kr

토콜뿐만 아니라 양자전송, 양자 통신, 양자비밀공유의 분야에서도 다자간의 프로토콜들이 활발히 연구되고 있다.

고전적으로 비밀 공유 프로토콜은 특정 다수가 정보를 나누어 가지고, 구성원의 일부가 모여 그 정보를 다시 복원하는 일련의 과정을 말한다. 양자 비밀 공유 프로토콜은 1999년 Hillery와 Buzek[13]에 최초로 도입되었다. 그러나 이 논문을 비롯하여, 2005년 Zhang[19]의 논문 등등, 대부분의 양자 비밀 공유 프로토콜은 구성원이 단순히 정보를 나눠 가지는 (n,n) 형태를 띠고 있다. 고전적인 개념의 (k,n)(n명의 구성원 중 최소 k명이 모이면 비밀을 복원할 수 있다.) 프로토콜들은 1999년 Cleve[15]가 제시하긴 했지만 해당 논문에서는 (k,n) 프로토콜이 가져야 하는 일반적인 이론들을 정리하였을 뿐 본 논문과 같이 구체적인 프로토콜에 대하여 기술하지는 않았다.

본 논문에서, 우리는 $(n+1,2n)$ 양자 비밀 공유 프로토콜을 제안한다. Cleve가 일반적으로 막연하게 제시했던 (k,n) 프로토콜에 대한 구체적인 방법을 제시하고 있으며, 기존의 양자 비밀 공유와 달리 비밀을 전송할 때부터 사용자를 인증하고 이를 확인하기 때문에, 복원된 비밀이 외부로 유출되지 않으며, 최소의 인원으로 비밀을 복구할 수 있는 특징이 있다. 2절에서는 프로토콜에 사용되는 기본 개념들을 설명하고, 3절에서는 $(3,4)$ 양자 비밀 프로토콜과 $(n+1,2n)$ 양자 프로토콜을 제안한다. 4절에서는 제안된 프로토콜의 안전성을 분석하고 6절에서는 결론을 제시한다.

Ⅱ. GHZ 상태 얽힘 교환 (GHZ states swapping)

얽힘 상태[20]란 두 개의 양자 상태가 얽혀서 독립적으로 분리될 수 없는 상태를 말한다. 하나의 양자 상태 Ψ는 일반적으로 $(\alpha|0>+\beta|1>)$으로 표현된다. 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 이룬다. 이러한 큐빗이 두 개가 얽힌 $\frac{1}{\sqrt{2}}(|00>+|11>)$ 식을 생각해보자. 이 상태는 두 양자 상태가 텐서 곱(tensor product)된 $\psi\otimes\phi$ 형태로 나타낼 수 없다. 즉, $\frac{1}{\sqrt{2}}(|00>+|11>)\neq(\alpha_1|0>+\beta_1|1>)\otimes(\alpha_2|0>+\beta_2|1>)$와 같이 양자상태를 분리 할 수 없다. 자세한 설명을 위해 두 큐빗이 얽혀 있는 얽힘상태 네 개를 생각해보자. 이 상태는 양자역학에서 잘 알려진 벨 상태로써 각각이 얽힘상태에 있을 뿐만 아니라 서로 직교관계에 있다.

$$|\Phi^+>_{ij}\equiv\frac{1}{\sqrt{2}}(|00>_{ij}+|11>_{ij}) \quad (1)$$

$$|\Phi^->_{ij}\equiv\frac{1}{\sqrt{2}}(|00>_{ij}-|11>_{ij}) \quad (2)$$

$$|\Psi^+>_{ij}\equiv\frac{1}{\sqrt{2}}(|01>_{ij}+|10>_{ij}) \quad (3)$$

$$|\Psi^->_{ij}\equiv\frac{1}{\sqrt{2}}(|01>_{ij}-|10>_{ij}) \quad (4)$$

GHZ 상태[21-22]란 위와 같은 얽힘 상태가 세 개 이상의 큐빗에 대하여 일어나는 상태를 말한다. 위와 마찬가지로 $\frac{1}{\sqrt{2}}(|000>+|111>)$ 식을 생각해보자. 이 상태 역시 $\psi\otimes\phi\otimes\rho$ 형태로 나타낼 수 없다. 즉, $\frac{1}{\sqrt{2}}(|000>+|111>)\neq(\alpha_1|0>+\beta_1|1>)\otimes(\alpha_2|0>+\beta_2|1>)\otimes(\alpha_3|0>+\beta_3|1>)$이다. 이러한 상태를 GHZ 상태라고 한다.

GHZ 상태 교환은 그림 1에서 볼 수 있듯이 두 개의 GHZ 상태 각각에서 취한 두 개의 큐빗 1번과 4번 큐빗에 대하여 벨 측정[20]을 수행하면 이 측정을 통해 이전에는 얽혀 있지 않던 네 개의 2번, 3번, 5번, 6번 큐빗들이 얽힘 상태를 이루는 현상이다.

그럼 이제 두 개의 GHZ 상태가 텐서 곱으로 연결되어 있는 다음과 같은 상태를 생각해보자.

$$\frac{1}{\sqrt{2}}(|000>_{123}+|111>_{123})\otimes\frac{1}{\sqrt{2}}(|000>_{456}+|111>_{456}) \quad (5)$$

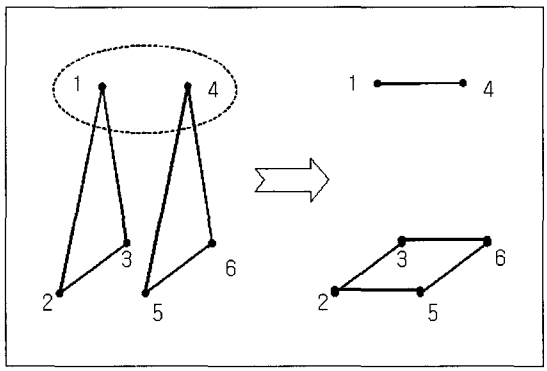
위 식을 전개하면

$$\frac{1}{2}(|000000>_{123456}+|000111>_{123456}+|111000>_{123456}+|111111>_{123456}) \quad (6)$$

이 된다. 여기서 1번, 4번 큐빗을 교환하여 위의 식 (1),(2),(3),(4)의 양자 상태로 결과값을 이끌어 내는 벨 측정을 하게 되면

$$\frac{1}{2}(|000000>_{142356}+|010011>_{142356}+|101100>_{142356}+|111111>_{142356})$$
$$=\frac{1}{2}((|00>+|11>)_{14}(|0000>+|1111>)_{2356}+(|00>-|11>)_{14}(|0000>-|1111>)_{2356}+(|01>-|10>)_{14}(|0011>+|1100>)_{2356}+(|01>-|10>)_{14}(|0011>-|1100>)_{2356}) \quad (7)$$

와 같은 결과가 나오게 된다. 즉, 두 개의 GHZ 상태 각각에서 한 큐빗씩을 취하여 이 두 큐빗에 국소적인 벨 측정을 수행하면 나머지 네 개의 큐빗들도 또 다른 GHZ 상태를 이루게 되는데 새로 생성된 GHZ 상태 사이에는 강한 상관관계가 나타난다. 이는 [그림 1]과 같은 도식으로 표현할 수 있다.



[그림 1] GHZ상태 얽힘 교환. 여기서 1,2,3,4,5,6은 큐빗 번호를 나타내며 선으로 연결된 큐빗은 서로 얽혀 있는 GHZ 상태 임을 나타낸 것이다. 초기에 1-2-3 과 4-5-6 GHZ 상태가 국소적인 1-4 벨 측정을 통해 2-3-5-6의 GHZ 상태로 변환된다[23].

본 논문의 프로토콜 설명에 앞서 사용되는 내용을 좀 더 자세히 이해하기 위해서 Hadamard 변환과 Pauli σ_x변환에 대해서 간단히 설명하겠다. Hadamard 연산은 양자상태를 바꿔주는 연산으로 다음과 같은 연산을 한다.

$$H=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \quad (8)$$

$$H|0>\geq\frac{1}{\sqrt{2}}(|0>+|1>) \quad (9)$$

$$H|1>\geq\frac{1}{\sqrt{2}}(|0>-|1>) \quad (10)$$

즉, $|x\pm>\geq\frac{1}{\sqrt{2}}(|0>\pm|1>)$ 라는 양자상태가 Hadamard 변환을 거치면 $H|x+>\geq|0>$, $H|x->=|1>$ 라는 결과가 나오게 된다. 결과적으로 Hadamard 변환은 측정되는 큐빗의 양자상태를 바꿔준다. 또한, Hadamard는 Unitary[20] 변환이므로 $HH=I$ 가 성립한다.

Pauli σ_x변환은 bit flip을 일으키는 연산으로 다음과 같이 작용한다.

$$\sigma_x=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} \quad (11)$$

$$\sigma_x|0>=|1> \quad (12)$$

$$\sigma_x|1>=|0> \quad (13)$$

Ⅲ. 인증된 양자 비밀 공유 프로토콜

이 절에서는 중재자인 Trent가 비밀 메시지를 생성하여 네 명의 인증된 사용자 Alice, Bob, Charlie, David에게 전달 후, 이 들 중 세 명 이상이 모였을 경우 그 비밀 메시지를 복원할 수 있도록 하는 양자 비밀 공유 프로토콜을 제안하겠다. 프로토콜은 식(1)~식(4)을 기저로 하는 벨 측정을 사용하며 식 (7)의 벨 측정결과에 따른 얽힘 교환의 결과를 이용한다. 또한 본 프로토콜은 중재자의 비밀을 나누어 가진 n명의 사용자들 중에서 최소 $\frac{1}{2}n+1$명이 모여서 원래의 비밀 메시지를 복원할 수 있다. 우선 네 명 중 세 명의 구성원이 모여서 비밀 공유에 성공하는 (3,4) 프로토콜을 보인 후, $(n+1,2n)$ 프로토콜로 확장하도록 하겠다.

프로토콜은 크게 비밀 메시지를 분배하는 과정과 복원하는 과정으로 나눌 수 있다.

3.1 중재자로부터 메시지 분배 과정

우선 메시지를 분배하는 과정을 살펴보자.

1) 중재자 Trent는 각각의 구성원 Alice, Bob, Charlie, David 와 BB84와 같은 기존의 양자 키분배 프로토콜을 이용하여 $2N$ 비트의 2진수 ID를 공유한다. 이 ID는 중재자와 구성원 사이의 비밀 정보값이다. ID의 형태는 $ID(Alice)=0_1 1_2 1_3 \ldots\ldots 0_{2N}$와 같은 이진 비트 수열이다.

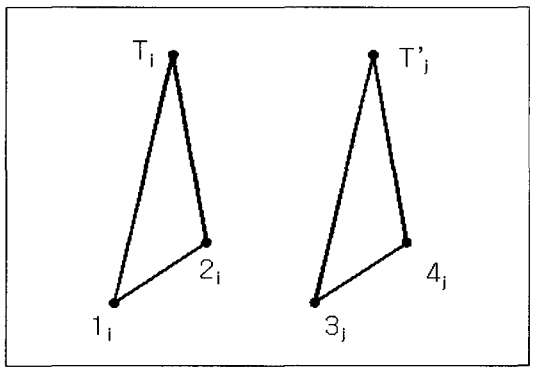
2) Trent는 통신에 사용되는 2N개의 아래와 같은 GHZ 상태 $\{\psi_1,\psi_2,\ldots,\psi_{2N}\}$를 준비한다.

$$\psi_i=\frac{1}{\sqrt{2}}(|000>+|111>) \quad (14)$$

3) Trent는 2N 개의 GHZ 상태를 두 개씩 묶어 N개의 GHZ 상태 쌍을 만들며, 각각의 GHZ 상태 쌍 Ψ_k에서 k는 1부터 N 까지의 번호를 가지게 된다.

$$\Psi_k=(\psi_i,\psi_j) \quad (15)$$

$(1\le k\le N, 1\le i\le 2N, 1\le j\le 2N)$



〔그림 2〕 GHZ상태 쌍 $\Psi_k=(\psi_i,\psi_j)$

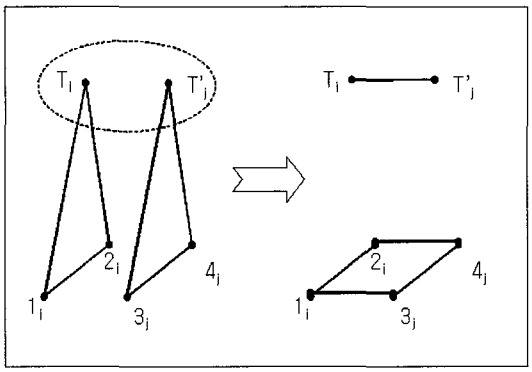
4) 〔그림 2〕에서 보듯이 모든 N개의 GHZ 상태 쌍 Ψ_k에 대하여 Trent는 각 GHZ 에서 하나씩 큐빗 T_i, T_j'을 갖고 나머지 네 큐빗 1_i, 2_i, 3_j, 4_j 는 각각의 사용자 ID를 담아 사용자에게 무작위로 전달한다. 예를 들어 보내주는 각 큐빗에 해당하는 번호 k를 각 구성원의 ID와 비교하여 해당 번호의 ID 가 1이면 Hadamard gate를 취하고 0인 경우에는 I 연산을 취해서 보낸다. 즉, Alice의 ID가 $ID(Alice)=0_1 1_2 1_3 \ldots\ldots 0_{2N}$라고 하면, Trent는 Alice에게 보내려고 하는 두 번째, 세 번째의 비트가 1인 순번의 큐빗들에 Hadamard gate를 취하고 나머지에는 I 연산을 취해서 보내준다.

5) 각 사용자들은 자신들이 가지고 있는 ID에 따라 해당 큐빗에 Hadamard 변환을 취하거나 취하지 않음으로써 Trent 가 보낸 큐빗을 원래의 GHZ 상태로 복원한다. 예를 들어 $k(k\le N)$번째 큐빗에 대하여 자신의 ID의 k번째 비트가 1일 경우 큐빗을 받은 후 Hadamard 변환을 취해주고, 0일 경우에는 그냥 큐빗을 받는다. 그럴 경우 $HH=I$ 이므로 원래의 상태가 복원된다.

6) Trent와 각 구성원들이 모든 GHZ 상태 쌍 $\Psi_k=(\psi_i,\psi_j)$ 을 나누어 가진 후, Trent는 모든 큐빗이 올바르게 전송되었는지를 확인하기 위해서 자신이 가지고 있는 N 개의 T_i-T_j'의 큐빗 쌍 중 임의의 m개에 대하여 벨 측정을 한 후, 모든 사용자에게 m $(m\le N)$ 개의 임의의 숫자를 알려준다. 각 구성원은 그 숫자에 해당하는 자신들의 큐빗에 대하여 국소적 측정을 취해서 그 결과값들을 Trent에게 알려준다. Trent는 자신의 벨 측정값과 사용자들이 보내온 국소적 측정값들을 비교함으로써 채널상에 도청자 존재 여부를 확인한다.

7) 중간에 도청자가 없이 모든 큐빗이 구성원에게 분배되었다고 판단이 되면, Trent는 도청확인을 위해 사용한 m개의 큐빗 쌍을 제외한 나머지 $N-m$쌍의 큐빗들에 σ_x변환을 취해주느냐 마느냐에 따라 $N-m$ bit의 메시지를 encoding 할 수 있다. 예를 들어 자신이 보내주려는 비밀 정보가 1001 이라고 가정하면, 첫 번째와 네 번째 GHZ 쌍 Ψ_1과Ψ_4에 대하여 자신이 가지고 있는 큐빗 T_i와 T_j' 중 하나의 큐빗에 σ_x 변환을 취해준다. 이렇게 변환을 거친 GHZ 쌍 Ψ_1과Ψ_4의 결과는 변환을 거치지 않은 쌍 Ψ_2과Ψ_3과 비교하여 다른 결과를 가지게 된다. Trent가 자신의 큐빗에 I 연산을 취했을 경우, Trent의 벨 측정결과에 따른 Alice,

Bob, Charlie, David가 얻게 될 결과값들은 식 (16)과 같이 나타낼 수 있다.



〔그림 3〕 T_i-T'_j벨 측정에 따른 GHZ상태 얽힘 교환. 여기서 1_i, 2_i, 3_j, 4_j 큐빗들은 식 (16)과 같은 국소적 측정값들을 가지게 된다.

$$\frac{1}{2}(|000000>_{T_i1_i2_iT'_j3_jA_j}+|010011>_{T_i1_i2_iT'_j3_jA_j}$$
$$+|101100>_{T_i1_i2_iT'_j3_jA_j}+|111111>_{T_i1_i2_iT'_j3_jA_j})$$
$$=\frac{1}{2}((|00>+|11>)_{T_iT'_j}(|0000>+|1111>)_{1_i2_i3_jA_j}$$
$$+(|00>-|11>)_{T_iT'_j}(|0000>-|1111>)_{1_i2_i3_jA_j}$$
$$+(|01>-|10>)_{T_iT'_j}(|0011>+|1100>)_{1_i2_i3_jA_j}$$
$$+(|01>-|10>)_{T_iT'_j}(|0011>-|1100>)_{1_i2_i3_jA_j})$$
(16)

σ_x 변환을 시켰을 경우, 식 (16)은 다음과 같이 변하게 된다. (T_i을 변환 시켰다고 가정)

$$\frac{1}{2}(|100000>_{T_i1_i2_iT'_j3_jA_j}+|110011>_{T_i1_i2_iT'_j3_jA_j}$$
$$+|001100>_{T_i1_i2_iT'_j3_jA_j}+|011111>_{T_i1_i2_iT'_j3_jA_j})$$
$$=\frac{1}{2}((|10>+|01>)_{T_iT'_j}(|0000>+|1111>)_{1_i2_i3_jA_j}$$
$$+(|10>-|01>)_{T_iT'_j}(|0000>-|1111>)_{1_i2_i3_jA_j}$$
$$+(|11>-|00>)_{T_iT'_j}(|0011>+|1100>)_{1_i2_i3_jA_j}$$
$$+(|11>-|00>)_{T_iT'_j}(|0011>-|1100>)_{1_i2_i3_jA_j})$$
(17)

8) 자신이 보내려는 비밀 정보에 따라 σ_x 변환을 취해준 후, GHZ 쌍에서 자신이 가지고 있는 두 큐빗들에 벨 측정을 수행한다. 이와 동시에 각 사용자들의 국소적인 측정 값들은 〔그림 3〕과 같이 양자 얽힘 교환에 의해 정해지게 된다.

지금까지 믿을만한 중재자인 Trent가 메시지를 분배하는 과정을 살펴보았다. 다음 절에서는 네 명의 사용자 중에서 세 명만이 모여서 Trent의 메시지를 복원하는 과정을 살펴보겠다.

복원 과정은 다시 인증 단계와 메시지 복원과정으로 나뉘게 된다. 사용자 인증 과정에서 사용되는 ID는 전체 $2N$ 비트 중에서 N+1부터 $2N$ 비트 까지를 사용할 것이다.

3.2.1 사용자 인증 과정

1) 네 명의 구성원 중 Alice, Bob, Charlie만이 모여서 Trent의 메시지를 복원하고자 하는 경우 Trent에게 세 명이 모였음을 알린다.
2) Trent는 각 세 명이 정당한 사용자인가를 인증하기 위하여 N+1부터 $2N$ 까지의 숫자 중 분배 과정에서 도청확인을 위해 사용한 m개의 숫자를 제외한 나머지 중에서 임의로 선택된 h $(1 \leq h \leq N-m)$ 개의 숫자를 각 사용자에게 알려준다.

〔표 1〕 ID를 통한 사용자 인증

Trent의 checking number		N+2			N+5			N+23			
Alice의 ID	1_{N+1}	0_{N+2}	1_{N+3}	0_{N+4}	0_{N+5}	.....	0_{N+22}	0_{N+23}	.....	1_{2N-1}	1_{2N}
Alice의 국소적 측정결과값	0_1	0_2	0_3	0_4	1_5	.....	0_{22}	1_{23}	.....	1_{N-1}	0_N
배타적 논리합 결과값		0			1			1			

〔표 2〕 Trent의 벨 측정에 따른 각 사용자의 국소적 측정 값

Trent가 취하는 변환	Trent의 벨 측정 값	구성원이 갖게 되는 GHZ 상태
I	$\|\Phi^{\pm}>_{ij}$	$\frac{1}{\sqrt{2}}(\|0000>\pm\|1111>)_{ABCD}$
	$\|\Psi^{\pm}>_{ij}$	$\frac{1}{\sqrt{2}}(\|0011>\pm\|1100>)_{ABCD}$
σ_x	$\|\Phi^{\pm}>_{ij}$	$\frac{1}{\sqrt{2}}(\|0011>\pm\|1100>)_{ABCD}$
	$\|\Psi^{\pm}>_{ij}$	$\frac{1}{\sqrt{2}}(\|0000>\pm\|1111>)_{ABCD}$

〔표 3〕 Trent의 벨 측정에 따른 각 사용자의 메시지 복원

구성원이 갖게 되는 GHZ 상태	Trent의 벨 측정 값	Trent가 취해준 변환
$\frac{1}{\sqrt{2}}(\|0000>\pm\|1111>)_{ABCD}$	$\|\Phi^{\pm}>_{ij}$	I
$\frac{1}{\sqrt{2}}(\|0011>\pm\|1100>)_{ABCD}$	$\|\Psi^{\pm}>_{ij}$	
$\frac{1}{\sqrt{2}}(\|0011>\pm\|1100>)_{ABCD}$	$\|\Phi^{\pm}>_{ij}$	σ_x
$\frac{1}{\sqrt{2}}(\|0000>\pm\|1111>)_{ABCD}$	$\|\Psi^{\pm}>_{ij}$	

3) 세 명의 사용자는 Trent로부터 받은 h개의 숫자에 해당하는 자신들 ID의 고전 비트수 h개와 그 순서에 해당하는 국소 측정값 h개를 배타적 논리합(exclusive OR)계산한다. 예를 들어 Trent가 $N+2$, $N+5$, $N+23$,.....라는 숫자 h개를 보냈다고 가정하면 자신들이 가지고 있는 ID의 네 번째, $N+2$ 번째, $N+5$ 번째, $N+23$ 번째 비트와 2번, 5번, 23번 큐빗의 국소 측정 결과값들의 배타적 논리합을 계산한다. 그리고 그 결과값을 Trent 에게 보내준다. 표 1은 Alice의 경우를 예를 들어 설명한 것이다. Alice는 Trent에게 배타적 논리합의 결과값 0, 1, 1,....(h개)를 보내준다.

4) Trent는 각 GHZ 쌍 Ψ_k의 벨 측정값을 가지고 있으며, 자신이 보내준 메시지에 따라 어떤 k에 encoding을 했는지 알고 있다. 따라서 Trent가 얻게 되는 벨 측정값과 자신이 취해준 변환에 대해서 알고 있으면 구성원이 얻게 될 국소적 측정값이 모두 동일한지 동일하지 않은 지를 판단할 수 있다. 이는 표 2를 보면 쉽게 구분할 수 있다. 또한 각 사용자의 ID를 가지고 있으므로, 사용자들이 보내는 배타적 논리합 결과값에 각 사용자의 ID를 다시 배타적 논리합 계산을 수행하면, 사용자들의 국소적 측정값을 알 수 있게 된다. 이를 통해 세 명이 정당한 사용자임을 인증할 수 있다.

3.2.2 메시지 복원 과정

1) Trent는 각 사용자가 정당한 사용자임을 확인하고 난 후, 자신의 벨측정 결과값들을 모두에게 공개한다.

2) Alice, Bob, Charlie는 Trent가 공개한 벨 측정 결과값들과 자신들이 가지고 있는 국소적인 측정값들을 비교함으로써 Trent의 비밀 메시지를 복원할 수 있다. 예를 들어, 임의의 순번의 큐빗에 대하여 자신들의 측정값이 모두 0000으로 같게 나왔다고 가정해보자. 표 1에서 보이듯이 이 때, 이들 구성원이 예상할 수 있는 Trent의 벨 측정 결과값은 $|\Phi^{\pm}>_{ij}$일 것이다. 그러나 Trent가 발표한 값이 $|\Psi^{\pm}>_{ij}$라고 한다면, 이들은 Trent가 σ_x변환을 해주었다는 사실을 유추할 수 있으며 Trent의 비밀 메시지는 고전 정보 1 비트가 된다는 것을 알 수 있다.

3.3 임의의 $2n$명으로 구성원 확장

본 프로토콜은 GHZ 상태를 늘리기만 하면 구성원의 수를 임의로 확장시키기 쉽다는 장점을 가진다. 세 개의 큐빗을 가지는 GHZ 상태 쌍으로 4명 중 3명 이상이 비밀을 복원할 수 있는 프로토콜을 만드는 방법과 같은 방법으로 $n+1$ 개의 큐빗을 가지는 GHZ 상태 쌍으로 n명 중 $n+1$명 이상이 비밀을 복원할 수 있는 프로토콜로 확장시킬 수 있다. 이는 기존의 양자 비밀 공유 기법들이 대부분 $2n$명이 나누어가진 정보를 복원하기 위해 $2n$명이 전부 모여야 하는 단점을 크게 개선한 부분이다. 그러나 $2n$명으로 확장시킨 프로토콜에서는 Trent의 벨 측정 결과값들이 완전 공개가 아닌 사용자들의 ID를 이용하여 변환시켜 준다.

우선 벨 측정 결과값 공개 이전의 과정은 다음과 같다.

중재자인 Trent는 $n+1$ 개의 큐빗을 가지는 GHZ 상태를 2N 개 준비한다. 하나의 GHZ 쌍은 다음과 같다.

$$\frac{1}{\sqrt{2}}(|000...0>_{123...(n+1)}+|111...1>_{123...(n+1)}) \otimes \frac{1}{\sqrt{2}}(|000...0>_{1'2'3'...(n+1)'}+|111...1>_{1'2'3'...(n+1)'}) \quad (18)$$

식 (18)을 전개하여 얽힘 교환을 계산하면 다음과 같다.

$$\begin{aligned}&\frac{1}{2}(|00...0>_{11'23...(n+1)2'3'...(n+1)'}\\&+|01000...0111...1>_{11'23...(n+1)2'3'...(n+1)'}\\&+|10111...1000...0>_{11'23...(n+1)2'3'...(n+1)'}\\&+|11...1>_{11'23...(n+1)2'3'...(n+1)'})\\&=\frac{1}{2}((|00>+|11>)_{11'}(|0...00>+|1...11>)_{23...(n+1)2'3'...(n+1)'}\\&+(|00>-|11>)_{11'}(|0...00>-|1...11>)_{23...(n+1)2'3'...(n+1)'}\\&+(|01>-|10>)_{11'}(|0..01..1>+|1..10..0>)_{23...(n+1)2'3'...(n+1)'}\\&+(|01>-|10>)_{11'}(|0..01..1>-|1..10..0>)_{23...(n+1)2'3'...(n+1)'})\end{aligned} \quad (19)$$

큐빗의 분배 확인 및 사용자 인증하는 과정까지는 (3,4) 프로토콜과 동일하다. 그럼 이제, Trent가 벨 측정 값들을 공개하는 부분을 살펴보자. Trent는 자신이 측정한 벨 측정값들에 대하여 $|\Phi^{\pm}>_{11'}$인 경우 0으로, $|\Psi^{\pm}>_{11'}$인 경우 1로 encoding하여 각 사용자들의 $N+1$비트부터 $2N$비트의 ID와 배타적 논리합을 시켜준 후 각 사용자에게 개별적으로 보내준다. 이 때, 처음 큐빗 상태 분배를 위해 사용한 m개의 비트는 제외한다. 각 사용자들은 Trent가 보내주는 값에 자신들의 $N+1$ 비트부터 $2N$ 비트까지의 ID를 배타적 논리합 시키면 Trent의 벨 측정 결과 값을 얻게 된다.

비밀을 복원하고자 하는 구성원들은 각자 Trent로부터 받은 벨 측정값이 동일한가를 확인하고 자신들의 국소적 측정값들을 비교함으로써 Trent의 σ_x 변환에 의한 메시지 값을 판단할 수 있다.

Ⅳ. 안전성

이 프로토콜에서 공격자는 전송되는 큐빗들에만 접근할 수 있다. 안전성을 살펴보기 위하여 우선 도청자가 중재자로부터 분배되는 큐빗을 가로채는 경우에 대하여 생각해보자. 또한 양자 비밀 공유의 중요한 성질인 절반보다 많은 구성원이 모여야 비밀을 복원할 수 있다는 기본적인 안전성에 대해서도 살펴보자. 중재자로부터 각 사용자에게 GHZ 상태가 분배되는 과정에서 생길 수 있는 채널 상에서의 에러 등은 privacy amplification 및 entanglement distillation[24-28]등을 이용하여 보정한다.

4.1. 도청자가 중재자로부터 분배되는 큐빗을 가로채는 경우

중재자가 GHZ 쌍을 만들어서 각 사용자들에게

무작위로 해당 큐빗을 날려주는 과정에서 도청자가 모든 큐빗 혹은 그 중 일부를 가로채서 사용자가 받은 것처럼 위장하려는 경우를 생각해 보자. 이 경우 전송되는 큐빗은 사전에 분배된 개인 ID에 의하여 Hadamard gate를 통해 변환된 상태이므로 ID를 가지고 있지 않은 사용자는 올바른 양자상태를 받을 수가 없다. 도청자가 하나의 큐빗에 대하여 올바른 양자상태를 받을 수 있는 경우는 Hadamard 변환 여부를 임의로 판단하는 방법밖에 없다. 도청자가 올바르게 Hadamard 연산을 취할 확률은 각 큐빗에 대하여 1/2이므로 모든 큐빗에 대하여 $(1/2)^N$의 확률을 가진다. 또한 네 명의 큐빗을 모두 가로채고자 한다면 이 확률은 $(1/2)^{4N}$이 될 것이며, 임의의 n명이 비밀 공유를 이루는 프로토콜을 생각한다면 확률은 $(1/2)^{nN}$으로 매우 작아질 것이다. 또한 이를 통과 했다고 가정하더라도 중재자가 자신의 벨 측정값을 공개하기 이전에 ID를 통한 인증이 다시 이루어지므로 공격자는 정당한 사용자들의 ID와 올바른 양자상태 변환을 이용한 측정 결과값 없이는 인증을 통과할 수 없다.

또한, 도청자가 분배되는 큐빗을 가로채지 않고 그 큐빗들에 대하여 임의의 큐빗을 걸어서 C-Not 변환[23]을 통해 그들이 갖게 되는 값을 똑같이 얻을 수 있는 경우에 대해서 생각해 볼 수 있다. 그러나 이 경우 역시, 나누어 가지는 큐빗의 정확한 양자상태를 알 수 없으면 자신이 걸어 놓은 사용자들의 큐빗에 대하여 올바른 값을 측정할 수 없으므로 도청자는 원하는 값을 얻을 수가 없다.

각 사용자들을 인증하는 과정에서 도청자가 중간자 공격(man in the middle attack)을 시도하는 경우에 대해서 생각해 보자. 사용자들이 Trent에게 자신의 국소적 측정값의 결과를 알려주는 과정에서 도청자가 그 정보를 가로채는 경우에 대해서 생각해 볼 수 있다. 그러나 이 역시 Trent에게 전송되는 정보는 측정값과 구성원들의 ID를 배타적 논리합 결과값이므로 ID가 없다면 이 측정치를 알아낼 수가 없다. 따라서 도청자가 가로채서 자신이 만든 임의의 결과를 보낸다고 하더라도 Trent가 쉽게 도청을 알아 낼 수 있다.

4.2 절반보다 작은 수의 구성원이 복원을 하려고 하는 경우

이 프로토콜의 핵심은 중재자의 비밀을 복원하려는 구성원들이 전부 같은 국소 측정값을 가지느냐 적어도 한 명은 다른 결과값을 가지느냐를 비교하는 것이다. 식 (7)을 살펴보았을 때 임의의 두 명이 모였는데 서로 다른 값을 가진다고 가정해보자. 이럴 경우 적어도 그 비트에 대해서만큼은 두 명이서도 Trent의 메시지를 복원할 수 있는 것이 아니냐고 물을 수 있을 것이다. 그러나 Trent는 자신의 결과값을 공개하기 이전에 사용자들에 관하여 인증과정을 거치기 때문에 정당한 인증자가 아닐 경우 자신의 벨측정값 공개를 거부하면 된다.

우선 임의의 두 명이 하나의 GHZ 쌍에 대하여 서로가 양자 얽힘 교환이 이루어지기 이전에 같은 GHZ 상태에 있었는지 그렇지 않은지를 알 경우 서로의 결과값이 언제나 동일한지 동일하지 않은 지를 유추하려고 하는 경우에 대하여 생각해 볼 수 있다. 그러나 Trent는 하나의 GHZ 쌍의 네 개의 큐빗을 무작위하게 각 사용자에게 나누어 주기 때문에 서로가 같은 어떤 GHZ 상태에 속해 있는 지를 구별할 수 없다. 따라서 누가 어떤 GHZ 상태에 속해 있었는지는 오직 Trent 만이 알고 있으므로 각 사용자는 누가 자신과 의미를 가지는 큐빗을 가졌는지를 정확히 알 수 가 없다.

그렇다면 (3,4) 프로토콜에서 임의의 두 명이 서로 다른 결과값을 가졌다고 가정 했을 때, 부분 정보를 노출 할 수 있는 경우를 생각해 보자. 이 부분은 1999년 Cleve가 제시했던 논문 중에 (3,4)프로토콜을 설명하는 부분에서 access structure를 구성하는 단계에서 그러한 문제를 피할 수 있다고 말하고 있다. 즉, 식 (16)이나 (17)에 의하면 특정 두 큐빗 만으로 부분 정보가 노출 될 우려가 있으나 Trent가 사용자들의 모임 여부를 확인할 수 있는 인증과정이 있기 때문에 임의의 두 사용자 만으로는 Trent의 비밀값을 복원할 수가 없다.

나중에 임의의 $2n$명으로 확정을 하였을 경우에는 참여하지 않은 자가 보다 높은 확률로 Trent의 메시지를 유추할 수 있다. 그렇기 때문에 $2n$명일 경우에는 Trent가 벨 측정값을 각 사용자들의 ID에 배타적 논리합을 취해준 결과값을 개별적으로 보내줌으로써 참여하지 않은 사람이 Trent의 메시지를 복원할 수 없도록 하였다.

물론 이러한 확률적인 부분은 사용자들의 ID와 국소적 측정결과 값들의 배타적 논리합의 결과를 Trent에게 인증 받는 부분을 제외 한 채 생각한 것이므로 인증과정이 도입된 후에는 확률적으로 유추를

한다고 하더라도 ID가 없으므로 Trnet의 인증을 통과할 수가 없다. 그러므로 절반보다 작은 수의 구성원이 메시지를 복원할 수 없다.

V. 다른 비밀 공유 프로토콜과의 비교

본 논문과 같이 양자 비밀 공유에 대한 여러 프로토콜들이 제안되어 있다. 그 중에서 최근 Zhang과 Li가 개발한 다자간 양자 비밀 공유 프로토콜[28]과 그 장단점을 비교해 보자. Zhang과 Li의 대략적인 프로토콜은 다음과 같다.

우선 세 명이서 양자 비밀 공유에 성공함을 보인 후, 다자간의 프로토콜로 확장 시키겠다.

(1) Alice는 비밀 메시지를 Bob과 Charlie에게 보내려고 한다.

(2) Bob은 N 개의 단일 큐빗을 준비해서 Charlie에게 보낸다. 이 때, 그 큐빗은 네 개의 양자 상태 $|H>=|0>$, $|V\geq|1>$, $|u\geq\frac{1}{\sqrt{2}}(|0>+|1>)$, $|v\geq\frac{1}{\sqrt{2}}(|0>-|1>)$ 중 임의의 한 상태를 가진다.

(3) Charlie는 이 큐빗들을 받아서 세 개의 Unitary operator I, U, U_H 중 하나를 무작위로 선택해서 각 큐빗에 연산을 취해준 후, Alice에게 보낸다. 여기서 각 변환들은 다음과 같다.

$$I=\begin{pmatrix}1&0\\0&1\end{pmatrix},\ U=\begin{pmatrix}0&1\\-1&0\end{pmatrix},\ U_H=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}$$

(4) Alice는 무작위로 일부의 큐빗을 선택하고 나머지는 저장한다. 그리고 그 선택된 큐빗들의 위치를 공개한다. 즉, 1부터 N까지의 큐빗 중 무작위로 선택된 큐빗들의 번호를 공개한다. Alice는 선택된 그 큐빗들에 대하여 각각 다음의 두 가지 행위 ①, ② 중 하나를 무작위로 선택한다. ① : Bob이 그 해당 큐빗의 초기 상태를 공개한 후, Charlie가 그 큐빗에 어떤 Unitary 변환이 취해졌는지를 공개하게 한다. ② : Charlie 가 먼저 해당 큐빗에 대한 Unitary 변환을 공개하고 Bob이 그 해당 큐빗의 초기 상태를 공개하게 한다. 그 후, Alice는 그 해당 큐빗들에 대하여 Charlie가 공개한 unitary 변환을 취해주고 Bob이 공개한 초기 상태를 사용해 그 큐빗을 측정한다. 측정이 끝나면, Alice는 에러 비율을 확인함으로써 채널상에 도청자가 있었는지를 확인할 수 있다.

(5) 도청자가 없음을 확인한 후, Alice는 자신의 비밀을 encoding하기 위해 저장한 큐빗들에 대해 Unitary 변환 I 혹은 U 를 취해 준다. 2진 비트 0을 encoding하고 싶을 경우 자신의 큐빗에 I 연산을 취해주고, 1을 encoding하고 싶을 경우 U 연산을 취해 준다. 자신의 메시지를 encoding 한 후, 그 큐빗들을 Charlie에게 전달한다.

(6) Charlie가 큐빗을 받은 후, Bob과 Charlie가 서로 협력해야만 encoding된 큐빗에 대하여 정확한 측정 basis를 사용해 Alice의 비밀 메시지를 복원할 수 있다.

(7) Alice는 공개적으로 자신의 비밀의 일부를 노출함으로써 Charlie에게 encoding된 큐빗이 전달되는 과정에서 도청이 없었음을 확인시킨다.

이 프로토콜을 임의의 n명이 참여하는 (n,n)으로 확장시키기 위해서는 위 방법에서 Charlie가 하는 역할을 임의의 $n-2$명으로 늘려야 한다. 즉, Bob으로부터 받은 큐빗을 Charlie가 위의 과정처럼 수행한 후, 그 큐빗을 David에게 전달해서, 그 역시 Charlie와 같은 과정을 수행한 후, 다음 사람에게 전달한다. 이렇게 참여자를 늘려 마지막 $n-2$번째인 Zach가 그 큐빗에 같은 단계를 적용한 후, Alice에게 보낸다. 이 후의 과정은 위와 동일하다. 결과적으로 Alice의 encoding된 비밀 메시지를 복원하기 위해서는 Bob, Charlie,...Zach가 전부 모여서 협력해야만 한다.

본 논문에서 제안하는 비밀 공유 프로토콜과 위에서 설명한 Zhang과 Li의 비밀 공유 프로토콜을의 장단점을 비교해 보자.

Zhang과 Li의 프로토콜은 Alice의 비밀 메시지를 복원하기 위해 구성원이 전부 모여야만 하는 $[n,n]$ 비밀 공유 프로토콜이다. 참여자를 n명으로 늘리는 과정을 위해서 같은 (3)과정을 반복하는 참여자를 삽입하는 방법을 사용한다. 그러나 이러한 과정은 점점 더 많은 채널을 생성하게 만드는 결과를 만들어 낸다. 인위적인 공격자가 없다고 하더라도 채널 자체에서 오는 손실이나 오류가 발생할 가능성이 그만큼 많아지게 된다. 그러나 본 논문의 프로토콜은

구성원의 절반보다 많은 수인 $k(\geq \frac{1}{2}N+1)$명만으로 비밀 메시지를 복원할 수 있다. 또한 참여자를 n명으로 늘리는 과정 역시 GHZ 상태의 큐빗을 늘려주기만 하면 되기 때문에 채널이 늘어남으로 인해 발생할 수 있는 문제를 막을 수 있다.

도청자의 점검 방법에서 Zhang과 Li의 프로토콜은 (4)번 과정과 같이 큐빗의 일부에 대하여 각 사용자들의 정보를 무작위적으로 공개하게 하는 방법을 사용한다. 그러나 이는 사용자가 많아지면 많아질수록, 도청확인을 위해 사용되는 큐빗이 많아진다는 것을 의미한다. 다시 말해, 사용자가 많아질수록, 비밀 메시지의 효율성이 떨어진다고 볼 수 있다. 그러나 본 논문에서 제시한 분배과정에서의 도청자 확인 방법은 사용자가 늘어나더라도 도청 확인에 사용되는 큐빗의 양에는 변화가 없다. 또한 인증을 위해 사용되는 h개의 정보는 구성원의 ID에 의하여 감추어졌기 때문에 Alice가 자신의 비밀을 encoding하는 과정에서 재사용될 수 있으므로 상대적으로 높은 효율성을 가지고 있다고 말할 수 있다.

Zhang과 Li의 프로토콜은 채널상의 도청 여부만을 확인하기 때문에 각 구성원이 올바르지 못한 사람이 참여하더라도 확인할 방법이 없다. 그러나 본 논문에서 제시하는 인증과정은 메시지를 분배하는 중재자가 각 구성원을 인증할 수 있기 때문에 안전성의 측면에서 높은 가치를 부여 받는다.

Ⅵ. 결 론

기존의 양자 비밀 공유 프로토콜들[10-12]은 대부분 정보를 나누어가진 구성원 전부가 모여야만 원래의 비밀 정보를 복원할 수 있는 기법들이었다. 또한 전부가 아닌 일부가 모이는 프로토콜의 경우에도 아주 특별한 경우이기 때문에 임의의 n명으로 확장시키기에는 무리가 있었다. 그러나 본 프로토콜에서는 GHZ 상태 얽힘 교환과 벨 측정을 통하여 각 구성원이 전부 모이지 않아도 구성원의 절반보다 많은 인원만 모이면 Trent의 비밀 메시지를 복원할 수 있다. 또한 절반 이하의 구성원은 Trent의 비밀을 복원할 수 없어야 한다는 양자 비밀 공유의 기본적인 요구조건을 만족 시킨다. 그리고 GHZ 의 큐빗을 늘려주기만 하면 용이하게 임의의 n명으로 확장할 수 있다.

본 프로토콜의 또 다른 특징은 정보를 전달하는 중재자가 각 구성원을 인증할 수 있다는 사실이다. 이는 기존의 양자 비밀 공유 기법들과는 매우 차별화된 제안으로 정보를 나누어 주는 중재자와 정보를 복원하려는 다수의 구성원이 이루고 있는 양자 채널 시스템에 관하여 보다 현실적이면서도 구체적으로 적용될 수 있는 방법을 제시하였다고 볼 수 있다. 넓은 의미에서 본다면 이 논문에서 제시하는 프로토콜은 인증을 통한 일 대 다수의 양자 직접 통신을 포함하는 양자 비밀 공유라고 할 수 있다. 그런 의미에서 양자 통신 체계에 대한 보다 적용 가능한 예를 제시하는 구체적인 프로토콜이라고 할 수 있다.

참 고 문 헌

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

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

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

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

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

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

[7] C. H. Bennett and 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

[8] 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

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

[10] M. A. Nielsen, E. Knill, and R. Laflamme. "Complete quantum teleportation using nuclear magnetic resornance." *Nature*, 396(6706):52-55, 1998

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

[12] 홍창호, 이화연, 김지인, 임종인, 양형진, "Entanglement Swapping을 이용한 안전한 직접 통신 프로토콜", *한국정보보호학회 논문지*, 16(1), Feb 2005

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

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

[15] R. Cleve, D. Gottesman, Hoi-Kwong Lo. "How to Share a Quantum Secret." *Phys. Rev. Lett.* 83:648-651, 1999

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

[17] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, C. M. Simmons. "Pratical free-space Quantum key distribution over 1km", *Phys. Rev. Lett.* 81:3283-3286, 1998

[18] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Goran, P. R. Tapster, J. G. Rarity, "A step towards global key distribution", *Nature* 419:450, 2002

[19] Z. Zhang, Y. Hi, Z. Man, "Multiparty quantum secret sharing", *Phy. Rev. A* 71, 044301, 2005

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

[21] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, "Bell's theorem without inequalities" Am. *J. Phys.* 58, 1131

[22] D. Brouwmeester, Jian-Wei Pan, M. Daniell, H. Weinfurter, A. Zeilinger, "Observation of Three-Photon Greenberger- Horne-Zeilinger Entanglement" *Phys. Rev. Lett.* 82, 1345-1349(1999)

[23] S. Bose, V. Vedral, P.L. Knight, "Multiparticle generalization of entanglement swapping." *Phys. Rev. A* 46, 2229, 1992

[24] N. Gisin, G. Ribordy, W. Tittle, H. Zbinden, "Quantum Cryptography" *Rev. Mod. Phys.* 74, 145-195, 2002

[25] C. Bennett, D. P. DiVincenzo, J. A. Smolin, W. K. Wootters. "Mixed-state entanglement and quantum error correction." *Phys. Rev. A* 54, 3824-3851, 1996

[26] A. Ambainis, A. Smith, K. Yang. "Extracting Quantum Entanglement(General Entanglement Purification protocols)." 17th Annual IEEE conference on Computational Complexity (CCC2002) p103

[27] M. Murao, M. B. Plenio, S. Popescu, V. Vedral, P. L. Knight.

"Multipartite entanglement purification protocols." *Phys. Rev.* 57, R4075, 1998

[28] P. Chen, C. Li. "Distilling multi partite pure state from a finite number of copies of multiprtite mixed states", *Phys. Rev. A* 69, 012308, 2004

〈著者紹介〉

이 덕 진 (Duk-jin Lee) 정회원
2003년 2월: 고려대학교 자연과학대학 물리학과 학사
2006년 2월: 고려대학교 정보보호대학원 석사과정 수료
<관심분야> 양자암호, 양자 비밀 공유 프로토콜, 양자 인증

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, 양자 프로토콜, 양자 인증

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, 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 대학교 박사후 연구원
1999년 1월~1999년 12월: 미국 메릴랜드대학교 교환교수
1992년 3월~현재: 고려대학교 자연과학대학 디스플레이 반도체 물리학과 교수
2001년 3월~현재: 고려대학교 정보보호대학원 겸임 교수
<관심분야> 양자암호, 암호 프로토콜

임 종 인 (Jongin Lim)
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