情報保護學會論文誌
第15券 第2號, 2005. 4

일회용 ID 기반 양자 인증 및 키 분배 프로토콜*

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

Quantum Authentication and Key Distribution protocol based on one-time ID

Hwa-Yean Lee,[1†] Chang-Ho Hong,[1] Hyung-Jin Yang,[1,2‡] Jong-in Lim,[1]
[1]Graduate School of Information Security (GSIS), Korea University
[2]Department of Physics, Korea University

요 약

본 논문에서는 일방향 해쉬함수를 이용한 일회용 ID기반 양자 키 분배 프로토콜을 제안한다. 이 프로토콜은 일회용 ID를 이용하여 지정된 사용자들이 중재자와 상대방을 인증할 수 있도록 하였으며, 인증 후 남은 GHZ 상태를 이용하여 양자키를 공유할 수 있도록 고안되었다. 인증과 키 분배 과정에 중재자의 도움이 필요하지만, 인증 이후 분배되는 키에 대한 정보를 중재자에게도 노출시키지 않는다는 점에서 기존에 제안된 프로토콜과 비교하여 키의 안전성을 높였다.

ABSTRACT

We propose a Quantum Authentication and Key distribution protocol based on one-time ID using one-way Hash function. The designated users can authenticate each other and the arbitrator using their one-time ID and distribute a quantum secret key using remained GHZ states after authentication procedure. Though the help of the arbitrator is needed in the process of authentication and key distribution, our protocol prevents the arbitrator from finding out the shared secret key even if the arbitrator becomes an active attacker. Unconditional security can be proved in our protocol as the other QKD protocols.

Keywords : *Quantum Cryptography, Quantum authentication, Quantum key distribution*

Ⅰ. 서 론

양자 키 분배(QKD) 프로토콜은 양자 고유의 성질을 이용하여 도청을 확인하며, 완전 안전성이 보장되기 때문에 주목을 받고 있다. 1984년에 Bennett과 Brassard[1]에 의하여 처음 소개된 이후 B92[2] 및 EPR[3]을 비롯한 많은 양자 키 분배 프로토콜이 제안되었으며, 그에 대한 안전성 분석이 논의되었다.[4-6] 그러나 기존에 제안된 거의 모든 QKD 프로토콜들이 사용자 인증을 제공하지 않기 때문에 man-in-the middle 공격에 취약하다. 최근 들어 이러한 문제점을 해결하기 위하여 양자 시스템에 인증을 도입하려는 노력이 계속되고 있다.

1999년 Dusek, Myska 등등이 제안한 프로토

접수일 : 2005년 2월 14일 ; 채택일 : 2005년 3월 28일
* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 육성·지원사업의 연구결과로 수행되었습니다.
† 주저자 : hylee@korea.ac.kr
‡ 교신저자 : yangh@korea.ac.kr

콜[7]은 갑과 을이 사전에 인증수열을 공유하고 있다는 가정 아래 갑과 을이 상대방을 인증하도록 하고 있으며, 2001년 Shi, Guo 등등[8]은 갑과 을이 사전에 Bell 상태를 공유하고 있는 경우의 인증 방법을 제안하였다. 갑과 을 사이에 인증 수열이나 Bell 상태가 공유되어 있다는 것은 사전에 둘 사이에 안전한 의사소통이 있었다는 것을 전제로 한다. 그러나 임의의 사용자 사이에 이러한 비밀 정보나 양자 상태가 공유되어 있다는 가정은 양자 네트워크를 고려하면 현실적이지 않다. 한편 2000년에 Ljunggren Karlsson에 의해 제안된 프로토콜[9]과 Zeng Zhan에 의해 제안된 프로토콜[10]에서는 중재자를 도입하여 중재자가 갑과 을에게 상대방을 인증할 수 있는 정보나 양자 상태를 전달한 뒤 이를 통하여 인증을 수행하도록 한다. 이때 인증을 위한 정보와 양자 상태가 전달되는 채널은 중재자와 지정된 사용자 사이에 안전하게 연결되어 있다고 가정하고 있다. 그러나 실질적으로 중재자와 갑 중재자와 을 사이에 설정되는 채널에도 도청이나 오류 등이 발생할 수 있기 때문에 이 가정을 그대로 현실에 적용하기는 힘들 것으로 보인다. 2002년 Mihara에 의해 제안된 인증 프로토콜[11]은 사전에 공유된 얽힘 상태와 패스워드를 이용하여 자신을 시스템에 인증하는 방법이 소개되어 있으며, 인증서를 이용하여 유저를 인증하는 방법이 제안되어 있다. 그러나 이 방법은 n개의 GHZ 상태와 인증서를 이용하여 한 방향으로만 사용자 인증을 제공함으로써 또 다른 manin-the middle 공격에 노출될 수 있는 위험이 있다.

본 논문에서는 일방향 해쉬함수를 이용한 일회용 ID기반 양자 키 분배 프로토콜을 제안한다. 이 프로토콜에서는 중재자가 GHZ 입자를 각 유저의 인증키로 암호화하여 사용자에게 전달하기 때문에 지정된 사용자를 제외한 다른 사람이 이 큐빗에 연산을 취하거나 측정을 하게 되면 인증 확인과정에서 자신의 존재가 드러나게 된다. 만약 중재자가 아닌 삼자가 중재자로 가장하여 사용자에게 GHZ 입자를 보내는 경우에도 위와 같은 이유로 인증 확인 과정을 통과할 수가 없다. 따라서 인증 확인 단계가 통과된다면 사용자는 자신이 받은 큐빗이 중재자가 생성하였다는 사실과 자신이 통신하고 있는 상대가 지정된 사용자라는 것을 확인할 수 있다. 한편 기존에 제안된 인증된 양자 키 분배 프로토콜[12]과 비교하여 중재자가 능동 공격자가 되는 경우에도 갑과 을 사이에 공유된 키를 알 수 없도록 하는 특징을 갖고 있다.

II. 일회용 ID를 이용한 양자 키 분배 프로토콜

본 논문에서 제안하는 양자 키 분배 프로토콜은 고전적인 방법과 양자적인 방법을 혼합하여 사용자를 인증한 뒤 키를 분배하는 방식으로 크게 인증과 키 분배 두 부분으로 나눌 수 있다. 먼저 일회용 ID를 이용한 인증 방법을 소개한 뒤 키 분배 방식을 설명하도록 한다.

2.1 인 증

인증을 위한 사전 단계로 사용자는 신뢰할 수 있는 제 3의 기관인 중재자에게 자신의 비밀 식별 정보와 인증에 사용할 일방향 해쉬 함수를 등록한다. 중재자와 각 사용자는 자신의 비밀 식별 정보를 안전하게 보관한다고 가정한다. 예를 들어 사용자 갑의 비밀 식별 정보가 ID_A이고 일방향 해쉬 함수를 f라고 하면 큐빗을 암호화할 인증키는 $f(ID_A, m)$이 된다. 이때 m은 갑과 중재자가 함수 f를 사용한 횟수라고 정의하고 매번 함수를 호출할 때마다 갱신되는 값으로 외부로 노출되지 않는다고 가정한다. 을의 경우도 마찬가지로 을의 비밀 식별 정보를 ID_B 일 방향 해쉬 함수를 g 마지막으로 을이 사용하는 카운터를 n이라고 가정한다.

갑이 을과의 비밀통신을 원하는 경우 갑은 중재자에게 이 사실을 알리고 GHZ 상태 분배를 요청한다. 중재자는 다음 (식 1)과 같은 N개의 tripartite GHZ 상태 $|\Psi\rangle=(|\Psi_1\rangle, |\Psi_2\rangle, \ldots, |\Psi_N\rangle)$를 생성한다.

$$|\Psi_i\rangle=\frac{1}{\sqrt{2}}(|000\rangle_{AaB}+|111\rangle_{AaB}) \quad \text{(식 1)}$$

여기서 A는 갑, a는 중재자, B는 을이 갖게 될 큐빗을 나타낸다.

중재자는 인증키 $f(ID_A, m)$ $g(ID_B, n)$에 따라 위의 GHZ 상태를 암호화한 뒤 각 큐빗을 지정된 사용자인 갑과 을에게 전달한다. GHZ 상태 암호화는 $f(ID_A, m)$($g(ID_B, n)$)의 i번째 값이 0인 경우에는 $|\Psi_i\rangle$의 첨자 A(B)로 표현된 큐빗에 아무런 연산을 취하지 않고 1인 경우에는 Hadamard 연산 H

를 취한다. 인증키의 길이가 전달하고자하는 GHZ 상태 길이 N보다 작은 경우 m 또는 n값을 증가시켜가면서 충분히 많은 함수값 (예를 들어 $f(ID_A, m)$, $f(ID_A, m+1)$, $f(ID_A, m+2)$,...등등)을 계산하여 인증키로 사용한다.

갑과 을은 전달 받은 큐빗을 중재자와 같은 방법을 사용하여 복호화한다. 이후 갑과 을은 일정량의 큐빗을 측정하여 그 측정 결과값이 같은 지를 확인한다. 아래와 같은 절차에 따라 정확한 인증키를 갖고 있는 사용자만이 같은 결과를 얻게 되기 때문에 다른 결과가 나오면 인증이 실패한 것으로 간주하고 첫 단계부터 다시 시작한다. 세 단계에 걸쳐 시행되는 인증 과정은 다음 (식 2)로 요약할 수 있다.

$$|\Psi_i\rangle_1 = \frac{1}{\sqrt{2}}(|000\rangle_{AaB} + |111\rangle_{AaB})$$

$$|\psi_i\rangle_2 = \{[1 - f(ID_A, m)]I + f(ID_A, m)H\}_A \otimes \{[1-g(ID_B, n)]I + g(ID_B, n)H\}_B |\Psi_i\rangle_1$$

$$|\Psi_i\rangle_3 = \{[1-f(ID_A, m)]I + f(ID_A, m)H\}_A \otimes \{[1-g(ID_B, n)]I + g(ID_B, n)H\}_B |\Psi_i\rangle_2 = |\Psi_i\rangle_1 \quad \text{(식 2)}$$

이때 $|\Psi_i\rangle_1$은 초기의 GHZ 상태 $|\Psi_i\rangle_2$는 중재자가 인증키로 암호화한 이후의 상태 $|\Psi_i\rangle_3$은 갑과 을이 전달받은 GHZ 상태를 복호화한 이후의 상태를 나타낸다.

2.2 양자 키 분배 프로토콜

위의 인증을 통과하면 갑과 을은 상대방이 지정된 사용자라는 것과 자신이 받은 GHZ 상태가 중재자로부터 왔다는 것을 확인할 수 있다. 다음으로 양자키 분배를 위해서 인증에 사용하고 남은 GHZ 상태를 이용하여 양자키를 공유한다. 이전에 제안한 프로토콜[12]에서는 중재자가 적극적으로 공격에 나서는 경우 공유되는 키를 알아낼 수 있었으나, 본 논문에서 제안하는 프로토콜에서는 중재자가 공격자의 역할을 하는 경우에도 인증 후에 공유되는 키를 알 수 없다.

갑과 을은 각각 인증이 끝나고 남은 큐빗들에 무작위로 Pauli 연산 I와 σ_x중의 하나를 선택하여 연산을 취한다. 갑과 을은 자신이 취한 I 연산을 0으로 σ_x 연산을 1로 기록하여 보관한다. 연산이 끝나면 을은 자신의 큐빗을 갑에게 보낸다. 갑은 을에게 받은 큐빗과 자신의 큐빗을 다음 (식 3)과 같은 4개의 벨 상태로 구분할 수 있는 Bell 측정을 한다.

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B)$$

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) \quad \text{(식 3)}$$

표 1. 양자 키 분배 : 갑과 을의 연산이후 변화된 GHZ 상태

$\|\Psi\rangle$에 작용된 연산자		갑과 을의 연산 후의 GHZ 상태	4개의 벨 상태로 정리한 GHZ 상태
갑	을		
I_A	I_B	$\|G_0\rangle = \frac{1}{\sqrt{2}}(\|000\rangle_{AaB} + \|111\rangle_{AaB})$	$\frac{1}{2}\{(\|0\rangle+\|1\rangle)_a\|\Phi^+\rangle_{AB} + (\|0\rangle-\|1\rangle)_a\|\Phi^-\rangle_{AB}\}$
I_A	σ_{x_n}	$\|G_1\rangle = \frac{1}{\sqrt{2}}(\|001\rangle_{AaB} + \|110\rangle_{AaB})$	$\frac{1}{2}\{(\|0\rangle+\|1\rangle)_a\|\Psi^+\rangle_{AB} + (\|0\rangle-\|1\rangle)_a\|\Psi^-\rangle_{AB}\}$
σ_{x_1}	I_B	$\|G_2\rangle = \frac{1}{\sqrt{2}}(\|100\rangle_{AaB} + \|011\rangle_{AaB})$	$\frac{1}{2}\{(\|0\rangle+\|1\rangle)_a\|\Psi^+\rangle_{AB} - (\|0\rangle-\|1\rangle)_a\|\Psi^-\rangle_{AB}\}$
σ_{x_1}	σ_{x_n}	$\|G_3\rangle = \frac{1}{\sqrt{2}}(\|101\rangle_{AaB} + \|010\rangle_{AaB})$	$\frac{1}{2}\{(\|0\rangle+\|1\rangle)_a\|\Phi^+\rangle_{AB} - (\|0\rangle-\|1\rangle)_a\|\Phi^-\rangle_{AB}\}$

갑과 을이 각각 Pauli 연산을 취한 이후의 GHZ 상태 변화는 표 1과 같이 정리할 수 있다.

Bell 측정이 끝나면 갑은 측정이 끝났음을 중재자와 을에게 알리고 중재자에게 x축 방향으로의 측정결과를 요구한다. 갑이 $|\Psi^+\rangle$ 또는 $|\Phi^+\rangle$를 측정한 경우 중재자는 $|0_x\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$의 결과를 공개해야 하며 $|\Psi^-\rangle$ 또는 $|\Phi^-\rangle$를 측정한 경우에는 $|1_x\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$를 공개해야 한다. 갑은 자신의 측정값과 중재자의 공개정보가 같으면 도청이 없었다고 판단한 후 이를 을에게 알린다. 이후 갑은 $|\Psi^{\pm}\rangle$가 측정된 경우에는 자신의 연산 정보를 바꾸고 $|\Phi^{\pm}\rangle$가 측정된 경우는 자신의 연산정보 그대로를 사용하게 되는데 이와 같은 작업을 취하면 을이 사용한 연산 정보와 같은 연산 정보를 얻게 된다. 즉, 표 1에서 보이듯이 갑과 을이 다른 연산을 취한 경우에만 $|\Psi^{\pm}\rangle$가 측정되므로, 갑은 $|\Psi^{\pm}\rangle$를 측정하는 경우에만 자신의 연산 정보를 바꾸어 을과의 비밀키 후보로 사용한다. 이후 갑과 을은 공유된 연산정보에서 일정량의 비트를 공개하여 키 분배 과정에서의 공격자 병의 존재를 확인한다. 공개된 비트가 일치하여 공격자 병이 존재하지 않았다고 판단되면 채널 상의 오류 등을 제거하기 위하여 오류 정정이나 privacy amplification[13-15]등과 같은 방법을 적용시켜 비밀키를 추출해 낸다.

Ⅲ. 안전성 분석

제안된 기법의 안전성을 분석하기 위하여 우선 인증 단계에서 공격이 이루어지는 경우를 살펴본 뒤 키 분배 단계에서의 공격을 살펴보도록 하겠다.

3.1 인증 단계에서의 공격

인증 단계에서 중재자가 갑이나 을에게 전하는 GHZ 입자를 공격자 병이 가로챘다고 가정하자. 병이 가로챈 상태를 측정한 뒤에 원래의 의도된 사용자에게 큐빗을 전달하는 경우 병은 GHZ 입자를 암호화한 인증키 $f(ID_A, m)$과 $g(ID_B, n)$을 알 수 없기 때문에 올바른 측정 기저(x축 또는 z축)를 선택할 확률이 1/2이 되고 올바르지 않은 기저를 선택한 경우 인증과정을 통과하지 못할 확률이 1/2이 된다. 따라서 병이 인증과정을 통과하지 못할 확률은 도청한 큐빗 당 1/4이 된다. 예를 들어 갑에게 보내지는 큐빗을 가로채는 경우를 생각해보자 갑의 인증키 비트가 1이고 을의 인증키 비트가 0인 경우 중재자가 전달하는 상태는 (식 4)와 같이 $|\Psi_i\rangle$에 Hadamard 연산이 취해진 $|\Psi_i'\rangle_1$이 된다. 이 상태를 병이 x축으로 측정하게 되면 측정 결과에 따라 (측정 결과가 $|0_x\rangle$인 경우) (식 5)의 $|\Psi_i''\rangle_1$또는 (측정 결과가 $|1_x\rangle$인 경우) (식 6)의 $|\Psi_i'''\rangle_1$상태로 변하게 된다.

$$|\Psi_i'\rangle=\frac{1}{2}(|000\rangle_{AaB}+|100\rangle_{AaB}+|011\rangle_{AaB}-|111\rangle_{AaB}) \quad \text{(식 4)}$$

$$|\Psi_i''\rangle_1=\frac{1}{\sqrt{2}}(|000\rangle_{AaB}+|100\rangle_{AaB}) \quad \text{(식 5)}$$

$$|\Psi_i'''\rangle_1=\frac{1}{\sqrt{2}}(|011\rangle_{AaB}-|111\rangle_{AaB}) \quad \text{(식 6)}$$

병이 측정된 GHZ 입자를 갑에게 전달한 뒤 갑과 을이 각자의 인증키로 복호화하면 (식 5)의 $|\Psi_i''\rangle_1$ 상태는 $|000\rangle_{AaB}$으로, (식 6)의 $|\Psi_i'''\rangle_1$는 $|111\rangle_{AaB}$로 변하게 된다. 따라서 이 경우 병의 존재는 드러나지 않는다.

그러나 병이 (식 4)의 $|\Psi_i'\rangle$을 z축으로 측정하는 경우에는 다음과 같은 상태 중 하나로 GHZ 상태가 붕괴하게 되므로 1/2의 확률로 병의 존재를 확인할 수 있다.

$$|\Psi_i''\rangle_2=\frac{1}{\sqrt{2}}(|000\rangle_{AaB}+|011\rangle_{AaB}) \quad \text{(식 7)}$$

$$|\Psi_i'''\rangle_1=\frac{1}{2}(|100\rangle_{AaB}-|111\rangle_{AaB}) \quad \text{(식 8)}$$

이와 같이 인증 단계에서 공격자 병의 존재를 확인할 확률은 큐빗 당 1/4이 되고 적당한 개수의 큐빗을 인증에 이용하면 Man-in-the-middle 공격을 막을 수 있다.

한편 공격자 병의 존재가 드러남으로써 그때의 측정 기저가 일치 않는 다는 것을 확인하여 인증키 $f(ID_A, m)$ 또는 $g(ID_B, n)$의 몇 비트를 알아낸다고 하더라도 전체 인증키 값을 알아낼 수 없으며 인증키 몇 비트를 안다고 하더라도 인증키가 한번만 사용되기 때문에 다음의 공격에 이를 이용할 수 없다.

또한 일방향 함수와 GHZ 상태를 동시에 이용함으로써 인증키를 만들어냈던 비밀 아이디 ID_A 또는 ID_B 및 카운터 값 m,n을 알아낼 수 없다.

중재자가 아닌 제 3자인 병이 중재자로 가장하고 갑과 을에게 GHZ 상태를 전달하는 경우에도 갑과 을이 GHZ 입자를 받으면 자신의 인증키로 복호화하기 때문에, 병과의 연관성이 올바르게 성립하지 않을 뿐만 아니라 인증 확인 절차도 통과할 수 없다. 따라서 인증과정을 통과하면 갑과 을은 자신이 올바른 사용자와 통신하고 있다는 것을 확인할 수 있을 뿐만 아니라, 자신이 받은 GHZ 상태가 중재자로부터 온 것이라는 사실도 확인할 수 있다.

한편, 공격자 병이 갑이나 을의 인증키를 사전에 알고 있는 경우, 인증 단계에서의 공격자의 존재는 확인할 수 없다. 그러나 이러한 경우에도 공격자 병은 분배되는 비밀키를 알 수가 없다. 예를 들어, 공격자 병이 갑의 인증키를 알고 있다고 가정하자. 공격자 병이 분배되는 키의 정보를 알기 위해서는 우선, 중재자가 갑에게 전달하는 GHZ 상태를 가로채어 자신이 가진 상태와 얽힘 상태를 만들어 놓아야 한다. 이후, 을이 연산을 취한 뒤 갑에게 전달하는 큐빗을 가로채어, 미리 갑의 상태와 얽힘 상태로 만들어 놓은 자신의 큐빗과 Bell측정을 해야 한다. 이후, 병은 자신의 존재를 드러내지 않기 위하여 을이 보내는 것처럼 가장하여 임의로 상태를 생성한 뒤 갑에게 전달한다. 이러한 공격이 취해지면, 공격자 병의 개입으로 중재자와 갑, 을 사이의 측정의 연관성이 깨지게 되므로, 중재자는 Bell 측정에 따른 올바른 결과값 즉, $|0_x\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ 또는 $|1_x\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$를 공개할 확률이 한 큐빗 당 1/2이 된다. 키 분배에 사용된 모든 큐빗에 대해 중재자의 결과가 일치해야 하기 때문에, 이러한 공격은 거의 확실하게 알아낼 수 있다. 따라서 공격자가 고전적으로 생성된 인증키 값을 안다는 사실이 분배되는 비밀키의 안전성에 영향을 끼치지 않는다는 것을 알 수 있다.

표 2. 키 분배 단계의 공격 : 병의 측정이후 변화된 GHZ 상태

$\|\psi\rangle$에 작용된 연산자		갑과 을의 연산 이후의 GHZ 상태	병의 을 큐빗 측정치	붕괴된 GHZ 상태	병이 갑에게 보내는 큐빗	갑이 측정하는 Bell 상태 및 중재자의 측정값이 얽힌 상태
갑	을					
I_A	I_B	$\|G_0\rangle=\frac{1}{\sqrt{2}}(\|000\rangle_{AaB}+\|111\rangle_{AaB})$	$\|0_x\rangle$	$\|00\rangle_{Aa}+\|11\rangle_{Aa}$	$\|0_x\rangle_e$	$\frac{1}{2}(\|\phi^+\rangle_{Ae}\|0_x\rangle_e+\|\phi^-\rangle_{AB}\|1_x\rangle_e$ $+\|\psi^+\rangle_{Ae}\|0_x\rangle_e+\|\psi^-\rangle_{AB}\|1_x\rangle_e)$
			$\|1_x\rangle$	$\|00\rangle_{Aa}-\|11\rangle_{Aa}$	$\|1_x\rangle_e$	$\frac{1}{2}(\|\phi^+\rangle_{Ae}\|0_x\rangle_e+\|\phi^-\rangle_{AB}\|1_x\rangle_e$ $-\|\psi^+\rangle_{Ae}\|0_x\rangle_e-\|\psi^-\rangle_{AB}\|1_x\rangle_e)$
I_A	σ_{x_B}	$\|G_1\rangle=\frac{1}{\sqrt{2}}(\|001\rangle_{AaB}+\|110\rangle_{AaB})$	$\|0_x\rangle$	$\|00\rangle_{Aa}+\|11\rangle_{Aa}$	$\|0_x\rangle_e$	$\frac{1}{2}(\|\phi^+\rangle_{Ae}\|0_x\rangle_e+\|\phi^-\rangle_{AB}\|1_x\rangle_e$ $+\|\psi^+\rangle_{Ae}\|0_x\rangle_e+\|\psi^-\rangle_{AB}\|1_x\rangle_e)$
			$\|1_x\rangle$	$\|11\rangle_{Aa}-\|00\rangle_{Aa}$	$\|1_x\rangle_e$	$-\frac{1}{2}(\|\phi^+\rangle_{Ae}\|0_x\rangle_e+\|\phi^-\rangle_{AB}\|1_x\rangle_e$ $-\|\psi^+\rangle_{Ae}\|0_x\rangle_e-\|\psi^-\rangle_{AB}\|1_x\rangle_e)$
σ_{x_A}	I_B	$\|G_2\rangle=\frac{1}{\sqrt{2}}(\|100\rangle_{AaB}+\|011\rangle_{AaB})$	$\|0_x\rangle$	$\|01\rangle_{Aa}+\|10\rangle_{Aa}$	$\|0_x\rangle_e$	$\frac{1}{2}(\|\phi^+\rangle_{Ae}\|0_x\rangle_e-\|\phi^-\rangle_{AB}\|1_x\rangle_e$ $+\|\psi^+\rangle_{Ae}\|0_x\rangle_e-\|\psi^-\rangle_{AB}\|1_x\rangle_e)$
			$\|1_x\rangle$	$\|10\rangle_{Aa}-\|01\rangle_{Aa}$	$\|1_x\rangle_e$	$-\frac{1}{2}(\|\phi^+\rangle_{Ae}\|0_x\rangle_e-\|\phi^-\rangle_{AB}\|1_x\rangle_e$ $-\|\psi^+\rangle_{Ae}\|0_x\rangle_e+\|\psi^-\rangle_{AB}\|1_x\rangle_e)$
σ_{x_A}	σ_{x_B}	$\|G_3\rangle=\frac{1}{\sqrt{2}}(\|101\rangle_{AaB}+\|010\rangle_{AaB})$	$\|0_x\rangle$	$\|01\rangle_{Aa}+\|10\rangle_{Aa}$	$\|0_x\rangle_e$	$\frac{1}{2}(\|\phi^+\rangle_{Ae}\|0_x\rangle_e-\|\phi^-\rangle_{AB}\|1_x\rangle_e$ $+\|\psi^+\rangle_{Ae}\|0_x\rangle_e-\|\psi^-\rangle_{AB}\|1_x\rangle_e)$
			$\|1_x\rangle$	$\|01\rangle_{Aa}-\|10\rangle_{Aa}$	$\|1_x\rangle_e$	$\frac{1}{2}(\|\phi^+\rangle_{Ae}\|0_x\rangle_e-\|\phi^-\rangle_{AB}\|1_x\rangle_e$ $-\|\psi^+\rangle_{Ae}\|0_x\rangle_e+\|\psi^-\rangle_{AB}\|1_x\rangle_e)$

3.2 키 분배 단계에서의 공격

키 분배 단계에서의 공격은 을이 갑에게 보내는 큐빗에 대한 조작만을 고려하면 된다. 공격자 병이 을이 보내는 큐빗을 가로채어 z축으로 측정한 뒤 그대로 갑에게 전달하는 경우에는 아무런 정보를 얻을 수 없으며, 이러한 공격을 행하는 경우 중재자의 측정값 공개 시 큐빗 당 1/2의 확률로 자신의 존재가 드러나게 된다. 공격자 병이 을이 보내는 큐빗을 x 축으로 측정을 한 뒤, 측정한 비트를 보내는 경우를 생각해보자. 갑과 을의 연산에 따라 GHZ 상태는 $|G_0\rangle,|G_1\rangle,|G_2\rangle,|G_3\rangle$ 넷 중의 하나로 변하게 되며, 이 상태에 병이 연산을 취하면 표 2와 같은 결과를 얻게 된다.

표 2에서 보이듯, 갑은 자신과 을이 사용한 연산에 상관없이 모든 Bell 상태를 측정할 수 있으며, 이에 따른 중재자의 측정 결과 또한 원래의 연산 결과와 일치하여 공격자의 존재가 드러나지 않는다. 그러나 공격자는 자신의 측정값을 통해 아무런 정보도 얻을 수 없으며, 중재자가 공개하는 정보를 통해서는 단지 갑과 을이 같은 연산을 사용했는지 여부만을 알 수 있다. 이와 같은 공격은 키 분배의 마지막 단계인 비밀키의 일부분을 공개함으로써 공격자의 존재여부를 확인할 수 있다.

한편, 기존의 인증 기법[12]에서는 중재자가 적극적인 공격자가 되는 경우, 분배되는 키의 안전성을 보장하지 못하였지만, 본 논문에서 제안된 기법에서는 중재자가 을의 큐빗을 도청하는 경우에도 표 2와 같은 일반적인 공격과 유사한 결과를 얻게 되어 중재자의 도청을 확인할 수 있다.

Ⅳ. 결 론

본 논문에서 제안하는 프로토콜은 인증과 더불어 양자 키 분배를 제공함으로써, 기존의 양자 키 분배 기법의 주요한 문제였던 Man-in-the middle 공격을 막을 수 있다. 인증을 위해 중재자를 도입함으로써 등록된 임의의 사용자가 중재자를 통하여 상대방을 인증할 수 있고, 비밀키를 공유할 수 있다. 인증된 양자 키 분배 프로토콜에 Bell상태 대신에 GHZ 상태를 사용함으로써 쌍방향 인증을 제공할 뿐만 아니라, 중재자가 적극적인 공격자가 되는 경우에도 안전성을 보장할 수 있다.

한편, 새롭게 제안된 일회용 ID를 이용한 인증 방법은 양자적 성질을 이용할 뿐만 아니라, 인증키를 한번만 사용하고 폐기하도록 하기 때문에 고전적 및 양자적으로 인증키에 대한 안전성이 보장된다. 이러한 일회용 ID 인증방법은 양자 서명 기법, 양자 키 분배, 양자 원격 전송 등등의 양자 암호 전반에 걸쳐 적용될 수 있을 것으로 기대된다. 앞으로 실제적인 양자 암호구현을 위하여 일회용 ID 인증방법과 관련된 다양한 양자 암호 프로토콜 연구와 더불어 새로운 인증 방법 개발 등에 많은 노력을 기울여야 할 것이다.

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] Charles H. Bennett, "Quantum Cryptography Using Any Two Nonorthogonal States", Phys. Rev. Lett. 68, 3121 (1991).

[3] Artur K. Ekert, "Quantum cryptography based on Bell' s theorem", Phys. Rev. Lett. 67, 661 (1991).

[4] Dominic Mayers, "Unconditional security in Quantum Cryptography", ArXiv:quant-ph/9802025 (1998)

[5] Hoi-Kwong Lo and H.F.Chau, "Unconditional security of Quantum key distribution over arbitrarily long distances", science vol 283 pp2050~2056(1999)

[6] Peter W. Shor, John Preskill, "Simple proof of security of the BB84 quantum key distribution protocol", Phys. Rev. Lett. 85, 441-444 (2000)

[7] iloslav Dusek, Ondrj Haderka, Martin Hendrych, and Robert Myska, "Quantum Iidentification system", Phys. Rev. A 60, 149-156 (1999)

[8] Bao-Sen Shi, Jian Li, Jin-Ming Liu, Xiao-Feng Fan, Guang-Can Guo, "Quantum key distribution and

quantum authentication based on entangled state ", Physics Letters A 281, 83-87 (2001)

[9] Guihua Zeng and Weiping Zhang, "Identity verification in quantum key distribution", PHYSICAL REVIEW A, VOLUME 61, 022303 (2000)

[10] Daniel Ljunggren, Mohamed Bourennane, and Anders Karlsson, "Authority-based user authentication in quantum key distribution", PHYSICAL REVIEW A, VOLUME 62, 022305 (2000)

[11] Takashi Mihara, "Quantum identification schemes with entanglements", Phys. Rev. A 65, 052326 (2002)

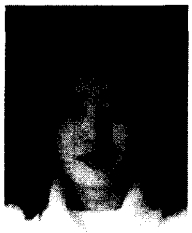
[12] 이화연, 홍창호, 이덕진, 양형진, 임종인, "인증된 양자 키 분배 프로토콜", 정보보호학회 논문지 제 14권, 제 2호 pp49-55 (2004)

[13] A. Ambainis, A.Smith, and Ke Yang, "Extracting Quantum Entanglement (General Entanglement Purification Protocols)", 17th Annual IEEE conference on Computational Complexity (CCC2002) p103

[14] M. Murao, M. B. Plenio, S. Popescu, V. Vedral, and P. L. Knight, "Multipartite entanglement purification protocols", Phys. Rev. 57, R4075 (1998)

[15] Ping-Xing Chen and Cheng-Zu Li, "Distilling multipartite pure state from a finite number of copies of multipartite mixed states', Phys. Rev. A 69, 012308 (2004)

〈著者紹介〉



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

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

양 형 진 (Hyung-jin Yang)
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 물리학과 교수
2001년 3월~현재: 고려대학교 정보보호대학원 겸임교수
〈관심분야〉 양자암호, 암호프로토콜

임 종 인(Jong-in Lim)
1980년 2월: 고려대학교 수학과 학사
1982년 2월: 고려대학교 수학과 석사
1986년 2월: 고려대학교 수학과 박사
1986년~2001년 1월: 고려대학교 수학과 교수
1999년~현재: 고려대학교 정보보호기술연구센터 센터장, 한국정보보호진흥원 사외이사
2000년~현재: 고려대학교 정보보호대학원 원장, 정보통신부 정보보호 자문위원
2003년 4월: 국가정보원/국가보안기술연구소 정보보안/암호정책 자문위원
2003년 11월~현재: 국무총리산하 개인정보보호심의위원회 위원
〈관심분야〉 사이버법률, 포렌식, 프라이버시, 암호기술, 양자 암호 등등