情 報 保 護 學 會 誌
第 14 券 第 3 號, 2004. 6

양자 인증 및 양자 서명 기법

이 덕 진*, 이 화 연*, 임 종 인**, 양 형 진***

요 약

본 연구에서는 양자 인증 기법 및 양자 서명 기법을 살펴보고 양자 암호 분야의 연구 방향을 제시하고자 한다. 기존에 제안된 양자 인증 기법 중 고전적인 인증 수열을 이용한 인증 기법과 양자 고유의 얽힘 상태를 이용한 인증 기법을 소개한다. 양자 서명기법에서는 양자 역학의 고유한 성질을 만족하는 특징인 GHZ 상태를 이용하여 믿을 만한 제 삼자의 중재를 통하여 서명 검증을 수행한다.

Ⅰ. 서 론

최근 미국에서 양자 암호기 시판[1]을 계기로 양자 암호에 대한 관심이 높아지고 있다. 양자 암호기는 양자 키 분배 프로토콜[2,3]을 구현한 기계로 양자 고유의 성질을 이용하여 도청이 불가능하도록 고안되었다.

그러나 양자 키 분배 프로토콜[2,3]은 분배된 키에 대한 완전 안전성은 보장하지만 양자 상태를 공유하는 대상에 대한 인증을 제공하지 않는다. 이에 따라 멀티 유저를 기반으로 하는 양자 시스템 구축에 있어서 현재의 양자 키 분배 프로토콜을 그대로 이용하기는 어렵다.

양자 시스템에서도 고전적인 인증 프로토콜[4~6]과 같이 사용자 인증을 제공하는 양자 인증 기법의 필요성이 대두됨에 따라 이 분야의 연구[7~9]가 양자 키 분배 프로토콜 분야와 함께 진행되고 있다.

한편, 현재의 양자 암호 분야의 연구가 양자 키 분배 프로토콜의 개발, 안전성 분석 및 구현 등에 중점을 두고 있기 때문에 양자 서명 기법[10,11]에 대한 연구는 양자 인증 기법과 비교해서도 거의 연구 결과가 없다고 할 수 있다.

본 연구에서는 양자 키 분배 프로토콜에 비하여 상대적으로 연구 및 개발이 미진한 양자 인증 및 서명 분야를 살펴보고 양자 암호 분야에서의 연구 방향을 제시하고자 한다. 2절에서는 고전적인 인증 수열을 이용한 양자 인증 기법 인증 기법 및 얽힘 상태를 이용한 양자 인증 기법을 기술하고, 3절에서는 GHZ 상태를 이용한 양자 서명 기법을 소개하도록 하겠다.

Ⅱ. 양자 인증 기법

1. 인증 수열을 이용한 양자 인증 기법

1998년에 Miloslav Dusek가 제안한 양자 인증 시스템[12]은 고전적인 인증프로토콜과 양자 키 분배 프로토콜의 결합으로 이루어져있다. 인증을 원하는 갑과 을은 사전에 공유한 인증 수열 체크를 통해 서로를 인증한다. 한번 사용된 인증 수열은 폐기되며, 인증이 끝난 후에 양자 키 분배를 통해 인증 수열을 갱신한다. 이 기법에서 양자 키 분배 프로토콜은 무조건적으로 안전하다고 증명된 BB84 프로토콜[2]이 이용된다. 이 양자 인증 기법은 오류가 없는 open 채널을 이용한 경우와 인증된 공개 논의를 통하는 경우 두 가지로 나누어서 살펴볼 수 있다.

1.1 Unjammable open 채널에서의 인증 기법

갑과 을은 사전에 몇 개의 인증 수열 triad(세 개의 큐빗을 한 묶음으로 하는 것)을 공유하고 있다고 가정한다.

1) 갑과 을은 각자 자신이 갖고 있는 인증 수열 중

* 고려대학교 정보보호대학원 ({hubble, hylee}@cist.korea.ac.kr)
** 고려대학교 정보보호대학원 원장 (jilim@korea.ac.kr)
*** 고려대학교 물리학과 교수 (yangh@korea.ac.kr)

사용하지 않은 첫 번째 triad의 위치를 공개한다. 공개된 위치가 같은 경우는 그 triad부터 사용하고, 다른 경우, 위치 정보가 큰 triad를 선택한다.

2) 갑은 첫 번째 triad의 인증 정보를 을에게 보낸다.
3) 을은 갑이 보낸 정보가 자신이 갖고 있는 것과 일치하는 지를 확인하고 만약 같지 않으면 을은 통신을 중단하고 다음 triad로 자신의 인증 수열 초기 위치를 이동시킨다. 만약 그 정보가 같다면, 갑에게 두 번째 triad의 인증 정보를 보낸다.
4) 갑은 을의 두 번째 인증 정보가 자신의 것과 일치하는 지를 비교한다. 만약 틀리다면 통신을 중단하고 을의 경우와 마찬가지로 인증 수열의 초기 위치를 이동시킨다. 만약 그 정보가 같다면 갑은 을에게 세 번째 인증 정보를 보낸다. 을이 세 번째 인증 정보가 정확하다는 것을 확인하면 인증은 성공적으로 끝난다.
5) 사용된 인증 수열을 보충하기 위하여 갑과 을은 양자 키 분배 프로토콜을 이용하여 인증 수열을 보충하고 인증 수열 초기 위치를 설정한다.

인증 과정에서 세 단계 통신이 필요한 이유는 다음과 같다. 도청자(병)가 을인 척 가장하여 갑으로부터 첫 번째 인증 정보를 얻는 경우, 갑은 병이 정확한 두 번째 인증 큐빗을 보낼 수 없기 때문에 을이 아니라는 것을 알게 된다. 따라서 갑은 통신을 중단하고 사용한 triad를 버린다. 이후에 병은 첫 번째 triad의 인증 정보를 알고 있으므로 을에게 갑인 척 가장할 수 있다. 그러나 을은 병이 세 번째 인증 정보를 모르기 때문에 갑이 아니라는 것을 확신할 수 있다.

1.2 인증된 공개 논의를 통한 인증기법

갑과 을이 초기에 비밀 정보를 공유하고 있는 경우의 인증 과정은 다음과 같다.

1) 갑과 을은 BB84 프로토콜과 같은 방법으로 양자 상태를 전송한다. 즉 갑이 두 개의 bases 중 임의로 선택한 bases를 이용해 큐빗 정보를 생성하여 을에게 전달한다. 을도 갑과 마찬가지로 같은 두 개의 bases중 임의로 한 bases를 선택하여 갑에게 받은 큐빗을 측정한다.
2) 갑과 을은 서로 공유된 비밀 정보 중 사용되지 않은 첫 번째 비트의 위치를 공개한다. 공개된 비트의 위치 정보가 다를 경우 위치 정보가 큰 것부터 인증에 이용한다. 다음 세 단계의 인증 공개 논의를 수행하여 에러 비율을 추정[12]하고 상호 인증을 보조한다.
   2-1 을은 에러 비율 추정을 위하여 무작위로 비트를 선택하고 이 위치 정보 및 인증 수열의 첫 번째 triad를 갑에게 보낸다.
   2-2 갑은 인증 수열 정보를 확인하고 다를 경우 통신을 중단한다. 그렇지 않다면 인증 수열의 두 번째 triad 및 을이 선택한 위치의 큐빗 생성 bases 및 비트 정보를 전달한다.
   2-3 을은 두 번째 인증 triad를 확인하고 같지 않다면 통신을 중단한다. 을은 갑이 보낸 base와 자신이 측정한 base를 비교하여 bases가 일치하는 큐빗 정보를 보관하고, 에러 율을 추정한다.(원칙적으로 base가 같으면 측정치가 같아야 하기 때문에 이를 이용하여 에러 율을 추정할 수 있다.) 을은 세 번째 인증 triad 및 추정된 에러 비율을 갑에게 알린다. 갑은 세 번째 인증 triad를 확인하고 다르다면 통신을 중단한다.
3) 갑과 을은 에러 비율이 최대 허용치 보다 작다면 공개되지 않은 큐빗의 base를 비교하여 1차 공유키를 얻는다. 에러 비율이 허용치 보다 크다면 도청이 존재한 것으로 판단한다.
4) 갑과 을은 1차 공유키에서 error correction과 privacy amplification 과정[13]을 통하여 최종 공유키를 생성한다. 이 두 과정을 통해, 도청자가 가지고 있는 정보의 양을 줄이고 1차 공유키에 발생된 오류를 없앤다.
5) 갑과 을은 최종 공유키를 차후에 인증 정보로 사용하기 위하여 인증 수열에 덧붙인다.

위의 인증 기법을 이용하는 경우, 인증 수열이 한번만 사용되고 폐기되기 때문에 양자 전송에 이용되는 큐빗은 오류 정정 후 공유되는 키의 길이가 인증 및 신분 확인을 위해 사용된 비트 수보다 훨씬 크게 되도록 선택되어야 한다.

2. 얽힘 상태를 이용한 양자 인증 기법

2002년 Takashi Mihara가 제안한 얽힘 상태를 이용한 인증 기법[14]을 살펴보도록 하자. 이 기법에서는 중재자가 사전에 사용자에게 양자 인증서를 발급해주고,

키 분배 등의 경우 인증이 필요한 때에 발급한 인증서를 확인해주는 방법으로 사용자를 인증한다.

갑이 자신의 신원을 을에게 증명하고자 한다는 가정아래, 인증서 발급과 신원확인 등 두 부분으로 나누어서 인증 기법을 살펴보도록 하겠다.

인증서 발급

(1) 중재자는 고전 암호에서 사용하는 방법과 유사하게 갑의 신원 인증정보를 생성한다. 이 인증정보 I(갑)을 n 비트의 수열이라고 가정하자.

(2) 중재자는 I(갑)을 다음과 같이 쪼갠다.
I(갑) = I_A(갑)⊕I_{pub}(갑)⊕I_{TA}(갑)

(3) 중재자는 I_A(갑)를 갑에게 전달하고 I_{pub}(갑)를 갑의 공개 인증 정보로 공개한다. 이후, 중재자는 I(갑)와 I_{TA}(갑)를 안전하게 저장한다.

인증서 검증에 대한 설명을 위하여 위에서 언급된 갑의 인증정보들을 다음과 같이 비트 형태로 표현하도록 하자.

I(갑) = $(I_1, I_2, \ldots, I_n)$
I_A(갑) = $(I_{A1}, I_{A2}, \ldots, I_{An})$
I_{pub}(갑) = $(I_{pub1}, I_{pub2}, \ldots, I_{pubn})$
I_{TA}(갑) = $(I_{TA1}, I_{TA2}, \ldots, I_{TAn})$

인증서 검증

1) 을은 중재자에게 갑의 신원 인증을 요구한다.

2) 중재자는 다음과 같은 n개의 얽힘 상태 $|\phi_1\rangle, |\phi_2\rangle, \ldots, |\phi_n\rangle$를 생성한다.

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

3) 중재자는 각각의 얽힘 상태의 첫 번째 입자를 갑에게, 두 번째 입자를 을에게 보내고 마지막 입자를 자신이 보관한다.

4) $1 \le i \le n$ 에 대해서 다음을 반복한다.

a. 만약 $I_{Ai}=0$이면, 갑은 자신의 상태에 아무런 연산을 취하지 않고, $I_{Ai}=1$이면 Z연산을 취한다.

b. 만약 $I_{pubi}=0$이면, 을은 자신의 상태에 아무런 연산을 취하지 않고, 그렇지 않으면 Z연산을 취한다.

c. 만약 $I_{TAi}=0$이면, 중재자는 자신의 상태에 아무런 연산을 취하지 않고 그렇지 않으면 Z연산을 취한다.

결과적으로, I_A(갑)⊕I_{pub}(갑)⊕I_{TA}(갑) = 0인 경우, $|\phi_i\rangle$는

$$|\phi'_i\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

으로 변하고, 그렇지 않으면

$$|\phi'_i\rangle = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$$

으로 변한다.

5) 갑, 을, 중재자는 공개 채널을 통하여 자신의 연산의 끝났음을 알린다.

6) 갑, 을, 중재자는 자신이 갖고 있는 모든 입자에 Hadamard 연산 H을 취한다.

만약 I_A(갑)⊕I_{pub}(갑)⊕I_{TA}(갑) = 0이면, $|\phi'_i\rangle$는

$$|\phi''_i\rangle = \frac{1}{2}\sum_{a_i \oplus b_i \oplus t_i = 0} |a_i b_i t_i\rangle$$

이 되고, 그렇지 않으면

$$|\phi''_i\rangle = \frac{1}{2}\sum_{a_i \oplus b_i \oplus t_i = 1} |a_i b_i t_i\rangle$$

이 된다.

7) 갑, 을, 중재자는 공개 채널을 통하여 자신의 연산의 끝났음을 알린다.

8) 갑은 모든 연산이 끝난 자신의 입자를 Z축을 기저로 측정한 결과값 $a=(a_1, a_2, \ldots, a_n)$을 공개 채널을 통하여 중재자에게 전달한다.

9) 을 또한 자신의 입자를 Z축을 기저로 측정한 결과값 $b=(b_1, b_2, \ldots, b_n)$을 공개 채널을 통하여 중재자에게 전달한다.

10) 중재자 또한 자신의 입자를 Z축을 기저로 측정하여 결과값 $t=(t_1, t_2, \ldots, t_n)$를 얻는다.

11) 마지막으로 중재자는 $I(갑)=a\oplus b\oplus t$ 인지를 확인하고 그 결과를 을에게 전달한다.

위의 증명 과정이 올바르게 수행되면, 을은 $a\oplus b\oplus t=I_A\oplus I_{pub}\oplus I_{TA}=I(갑)$을 통해 갑의 신원을 확인할 수 있다.

Ⅲ. 양자 서명 기법

양자 서명 기법은 양자의 고유한 성질을 만족하는 서명 기법으로 중재자가 메시지에 대한 인증을 제공하는 기법이다. 양자 암호에는 계산량에 그 안전성을 둔 공개키 암호가 적용될 수 없으므로 대칭키 암호 형태만이 존재하게 된다. 따라서 기존에 제안된 양자 서명 기법[10,11]은 모두 중재자가 필수적으로 기법에 포함되어 서명을 검증하도록 디자인 되었다.

본 논문에서 소개하는 양자 서명 기법은 2002년에 G. Zeng과 C. H. Keitel이 제안한 기법으로 양자 키 분배 프로토콜과 GHZ triplet 상태를 이용하고 있다.

고전적인 서명과 마찬가지로 양자 서명은 다음의 요건들을 만족시켜야 한다.

1) 수신자나 공격자가 서명이 생성된 이후에 그것에 대해 위·변조가 불가능해야 한다.
2) 서명자는 서명과 서명된 메시지에 대하여 부인할 수 없어야 하며, 수신자는 메시지와 서명을 받았다는 사실을 부인할 수 없어야 한다.
3) 각각의 메시지는 새로운 서명에 할당되어야 하며, 그 서명과 분리되지 않아야 한다.
4) 양자 서명은 양자 역학적 특징을 포함하고 있어야 한다.

일반적인 서명과 달리 양자 서명 기법은 모든 통신에 중재자가 참여하여 서명된 메시지를 인증하고 검증한다. 중재자가 메시지와 서명의 전체 내용을 알 수 있기 때문에, 중재자의 신용 및 중립성이 보장되어야 한다.

양자 서명 기법은 준비, 서명 생성, 그리고 서명 검증의 세 단계로 나누어서 진행된다.

앞으로 서명자를 갑, 서명을 받는 수신자를 을, 공격자를 병이라고 하겠다. 한편 양자 메시지의 집합(큐빗)을 P, 큐빗과 고전비트를 포함할 수 있는 서명의 집합을 S, 양자키 혹은 고전키를 포함하는 키를 K, 양자 서명 알고리즘을 QS, 양자 확인 알고리즘을 QV라고 하자.

서명 $|S\rangle$와 키는 양자적 혹은 고전적 정보일 수 있지만 서명과 확인 알고리즘은 양자적 성질을 만족하여야 한다.

1. 준비 단계

갑, 을, 중재자는 갑과 중재자, 을과 중재자 사이에 비밀키를 공유하고 GHZ triplet 상태를 생성하여 나누어 갖는다.

1) 키 생산 및 분배

갑과 을은 양자키 분배 프로토콜을 이용하여 각각 비밀키 K_a, K_b을 중재자와 공유한다.

2) GHZ 상태의 생산 및 분배

중재자가 갑(혹은 을)의 신청을 받으면 GHZ triplet 상태 수열을 생성한 후, 각 GHZ triplet 상태의 한 입자씩을 갑과 을에게 분배하고 남는 하나는 자신이 보관한다. GHZ triplet 상태는 여덟 개의 orthonormal 상태를 가질 수 있지만 편의상 다음과 같은 상태를 공유한다고 가정한다.

$$|\phi\rangle=\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)$$

단계 1)의 과정을 통해 시스템이 구축되면, 이후의 통신에서는 키분배를 반복하지 않아도 된다. 그러나 단계 2)의 과정은 각각의 서명 생성 요청이 있을 때마다 매번 다시 실행되어야 한다.

2. 서명 생성 단계

갑이 보내고자 하는 메시지를 준비하고 이 메시지에 대한 서명을 생성한다. 즉, 서명 알고리즘 QK_S를 통해 양자 메시지 $|P\rangle$에 대한 서명 $|S\rangle$를 생성한다.

1) 갑은 메시지 n 비트에 대하여 다음과 같은 양자상태 $|P\rangle$를 생성한다.

$$|P\rangle=|p_1\rangle,|p_2\rangle,\ldots,|p_n\rangle$$

임의의 큐빗 $|P_i\rangle$ (i=1,2,....,n)은 orthogonal

basis $\{|0\rangle,|1\rangle\}$를 이용하여 다음과 같이 표현된다.

$$|P_i\rangle = \alpha_i|0\rangle + \beta_i|1\rangle$$

여기에서 α_i,β_i는 $|\alpha_i^2|+|\beta_i|^2=1$을 만족시키는 복소수이다.

위의 식을 이용하여 갑의 메시지 $|P\rangle$을 다음과 같이 표현할 수 있다.

$$|P\rangle = \alpha_1|0\rangle+\beta_1|1\rangle, \alpha_2|0\rangle+\beta_2|1\rangle, \ldots, \alpha_n|0\rangle+\beta_n|1\rangle$$

2) 갑은 자신의 비밀키를 이용하여 메시지 $|P\rangle$에 대한 양자 상태 $|R$ 을 생성한다.

가. 갑은 키 $K_a=\{|K_a^1\rangle, |K_a^2\rangle, \ldots, |K_a^n\rangle\}$ 를 측정 연산자 $M_{K_a}=\{M_{K_a^1}^1, M_{K_a^2}^2, \ldots, M_{K_a^n}^n\}$로 변환한다. 예를 들어, $|K_a^i\rangle=0$인 경우 $M_{K_a^i}^i$를 수직편광판에 대응 시키고, $|K_a^i\rangle=1$인 경우 $M_{K_a^i}^i$를 대각 편광판에 대응시킨다. 이때 측정 연산자 $M_{K_a^i}^i$는 $M_{K_a^i}^i|M_a^i\rangle=\lambda_i|K_a^i\rangle$를 만족시킨다.

나. 변환이 끝나면, 갑은 M_{K_a}을 이용하여 정보 큐빗 수열 $|P\rangle$을 측정하여 $|R\rangle=M_{K_a}|P\rangle=|r_1\rangle,|r_n\rangle,\ldots,|r_n\rangle$을 얻는다. 여기에서 $|r_i\rangle=M_{K_a^i}^i|p_i\rangle$을 만족한다.

이 $|R\rangle$은 갑의 메시지와 관련된 비밀 정보이며 양자적인 특성과 갑의 행동 모두를 포함한다.

3) 갑은 메시지 $|P\rangle$의 각 큐빗과 자신이 가지고 있는 GHZ 입자에 Bell 측정[15]을 한다. 이 경우 다음과 같은 식에 의하여 네 개의 Bell state가 1/4의 확률로 측정된다.

$$\begin{aligned}|\phi\rangle_i &= |p_i\rangle\otimes|\phi\rangle \\ &= \frac{1}{2}\{\ |\Psi_{12}^+\rangle_a(\alpha_i|00\rangle_{Ab}+\beta_i|11\rangle_{Ab}) \\ &\quad +|\Psi_{12}^-\rangle_a(\alpha_i|00\rangle_{Ab}-\beta_i|11\rangle_{Ab}) \\ &\quad +|\Phi_{12}^+\rangle_a(\beta_i|00\rangle_{Ab}+\alpha_i|11\rangle_{Ab}) \\ &\quad +|\Phi_{12}^-\rangle_a(\beta_i|00\rangle_{Ab}-\alpha_i|11\rangle_{Ab})\}\end{aligned}$$

여기에서 a는 갑, A는 중재자, b는 을을 가리키며 네 개의 Bell 상태[16]는 다음과 같다.

$$|\Psi_{12}^+\rangle=\frac{|01\rangle+|10\rangle}{\sqrt{2}},\quad |\Phi_{12}^+\rangle=\frac{|00\rangle+|11\rangle}{\sqrt{2}}$$

4) 갑은 n 번의 Bell 측정을 수행하여 다음과 같은 측정결과 M_a를 얻는다.

$$M_a=\{M_a^1, M_a^2, \ldots, M_a^n\}$$

여기에서 M_a^i는 네 개의 Bell 상태 $\{|\Psi_{12}^+\rangle, |\Psi_{12}^-\rangle, |\Phi_{12}^+\rangle, |\Phi_{12}^-\rangle\}$ 중 하나이다.

5) 갑은 M_a와 $|R\rangle$을 비밀키 K_a로 암호화하여 메시지 $|S$ 에 대한 양자 서명 $|S\rangle$을 생성한다.

$$|S\rangle=K_a(M_a,|R\rangle)$$

M_a가 양자 역학적 Bell 상태로 구성되어 있을 지라도 고전 비트로 표현될 수 있으며, 고전비트로 표현되는 경우 one-time pad를 이용하여 암호화 하고 $|R\rangle$은 "양자 상태 연산" 방법을 통해 암호화 될 수 있다. 또는 M_a를 양자 큐빗 $|M_a\rangle$로 만들어 M_{K_a}을 이용하여 $|M_a\rangle$와 $|R\rangle$ 전체를 "양자 상태 연산"을 통해 암호화 한다.

6) 갑은 메시지 $|P\rangle$와 서명 $|P\rangle$를 을에게 보낸다.

3. 서명 검증 단계

양자 서명 확인 단계에서 을은 중재자의 도움을 통해 갑의 서명을 검증한다.

을은 양자 서명 검증 알고리즘 QV_K을 통하여 갑의 서명 $|S\rangle$을 검증하여 메시지 $|P\rangle$가 갑에 의해 생성됐는지 여부를 확인한다. 이 단계에서는 을이 서명에 사용된 갑의 비밀키를 가지고 있지 않기 때문에 서명을 검증하기 위해서 중재자의 개입이 필수 불가결하다.

1) 을은 자신의 GHZ 입자 열을 x방향으로 측정한다. 측정 결과를 M_b라고 하면 M_b는 다음과 같이 표현된다.

$$M_b=\{M_b^1, M_b^n, \ldots, M_b^n\}$$

여기에서 M_b^i는 $|+x\rangle=1/\sqrt{2}(|0\rangle+|1\rangle)$나

$|-x\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle)$ 중 하나이다.

을은 자신의 비밀키 K_b를 이용하여 갑과 같은 방법으로 $M_b, |S\rangle, |P\rangle$을 암호화한 뒤 그 결과값 $y_b = K_b(M_b, |S\rangle, |P\rangle)$를 중재자에게 전달한다.

2) 중재자는 K_a, K_b를 이용해 y_b를 복호화 한다.

중재자는 복호화한 정보를 가지고 GHZ 상태의 연관성[17]을 이용하여 $|R'\rangle$을 생성한다. 중재자는 메시지의 무결성을 살펴보기 위하여 자신이 생성한 $|R'\rangle$과 서명에서 복호화 시킨 $|R\rangle$이 같은지를 살펴보고 그 결과를 다음과 같이 γ에 기록한다.

$$\gamma = \begin{cases} 1 & \text{만약 } |R'\rangle = |R\rangle = M_{K_a}|P\rangle \\ 0 & \text{만약 } |R'\rangle \neq |R\rangle = M_{K_a}|P\rangle \end{cases}$$

3) 중재자는 자신의 GHZ 입자를 측정하여 측정결과 $M_t = \{M_t^1, M_t^2, ..., M_t^n\}$를 얻는다. 이전 단계에서 중재자는 갑과 을의 측정 결과 M_a, M_b를 얻었기 때문에 쉽게 자신의 상태를 결정할 수 있다. 여기에서 M_t^i는 을의 측정기저와 같은 $|+x\rangle$이거나 $|-x\rangle$이다.

중재자는 $M_a, M_b, M_t, \gamma, |S\rangle$을 키 K_b로 암호화한 결과값 y_{tb}를 을에게 보낸다.

$$y_{tb} = K_b(M_a, M_b, M_t, \gamma, S\rangle)$$

4) 을은 y_{tb}을 복호화하여 $M_a, M_b, M_t, |S\rangle, \gamma$ 를 얻는다.

5) 을은 매개변수 γ를 통하여 갑의 서명 $|S\rangle$를 검증한다. 만약 $\gamma = 0$이면 서명은 위조된 것이며 을은 그 메시지 $|P\rangle$를 즉시 버린다. 만약 $\gamma = 1$이면 을은 다음 단계를 수행한다.

6) 을은 M_a, M_t 및 다른 변환 (뒤에서 다룸)등을 이용하여 메시지 $|P'\rangle$을 계산한다.

만약 $|P'\rangle = |P\rangle$이면, 서명은 올바르게 생성되었으므로 을은 $|P\rangle$를 받아들인다. 그렇지 않으면 메시지를 거부한다.

$|P'\rangle$은 을의 GHZ 입자가 검증단계 1에서 측정되었기 때문에 계산으로부터 얻어지는 값이다. 만약 갑의 결과가 $|\Psi_{12}^+\rangle$이거나 $|\Psi_{12}^-\rangle$ 인 경우, 을의 GHZ 입자에 대한 density matrix는 다음과 같다.

$$\rho_b = |\alpha_i|^2 |0\rangle_b b\langle 0| + |\beta_i|^2 |1\rangle_b b\langle 1|$$

반면, 나머지 두 경우, 즉 $|\Phi_{12}^+\rangle$이거나 $|\Phi_{12}^-\rangle$인 경우, 을의 GHZ 입자에 대한 density matrix는 다음과 같다.

$$\overline{\rho}_b = |\beta_i|^2 |0\rangle_b b\langle 0| + |\alpha_i|^2 |1\rangle_b b\langle 1|$$

따라서 을은 $|p_i\rangle$을 복구하기 위하여 M_a, M_t 및 다음 변환 등이 필요하다.

$$|\Psi_{12}^+\rangle_a |+x\rangle_A \rightarrow I, \quad |\Phi_{12}^+\rangle_a |+x\rangle_A \rightarrow \sigma_x$$
$$|\Psi_{12}^+\rangle_a |-x\rangle_A \rightarrow \sigma_z, \quad |\Phi_{12}^+\rangle_a |-x\rangle_A \rightarrow \sigma_x\sigma_z$$
$$|\Psi_{12}^-\rangle_a |+x\rangle_A \rightarrow \sigma_z, \quad |\Phi_{12}^+\rangle_a |+x\rangle_A \rightarrow \sigma_x\sigma_z$$
$$|\Psi_{12}^-\rangle_a |-x\rangle_A \rightarrow I, \quad |\Phi_{12}^-\rangle_a |-x\rangle_A \rightarrow \sigma_x$$

여기에서 $\sigma_i, i = x, y, z$는 Pauli matrix 이고, I는 항등 행렬이다.

예를 들어서 갑의 결과값이 $|\Psi_{12}^+\rangle$이면, 중재자와 을의 얽힌 상태는 $|\varphi\rangle_{AB} = \alpha_i|00\rangle + \beta_i|11\rangle$이어야 한다. 이는 다음과 같이 표현될 수 있다.

$$|\varphi\rangle_{Ab} = \frac{\sqrt{2}}{2}|+x\rangle_A(\alpha_i|0\rangle_b + \beta_i|1\rangle_b) + \frac{\sqrt{2}}{2}|-x\rangle_A(\alpha_i|0\rangle_b - \beta_i|1\rangle_b)$$

중재자의 결과가 $|+x\rangle$이면 I연산을 취해 메시지 $|p_i\rangle = \alpha_i|0\rangle_b + \beta_i|1\rangle_b$를 얻어낼 수 있고, $|-x\rangle$이면 σ_z 연산을 취해 메시지 $|P_i\rangle$를 복구할 수 있다.

3. 안전성 분석

3.1 위조 불가능

을이 갑의 서명을 위조하려한다고 가정했을 때, 을은 갑의 비밀키(서명키) K_a를 알 수 없기 때문에 올바른 비밀 정보 $|R\rangle$을 생성할 수 없으며, 이에 따라 변수 γ값이 올바르지 않게 되어 위조가 불가능하다.

위조자가 갑이나 을의 키의 일부 정보를 알고 있다고 하더라도, 갑의 측정 결과 M_a값을 알 수 없기 때문에 검증 조건 $|P'\rangle = |P\rangle$을 만족시킬 수 없다. 즉, GHZ 상태의 연관성이 공격자의 위조를 막아준다.

3.2 부인 방지

갑은 서명 생성 시 자신의 키 K_a에 대한 정보가 서명에 포함되므로 자신이 생성한 서명을 부인할 수 없다. 한편 을은 갑의 서명 $|S\rangle$를 검증하기 위해서 중재자의 도움을 요청할 수 밖에 없으므로, 서명 수신을 부인할 수 없다.

중재자의 의존도를 줄이기 위해서 다음과 같은 방법을 사용할 수 있다. 서명 검증 과정 1에서 을은 y_b를 중재자가 아니라 갑에게 전달한다. 갑은 새로운 서명값 $|S'\rangle = K_a(M_a, |R\rangle, y_b)$을 생성하여 중재자에게 보낸다. 중재자는 단계 3에서 y_{tb}를 다음과 같이 변형하여 을에게 보낸다.

$$y_{tb}' = K_b(M_a, M_b, M_t, \gamma, |S'\rangle)$$

이러한 과정이 끝나면 $|S\rangle$에는 갑과 을의 키가 모두 포함되어 있게 되므로 을은 갑에게서 받은 서명을 부인할 수 없다.

Ⅳ. 결 론

지금까지 양자 역학의 특징을 이용한 양자 인증 기법과 양자 서명 기법에 대해 살펴보았다. 인증 기법은 양자 키분배 프로토콜에서 발생할 수 있는 문제를 보완하기 위해서 앞으로도 연구가 계속 되어야 하는 부분이며 양자 암호가 차세대 암호로 개발되는 과정에서 반드시 수반되어야 하는 과정이다. 양자 서명 기법에서는 중재자에 대한 의존도가 높고 중재자가 악의적일 경우에 대한 대책이 현재까지 나와 있지 않다. 양자 서명과 관련하여 위와 관련된 다양한 접근 방법이 논의되어야 할 것이다. 그만큼 양자 암호 분야에는 양자 키 분배 프로토콜뿐만 아니라 양자 secret sharing 프로토콜, 양자 인증 스킴, 양자 서명 스킴 등 다양한 분야가 존재한다. 이에 대한 인식제고와 함께 다양한 양자 암호 분야에 대한 지속적인 관심과 연구 활동이 이루어져야 할 것이다.

참 고 문 헌

[1] www.magiqtech.com

[2] Charlse H.Bennett and Gilles Brassard, "Quantum Cryptography : Public key distribution and coin tossing" in proceeding of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India 1984, (IEEE Press, 1984)

[3] Artur K. Ekert, "Quantum Cryptography Based on Bell's theorem" Phys Rev. Lett, 67(6) : 661-663, 1991

[4] A. Fiat, A. Shamir. "How to prove yourself : practical solutions to identification and signature problems." Lecture Notes in Computer Science, 263(1987), 186-194

[5] U. Feige, A. Fiat, A. Shamir. "Zero-knowledge proofs of identity." Journal of Cryptology, 1(1988), 77-94

[6] L. C. Guillou, J.-J. Quisquater. "A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory." Lecture Notes in Computer Science, 330(1988), 123-128.

[7] Daniel Ljunggren, Mohamed Bourennane, and Anders Karlsson, "Authority-based user authentication in quantum key distribution" Phys. Rev. A62, 022305 (2000)

[8] Guihua Zeng and Weiping Zhang, "Identity verification in quantum key distribution" Phys. Rev. A61, 022303 (2000)

[9] Bao-Sen Shi, Jian Li, Jin-Ming Liu, Xiao-Feng Fan, Guang-Can Guo, "Quantum key distribution and quatnum authentication based on entangled state" Phys. Lett. A281, 83-87 (2001)

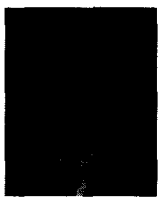
[10] Guihua Zeng and Christoph H. Keitel, "Arbitrated quantum-signature scheme" Phys. Rev. A65, 042312 (2002)

[11] Hwayen Lee, Changho Hong, Hyunsang Kim, Joingin Lim, HyungJin Yang, "Arbitrated quantum signature scheme with message recovery" Physics letters A 321, 295-300 (2005)

[12] Miloslav Dusek, Ondrj Haderka, Martin Hendrych and Robert Myska, "Quantum

identification system", Phys Rev. A60, 149 (1998)
[13] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptology 5, 3 (1992)
[14] Takashi Mihara, "Quantum identification schemes with entanglements", Phys Rev, A65, 052326
[15] A. Nielsen and L. Chuang, "Quantum information and Quantum information", CAMBRIDGE UNIVERSITY PRESS
[16] P.G.Kwait, K.Mattle, H.Weinfurter, and A.Zeilinger, "New High-Intensity Source of Polarization-Entangled Photon Pairs" Phys. Rev. Lett. 75, 4337 (1995)
[17] M.Hillery, V.Buzek, and A.Berthiauma, "Quantum secret sharing" Phys. Rev. A59, 1829 (1999)

〈著 者 紹 介〉



이 덕 진 (Duk-jin Lee)

2003년 2월 : 고려대학교 자연과학대학 물리학과 학사
2003년 3월~현재 : 고려대학교 정보보호대학원 석사과정
관심분야 : 양자 암호, 암호 프로토콜

이 화 연 (Hwa-Yean Lee)

2001년 2월 : 고려대학교 수학과 학사
2003년 2월 : 고려대학교 정보보호대학원 석사
2003년 3월~현재 : 고려대학교 정보보호대학원 박사과정
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

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 메릴랜드대학교 교환교수
1992년 3월~현재 : 고려대학교 자연과학대학 물리학과 교수
2001년 3월~현재 : 고려대학교 정보보호대학원 겸임교수
관심분야 : 양자암호, 암호프로토콜