情報保護學會論文誌
第13券 第1號, 2003. 2

메시지 복구형 양자 서명 기법*

이 화 연**, 양 형 진***, 이 동 훈**, 이 상 진**, 임 종 인**

Quantum signature scheme with message recovery

Hwayean Lee**, HyungJin Yang***, Dong-Hoon Lee**, Sangjin Lee**, Jongin Lim**

요 약

본 논문에서는 Greenberger-Horne-Zeilinger(GHZ) 상태를 사용하는 메시지 복구형 양자 서명 기법을 제시한다. 이 기법은 기존의 양자 서명과 마찬가지로 중재자가 서명을 확인해주는 형식을 띄고 있으나, 기존에 제시된 양자 서명 기법에 비하여 메시지를 암호화시켜 외부에서 메시지에 대한 기밀성을 동시에 제공한다. 이와 더불어 전송상 효율을 높였으며, Bell측정을 사용하지 않고 단순 측정만을 사용함으로써 사용자의 편의를 증가시켰다.

ABSTRACT

We propose a quantum signature scheme with message recovery implemented by a symmetrical quantum key cryptosystem and Greenberger-Horne-Zeilinger(GHZ) triplet states. The suggested scheme relies on the availability of an arbitrator and can be divided into two schemes : one is using a public board and the other is not. The two schemes give us the confidentiality of a message and the higher efficiency in transmission. We propose a quantum signature scheme with message recovery using Greenberger-Horne-Zeilinger(GHZ) triplet states.

Keyword : *양자 암호, 양자 서명 기법*

Ⅰ. 서 론

양자 암호는 기존의 암호 시스템과 달리 양자 역학의 고유한 성질을 이용하도록 고안된 암호 시스템이다. 양자 계산에서는 양자 역학의 고유한 성질인 중첩(superposition)상태를 이용하여 정보를 표현하기 때문에 기존 시스템에 비하여 적은 자원을 가지고도 복잡한 연산을 빠르게 할 수 있다. 또한 측정에 의해 상태가 붕괴되기 때문에 도청을 확인할 수 있게되어 암호 시스템의 안전성을 높일 수 있다.

현재까지 양자 키 분배 프로토콜(Quantum key distribution)[1~4]과 이 프로토콜 등의 안전성 분석[5~7], 양자 식별 기법(Quantum identification scheme)[8,9], 양자 서명 기법(Quantum signature scheme)[10,11] 등을 비롯하여 여러 분야에서 연구가 진행 중이다.

전통적인 서명기법은 평문과 서명을 함께 보내는 메시지 첨부형(signature with appendix)과 서명만을 보내어 서명된 평문을 서명에서 복구할 수 있는 메시지 복구형(signature with message recovery)으로 분류된다. 또한 전통적인 서명기법에서의 서명은 임의의 검증자에 의해서 검증 가능한 특성을 지니고 있다. 임의의 검증자에 의해 검증 가능한 양자 서명 기법은 아직 문헌에서 제안되지 않았으며 [10,11]에서 제안된 양자 서명 기법은 오직 서명자가 지정한 검증

* 본 연구는 고려대학교 특별연구비에 의해 수행되었습니다.
** 고려대학교 정보보호기술연구센터(CIST)({hylee, donghlee, sangjin, jilim}@cist.korea.ac.kr)
*** 고려대학교 정보보호대학원(yangh@korea.ac.kr)

자(designated confirmer)에 의해서만 검증 가능한 메시지 첨부형 기법이다.

본 논문에서는 지정한 검증자가 있는 메시지 복구형 양자 서명기법을 제안한다. 이 기법에서 서명의 검증은 [10]에서와 동일하게 중재자를 통하여 이루어지도록 고안되었고, 메시지의 암호화는 중재자와 서명 수신자 이외에는 메시지를 확인할 수 없도록 키로 한번 더 암호화하도록 하였다. 이 서명 기법에는 기존의 공개 보드를 이용하는 방법과 공개 보드를 이용하지 않고 서명을 전달하는 두 가지 방법이 존재한다.

기존에 제시되었던 양자 서명 기법[10]에 비하여 본 논문에서 제시하는 양자 서명 기법은 메시지를 암호화하여 타인이 메시지에 대한 정보를 얻을 수 없도록 했을 뿐만 아니라, 전송상의 효율을 높였으며, 측정에 있어서 간단한 방법을 사용하여 부담을 줄였다. [10]에서 제시된 양자 서명 기법에 메시지 기밀성을 제공하기 위해서는 다음과 같은 과정이 추가되어야 한다. 서명 생성자가 중재자와 공유된 키를 이용하여 메시지를 암호화시켜 수신자에게 전송한다. 수신자는 암호화된 메시지와 서명을 중재자에게 전송한다. 이 경우 [10]에서 제시된 양자 서명 기법의 수정이 필요하지만, 그것을 고려하지 않는다고 가정한다. 중재자는 메시지를 서명 생성자와 공유된 키로 복호화 한 뒤, 이를 다시 수신자와 공유된 키로 암호화시켜 수신자에게 전송한다. 위와 같은 과정은 통신상에서도 효율을 낮출 뿐만 아니라, 서명 생성자와 수신자, 그리고 중재자에게 번거로운 일이 된다.

본격적으로 양자 서명 기법을 제시하기 전에 2절에서 기본적인 양자역학의 성질을 살펴보고, 3절에서 메시지 복구 양자 서명 기법을 제시하도록 한다. 4절에서는 제안된 기법의 안전성을 분석하고, 제시된 서명 기법들을 비교하도록 한다. 마지막 5절에서는 결론을 짓도록 하겠다.

II. 양자역학의 기본 성질

양자 계산에서의 정보의 최소 단위를 양자 비트(quantum bit) 또는 큐빗(qubit)이라고 한다. 보통 고전 비트 0,1에 대응하여 $|0\rangle$ 또는 $|1\rangle$을 사용한다. 일반적인 큐빗은 $|\phi\rangle=\alpha|0\rangle+\beta|1\rangle$로 표현되며, 여기서 α,β는 복소수이다. 이때 $|\alpha|^2,|\beta|^2$은 각각 $|0\rangle$과 $|1\rangle$이 측정될 확률을 나타낸다. α,β는 임의의 값을 가질 수 있기 때문에, 큐빗의 상태는 일반적으로 $|0\rangle$도 $|1\rangle$도 아닌 중첩 상태이다. 이러한 중첩상태를 측정하게 되면 큐빗은 측정의 고유상태인 $|0\rangle$또는 $|1\rangle$상태로 변하게 되어 이전에 가지고 있던 중첩에 대한 정보를 잃어버리게 된다.

편광의 예를 들어 살펴보자.

수평과 수직 방향으로 편광된 상태를 각각 $|0^\circ\rangle$와 $|90^\circ\rangle$ 또는 $\begin{pmatrix}1\\0\end{pmatrix}$과 $\begin{pmatrix}0\\1\end{pmatrix}$로 표현하자. 그러면, 45°나 135°로 편광된 광자는 $|0^\circ\rangle$와 $|90^\circ\rangle$의 선형결합으로 다음과 같이 표현된다.

$$|45^\circ\rangle=\frac{1}{\sqrt{2}}\left(\begin{pmatrix}1\\0\end{pmatrix}+\begin{pmatrix}0\\1\end{pmatrix}\right)=\frac{1}{\sqrt{2}}(|0^\circ\rangle+|90^\circ\rangle)$$

$$|135^\circ\rangle=\frac{1}{\sqrt{2}}\left(-\begin{pmatrix}1\\0\end{pmatrix}+\begin{pmatrix}0\\1\end{pmatrix}\right)=\frac{1}{\sqrt{2}}(-|0^\circ\rangle+|90^\circ\rangle)$$

역으로, $|0^\circ\rangle$, $|90^\circ\rangle$의 상태는 $|45^\circ\rangle$, $|135^\circ\rangle$의 선형결합으로 표시된다.

$$|0^\circ\rangle=\frac{1}{\sqrt{2}}(|45^\circ\rangle-|135^\circ\rangle)$$

$$|90^\circ\rangle=\frac{1}{\sqrt{2}}(|45^\circ\rangle+|135^\circ\rangle)$$

위 식에 따라 $|0\rangle$상태를 대각형(×)편광판으로 측정하면 45°나 135°로 편광된 빛이 각각 1/2의 확률로 측정된다. 측정 후의 상태는 각각 $|45^\circ\rangle$와 $|135^\circ\rangle$인데, 이는 $|0^\circ\rangle$와 $|90^\circ\rangle$ 상태의 선형결합이기 때문에 십자형(+)편광판을 사용하여 다시 측정하더라도 $|0^\circ\rangle$와 $|90^\circ\rangle$가 각각 1/2의 확률로 측정된다. 이는 십자형 편광판과 관련된 정보를 완전히 소실하였다는 것을 의미한다.

III. 양자 서명 기법

양자 서명 기법을 소개하기 전에 앞으로 사용될 용어를 정의하도록 한다. Alice는 서명 생성자, Bob은 서명 수신자를 표현한다.

본 논문에서 제시하는 양자 서명 기법은 기존의 양자 서명 기법[10]과 마찬가지로, 초기 단계(initial phase), 서명 단계(signature phase), 검증 단계(verification phase)로 나누어진다.

초기 단계(Initial phase)는 서명 기법을 실행하기 전에 사전에 준비하는 과정으로, 중재자와 Alice, 중재자와 Bob 사이에 기존에 정립된 양자 키 분배 프로토콜[1~4] 등을 사용하여 키를 분배하는 과정이 포함

된다. 이러한 양자 키 분배 프로토콜 등은 완전 안전성이 보장된다고 증명[5~7]되어 있기 때문에 본 논문에서는 그냥 받아들이고 사용하도록 한다. 이와 더불어 초기 단계에는 서명 검증을 위하여 Greenberger - Horne - Zeilinger(GHZ) 상태[13,14]를 중재자가 생성하여 Alice와 Bob에게 하나씩 분배하는 과정이 포함된다.

서명단계(signature phase)는 Alice가 메시지 P를 생성하고 이에 대한 서명 값 S를 생성하는 과정이다.

마지막으로 검증 단계(verification phase)는 Bob이 중재자의 도움을 받아 서명을 검증하는 과정으로 Bob과 중재자의 연산 두 부분으로 나눠질 수 있다.

먼저 공개보드를 이용하여 서명을 생성하는 경우를 살펴보도록 하겠다.

서명 기법의 초기 단계에서는 위에서 설명한 대로 Alice와 중재자, Bob과 중재자 사이에 양자 키 분배 프로토콜을 이용하여 키를 분배한다. 이후 메시지의 개수가 n인 경우 중재자가 n개의 GHZ 상태 $|\Psi\rangle=|\phi_1,\phi_2,\ldots,\phi_n\rangle$를 생성하여 Alice와 Bob에게 큐빗을 분배한다.

초기 단계(initial phase)

1. Alice와 중재자, Bob과 중재자가 키를 공유한다. 이를 각각 K_a, K_b로 표기한다.
2. 중재자가 n개의 GHZ 상태 $|\Psi\rangle=|\phi_1,\phi_2,\ldots,\phi_n\rangle$를 생성하고 Alice와 Bob에게 큐빗을 분배한다.

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

   (여기에서 a는 Alice, b는 Bob, A는 중재자가 나눠 갖게 될 큐빗이다.)

서명 단계(Signature phase)는 Alice가 서명을 생성하는 단계인데 그 과정은 다음과 같다.

우선 Alice는 서명할 메시지 $P=(p_1,p_2,\ldots,p_n)$를 준비한다(이때 p_i는 고전 비트를 의미한다). p_i가 0이면 자신이 가진 GHZ 상태에 아무런 연산을 취하지 않고, p_i가 1이면, 비트 플립연산 (X)을 취한다. 이후 GHZ 상태를 측정하여 측정치 $a=(a_1,a_2,\ldots,a_n)$ 를 구한다. 한편, 메시지 P를 중재자와 공유된 키 K_a에 대응하는 편광판을 이용하여 양자 상태로 변화시킨다.

예를 들어, $K_{a_i}=0$ 이면 십자형 (+)편광판을 사용하고, $K_{a_i}=1$ 이면 대각형 (×)편광판을 사용한다고 하자. 십자형 편광판에서 0은 |—〉으로 표현하고, 1은 |↑〉로 표현하며, 대각형 편광판의 경우 0은 |／〉로, 1은 |＼〉로 표현한다. 이러한 방법으로 고전 메시지를 양자 상태로 변환시키면, 키 K_a를 알아야만 정확한 P에 대한 정보를 얻을 수 있다.

위와 같이 측정치 a와 P를, 기존의 서명 기법[10]과 같은 방법으로 암호화하여 서명을 생성한다. 이때 중재자와 공유된 키 K_a가 비밀키의 역할을 하게 된다. 이를 수식으로 적으면 다음과 같이 나타낼 수 있다.

$$|S\rangle=E_{K_a}(a,P)$$

Alice는 최종적으로 생성된 서명 $|S\rangle$를 Bob에게 양자 채널을 이용하여 전송하고, 미리 구해놓은 측정치 a를 공개보드에 올려놓는다.

서명 생성(signature phase) 단계

1. Alice는 메시지 $P=(p_1,p_2,\ldots,p_n)$를 생성하고 다음의 연산을 취한다.

   $p_i=0$ 인 경우 : 자신의 GHZ 상태에 연산을 취하지 않는다.

   $p_i=1$ 인 경우 : 자신의 GHZ 상태에 $X=\begin{pmatrix}0&1\\1&0\end{pmatrix}$ 연산을 취한다.
2. Alice는 자신의 GHZ 상태를 측정하여 측정치 $a=(a_1,a_2,\ldots,a_n)$를 생성한다.
3. Alice는 중재자와 공유된 키 K_a에 대응하는 편광판을 통해 메시지 P를 양자상태로 만든다.

   $|R_a\rangle=M_{K_a}(P)=\{|r_{a_1}\rangle,|r_{a_2}\rangle,\ldots,|r_{a_n}\rangle\}$,

   $|r_{a_i}\rangle=M^{i}_{K_{a_i}}|p_i\rangle$
4. Alice는 위에서 생성한 $a,|R\rangle$을 키 K_a로 암호화하여 서명 $|S\rangle$를 생성한다.

   $|S\rangle=E_{K_a}(a,P)$
5. Alice는 서명 $|S\rangle$를 Bob에게 전송하고, a를 공개보드에 기재한다.

서명 검증 단계(Verification phase)는 서명을 검증하는 단계로서 중재자가 필수적인 단계이다. Alice가 생성한 서명 $|S\rangle$가 중재자와 공유된 키 K_a로 암호화되어 있기 때문에, Bob 혼자서는 이를 검증할 수 없다.

서명 검증 단계는 우선 Bob이 메시지를 복구하는 것으로 시작된다. 자신의 GHZ 상태를 측정하여 측정치 $b=(b_1,b_2,\ldots,b_n)$를 구하고 공개보드에서 a를

가져와 메시지 $P=a\oplus b$를 복구한다.

메시지 P가 복구될 수 있는 원리를 살펴보면 다음과 같다. 처음 공유된 GHZ 상태는 Alice, Bob, 중재자가 모두 같은 비트만을 측정하도록 얽혀져 있었다. 그런데 Alice가 $p_i=1$인 경우에만 비트 플립 연산 (X)을 취했기 때문에, $p_i=1$인 경우에만 Alice의 측정치가 중재자와 Bob의 측정치와 반대로 나오게 된다. 따라서 a에 Bob만의 측정치 b를 XOR 하면 원래의 메시지 P가 복구된다.

Bob은 위와 같은 방법으로 복구한 P를, Alice가 사용한 방법과 같이, 중재자와 공유된 키 K_b에 대응하는 편광판을 이용하여 양자 상태로 변형시킨다. 이 결과값을 $|R_b\rangle$라고 하자.

Bob은 Alice에게 받은 서명 $|S\rangle$와 $|R_b\rangle$를 K_b로 암호화시킨 결과값 $|T\rangle=K_b(|R_b\rangle,|S\rangle)$를 중재자에게 전송한다.

중재자는 Bob으로부터 받은 $|T\rangle$를 K_b로 복호화 하여 서명 $|S\rangle$와 $|R_b\rangle$를 알아낸다. 또한, K_a를 사용하여 a와 $|R_a\rangle$를 복호화 한다. 한편, 중재자가 가지고 있는 GHZ상태를 측정하여 측정치 $A=(A_1,A_2,\ldots,A_n)$를 구하고 메시지 P를 Bob과 같은 방식으로 계산해 낸다. 이때 중재자는 공개 보드에 올려진 Alice의 측정치 a를 사용하지 않고, 서명에 포함되어 있는 a를 이용하는데, 이는 공개보드 무결성을 한 번 더 검증할 수 있게 한다.

중재자는 복호화 한 메시지 P를 이용하여 $|R'_a\rangle$를 계산하고 $|R_a\rangle$와 같은 지 여부를 확인한다. 같으면 $\gamma_a=0$으로, 다르면 $\gamma_a=1$로 놓는다. 즉 γ_a가 Alice에 대한 서명의 진위 여부를 나타내는 값이 된다. 한편 중재자는 메시지 P를 이용하여 $|R'_b\rangle$를 계산하고 $|R_b\rangle$와 같은 지 여부를 확인한다. 같으면 $\gamma_b=0$으로, 다르면 $\gamma_b=1$로 놓는다. 여기서 γ_b의 값은 Bob이 복구한 메시지에 대한 검증이라고 할 수 있다.

마지막으로 중재자는 $|S\rangle$로부터 계산한 Alice의 측정치 a와 γ_a,γ_b를 Bob과 공유된 키 K_b로 암호화하여 Bob에게 전달한다.

Bob은 이 내용을 복호화 하여, γ_a,γ_b를 통하여 Alice의 서명을 인증하고, 자신의 메시지가 정확한지 여부를 확인한다. γ_a,γ_b가 모두 0인 경우는 서명생성과 메시지 전달이 잘 수행된 것이지만, $\gamma_a=1$이면 γ_b값에 상관없이 서명을 거부한다. 한편 $\gamma_a=0$이고 $\gamma_b=1$인 경우는 서명은 인정하되, 중재자로부터 받은 a로 메시지를 다시 복원해야한다.

서명 검증(verification phase) 단계

1. Bob은 자신이 가진 GHZ 상태를 측정하여 측정치 $b=(b_1,b_2,\ldots,b_n)$를 생성한다.
2. Bob은 공개보드에서 a를 가져와 메시지 P를 다음과 같이 복구한다.
   $P=a\oplus b$
3. Bob은 중재자와 공유된 키 K_b에 대응하는 편광판을 통해 메시지 P를 양자상태로 만든다.
   $|R_b\rangle=M_{K_b}(P)=\{|r_{b1}\rangle,|r_{B2}\rangle,\ldots,|r_{bn}\rangle\}$,
   $r_{bi}=M^i_{K_b}|p_i\rangle$
4. Bob은 Alice로부터 받은 서명 $|S\rangle$와 $|R_b\rangle$를 비밀키 K_b로 암호화시킨 결과값 $|T\rangle$를 중재자에게 전송한다.
   $|T\rangle=E_{K_b}(|S\rangle,|R_b\rangle)$
5. 중재자는 $|T\rangle$를 키 K_b,K_a로 복호화 하여 $a,|R_a\rangle$, $|R_b\rangle$를 알아낸다.
6. 중재자는 자신의 GHZ 상태를 측정하여 측정치 $A=(A_1,A_2,\ldots,A_n)$를 구하고 메시지 P를 계산한다.
7. 중재자는 $|R'_a\rangle,|R'_b\rangle$를 생성하고, $|R_a\rangle,|R_b\rangle$와 같은지 여부를 γ_a,γ_b에 기록한다.
   $\gamma_a=\begin{cases}0 & \text{if } |R'_a\rangle=|R_a\rangle\\ 1 & \text{if } |R'_a\rangle\neq|R_a\rangle\end{cases}$
   $\gamma_b=\begin{cases}0 & \text{if } |R'_b\rangle=|R_b\rangle\\ 1 & \text{if } |R'_b\rangle\neq|R_b\rangle\end{cases}$
8. 중재자는 서명 $|S\rangle$로부터 이끌어낸 a와 γ_a,γ_b 그리고 $|S\rangle$를 키 K_b로 암호화한 값 $|V\rangle$를 Bob에게 전달한다.
   $|V\rangle=E_{K_b}(a,\gamma_a,\gamma_b,|S\rangle)$
9. Bob은 $|V\rangle$를 복호화 하여 a,γ_a,γ_b를 구한다. $\gamma_a=0$이면 서명을 인정하고 그렇지 않으면 서명을 거부한다. $\gamma_b=1$인 경우 복호화 한 a를 통해 메시지 P를 다시 복구한다.

이상으로 공개보드를 사용한 양자 서명 기법을 살펴보았다. 공개보드를 사용하지 않는 경우는 Bob이 메시지를 복구하는 작업이 중재자의 서명 검증 이후에 이루어진다는 단점이 있기는 하지만, 메시지에 대한 어떤 정보도 중재자 외에는 전달되지 않고, Bob의 신원을 한번 더 검증할 수 있을 뿐만 아니라, Bob 역시 중재자를 한번 더 검증할 수 있다.

공개 보드를 사용하지 않는 양자 서명 기법의 초기단계는 위에서 제시한 기법과 동일하기 때문에 서

명 단계와 서명 검증단계만을 간단히 정리하겠다.

서명 생성(signature phase) 단계

1. Alice는 메시지 $P=(p_1, p_2, \ldots, p_n)$를 생성하고 다음의 연산을 취한다.
   $p_i=0$인 경우 : 자신의 GHZ 상태에 연산을 취하지 않는다.
   $p_i=1$ 인 경우 : 자신의 GHZ 상태에
   $X=\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$연산을 취한다.
2. Alice는 자신의 GHZ 상태를 측정하여 측정치 $a=(a_1, a_2, \ldots, a_n)$를 생성한다.
3. Alice는 중재자와 공유된 키 K_a에 대응하는 편광판을 통해 메시지 P를 양자상태로 만든다.
   $|R_a\rangle = M_{K_a}(P) = \{|r_{a1}\rangle, |r_{a2}\rangle, \ldots, |r_{an}\rangle\}$,
   $r_{ai} = M^{i}_{K_a}|p_i\rangle$
4. Alice는 위에서 생성한 $a, |R_a\rangle$을 키 K_a로 암호화하여 서명 $|S\rangle$를 생성한다.
   $|S\rangle = E_{K_b}(a, |R_a\rangle)$
5. Alice는 서명 $|S\rangle$를 Bob에게 전송한다.

서명 검증(verification phase) 단계

1. Bob은 자신이 가진 GHZ 상태를 측정하여 측정치 $b=(b_1, b_2, \ldots, b_n)$를 생성한다.
2. Bob은 Alice로부터 받은 서명 $|S\rangle$와 b를 비밀키 K_b로 암호화시켜 결과값 $|T\rangle$를 중재자에게 전송한다.
   $|T\rangle = E_{K_b}(|S\rangle, b)$
3. 중재자는 $|T\rangle$를 키 K_b, K_a로 복호화하여 $a, |R_a\rangle$, b를 알아낸다.
4. 중재자는 자신의 GHZ 상태를 측정하여 측정치 $A=(A_1, A_2, \ldots, A_n)$를 구하고 메시지 P를 계산한다.
5. 중재자는 $|R'_a\rangle$를 생성하여 $|R_a\rangle$와 같은 지 여부를 검사하여 γ_a에 기록한다.
   $\gamma_a = \begin{cases} 0 & \text{if } |R'_a\rangle = |R_a\rangle \\ 1 & \text{if } |R'_a\rangle \neq |R_a\rangle \end{cases}$
   또한 Bob으로부터 받은 측정치 b와 자신의 측정치 A가 같은 지 여부를 검사하여 γ_b에 기록한다.
   $\gamma_a = \begin{cases} 0 & \text{if } b=A \\ 1 & \text{if } b\neq A \end{cases}$
6. 중재자는 $\gamma_b=1$일 경우, 서명 수신자가 올바르지 않다고 판단하고 Alice에게 이 사실을 통보하고 멈춘다.
   한편 $\gamma_b=0$인 경우, 키 K_b에 대응하는 편광판을 통해 메시지 P를 양자상태로 만든다.
   $|R_A\rangle = M_{K_b}(P) = \{|r_{A1}\rangle, |r_{A2}\rangle, \ldots, |r_{An}\rangle\}$,
   $r_{bi} = M^{i}_{K_b}|p_i\rangle$
7. 중재자는 서명 $|S\rangle$와 이로부터 이끌어낸 a와 γ_a 그리고 $|R_A\rangle$를 키 K_b로 암호화한 값 $|V\rangle$를 Bob에게 전달한다.
   $|V\rangle = E_{K_b}(a, \gamma_a, |R_A\rangle, |S\rangle)$
8. Bob은 $|V\rangle$를 복호화 하여 $a, \gamma_a, |R_A\rangle$를 구한다.
9. Bob은 복호화한 a를 통해 메시지 P를 구하고, $|R'_A\rangle$을 계산하여 $|R_A\rangle$과 같은 지를 확인한다.
   $|R'_A\rangle \neq |R_A\rangle$인 경우, 중재자를 신뢰할 수 없기 때문에 서명검증 과정을 다시 반복한다.
   $|R'_A\rangle = |R_A\rangle$인 경우, $\gamma_a=1$이면 서명을 인정하고 그렇지 않으면 서명을 거부한다.

Ⅳ. 안전성 분석 및 서명 기법 비교

제시된 양자 서명 기법에서는 중재자가 있어야만 서명을 검증할 수 있다. 이는 양자 시스템에서 공개키를 이용하는 기법이 아직까지 제안되지 못했기 때문이다. 기존의 공개키 시스템의 안전성은 인수분해 문제나 이산대수 문제와 같은 계산의 어려움에 근거하고 있는데, 이러한 문제들은 94년에 제안된 Shor의 알고리즘으로 다항식 시간 안에 해결될 수 있다고 증명되었다. Shor의 알고리즘은 이론적으로 증명되었을 뿐만 아니라, 2001년 겨울 IBM에 의하여 양자 컴퓨터를 이용하여 실험적으로도 증명되었다. 이에 따라 양자 암호체계에서는 기존의 공개키 시스템의 기반이었던 인수분해 문제나 이산대수 문제 등을 더 이상 사용할 수 없기 때문에 새로운 양자 공개키 시스템에 대한 연구가 필요하다. 양자 암호가 본격적으로 연구되기 시작한지 얼마 되지 않았기 때문에 양자 공개키 시스템에 대한 연구는 아직 정립되지 않았다. 이와 같은 이유로 현재까지는 양자 서명 시스템에서는 지정된 검증자가 존재하는 서명 기법만이 존재한다고 할 수 있다.

중재자가 있는 양자 서명의 안전성 분석은 서명을 위조할 수 있는 지의 여부와, 서명을 받은 Bob이 그 서명을 거부할 수 있는 지의 여부를 살펴보는 것으로도 충분하다. 서명에 사용되는 키가 한번만 사용되기 때문에 키의 누출이 다음 번 서명에 영향을 미치지 않기 때문이다.

4.1 서명 위조 불가능

Eve(공격자)가 Alice의 서명을 위조하고자 한다면, 우선 초기화 단계에서 공유된 키 K_a값을 알아야만 한다. 그러나 양자 키 분배 프로토콜의 완전 비밀성에 따라 키를 알아내는 것은 불가능하다. 따라서 올바른 $|R_a\rangle$ 값을 생성해 낼 수 없고, 서명 위조가 불가능하다. 따라서 검증 시 γ_a 값이 1이 되어 서명검증을 통과 할 수 없다.

공개 보드를 이용하는 경우부터 자세히 살펴보도록 하자. 이 경우, Eve가 얻을 수 있는 값은 오직 $a,|S\rangle,|T\rangle,|V\rangle$ 값뿐인데, 이로부터 키 K_a를 알아내는 것은 불가능하다. 한편 $a,|V\rangle$를 통하여 키 K_b값에 대한 약간의 정보는 알아낼 수 있다. $|V\rangle$가 공개된 a와 두개의 비트 정보 γ_a,γ_b 만을 포함하는 값이기 때문에 키의 노출이 우려될 수 있지만, $|V\rangle$가 전달된 뒤에나 키 K_b에 대한 정보가 누출됨으로 실제로 서명 기법에는 거의 영향을 끼치지 않는다. 이때, K_{b_i}가 0일 때, 1이라고 추정하고 a_i를 계산해도 공개 게시판과 동일한 a_i가 나올 확률이 1/2이기 때문에 완벽하게 키 값을 알아내기는 힘들다.

한편, 공개 보드에 기재된 a를 Eve가 변형시킬 수 있다고 가정하자. 이 또한 서명 검증과정에서 Bob이 위조여부를 확인할 수 있고, 정확한 메시지를 복구할 수 있기 때문에 문제가 되지 않는다.

공개보드를 사용하지 않는 경우를 살펴보면, 위와 마찬가지로 키 K_a에 대한 정보가 누설되는 것은 거의 불가능하다. a가 공개되지 않기 때문에 키 K_b를 알아내는 것 또한 키 K_a와 같은 이유로 불가능하다.

본 논문에서 제시한 양자 서명의 특징을 메시지 암호화 측면에서 간단히 살펴보자. Eve가 메시지를 알아내려면 기본적으로 K_a또는 K_b를 알아야만 한다. 그러나 이 값들은 채널 상에서 암호화된 형태로든, 암호화되지 않은 형태로든지 간에 전송되지 않기 때문에 알아낼 수 없다. 따라서 메시지 P를 알아낼 수 없다. 또한 공개보드를 사용하지 않는 경우는 이 키와 더불어 초기 단계에서 분배되는 GHZ상태를 가로채서 가지고 있어야만 메시지를 확인할 수 있게 된다. 이 두 가지 조건을 동시에 만족시키는 것 자체가 불가능하기 때문에, Eve는 메시지에 대한 어떤 정보도 알아낼 수 없을 뿐만 아니라, 서명이 통과되었는지 또한 알아낼 수 없다.

4.2 서명인의 부인방지

만약 Alice가 자신의 서명에 대해 부인을 한다면, 그것은 금방 확인할 수 있다. 서명 $|S\rangle$에 Alice의 키 K_a의 정보가 포함되어 있기 때문에, 중재자가 Alice의 서명여부를 확인할 수 있다. 이러한 이유 때문에 중재자의 중립성은 매우 중요하다. 중재자가 마음만 먹으면 얼마든지 서명을 위조할 수 있기 때문이다. 이 논문에서는 중재자가 중립적이고 믿음직하다는 것을 전제로 하고 있기 때문에 이에 대한 논의는 하지 않도록 한다.

4.3 수신자의 부인방지

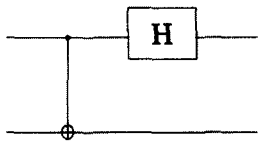
양자 서명에서는 수신자가 서명을 받지 못했다고 주장할 수 없다. 이는 서명을 검증하기 위해서는, 서명인의 키를 공유하고 있는 중재자의 도움이 필요하기 때문이다, 서명을 검증했다는 것 자체가 서명을 받았다는 것을 전제로 하기 때문에 서명을 받은 것을 부인할 수가 없다. 메시지에 대한 내용 또한 공개보드의 내용이 틀렸다고 하더라도 중재자로부터 메시지에 대한 정보를 받아볼 수 있기 때문에 메시지 내용을 알지 못했다고 주장할 수는 없다. 한편 공개보드를 사용하지 않는 경우 또한 수신자가 메시지를 복구할 수 있기 때문에 부인방지가 불가능하게 된다.

4.4 양자 서명 기법의 비교

기존의 양자 서명 기법[10]과 비교하여 본 논문에서 제안된 두 기법은 [표 1]에서 보여지듯 대략20~30% 정도의 전송부담을 줄였다. 또한 실질적인 측정에 있어서 Bell측정을 사용하지 않고 기본측정만을 사용하여 사용자의 편의를 증진시켰다. Bell측정의 경우, [그림 1]과 같이 측정시 한 개의 Hadamard 게이트(H)와 XOR 연산을 이용하여 연관된 큐빗 두 개를 동시에 측정해야하는 반면, 기본측정은 각 큐빗을 기본

〔표 1〕 메시지의 길이가 n인 경우 양자 서명 기법에서 전송되는 큐빗의 양

	기존의 양자 서명 기법[10]	공개보드를 이용한 양자 서명 기법	공개보드를 사용 않는 양자 서명 기법
서명 전달 Alice→ Bob	3n	2n	2n
Bob→중재자	3n	3n	3n
중재자→Bob	5n+1	3n+2	4n+1



〔그림 1〕 Bell 측정 gate

기저로 측정한다. 따라서 본 논문에 제시된 두 서명 기법에서는 전체 측정량의 절반정도를 차지하는 Bell 측정을 기본측정으로 대체하여 사용자의 편의를 증진시켰다.

한편 양자 서명 기법은 메시지 서명에 그치지 않고, 메시지 암호화까지 수행함으로써 기존의 암호화단계와 서명 생성하는 단계를 간단하게 줄였다.

기존 양자 서명 기법에서는 Bob이 서명을 검증하기 위하여 GHZ 상태를 복원하도록 고안되었는데, 이는 Bob의 연산이 상대적으로 클 뿐만 아니라 양자 상태를 다루는 위험이 크다. 이에 반하여 본 논문에서 제안한 양자 서명 기법 두 개 모두 Bob의 검증 과정을 간단히 하였으며, 공개보드를 이용하지 않는 서명 기법에서는 Bob과 중재자에 대한 신원확인을 서로가 한 번씩 더 할 수 있도록 고안되어 더욱 안전해졌다.

V. 결 론

양자 암호에서는 공개키 개념이 아직까지 확립되지 않았기 때문에 지정된 검증자만이 서명을 검증할 수 있는 서명 기법만이 존재한다. 본 논문에서는 기존체계의 시스템인 공개 게시판을 이용하는 양자 서명 기법과 양자 시스템만을 이용하는 양자 서명 기법 두 가지를 제시하였다. 이 기법들은 GHZ상태를 이용하여 메시지의 암호화와 서명 검증을 하도록 고안되었으며, [표 1]에 보이듯 기존에 제시된 중재자를 통한 양자 서명에 비하여, 전송상의 효율을 높였으며, 실제적인 구현에 있어서 Bell 측정을 사용하지 않음으로써 측정의 편리함을 가져왔다고 할 수 있다.

앞으로도 전통적인 서명 기법과 동일한, 임의의 검증자가 서명을 검증할 수 있는 양자 서명 기법뿐만 아니라, 안전성 분석을 비롯하여, 다른 양자 암호 분야에 대한 연구가 활발하게 이루어져야 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] Artur K. Ekert, "Quantum cryptography based on Bell' s theorem", Phys. Rev. Lett. 67, 661 (1991).

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

[4] Peter W. Shor and John Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol", arXiv:quant-ph/003004 (2000).

[5] Stephen M. Barnett, and Simon J. D. Phoenix, "Information-theoretic limits to quantum cryptography", Phys. Rev. A. 48, 1 (1993).

[6] Artur K. Ekert, Bruno Huttner, G. Massimo Palma, and Asher Peres, "Eavesdropping on quantum - cryptographical systems", Phys. Rev. A. 50, 2 (1994).

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

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

[9] Howard Banum, "Quantum secure identification using entanglement and catalysis", arXiv:quant-ph/9910072 (1999).

[10] Guihua Zeng and Christoph H. Keitel, "Arbitrated quantum-signature scheme", Phys. Rev. A. 65, 042312 (2002).

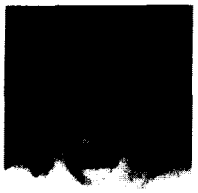
[12] Daniel Gottesman and Isaac L. Chuang, "Quantum Digital Signatures", arXiv:quant-ph/0105032 (2001)

[13] D. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, "Bell's theorem without inequalities", Phys. 58, 1131 (1990).

[14] Dik Bouwmeester, Jian-Wei Pan, Matthew Daniell, Harald Weinfurter, and Anton Zeilinger, "Observation of There-Photon Greenberger-Horne-Zeilinger Entanglement", Phys. Rev. Lett. 82,7 (1999).

[15] A. R. Calderbank and Peter W. Shor, "Good quantum error-correcting codes exit", Phys. Rev. A. 54,2 (1996).

〈著者紹介〉



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, CMVP

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

이 동 훈 (Dong-Hoon Lee)
1984년 2월 : 고려대학교 경제학과 학사
1987년 2월 : Oklahoma Univ. 전산학 석사
1992년 2월 : Oklahoma Univ. 전산학 박사
1993년 3월~현재 : 고려대학교 전산학과 정교수
2000년 3월~현재 : 고려대학교 정보보호대학원 교수
<관심분야> 암호이론, 암호 프로토콜, 정보이론, 양자 암호

이 상 진 (Sang-jin Lee)
1987년 2월 : 고려대학교 수학과 학사
1989년 2월 : 고려대학교 수학과 석사
1994년 2월 : 고려대학교 수학과 박사
1989년 2월~1999년 2월 : 한국전자통신연구원 선임 연구원,
1999년 3월~2001년 8월 : 고려대학교 자연과학대학 조교수
2001년 9월~현재 : 고려대학교 정보보호대학원 부교수
<관심분야> 블록 암호 및 스트림 암호 분석 및 설계, 암호 프로토콜, 공개키 암호 알고리즘 분석, 양자 암호

임 종 인 (Jong-in Lim)
1980년 2월 : 고려대학교 수학과 학사
1982년 2월 : 고려대학교 수학과 석사
1986년 2월 : 고려대학교 수학과 박사
1999년 2월~현재 : 고려대학교 자연과학대학 정교수, 한국통신정보보호학회 편집위원장, 고려대학교 정보보호대학원 원장, 고려대학교 정보보호기술연구센터 센터장
<관심분야> 블록 암호 및 스트림 암호 분석 및 설계, 암호 프로토콜, 공개키 암호 알고리즘 분석, 양자 암호