네트워크 상에서의 안전한 "고스톱" 프로토콜

오 형 근°, 박 희 운, 이 임 영
순천향대학교 공과대학 컴퓨터학부

Secure "Go-Stop" Protocol on the Network

Hyung-Geun Oh°, Hee-Un Park, Im-Yeong Lee
Department of Computer Science, College of Engineering,
Soonchunhyang University

요 약

최근 들어 컴퓨터 통신의 확산과 더불어 인터넷의 사용이 급증하고 있다. 또한 인터넷의 활용 분야도 그 범위가 확대되고 있으며 사용자들은 이러한 인터넷을 이용해서 각종 게임을 즐기기도 한다. 그런데 인터넷과 같은 개방된 네트워크 상에서 고스톱과 같은 게임을 공정하게 실행하기 위해서는 각 참여자 및 화투 패에 대한 유효성 확인 절차가 반드시 필요하게 된다. 따라서 본 논문에서는 인터넷을 통하여 전자 고스톱이라고 일컫는 게임을 안전하게 수행할 수 있도록 새로운 프로토콜을 제안하고자 한다.

1. 서론

오늘날 컴퓨터의 폭넓은 보급과 네트워크 환경의 발달은 사회의 전반적인 활동 모습을 크게 변화시키고 있다. 또한 네트워크의 네트워크(A Network of Networks)로서 인터넷(Internet)이 등장하면서부터 이러한 추세는 더욱 고조되고 있는 실정이다.

인터넷은 이제 단순한 정보통신의 통로이라기보다는 시간과 공간을 초월한 새로운 패러다임으로 다가오고 있다. 현재 전세계 인터넷 호스트의 수는 1997년 현재 약 1950만개에서 매년 25.9%의 증가를 보이고 있으며 국내 호스트의 숫자도 1997년 말 131,005개에서 매년 평균 약 26.9%의 증가를 보여 2002년에는 약 43만개에 이를 것으로 보인다. 인터넷 이용자 수도 1997년 9,500만 명에서 2002년에는 약 2억 7,600만 명에 이를 것으로 보이며 국내 이용자도 2002년경에는 약 1,900만 명에 달할 것으로 예상이 되고 있다.

이렇듯 네트워크 기술과 이용환경이 발전하면서 사용인구 수도 급증하고 있으며 또한 이들을 대상으로 다양한 서비스들이 등장하고 있다.

이러한 상황을 반영하여 최근 새롭게 선보이고 있는 게임 툴 들은 대부분 네트워크 상에서 다중사용자들이 참여할 수 있는 네트워크 게임들이다. 네트워크 게임들은 단일 사용자 게임보다 사용자들에게 많은 흥미와 재미를 가져다주기 때문에 그 이용자 수도 급증하고 있다.

이에 본 논문에서는 국내에서 많은 사람들이 이용하고 있는 화투 게임들 중 "고스톱"이라는 게임을 오픈된 네트워크 상에서 다중 사용자들이 수행할 수 있는 프로토콜을 제시하고 있다. 먼저 제 2장에서는 기존에 제시되었던 Mental Poker Protocol에 대해 언급을 하고 있다. 제 3장에서는 이를 이용하여 사용자들의 부정 소지를 없애면서 안전하게 고스톱 게임을 수행할 수 있는 개선된 제안 프로토콜에 대해 알아본다. 그리고 제 4장에서는 제안된 프로토콜의 안전성에 대해 알아보고 결론을 내린다.

2. Mental Poker

이 프로토콜은 coin flip protocol과 비슷하며 각 참여자는 e-mail을 통해서 다수의 사람과 Poker를 하는 것으로 가정하고 있다. 기본적인 mental poker 프로토콜에서 Alice는 카드를 위한 모든 메시지를 생성하여 암호화 한 뒤 Bob에게 보낸다. Bob은 랜덤하게 5개의 메시지를 선택해 그의 공개키로 암호화하여 다시 Alice에게 보낸다. Alice는 메시지를 복호화하여 Bob에게 보내고 Bob은 그 메시지를 복호화하여 카드를 소유하게 된다. Alice의 카드는 Bob이 선택을 하여 Alice에게 보내준다. 게임을 하는 동안 프로시져를 다시 수행하여 카드를 더 분배할 수가 있다. 게임이 끝날 때에는 Alice와 Bob은 그들의 카드와 키 쌍을 공개한다. 이러한 기본적인 프로토콜은 다수의 사람으로 확장이 가능하다.

● 프로토콜

(1) Alice는 52장의 메시지를 생성한다. 이 각각의 메시지에는 unique random string을 포함하고 있으며 Alice의 공개키로 암호화한다.

$$\text{Alice} : E_{K_A^U}(M_{1,2,\ldots,52})$$

(2) 암호화된 52장의 메시지를 Bob에게 전송한다.

(3) Bob은 5장의 메시지를 random하게 선택을 하고 자신의 공개키로 암호화한다. 그리고 이 암호화한 메시지를 Alice에게 다시 전송한다.

$$\text{Bob} : E_{K_B^U}(E_{K_A^U}(M_{1,2,3,4,5})) \longrightarrow \text{Alice}$$

(4) Bob은 나머지 47장의 메시지를 Carol에게 전송한다.

(5) Carol은 47장의 메시지 중에서 5장의 메시지를 랜덤하게 선택하고 자신의 공개키로 암호화한다. 그리고 이 암호화한 메시지를 Alice에게 다시 전송한다.

$$\text{Carol} : E_{K_C^U}(E_{K_A^U}(M_{6,7,8,9,10})) \longrightarrow \text{Alice}$$

(6) Alice는 Bob과 Carol에게서 받은 이중 암호문을 자신의 개인키로 복호화 한 뒤 Bob과 Carol에게 전송한다.

$$\text{Alice} : D_{K_A^R}(E_{K_B^U}(E_{K_A^U}(M_{1,2,3,4,5})))$$
$$= E_{K_B^U}(M_{1,2,3,4,5})$$
$$D_{K_A^R}(E_{K_C^U}(E_{K_A^U}(M_{6,7,8,9,10})))$$
$$= E_{K_C^U}(M_{6,7,8,9,10})$$

(7) Bob과 Carol은 메시지를 자신의 개인키로 복호화한다.

$$\text{Bob} : D_{K_B^R}(E_{K_B^U}(M_{1,2,3,4,5})) = M_{1,2,3,4,5}$$

$$\text{Carol} : D_{K_C^R}(E_{K_C^U}(M_{6,7,8,9,10}) = M_{6,7,8,9,10}$$

(8) Carol은 나머지 42장의 메시지 중에서 5장을 random하게 선택하고 이 메시지를 Alice에게 전송한다. 그리고 Alice는 이 전송 받은 메시지를 자신의 비밀키로 복호화 한 뒤 각 참여자는 게임을 시작한다.

$$\text{Carol} : E_{K_A^U}(M_{11,12,13,14,15}) \longrightarrow \text{Alice}$$

이 프로토콜에서 만약 Alice가 승리한다면 Alice는 키 쌍과 메시지를 공개하고 Bob과 Carol은 이 메시지가 정당한 메시지인지를 확인한다. Bob은 Alice로부터 받은 52장의 메시지가 올바른 것인지 Alice의 개인키로 확인할 수가 있으며 Carol은 Alice의 개인키로 Carol이 전송해준 5장의 메시지를 확인하고 Alice의 공개키로 Alice가 보인 카드를 암호화한 것과 Carol이 Alice에게 보내준 것과 같은 지를 확인한다.

Bob과 Carol이 승리한다면 역시 Bob과 Carol도 메시지와 키 쌍을 공개하고 Alice는 공개된 카드의 random string을 확인하여 카드의 유효성을 확인한다. 그리고 Alice가 가진 메시지($E_{K_B^U}(M_{1,2,3,4,5})$ or $E_{K_C^U}(M_{6,7,8,9,10})$)와 공개된 카드를 승리자의 공개키로 암호화 한 것이 일치하는 지 검사함으로써 카드가 위·변조가 되지 않았는지 확인할 수 있다.

이밖에 손안의 내용을 보이지 않으면서 카드를 확인하도록 하는 프로토콜에 제안이 되었으며[3], 정보누출에 관한 문제를 해결하는 n명의 포커 프로토콜은 C.Crepeau[4]에 의해 향상이 되었다. 만약 카드의 이진 표현이 이차잉여류라면 그 때 카드의 암호화도 이차잉여류가 될 수가 있으며 이것은 어떤 카드에 "mark"하는데 이용이 가능한데 Goldwasser와 Micali는 이에 대한 문제를 해결[5]하고 있다.

3. 전자 고스톱

본 논문에서 제안하고 있는 고스톱 게임은 기본적으로 3명이 하는 게임이다. 최대 5명으로 확장할 수가 있으며 이때 2명은 자신이 가진 패를 판다. 각각의 참여자는 상대방을 보지 못하는 곳에서 네트워크를 통하여 게임에 참가한다.

3.1 요구 조건

게임을 공정하게 실행하기 위해서는 각 참여자가 가지는 화투 패에 대해 그 유효성을 확인하여야 하며 이를 위해 다음과 같은 요구 조건은 반드시 충족되어야 한다.

(1) 화투는 네트워크 상에서 안전하게 전송되어야 한다.

(2) 화투는 재 사용될 수 없으며 복사·위조 등으로 인한 부정사용을 할 수가 없어야 한다. 즉, 한 번 이상 사용될 수가 없어야 한다.

(3) 참여자가 가지고 있는 화투 패나 정보가 공개된 화투 패는 언제나 유효성 검사를 할 수가 있어야 한다.

(4) 게임이 종료되었을 때, 즉 "STOP" 되었을 때 화투 패의 불법적인 교환이 없어야 한다.

(5) 한 참여자가 가지고 있는 화투 패는 다른 참여자에게 이전이 가능하여야 한다.

3.2 포커 게임과 고스톱 게임과의 차이점

포커 게임과 고스톱 게임은 패를 안전하게 분배하고 위·변조 등의 불법적인 사용을 하지 못하게 해야 한다는 점에서 유사하다. 그러나 포커 게임에서는 자신이 가지고 간 패를 공개하기만 하면 되는데 반해 고스톱 게임에서는 다른 사람의 패를 가지고 오기도 해야하며 자신의 패를 다른 사람에게 전송해 주기도 해야 한다. 여기서 패에 대한 소유권 이전 문제가 제기 될 수 있다. 또한 포커에서는 패를 받기만 하면 되는데 고스톱에서는 자신의 패를 내 놓기도 하고 공개된 패를 같이 가져오기도 해야 한다.

이와 같이 포커 게임보다는 고스톱 게임시 고려해야 할 사항이 많으며 참여자간의 패 이동이 많아 안전성에 대한 많은 제약이 따를 수 있어 이 문제에 대한 명확한 해결이 선행되어야 한다.

3.3 고려사항

네트워크 상에서 수행하는 게임의 특성으로 인해 다음과 같이 시스템 파라메타를 정의한다.

· TD(Trusted Dealer)
  패를 돌리고 섞는 역할을 하는 신뢰하는 딜러. TD는 자신의 서명을 붙여 화투 패를 생성하며 참여자에게 분배한다. 또한 뒤집지 않은 패를 참여자가 공개한 패와 맞추어 재 전송해 주기도 한다. 화투 게임을 시작하기 전에 TD는 화투 패 M을 생성한다.

· 참여자들의 공개키/비밀키 쌍
  TD : K_T^u, K_T^R Alice : K_A^u, K_A^R
  Bob : K_B^u, K_B^R Carol : K_C^u, K_C^R
  - 각 참여자들은 게임 시작 전에 공개키/비밀키 쌍을 생성한다.

· R.N(Random Number) : 초기 화투 패 생성시 TD가 붙이는 unique한 Random Number.

· S.N(Serial Number) : TD를 통해 패를 가져갈 때 수행 순서에 따라 붙이는 순차적인 숫자

· M : 화투 패

· D(Data) : 화투 패 M의 내용

· M_i : TD로부터 분배받은 화투 패

· M'_i : 수행되어 가지고 온 화투 패

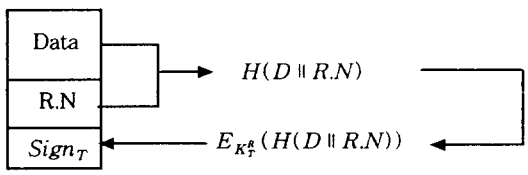
· $Sign_T$: R.N를 포함하는 TD의 초기 전자서명

· $Sign'_T$: 수행후 TD가 새롭게 부여하는 S.N가 포함된 전자서명

3.4 화투 패 생성 단계

먼저 TD는 48장의 화투를 생성하여 6장은 참여자들에게 공개하고 나머지 42장은 TD가 분배하기 위해 자신의 공개키로 암호화하여 게임 참여자들에게 분배한다. 이때 화투 M의 위·변조 등의 부정한 사용을 방지하기 위해 Random Number와 TD의 전자서명을 만들어 화투 M을 생성한다.

(1) 화투(M) 48장을 만들어 낸다.
  TD는 프로토콜의 마지막에 각각의 화투 M에 대한 인증(authentication)을 위해 화투 내용 D에 TD의 서명을 붙이며 이때 Random Number가 생성이 되어 들어가게 된다.
  화투 $M = (D \| R.N \| E_{K_T^R}(H(D \| R.N)))$



[그림 1] 화투 M의 생성

(2) TD는 패를 돌리기 전에 48장의 화투 중에서 랜덤하게 6장의 화투를 선택하여 Alice, Bob 그리고 Carol에게 이 6장의 화투 정보를 제공한다.

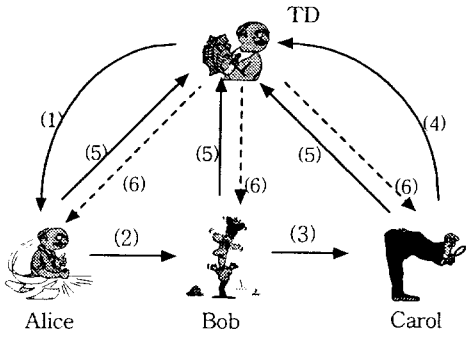
(3) TD는 Alice, Bob 그리고 Carol에게 화투를 분배

하기 전에 자신의 공개키로 각각의 화투를 암호화한다.

$$E_{K_K^U}(M_1),\ E_{K_K^U}(M_2),\ \ldots,\ E_{K_K^U}(M_{42})$$

3.5 화투 패 분배 단계

화투 패 분배 단계에서 TD는 자신이 생성한 42장의 화투 패를 첫 번째 사람에게 전달한다. 각각의 참여자들은 다른 사람들의 화투 M을 선택한 뒤 전달하려하는 사람의 공개키로 암호화하여 TD에게 전달한다. TD는 자신의 비밀키로 복호화한 뒤 화투 M을 전달한다.



[그림 2] 화투 M 분배단계

(1) TD는 화투 생성 단계에서 생성한 42장의 화투를 먼저 TD의 공개키로 암호화하여 Alice에게 전달한다.

TD : $E_{K_T^U}(M_{1,2,\ldots,42})$ ⟶ Alice

Alice는 42장의 화투 중에서 Bob이 가지게 될 7장의 화투 패를 랜덤하게 선택을 한다.

Alice : $E_{K_T^U}(M_{1,2,\ldots,7})$

Alice는 Bob만이 패를 가지고 가서 볼 수 있도록 하기 위해 Alice 자신이 선택한 7장의 화투 패를 Bob의 공개키로 암호화한다.

$$E_{K_B^U}(E_{K_T^U}(M_{1,2,\ldots,7}))$$

(2) Alice는 자신이 선택한 7장의 화투 패를 제외한 나머지 35장의 화투 패를 다음 차례인 Bob에게 전달한다.

Alice : $E_{K_T^U}(M_{8,9,\ldots,42})$ ⟶ Bob

Bob은 Alice에게서 받은 35장의 화투 패 중에서 7장을 랜덤하게 선택을 한다.

Bob : $E_{K_T^U}(M_{8,9,\ldots,14})$

Bob은 단계 (1)에서와 마찬가지로 자신이 선택한 7장의 화투 패를 Carol의 공개키로 암호화한다.

$$E_{K_C^U}(E_{K_T^U}(M_{8,9,\ldots,14}))$$

(3) Bob은 자신이 선택한 화투 패를 제외한 다른 28장의 화투 패를 Carol에게 전달한다.

Bob : $E_{K_T^U}(M_{15,16,\ldots,42})$ ⟶ Carol

Carol은 Bob에게서 받은 28장의 화투 패 중에서 7장을 랜덤하게 선택을 한다.

Carol : $E_{K_T^U}(M_{15,16,\ldots,21})$

Carol은 자신이 선택한 7장의 화투 패를 다음 순서에 있는 Alice의 공개키로 암호화한다.

$$E_{K_A^U}(E_{K_T^U}(M_{15,16,\ldots,21}))$$

(4) Carol은 자신이 선택한 화투 패를 제외한 나머지 21장의 화투 패를 TD에게 전달한다.

Carol : $E_{K_K^U}(M_{22,23,\ldots,42})$ ⟶ TD

(5) 21장의 화투 패를 받은 TD는 고스톱 게임을 실행할 때에 뒤집어 주기 위해 공개하지 않고 TD 자신이 가지고 있게 된다.

Alice, Bob, 그리고 Carol은 자신들이 선택하여 다음 순서에 있는 사람의 공개키로 암호화한 화투 패들을 TD로 보내어 TD가 암호화 한 것을 복호화한다.

$$D_{K_T^R}(E_{K_B^U}(E_{K_T^U}(M_{1,2,\ldots,7}))) = E_{K_B^U}(M_{1,2,\ldots,7})$$

$$D_{K_T^R}(E_{K_C^U}(E_{K_T^U}(M_{8,9,\ldots,14}))) = E_{K_C^U}(M_{8,9,\ldots,14})$$

$$D_{K_T^R}(E_{K_A^U}(E_{K_T^U}(M_{15,16,\ldots,21}))) = E_{K_A^U}(M_{15,16,\ldots,21})$$

(6) TD는 복호화한 화투 패를 다시 분배한다. 이때 각 화투 패는 각각 Alice, Bob 그리고 Carol의 공개키로 암호화가 되었기 때문에 참여자들이 무엇을 선택했는지 알 수 없다.

(7) 각 참여자들은 TD로부터 패를 받아 자신의 비밀키로 복호화함으로써 화투 패를 가지게 된다.

Alice : $D_{K_A^R}(E_{K_A^U}(M_{15,16,\ldots,21}))$

$= M_{15,16,\ldots,21}$

Bob : $D_{K_B^R}(E_{K_B^U}(M_{1,2,\ldots,7}))$

$= M_{1,2,\ldots,7}$

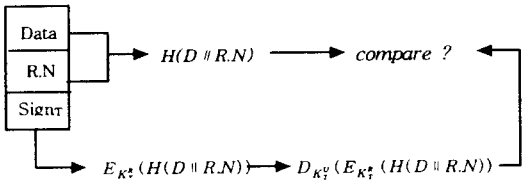
Carol: $D_{K_C^R}(E_{K_C^U}(M_{8,9,\ldots,14}))$

$= M_{8,9,\ldots,14}$

3.6 분배받은 화투 패에 대한 유효성 검사

Alice, Bob 그리고 Carol은 화투 패의 분배과정에

서 있을 수 있는 각 화투의 위·변조 여부를 알기 위해 TD의 공개키로 TD의 서명을 확인한다.



[그림 3] TD 서명의 유효성 검사

3.7 화투 패의 관리

고스톱 게임시에는 각 참여자간에 많은 패 교환이 이루어지며 이때에 악의를 가진 참여자에 의해 패의 위·변조가 발생할 수 있다. 이에 다음에서는 게임 수행시에 발행할 수 있는 각 경우에 대해 안전하게 패를 관리하는 방법에 대해 고려해 본다.

(1) 가지고 온 화투 패를 공개하는 경우

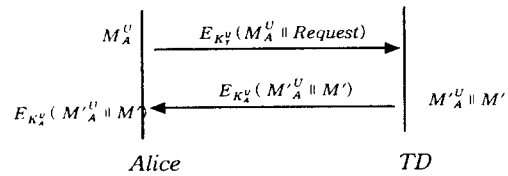
각 게임의 참여자가 가지고 간 화투 패는 다른 사람들이 볼 수 있도록 화투 패에 대한 정보를 제공한다. 이때에 소유한 화투 패가 자신의 것임을 증명하기 위해 자신의 ID를 기록한 후 그에 대한 소유자의 서명을 붙인다.

Alice, Bob, Carol :

$$M'^{U}_{A,B,C} = (M' \| ID_{A,B,C} \| E_{K^R_{A,B,C}}(H(D \| ID_{A,B,C})))$$

(2) 바닥에 깔린 화투 패(M')를 가져오는 경우

만약 Alice가 TD의 공개 화투 패(바닥에 깔린 화투 패) 중에서 자신의 패와 일치하는 패가 있으면 자신의 화투 패를 TD에게 전달한 뒤 일치하는 패를 가져온다. Alice의 패(M_A^U)와 Request문을 TD의 공개키로 암호화하여 TD에게 보낸다. 여기서 Request문은 Alice가 가져오기를 원하는 패(M')에 대한 정보가 수록이 되어 있다. TD는 이 패를 복호화 한 뒤 Alice가 원하는 화투 패와 함께 Alice의 공개키(K_A^U)로 암호화하여 보낸다. 이때 TD는 화투 패 발행시에 자신이 붙였던 Random Number와 자신의 서명($Sign_T$)을 삭제하고 화투 게임 순서에 따르는 sequential serial number(S.N)와 새로운 서명($Sign_T'$)을 붙여 Alice에게 전달한다.



[그림 4] 바닥에 깔린 화투 패 가져오기

여기서,

$$M'^{U}_{A} = (D \| S.N \| E_{K_T^R}(H(D \| S.N)) \| ID_A \| E_{K_A^R}(H(D \| ID_A)))$$

$$M' = (D \| S.N \| E_{K_T^R}(H(D \| S.N)))$$

그리고 새로운 화투 패를 가져온 Alice는 M'에 자신의 ID_A와 서명을 첨가시킨 뒤 화투(M'^U_A)를 공개한다.

(3) 다른 사람의 공개된 화투 패를 가져오는 경우

만약 Alice가 Bob의 화투 패를 가져 올 경우 Bob은 공개된 자신의 화투 패(M'^U_B)에서 Bob의 ID_B와 서명을 제거한 뒤 Alice의 공개키로 암호화하여 전달한다.

Bob: $M'^U_B = (M' \| ID_B \| E_{K_B^R}(H(D \| ID_B)))$

↓

Alice: $E_{K_A^U}(M' = (D \| S.N \| E_T^R(H(D \| S.N)))$

그리고 나서 가져온 화투 패를 복호화 한 뒤 자신의 식별자 ID_A와 서명을 붙인다.

$$Alice : D_{K_A^R}(E_{K_A^U}(M')) = M'$$

$$M'^U_A = (M' \| ID_A \| E_{K_A^R}(H(D \| ID_A)))$$

3.8 "STOP"시 화투 패에 대한 유효성 검사

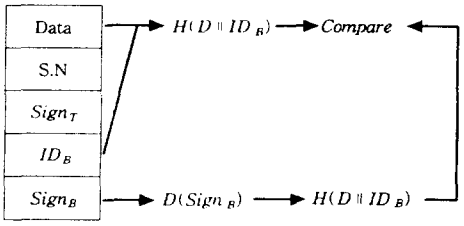
화투 M'에 대한 유효성 검사는 화투 게임 참가자들 중에서 어느 한 사람이 먼저 점수가 3점 이상 나서 "STOP"을 하였을 경우 그 사람이 가지고 있는 화투 M들에 대해서 다른 모든 참가자가 검사함으로써 이루어진다.

만약 Bob이 점수가 제일 먼저 났다고 하면 Bob은 TD와 Alice와 Carol에게 자신의 모든 패를 전송한다. 그리고 TD는 자신의 공개키/비밀키 쌍을 공개한다. 화투 패를 받은 TD와 Alice와 Carol은 먼저 Bob의 서명을 확인하고 TD가 화투 패 생성시 만들었던 서명을 검사함으로써 화투 패에 대한 유효성을 검사한다.

$$Bob \ : \xrightarrow{E_{K_R^U}(M'_{1,2,\ldots,i} \| ID_{B_{1,2,\ldots,i}} \| Sign_{B_{1,2,\ldots,i}})} \text{TD, Alice, Carol}$$

- *Bob*의 서명 확인

$$H(D \| ID_B) =? D_{K_B^U}(E_{K_B^R}(H(D \| ID_B)))$$



[그림 5] 화투 M의 소유자 서명 확인

- *TD, Alice, Carol*

$$: D_{K_T^U}(E_{K_T^U}(M'_{1,2,\ldots,i} \| ID_{B_{1,2,\ldots,i}} \| Sign_{B_{1,2,\ldots,i}}))$$

$$= M'_{1,2,\ldots,i} \| ID_{B_{1,2,\ldots,i}} \| Sign_{B_{1,2,\ldots,i}}$$

그리고 TD의 서명 확인 과정은 [그림3]과 같다.

4. 제안 프로토콜의 고찰

네트워크 상에서의 고스톱 게임은 각 화투 패의 잦은 이동으로 전송시 또는 소유단계에서 보안상의 많은 취약점을 나타내고 있다. 따라서 앞에서 언급하였던 요구 조건들을 만족시켜 주지 못하면 게임의 수행이 어렵게 된다. 이에 본 제안 방식에서는 원활한 게임 진행을 위해 앞서 언급한 요구 조건들을 모두 충족 시켜 주고 있다.

우선 각 화투 패마다 Random Number가 들어가 있어 중복 사용할 때 발견하기가 용이하며 TD의 전자서명이 되어있어 위·변조가 불가능하다. 그리고 네트워크 전송시 수신자의 공개키로 암호화되어 있기 때문에 제 3자가 전송 내용을 볼 수가 없다. 자신이 가지고 온 패는 다른 참여자들에게 그 패에 대한 정보를 제공하여 항상 볼 수 있도록 하며 sequential serial number 정보도 함께 제공함으로써 "STOP"되었을 때 수행되지 않은 패와 기존의 수행된 패가 교환 불가능하도록 해 주고 있다. 각 참여자와 TD는 화투에 자신들만이 아는 메시지를 결합시켜 화투 분배 단계에서 공모를 할 수 있다. 그러나 화투 패 분배시 자신의 패를 선택하는 것이 아니라 다른 사람의 패를 선택하여 분배함으로써 TD와 참여자간의 공모를 방지하고 있다.

5. 결론

인터넷과 같은 개방된 네트워크에서 화투 게임과 같은 프로토콜은 메시지에 대한 인증이 확인되지 않으면 게임을 수행할 수가 없다. 그러나 항상 정보의 노출 위험성과 게임 참여자 및 제 3자의 데이터 위·변조의 위험성이 상존하기 때문에 이에 대한 문제 해결 노력을 하여야한다.

이를 위해 본 제안 방식에서는 TD라는 공정한 딜러를 두어 화투 패를 생성하며 그 유효성을 확인해 주는 역할을 하고 있다. 또한 화투 전송시 또는 다른 사람으로부터 화투를 가져올 경우 그 화투에 대한 인증 확인을 만족시키기 위해 암호 알고리즘과 전자서명(Digital Signature)이라는 프로토콜을 사용하고 있다.

본 제안 방식의 연구 결과로서 단순한 게임 프로토콜에의 적용뿐만 아니라 다자간에 있어서의 메시지 교환시 메시지 인증과 중요한 데이터 및 키를 공정히 분해하는 프로토콜에도 적용이 될 수 있을 것이다.

6. 참고 문헌

[1] Bruce Schneier. "Applied Cryptography", John Wiley & Sons, pp92-95, 1996

[2] S.Fortune and M.Merritt, "Poker Protocols", Advances in Cryptology: Proceedings for CRYPTO 84, Springer-Verlag, pp454-464, 1985

[3] C.Crepeau, "A Zero-knowledge Poker Protocol That Achieves Confidentiality of the Player's Strategy" Advanced in Cryptology-CRYTO '86 Proceedings, Springer-Verlay, pp239-247, 1987

[4] C. Crepeau, "A Secure Poker Protocol That Minimizes the Effect of Player Coalitions", Advances in Cryptology CRYPTO '85 proceedings, Springer-Verlag, pp73-86, 1986

[5] S.Goldwasser, S. Micali. "Probablistic Encryption and How to Play Mental Poker keeping Secret All Partial Information", Journal of Computer and System Sciences. v.28, n.2, pp270-299, Apr 1984

[6] 한국전자통신연구소 편저, "현대암호학", 1991

[7] 최용락,소우영,이재광,이임영"통신망정보보호", 도서출판 그린, 1997