전자상거래 프로토콜에서 공정한 교환의 익명성 보장기법

김창덕*, 김상진**, 오희국*

*한양대학교 컴퓨터공학과, **한국기술교육대학교 인터넷미디어공학부

An Anonymous Fair Exchange Scheme for E-Commerce Protocol

Chang-deok Kim*, Sang-jin Kim**, Hee-kuck Oh*

*Department of Computer Science and Engineering Hanyang Univ.
**School of Internet-Media Engineering, Korea Univ. of Technology and Education

요 약

전자상거래에서 공정한 교환은 매우 중요한 요구 사항이다. 그러나 기존의 공정한 교환은 서명에 관련한 것이라서 익명성을 보장하지 못하였다. 본 논문에서 제안하는 프로토콜은 다음과 같은 몇 가지 중요한 특징을 가지고 있다. 첫째, 공정한 교환을 보장한다. 둘째, 참여자는 자신이 원하는 아이템을 반드시 받을 수 있다. 셋째, 문제가 발생한 경우가 아니면 진행 중에 신뢰기관(trusted third party)에게 중재를 요청하지 않는다. 마지막으로 고객의 익명성을 보장한다. 지금까지의 전자상거래 프로토콜은 위에서 말한 모든 조건을 동시에 만족시키지 못하고 있다. 또한 기존 전자상거래 프로토콜에서는 익명성 보장 문제로 공정한 교환을 적용하지 못하였다. 본 프로토콜에서는 공정한 교환을 이용하여 지불과정의 원자성을 보장하면서 익명성 문제까지 해결한 기법을 제안한다.

I. 서론

전 세계 IT환경은 컴퓨터의 폭 넓은 보급과 네트워크의 초고속화가 이루어지면서 인터넷의 이용자 수는 급격히 증가하고 있다. 더구나 웹 기술과 보안 기술의 발달로 이 거대한 사이버 공간을 상거래의 시장으로 활용할 수 있게 되었다. 현재 인터넷을 이용한 전자상거래의 양은 눈부신 성장세를 보이고 있으며, 포레스트 리서치(Forrester Research)는 2004년도 전 세계 전자상거래 시장규모가 약2조7천억달러가 될 것으로 추정하고 있다. 이러한 추세가 이어지면 인터넷을 통한 전자상거래 시장은 머지않아 기존 시장을 뛰어넘을 것이다. 그러나 전자상거래에 기존 지불매체를 적용하기가 어렵다. 따라서 전자상거래가 보다 활성화되기 위해 가장 시급한 문제 중에 하나가 서비스 대금이나 상품 대금을 지불할 때 사용할 수 있는 안전한 지불시스템(payment system)의 보급과 대중화이다.

전자상거래는 고객이 상점에게 대금을 지불하고 상점은 고객에게 상품을 전달하는 두 단계로 이루어진다. 그러나 네트워크를 이용하는 전자상거래에서 고객과 상인은 서로를 신뢰하지 않는 관계이다. 언제 네트워크가 끊어질지 모르며 또한 누군가 고의적으로 프로토콜을 종료할 수 있다. 이렇게 신뢰하지 않는 두 참여자가 서로 가지고 있는 아이템을 교환하기를 원한다고 하자. 한 참여자가 자신의 아이템을 다른 참여자에게 주었을 경우 그 참여자는 반드시 다른 참여자의 아이템을 받아야 하며, 그렇지 않을 경우에는 서로 상대방 아이템에 관한 어떠한 정보도 알지 못하도록 하여 누구도 이득을 얻을 수 없도록 해야 하는데 이러한 교환방식을 공정한 교환(fair exchange)이라 한다. 하지만 지금까지의 공정한 교환의 연구 분야는 두 참여자가 각자 자신의 서명을 교환하는 서명의 공정한 교환과 문서에서 두 참여자가 서명을 하는 계약서명(contract signing) 등이 있었다. 두 가지 방법 모두 서명기법으로 익명성을 제공하지 못한다. 이러한 서명기법을 그대로 전자상거래에 적용하기에 어려움이 따른다. 따라서 익명성을 제공하는 공정한 교환기법의 연구가 필요하다.

본 논문에서는 공정한 교환기법을 이용하여 지불과정의 원자성을 보장하고 익명성 문제를 해결하여 전자상거래 프로토콜에 사용할 수 있는 공정한 교환방법을 제안하고 있다. 대칭키암호화를 이용하여 계산량을 줄이고 라벨을 이용하여 지불의 원자성을 보장한다. 상품은 전자형태로 교환되며 은행 이외 참여자는 지불 토큰을 만들 수 없다. 더욱이 고객은 상점에게 신분을 밝히지 않고 프로토콜에 참여할 수 있기 때문에 다른 참여자들이 공모로부터 고객의 익명성을 보호한다.

II. 관련연구

기존의 공정한 교환에는 여러 접근방법이 있는데 먼저 점진적인 접근방법(gradual approach)이다[1,2]. 이 방법은 신뢰기관 없이 두 참여자가 서로 많은 회수의 통신을 거듭하면서 공정하게 교환할 확률을 높여 나가는 방식이다. 하지만 많은 통신이 필요하여 비효율적이고 두 참여자의 계산능력이 같다는 비현실적인 가정을 하고 있어서 실제로 사용하기는 어렵다. 다음으로 온라인 신뢰기관을 사용하는 방법(on line trusted third party approach)이 있다[3]. 이것은 신뢰기관이 두 참여자의 아이템을 받고 그 아이템이 올바른지를 확인한 후 각각 상대 참여자에게 전달하는 방식이다. 이 방식은 항상 신뢰기관이 교환에 참여해야 하고 교환되는 모든 아이템을 신뢰기관이 볼 수 있다는 단점을 가지고 있다. 이를 해결하기 위한 방법으로 부분적으로 신뢰기관을 사용(semi trusted third party approach)하지만 이것 역시 신뢰기관이 항상 교환에 참여해야 하는 단점을 가지고 있다[4]. 또 다른 방법으로는 신뢰기관의 참여를 줄이기 위해 참여자의 부정이나 통신상의 오류가 거의 일어나지 않는다는 낙관적(optimistic)인 접근방법이 있다[5]. 따라서 분쟁이 발생할 경우에만 신뢰기관이 참여하는 방식이다. 하지만 이러한 공정한 교환은 서명의 교환을 목적으로 하고 있기 때문에 전자상거래에 적용하기 어려우며 전자상거래의 중요한 특성인 익명성을 제공하지 못한다.

1. Ray and Ray의 프로토콜

Ray and Ray는 전자상거래 프로토콜에서 익명성을 제공하는 공정한 교환 방법을 제안하였다[6]. 이 방법은 분쟁이 발생했을 때만 신뢰기관이 프로토콜에 참여하는 낙관적인 접근방법을 사용하였다. 상점은 자신의 상품을 등록하기를 원하면 먼저 신뢰기관에 상품과 공개키 쌍 (K_1, K_1^{-1}) 그리고 상품거래 T_i동안 사용할 공개키 쌍 $(+K_{Mi}, -K_{Mi})$을 생성해서 그중 공개키를 전달하면 신뢰기관은 상품을 공개키 쌍 중 하나로 암호화하여 상품설명과 암호화된 상품 그리고 공개키 $+K_{Mi}$을 웹에 광고한다. 고객은 신뢰기관의 웹사이트로부터 원하는 상품을 다운받고 상인에게 구매의사를 표시한다. 상점은 고객에게 K_1을 알고있어도 K_2을 알 수 없는 키 $K_1 \times K_2$을 준다. 고객은 상품의 유효성을 확인하기 위해 theory of cross validation을 사용한다[7]. 원하는 상품이면 은행에 지불토큰 생성을 요청하고 은행으로부터 받은 토큰을 상점에게 전달한다. 상점은 받은 토큰을 자신의 은행에 주고 예금액 증가를 요청하면 은행은 예금액 증가결과를 상점에게 확인시킨다. 예금액 증가를 확인하면 상점은 고객에게 상품 해독키 K_1^{-1}을 준다.

2. Ray and Ray 프로토콜의 문제점

Ray and Ray가 제안한 프로토콜에 다음과 같은 문제점이 있다. 신뢰기관에 상품을 등록하는 과정에 상품과 공개키 쌍을 아무런 가정 없이 신뢰기관에 전송한다. 이 과정에서 상품과 공개키가 노출될 수 있다. 또한 제공되는 디지털 상품이 영화나 동영상처럼 크기가 크면 공개키 암호화를 이용하므로 신뢰기관의 부담이 가중된다. 왜냐면 상점이 하나가 아니고 상점마다 여러가지상품을 등록하게 되면 신뢰기관의 본연의 목적보다 상품등록이 더 많은 비중을 차지하게 되며 병목현상(bottleneck flow)이 발생된다. 그리고 상품을 신뢰기관에서 다운받아야 하므로 신뢰기관은 항상 온라인상태를 유지해야 한다. 이것은 전자상거래 프로토콜이 가져야할 조건에 위배된다. 더욱이 상품의 유효성 확인을 위해서 theory of cross validation을 이용하는데 이 방법은 고객이 암호화된 상품을 두 번 받아서 두 암호문이 같은 상품을 암호화 한 것을 확인한다. 이렇게 같은 상품을 두 번 받기 때문에 효율성이 많이 떨어지는 문제점을 가지고 있다. 마지막으로 상품하나를 아무런 문제없이 판매하기 위해서는 사전준비를 제외하고도 총 8번의 메시지 교환이 필요하다. 이렇게 많은 메시지 교환은 실질적으로 구현하기에 비현실적인 문제점일 가지고 있다.

III. 제안하는 프로토콜

이 장에서는 Ray and Ray가 제안한 프로토콜의 문제점을 해결하여 신뢰기관의 부담을 줄이고 공정한 교환을 만족하여 지불의 원자성을 보장하며 고객의 익명성까지 만족하는 프로토콜을 제안하고 있다. 본 논문에서는 대칭키와 라벨로 구성

표 1: 프로토콜에서 사용되는 기호

기 호	설 명
C, M, TP	고객, 상인, 신뢰기관
CB, MB	고객거래은행, 상인거래은행
C_{acct}, M_{acct}	고객계좌정보, 상인계좌정보
m	고객이 구매하는 상품
PO	고객의 m구매의사
T_i	m의 구매가 포함된 거래
$-K_a$, $+K_a$	a의 개인키와 공개키
$-K_{ai}$, $+K_{ai}$	T_i에만 사용되는 a의 키쌍
$-K_B$, $+K_B$	은행의 공동 개인키와 공개키
$CS(X)$	X의 암호화 체크섬
$h(X)$	X의 해쉬값
K_i, $label_i$	상품을 암호화할 키 쌍
Pay	상품에 대한지불
P	지불토큰

된 키 쌍을 이용한다. 대칭키암호화를 이용하므로 큰 상품을 암호화할 때 생기는 계산량을 줄일 수 있고 라벨을 이용하여 공정한 교환을 만족하므로 지불의 원자성도 만족한다. 또한 프로토콜 진행간에 고객은 가짜신분을 사용하므로 익명성 보장도 가능하다.

1. 표기법 및 가정

본 프로토콜에서는 표 1과 같은 표기법을 사용한다.

2. 준비사항

전자상거래 프로토콜을 시작하기 전에 다음과 같은 준비단계를 먼저 진행한다. 이것은 그림 1 프로토콜 진행도의 ⓪에 해당한다.

1) 상점은 신뢰기관에 키 쌍을 등록: 상점은 상품암호화에 사용할 대칭키와 라벨 쌍들을 신뢰기관의 공개키로 암호화하여 신뢰기관에 전송하면 신뢰기관은 라벨과 대칭키의 해쉬값에 서명해서 상점에 주어 키 쌍의 사용을 허가한다.

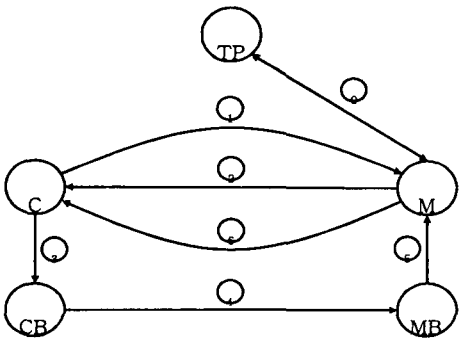

그림 1: 프로토콜 진행도.

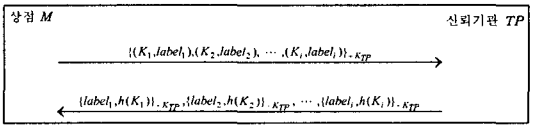

그림 2: 준비사항.

2) 상점은 자신의 웹에 상품의 설명과 상품번호 그리고 자신의 공개키를 광고한다.

3) 고객은 상점의 웹페이지에서 원하는 상품이 있는지를 확인한다.

3. 기본 프로토콜

프로토콜에서 부정한 참여자나 조기에 종료되는 경우는 없다고 가정하고 진행된다. 부정이나 조기 종료에 관한 해결은 다음 장에서 살펴보기로 하자.

메시지 1. 고객은 상점에 다음 3가지 정보를 보내면서 전자상거래 프로토콜을 시작한다. (i) 상품주문, PO. (ii) 상품주문 체크섬에 대한 서명, $\{CS(PO)\}_{-K_C}$, (iii) 상점의 공개키로 암호화한 고객의 공개키, $\{+K_{Ci}\}_{+K_M}$

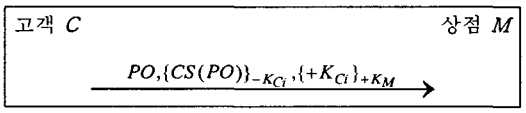

그림 3: 주문 프로토콜.

상품주문에는 고객의 가짜신분과 원하는 상품번호 그리고 지불가격 등 필수정보를 포함하고 있다. 고객은 상품주문의 체크섬을 생성하여 서명하는데 이것으로 상점이 주문을 확실하게 받았는지 확인이 가능하다. 또한 거래동안 사용할 공개키를 상점에 공개키로 암호화하여 침입을 방지한다.

메시지 2. 상점은 메시지 1을 받은 다음 주문이 올바른지 확인한 후 올바르지 않으면 프로토콜 중단 메시지 $\{Abort\}_{-K_M}$을 고객에게 보내고, 올바른 주문이면 다음 메시지를 고객에게 전송한다. (i) 상품주문 체크섬에 대한 서명, $\{CS(PO)\}_{-K_M}$, (ii) 신뢰기관으로부터 사용허가 받은 대칭키로 암호화된 상품, $\{m\}_{K_i}$, (iii) 암호화된 상품의 유효성을 확인하기 위한 해쉬값, $h(\{m\}_{Ki})$, (iv) 상품번호와 라벨 그리고 상점계좌정보, (v) 암호화에 사용된

라벨과 키의 해쉬값, $\{label_i, h(K_i)\}_{-K_{TP}}$

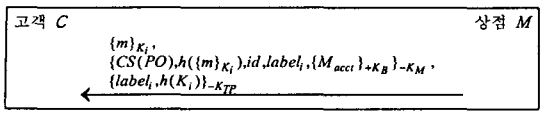

그림 4: 주문확인 프로토콜.

메시지 3. 고객은 메시지 2에서 받은 다음 중단 메시지이면 프로토콜을 중단하고 주문에 대한 확인 메시지이면 해쉬값을 이용하여 유효성을 확인하고 구입의사가 있으면 은행에게 상점에 대한 지불을 요청한다. 만약 유효성이 확인되지 않거나 구입의사가 없으면 메시지 3을 은행에게 보내지 않고 상점에게 프로토콜 중단 메시지 $\{Abort\}_{-K_C}$을 보낸다.

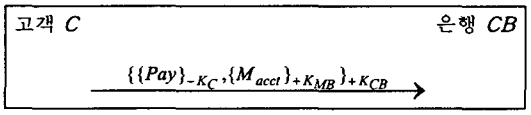

그림 5: 지불요청 프로토콜.

지불요청에 대해 고객이 서명을 하고 상점으로부터 받은 계좌정보와 같이 고객은행 공개키로 암호화해서 전송한다.

메시지 4. 메시지 3에서 지불을 보고 고객의 계좌에서 인출하여 지불토큰 P을 만들어 은행이 서명하고 상점의 암호화된 계좌정보와 같이 은행간의 공개키로 암호화하여 상점거래은행에 보낸다.

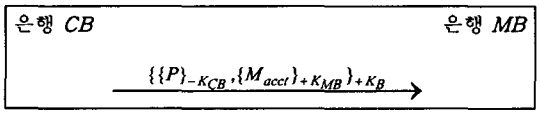

그림 6: 지불 프로토콜.

메시지 5. 상점거래은행은 자신의 개인키를 이용해 암호화된 상점의 계좌정보를 해독하여 상점의 예금액을 증가시킨 후 결과를 상점의 공개키로 암호화하여 상점에 전송한다.

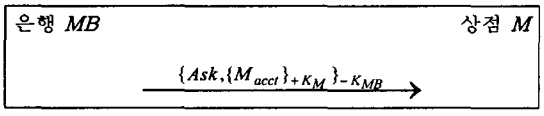

그림 7: 지불승인 프로토콜.

상점의 증가된 계좌정보를 상인의 공개키로 암호화고 두 가지를 다시 은행이 서명하여 계좌정보를 보호한다.

메시지 6. 은행으로부터 예금액 증가 승인 메시지를 받으면 자신의 개인키로 해독하여 확인한 후 상품 해독키 K_i을 고객에게 전송한다.

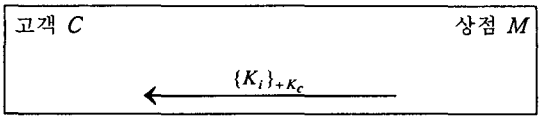

그림 8: 상품 해독키 전송 프로토콜.

고객은 받은 메시지를 자신의 개인키로 해독하여 상품 해독키를 얻으면 프로토콜은 종료된다. 지금까지는 프로토콜이 이상 없이 진행되는 이상적이 경우이다. 만약 참여자중 누군가 부정을 하거나 네트워크가 중단될 경우 낙관적인 접근방법을 이용하여 해결한다. 이 해결방법은 다음 장에서 논하기로 한다.

4. 분쟁 해결방법

공정한 교환은 각 참여자가 원하는 아이템을 얻거나 아니면 상대방 아이템에 관한 어떠한 정보도 얻지 못하도록 하는 것이다. 위에서 제안한 프로토콜에서 공정한 교환이 이루어지면 상점이 지불을 받으면 고객은 원하는 상품을 받거나 아니면 고객과 상점 모두 어떠한 이득도 없는 상태가 되도록 보장한다. 고객은 암호화된 상품과 상품의 해독키를 모두 얻어야만 상품을 받았다고 할 수 있다. 상점은 지불이 올바르게 되었는지 확인되면 지불을 받았다고 한다. 이렇게 모두가 올바르게 행동하면 프로토콜은 이상 없이 진행되고 공정한 교환이 보장된다.

만약 한 참여자가 다른 참여자로부터 메시지를 받기 위해 기다리는 시간이 정해져 있지 않거나 예상할 수 없으면 참여자는 메시지를 받기 위해 기다려야하는 문제가 발생한다. 이런 문제를 해결하기 위해 각 메시지에 종료시간을 추가하여 쉽게 해결할 수 있다. 만약 메시지를 수신한 참여자가 종료시간을 받지 못했으면 수신자에게 종료시간을 알려달라는 메시지를 전송해서 해결할 수 있다. 만약 메시지에 응답이 없으면 수신자가 프로토콜을 진행하지 않는다고 가정하고 프로토콜을 종료하거나 분쟁을 해결한다.

만약 한 참여자가 고객과 상인이 모두 올바르게 행동하면 고객은 원하는 상품을 얻고 상점은 지불을 받게된다. 하지만 어느 한쪽이 부정을 저지르거나 네트워크의 오류가 발생하면 분쟁이 일어날 수 있다. 제안하는 프로토콜에서는 크게 두 가지 경우의 분쟁이 발생할 수 있으며, 각 분쟁이 발생

하면 다음과 같은 방법으로 해결한다.

분쟁 발생 유형 1. 상점이 부정을 하거나 불만이 있는 경우.

1) 상점이 메시지 4에서 올바른 지불을 받고 메시지 5에서 상품 해독키를 보내지 않으면 고객은 메시지 2에서 받은 정보 $\{CS(PO), h(m)_K), id, label_i, \{M_{acct}\}_{K_B}\}_{K_M}$을 가지고 신뢰기관에 분쟁해결을 요청한다. 신뢰기관은 라벨정보와 상품을 확인하고 상점에게 상품 해독키를 요청한다. 만약 상점이 요구를 거부하거나 잠적하면 신뢰기관은 라벨을 통해 상점이 처음에 등록한 키 쌍에서 사용한 키를 찾아 고객에게 보내면 분쟁은 해결된다.

2) 상점이 고객에게 올바르지 않은 상품 해독키를 보내면 이것 역시 1)과 같은 방법으로 해결할 수 있다.

3) 상점이 지불을 받지 못했거나 상품에 대한 올바른 지불이 아니라고 생각하면 고객에게 상품 해독키를 보내지 않으면 된다.

분쟁 발생 유형 2. 고객이 부정을 하거나 불만이 있는 경우.

1) 고객이 지불을 하고 상품 해독키를 받지 못했다고 요구를 하는 경우 고객은 지불 $\{Pay\}_{-K_C}$과 상점으로부터 받은 계좌정보 $\{M_{acct}\}_{+K_{MB}}$을 신뢰기관에게 보내면 이 정보를 고객거래은행에게 주고 메시지 4부터 다시 수행한다.

2) 고객이 지불에 부정을 저지를 경우 상점은 고객에게 접속하여 지불을 요구할 수 있고 고객이 거부하면 상품 해독키를 보내지 않으면 된다.

3) 고객이 잘못된 상품 해독키를 받았다고 요구하는 경우는 분쟁 발생 유형 1의 1)과 같은 경우로 그동안 고객이 받은 정보를 신뢰기관에 전달하면 신뢰기관이 잘못을 판단하여 분쟁을 해결한다.

위와 같이 두 가지 경우를 제외하고는 분쟁이 발생하지 않는다.

이 프로토콜에서 공정한 교환은 M이 지불토큰을 받으면 C는 물건을 받거나 아니면 아무도 이득이 없는 상태가 되는 것을 보장한다. C는 암호화된 상품과 요구한 해독키를 모두 얻어야만 상품을 받았다고 한다. M은 받은 지불토큰이 맞는지 확인되면 지불토큰을 받았다고 한다. 모두가 올바르게 행동하면 프로토콜이 진행되고 공정한 교환이 보장된다.

5. 익명성 보장

이 프로토콜에서 가장 중요한 목적은 모든 상황에서 고객의 익명성을 보호하는 것이다. Low 등이 제안한 프로토콜에서 보면 서명하지 않은 참여자는 고객과 상점의 관계에 대한 충분한 정보를 얻지 못한다[8]. 또한 모든 참여자가 공모하면 고객의 정보를 얻을 수 있지만 모든 참여자가 공모하는 것은 불가능하다. 참여자가 공모를 하기 위한 필요조건의 두 참여자가 서로의 신원정보를 알아야하고, 서로 교환 조건이 만족하는 공동부분을 가지고 있어야한다. 표 2에 표기법은 Y와 N 그리고 M으로 표시하고 각각은 Yes, No, Maybe를 나타낸다. 표 2를 살펴보면 참여자 혼자서는 고객과 상점의 관계에 대한 충분한 정보를 알 수 없다. 정보를 얻기 위한 공모의 형태는 다음과 같다.

1) 두 참여자의 공모

아래 주어진 공모의 형태를 살펴보면 두 참여자가 공모를 통하여 어떤 정보를 얻는지 알 수 있다.

1. 신뢰기관과 상점의 공모: 상점은 신뢰기관이 공모를 통하여 알 수 있는 새로운 정보는 아무것도 없다. 이 공모의 결과 신뢰기관의 상점의 정보를 소유하게된다.

2. 신뢰기관과 은행의 공모: 신뢰기관과 은행은 공모를 해서 얻을 수 있는 이득이 아무것도 없다. 따라서 공모하지 않을 것이다.

3. 상점과 고객은행의 공모: 상점과 고객은행은 서로의 신원을 알 수 없으므로 공모할 수 없다.

4. 상점과 상점은행의 공모: 상점은 자신의 은행과 공모를 통하여 알 수 있는 새로운 정보는 아무것도 없다. 이 공모를 하면 오히려 상점의 정보를 은행에게 알려주게 된다.

5. 은행간의 공모: 은행간에 공모로 새로 알 수 있는 정보가 없다. 따라서 공모하지 않을 것이다.

위 결과 두 참여자의 공모로는 고객과 상점간의 관계에 대한 정보를 알 수 없으므로 고객의 익명성은 보장된다.

2) 세 참여자의 공모

위에 두 참여자의 공모에서 살펴보면 공모가 가능한 경우는 1)과 4)뿐 이다. 따라서 세 참여자의 공모는 신뢰기관과 상점 그리고 상점의 은행사이에서 일어난다. 세 참여자가 공모를 하려면 참여자 모두가 공동으로 얻을 수 있는 정보가 있어야 한다. 그러나 표 2에서 세 참여자는 모두 고객에

표 2. 각 참여자가 알고 있는 정보.

정 보	CB	MB	M	TP
C	Y	N	N	N
CB	Y	N	N	N
MB	N	Y	Y	N
M	N	Y	Y	N
TP	N	N	Y	Y
C_{acct}	Y	N	N	N
M_{acct}	N	Y	Y	N
PO	N	N	Y	M
$+K_M$	N	Y	Y	N
$+K_{Ci}$	N	N	Y	M
$+K_C$	Y	N	N	N
$(m)_{Ki}$	N	N	Y	M
Pay	Y	N	N	M
P	Y	Y	N	N

대한 정보를 알지 못 한다. 따라서 세 참여자가 공모하여도 고객과 상점간의 관계에 대한 어떠한 정보도 얻을 수 없으므로 고객의 익명성은 보장된다.

IV. 결론

제안하는 프로토콜은 다음과 같은 특징을 가지고 있다. 첫째, 모든 상황에서 공정한 교환을 제공한다. 둘째, 분쟁이 발생하지 않으면 신뢰기관을 이용하지 않는다. 셋째, 고객에게 지불 전에 자신이 원하는 상품인지 확인할 수 있도록 한다. 마지막으로 고객의 익명성을 보장한다. 하지만 준비사항에서 신뢰기관에게 상점이 사용할 대칭키와 라벨을 등록할 때 너무 많은 키를 등록하면 키 관리에 문제가 발생하고 상품을 얻기 위해 아직도 너무 많은 메시지교환회수를 가지고 있다. 추후에 해쉬체인을 이용하여 키 관리 문제를 해결하고 메시지교환회수를 줄인 효율적인 방법이 요구된다.

참고문헌

[1] S. Even, O. Goldreich, and A. Lempel, "A Randomized Protocol for Signing Contracts," Communications of the ACM, vol. 28, no. 6, pp. 637-647, ACM Press, 1985.

[2] M. Ben-Or, O. Goldreich, S. Micali, and R. Rivest, "A Fair Protocol for Singing Contracts," *IEEE Trans. on Information Theory*, IT-36(1), pp. 40-46, IEEE Press. 1990.

[3] B. Cox, J. D. Tygar, and M. Sirbu, "NetBill Security and Transaction Protocol," *First USENIX Workshop on Electronic Commerce*, pp. 77-88, 1995.

[4] M. K. Fanklin and M. K. Reiter, "Fair Exchange with a Semi-Trusted Third Party," *Proc. of the 4th ACM Conf. on Computer and Communications Security*, pp. 1-6, ACM Press, 1997.

[5] N. Asokan, M. Schunter, M. Waidner, "Optimistic Protocols for Fair Exchange," *Proc. of the 4th ACM Conf. on Computer and Communications Security*, pp. 6-17, ACM Press, 1997.

[6] I. Ray, I. Ray, and N. Narasimhamurthi. "A Fair Exchange Protocol with Automated Dispute Resolution," *Technical report*, University of Michigan-Dearborn, 2000.

[7] I. Ray, and I. Ray, "An Anonymous Fair-Exchange E-Commerce Protocol," *Proc. of the 1st International Workshop on Internet Computing and E-Commerce*, San Francisco, CA. 2001.

[8] S. Low, N. Maxemchuk, and S. Paul. "Anonymous Credit Cards. In J. Stern, editor," *Proc. of the 2nd ACM Conf. on Computer and Communication Security*, pp. 108-117, Fairfax, Virginia, Nov. 1994.