

---

# 디지털 상품 거래를 위한 네트워크형 전자결제 시스템 설계 및 구현

한재균\* · 한승조\*

## A Design and Implementation of a Network-type Electronic Payment System Optimized for Digital Goods

Jae-Kyun Han\* · Seung-Jo Han\*

---

이 논문은 2003학년도 조선대학교 교비 지원에 의한 연구 결과입니다.

---

### 요 약

인터넷이 상거래를 변환시키면서, 지불 방법이 인터넷을 통한 상거래를 성공적으로 이끄는 데에 중요한 요소가 되고 있다. 전자 화폐는 기존 실물 화폐가 가지는 모든 특성들을 가지면서 모든 거래에 대해 보안성을 보장해 준다. 따라서 전자 화폐를 기반으로 하는 인터넷 지불 시스템이 향후 전자 상거래에 있어서 안전하고 효율적인 지불 방법으로 기대된다. 디지털 상품과 같은 콘텐츠 상품은 상품의 전달과 대금 지불이 동일 네트워크에서 이루어질 수 있다는 특성을 가진다. 이것은 전자 상거래 시스템의 설계를 최적화하는데 도움이 된다. 본 논문에서는 인터넷을 통한 디지털 상품을 거래하기 위해 특별히 설계된 전자 지불 프로토콜을 제안한다. 제안된 프로토콜은 가상 ID를 사용하여 익명성을 보장하고 지불 단계를 최소화시켰다.

### ABSTRACT

As the Internet continues to transform the commerce, the method of payment is one of critical components to conduct successful business across the internet. An electronic cash has all characteristics of traditional commodity cash and ensures security for all transactions. Accordingly an internet billing system based electronic cash is expected as the secure and efficient payment method in future electronic commerce. Digital Contents such as digital goods and services have the special characteristic that both the delivery of the goods and the transfer of money can be accomplished on the same network. This allows the optimizations in the design of an electronic commerce system. In this paper, we propose an electronic payment protocol which is especially designed to purchase digital contents through internet. The proposed protocol guarantees anonymity by using a virtual ID, and minimizes payment processing steps.

### 키워드

전자지불, 전자상거래, 전자화폐, 정보보안

### 1. 서 론

인터넷의 급속한 발전에 힘입어 기존에 존재하던 많은 실물 시장은 가상공간 상으로 이전하게 되

고 이 속에서 디지털 데이터를 기반으로 한 각종 상품 구입, 판매, 그리고 대금 지불이 이루어지게 될 것이다. 이 과정에서 가장 중요하게 거론되고 있는 것이 대금 지불 방법이다. 기존의 실물 화폐는 거래의 불편함, 휴대의 불편함, 그리고 제작비용, 원거리에서의 상품 구입에는 부적합하다. 한편, 신용카드를 이용한 지불 방법도 카드 번호의 노출 위험, 위조 가능성이 있으며 실물 화폐가 가지는 익명성, 오프라인성을 보장하지 않고 양도도 불가능한 많은 단점을 가지고 있다. 이러한 문제점을 보완할 수 있으며 인터넷을 기반으로 한 전자상거래와 같은 가상공간에서 사용자가 전자화폐를 서로 쉽게 주고받을 수 있는, 실물화폐를 대체할 수 있는 새로운 개념의 화폐로서[1] 전자화폐에 대한 연구 및 개발이 활발히 진행 중이다.

전자화폐란 실물화폐의 신용성에 기반을 두고, 기본 화폐가 지니고 있는 불편함을 해소시키기 위해 일정한 화폐 가치를 IC 카드나 PC 등에 디지털 가치로 저장했다가 온라인이나 오프라인 형태로 상품을 구매하거나 비용을 지불함으로써 원격지 이송에 따른 통신 기능, 휴대 및 보관의 편의 기능, 위조방지 기능 등을 추가한 새로운 전자적 결제 방법이라고 정의할 수 있으며, 화폐로서의 기능상 전자동전(Electronic Coin)[2]방식과 전자수표(Electronic Check)[3]방식으로 분류하는데, 액면 가치를 보증하기 위해 은행이 서명한 디지털 신호로 표현된 가치정보이다.

전자화폐에 대한 연구개발은 1982년 David Chaum의 은닉서명에 기반 한 추적 불가능한 온라인형 전자화폐 프로토콜이 처음 등장한 이래 전자화폐가 요구하는 여러 가지 조건들을 만족시키는 많은 방식들이 제안되어 오고 있으며, 전자지불 시스템의 프로토콜은 안전성 및 보안성을 위해 여러 가지 요구 사항을 고려하여야 한다 [4]. 이러한 시스템의 중요한 기술인 디지털 서명, 은닉 서명과 같은 인증 기능 및 보안은 공개키 기반구조(PKI)의 대표적인 RSA (Rivest-Shamir-Adleman)를 통한 암호화를 이용하여 보안기술에 기반을 둔 안전장치를 갖추는 것이 바람직할 것이다[5].

익명성이 제공되는 전자화폐 시스템에서 익명성을 오용함으로써 발생할 수 있는 각종 위협요소는 위조, 이중사용, 위장, 초과사용, 돈 세탁, 불법 구매, 약탈, 은행 강탈 등이 있다.

전자상거래에서 전자지불 프로토콜은 디지털 정보화(Independence), 재사용 불가능성(안전성), 익명성(Privacy, Untraceability), 오프라인성(Offline), 양도 가능성(Transferability), 분할 이용 가능성(Divisibility), 부정 사용자의 익명성 취소

(Anonymity Revocation of illegal user) 등을 요구하고 있다.

인터넷과 웹을 기반으로 한 온라인 쇼핑몰에서는 TV, 냉장고, DVD 등과 같은 상품뿐만 아니라 소프트웨어, 비디오 타이틀, MP3 오디오 파일 등과 같은 디지털 콘텐츠도 거래될 수 있다. 디지털 콘텐츠는 일반 상품과 달리 대금 결제가 이루어지면 메일이나 파일 전송 등의 방법으로 인수할 수 있는 장점이 있다.

본 논문에서는 공개키(PKI) 기반의 네트워크형 전자화폐 기반의 전자지불 프로토콜을 제안한다. 제안된 프로토콜은 콘텐츠(소프트웨어, 잡지 등)만을 취급하는 NetBill 시스템의 문제점인 익명성이 보장되지 않는 부분을 보완하였으며, 거래내역 DB에서는 접속 ID를 사용하여 잔액 및 사용내역을 제공받을 수 있도록 하였고, 온라인상에서 제공된 디지털 콘텐츠에 대해 인증번호를 부여함으로써 무단 복제 및 배포를 방지하고 최대한 안전성이 확보되도록 하였다.

본 논문의 구성은 다음과 같다. II장에서는 디지털 상품 거래를 위한 기존의 NetBill 시스템을 분석한 후, 이의 단점들을 해결한 네트워크형 전자지불 프로토콜을 제안하고 이를 시범 구현한 예를 보여 준다. III장에서는 기존의 전자지불 프로토콜들과 제안된 프로토콜을 비교 분석하고, IV장 결론에서는 제안된 프로토콜의 주요 특징들을 기술한다.

## II. 디지털 상품 거래를 위한 전자지불 프로토콜

### 1. NetBill 시스템의 특징 및 문제점

NetBill은 콘텐츠만을 거래하기 위한 지불브로커 방식의 소액 지불 시스템이다[6]. 구매자는 NetBill 서버의 지불 승인을 받은 후 상품을 수령하고, 판매자는 결제가 일어난 후 상품을 전달하기 때문에 구매자와 판매자 모두가 상호 신뢰할 수 있으나, 매 서비스마다 NetBill 서버에 접속하여 확인 절차를 거쳐야 하고, 거래 단계도 복잡함으로 인하여 다른 지불 프로토콜에 비해서 전자 서명이 많이 쓰이는 단점이 있다.

또한, 판매자는 구매자의 신원을 파악하고, NetBill에 의한 모든 거래 정보는 서버에 기록되므로 거래를 추적할 수 있기 때문에 구매자와 판매자 모두 익명성이 보장되지 않는다.

### 2. 제안된 네트워크형 전자지불 프로토콜 2.1 프로토콜 개요

컨텐츠만을 취급하는 NetBill 시스템의 경우 고객과 상점 모두 익명성이 보장되지 않는 단점을 가지고 있으며, 고객은 지불승인을 받은 다음 상품을 수령하고, 상점은 결제가 일어난 후 상품을 전달하기 때문에 고객과 상점 모두 상호간에 신뢰할 수는 있지만, 구매 결정에서부터 컨텐츠를 이용할 수 있는 거래 단계가 복잡하다. 매 서비스마다 서버에 접속하여 확인 절차를 거치고, 거래 단계도 복잡함으로 인하여 다른 지불 프로토콜에 비해서 전자서명이 많이 쓰이는 단점도 있다.

따라서 본 논문에서 제안하는 전자지불 프로토콜은 상품이 모두 디지털로 되어 있기 때문에 상품 제공과 지불 사이에 생기는 공백으로 인한 불신이 발생하지 않는다는 점을 감안하여, 상품 주문과 지불을 동시에 처리함으로써 익명성이 보장되고 거래 단계를 최소화 할 수 있도록 설계하였다.

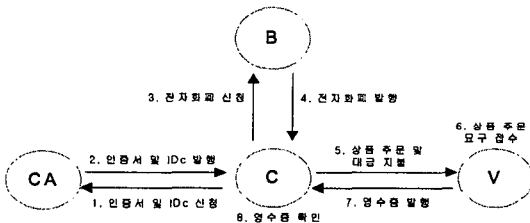


그림 1. 제안된 프로토콜의 전체 흐름도

◆제안된 전자지불 프로토콜을 설명하는데 사용되는 기호는 다음과 같다.

- CA : 인증기관
- B : 은행
- V : 판매자
- C : 구매자
- M : 문서
- ER : 공개키 암호알고리즘 암호
- DR : 공개키 암호알고리즘 복호
- Z : 압축 알고리즘
- KUA : A의 공개키
- KRA : A의 개인키
- E : 관용키 알고리즘 암호
- D : 관용키 알고리즘 복호
- Ks : 세션키
- H : Hash 알고리즘
- Certificate A : A의 인증서
- || : 연접(Concatenation) 연산

2.2 인증서 및 IDc

1) 인증서 및 IDc 신청

구매자의 익명성을 보장하기 위해서 구매자는 인증기관(CA)에 자신의 실명정보를 제공하고, 인증서와 익명성 유지를 위한 가상 ID를 신청한다. 구매자(C)는 자신의 실명정보(Customer)와 컨텐츠 구매에 사용할 가상 ID(IDc)를 CA의 공개키로 암호화하여 인증기관에 전송한다.

$$ERKUca \{ Customer || IDc \} \dots \dots \dots (\text{식 } 1)$$

2) 인증서 및 IDc 발행

인증기관(CA)은 구매자(C)의 신원을 확인하고 인증서, IDc와 함께 은행(B)의 공개키를 C의 공개키로 암호화하여 전송한다.

$$ERKUc \{ Certificate C || IDc || KUB \} \dots \dots \dots (\text{식 } 2)$$

2.3 전자화폐 신청 및 발행

1) 전자화폐 신청

구매자는 자신이 사용할 전자화폐의 금액만큼을 은행에 입금하고, 인증서와 IDc를 전송하여 전자화폐 발행을 요구한다. 구매자는 개인의 실명정보가 아닌 인증서와 IDc만을 사용하기 때문에 은행은 구매자의 개인실명 정보를 알 수 없고, 대신에 IDc만으로 거래를 하게 된다. 구매자는 인증서, IDc 및 전자화폐로 전환하고자하는 금액(Cash)을 은행의 공개키와 사용자의 비밀키로 암호화하여 전송한다.

$$ERKUb \{ ERKRc \{ Cash || IDc || Certificate C \} \} \dots \dots \dots (\text{식 } 3)$$

2) 전자화폐 발행

은행은 인증서와 IDc를 검증하고 입금된 금액에 맞는 전자화폐를 발행한다. 검증된 자료의 전자화폐 금액은 IDc의 정보로 DB에 저장하고, 구매자가 접속할 경우 상품 구매 내역 및 전자화폐 발행내역을 표시하고, 사용 가능한 전자화폐의 금액을 나타낸다. 구매자에게 전자화폐 발행금액(E-Cash)을 은행의 인증서를 첨부하여, 구매자의 공개키와 은행의 비밀키로 암호화하여 전송한다.

$$ERKUc \{ ERKRb \{ E-Cash || IDc || Certificate B \} \} \dots \dots \dots (\text{식 } 4)$$

2.3 상품 주문 및 대금 지불

구매자(C)는 인증기관으로부터 발급 받은 IDc로 DB에 접속하게 되고, 접속과 동시에 IDc의 구매자가 사용 가능한 전자화폐의 금액이 계산되어 사용

제한을 받는다. 구매자(C)는 판매자(V)의 준비된 상품 중에서 원하는 콘텐츠를 선택한 후 전자화폐 금액과 콘텐츠 정보를 전송하고 전송과 동시에 DB에 주문서의 내용을 등록한다. 주문서(M)를 Hash하고 자신의 개인키(KRc)로 암호화하는 과정을 통하여 주문서에 자신의 서명을 한다. 하지만 사용자의 실명정보는 알 수 없다.

$M = \{ID_c, \text{컨텐츠 번호}, \text{전자화폐 금액}, \text{전자 화폐 발행 번호}\} \dots\dots\dots$ (식 5)

$ERKRc\{H(M)\} \dots\dots\dots$ (식 6)

그리고 차후에 발생할 전송 및 변조여부의 시비를 확인 할 수 있도록 Hash된 주문서(H(M))를 보관한다. 그리고 M, ERKRc{H(M)}, Certificate C를 함께 압축하고 세션키(Ks)를 사용하여 관용키 암호 알고리즘으로 암호화한다.

$EKs\{Z[M || ERKRc\{H(M)} || Certificate\ C]\} \dots\dots\dots$ (식 7)

세션키(Ks)는 판매자(V)의 공개키(KUV)로 암호화한 후

$ERKUv\{Ks\} \dots\dots\dots$ (식 8)

세션키로 암호화한 주문서와 같이 판매자(V)에게 전송한다.

$EKs\{Z[M || ERKRc\{H(M)} || Certificate\ C] || ERKUv\{Ks\}\} \dots\dots\dots$ (식 9)

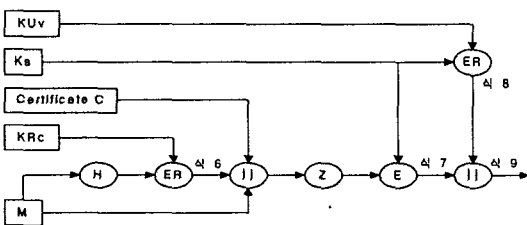


그림 2. 상품 주문 및 대금 지불

2.4 상품 주문 요구 접수

구매자(C)가 원하는 콘텐츠의 번호와 대금 지불에 관한 정보를 판매자(V)에 전송하면, 판매자는 주문서의 내용을 DB에서 판매자의 정보로 그 유효성을 검사하여 정당한 주문서인지를 판단한다. 판

매자(V)는 독단으로 신규 구매 DB를 생성할 수 없으며, 단지 문서의 내용을 판단하여 인증번호를 부여할지 만을 결정하고 정당한 주문서라면 인증번호를 부여한다. 따라서 판매자(V)가 부정한 거래할 수 없도록 하였다. 판매자(V)는 구매자(C)에게서 받은 주문서 중 ERKUv{Ks}를 자신의 개인키(KRV)를 사용하여 세션키(Ks)를 얻는다.

$DRKRv\{ERKUv\{Ks\}\} = Ks \dots\dots\dots$ (식 10)

구한 세션키(Ks)를 사용하여 관용키 암호화된 부분을 복호화 한다.

$DKs\{EKs\{Z[M || ERKRc\{H(M)} || Certificate\ C]\}\} = Z\{M || ERKRc\{H(M)} || Certificate\ C\} \dots\dots\dots$ (식 11)

사용된 압축을 풀어내고 Certificate C를 통하여 유효한 공개키인지 확인한다. 유효하지 않는 인증서이면 재전송을 요구하고, 유효한 인증서이면 다음 작업을 수행한다.

구매자(C)의 개인키(KRc)로 암호화 된 문서를 Certificate C에 포함되어있는 C의 공개키를 사용하여 복호화 한다.

$DRKUc\{ERKRc\{H(M)\}\} = H(M) \dots\dots\dots$ (식 12)

압축을 풀어낸 문서에 포함된 M을 Hash하고 (식 12)에서 나온 H(M)과 비교하여 다르다면 재전송을 요구하고 같으면 전송도중에 변조되지 않은 것으로 인정한다.

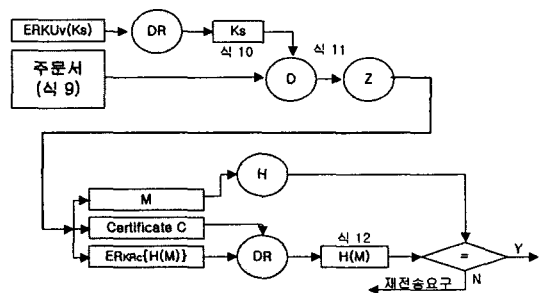


그림 3. 상품 주문서 복호화

2.5 영수증 발행

판매자는 구매자로부터 받은 정보와 전자화폐 내용에 이상이 없으면 상품을 발송하고 영수증을 발행한다. 영수증에 상품 인증 번호를 첨부하여 전송하게 되면 구매자는 상품 인증 번호를 입력하여

컨텐츠 상품을 다운로드받을 수 있다.

(식5)의 주문서와 상품인증번호(No\_Contents)의 해싱된 정보를 판매자의 개인키(KRv)로 서명을 한다.

$$ERKRv\{H(M || No\_Contents)\} \dots \dots \dots (식 13)$$

서명한 정보와 Certificate V, 수신 받은 날짜와 시간을 구매자의 공개키 Kuc로 암호화하여 전송한다.

$$ERKuc\{ERKRv\{H(M || No\_Contents)\} || Certificate V || Date/Time\} \dots \dots \dots (식 14)$$

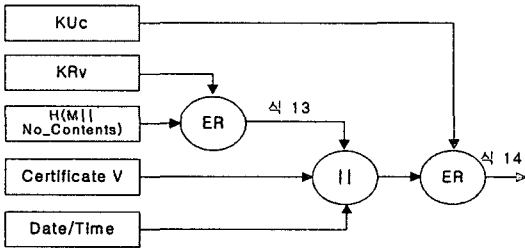


그림 4. 대금 지불에 관한 영수증 발행

2.6 영수증 확인

판매자(V)로부터 발행된 영수증으로 컨텐츠에 대한 대금이 정확하게 지불되었는지를 확인한다.

구매자(C)는 전송된 문서를 자신의 개인키(KRc)로 복호화 하여

$$DRKRc \{ERKuc \{ERKRv \{H(M || No\_Contents)\} || Certificate V || Date/Time\} = ERKRv \{H(M || No\_Contents)\} || Certificate V || Date/Time \dots \dots (식 15)$$

포함된 Certificate V가 유효한지를 확인하고, 유효하면 Certificate V에 포함된 판매자(V)의 공개키(KUv)를 이용하여 판매자(V)의 공개키로 서명된 H(M) 문서를 복호화 한다.

$$DRKUv \{ERKRv \{H(M || No\_Contents)\} = H(M) \dots \dots \dots (식 16)$$

여기에서 얻은 Hash된 문서(H(M))와 (식12)과정에서 발생한 H(M)을 비교함으로써 전송도중에 문서가 변조되지 않았음을 확인할 수 있다.

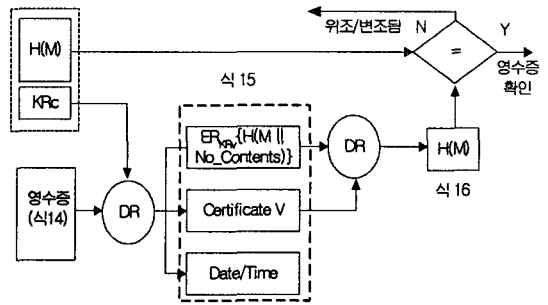


그림 5. 영수증 복호화 및 검증

3. 제안된 전자결제 시스템 구현

3.1 개발환경

- 프로그램 명칭 : Contents-Pay
- 환경 : Intel Pentium4 CPU2.00GHz 224MB RAM
- OS : Microsoft Windows XP
- 데이터베이스 : MySQL 3.23.49
- 개발 언어 : DELPHI 6 Enterprise

3.2 구현범위

은행과 관련된 부분은 은행과 연계된 이후에 사용될 수 있도록 은행에 전자화폐를 신청하는 부분만 처리하였고, 상품의 구입과 같은 전자화폐 사용내역에 중점을 두고 구현하였다.

데이터베이스 서버가 존재하고, 일반 사용자들이 사용하는 클라이언트용 소프트웨어를 개발하였으며, 서버에 접속 할 경우에는 ID와 비밀번호로 데이터베이스에 접속이 가능하도록 하였다.

전자화폐의 불법적인 사용이 이루어진 것으로 짐작되면 관리자의 특별한 권한으로 개인의 전자화폐 거래내역을 열람할 수 있도록 하여 익명성 철회가 가능하도록 하였다.

3.3 컨텐츠 구매 처리 화면

디지털 상품과 같은 정보 상품은 상품의 전달과 대금 지불이 동일 네트워크에서 이루어질 수 있다는 특성을 고려하여 구현하였으므로, 컨텐츠 구입 및 결제를 위해 자료를 전송하고, 서버에서 복호화가 완료되면 컨텐츠에 대한 결제는 완료되며 다운로드 할 수 있도록 하였다.

개인 신상에 관한 자료로 공개키, 개인키 및 인증서를 발급 받는다. 인증서는 모든 거래에 사용되

며, 인증서가 사용될 때는 실명이 아닌 등록된 ID 만을 사용하게 된다.

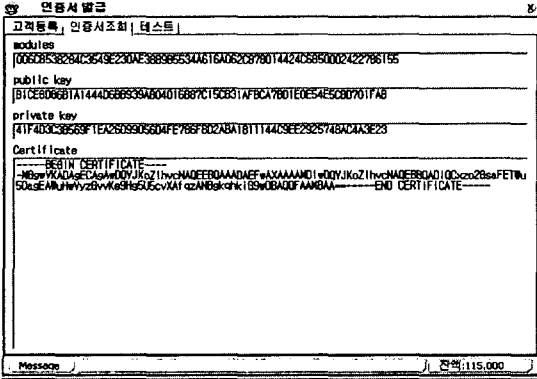


그림 6. 인증서 발급

상품 주문 및 결제가 동시에 처리되는 특성을 이용하여 결제가 완료되면 콘텐츠를 바로 다운로드 할 수 있도록 하였으며, 우측 하단에 사용 가능한 전자 화폐를 표시하여 잔액을 초과하는 콘텐츠는 구매가 이루어지지 않도록 하였다. 본인이 그동안 구입한 내역을 보여 주고 결제가 완료된 콘텐츠는 언제든지 다시 다운로드 할 수 있도록 하였다.

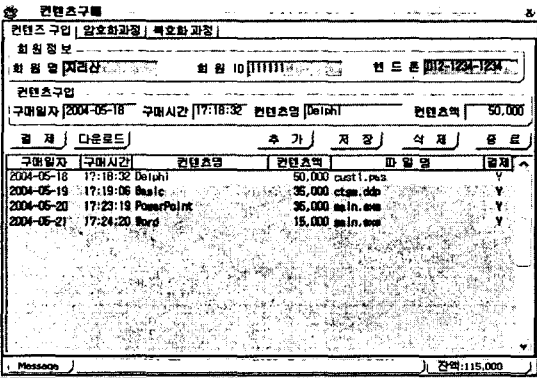


그림 7. 디지털 상품 구매 및 결제

암호화 및 복호화는 처리과정의 정확성을 위하여 단계마다 암호화 및 복호화 과정을 화면에 출력하도록 하였다. 실제 처리 과정에서는 사용자가 볼 수 없도록 하였다.

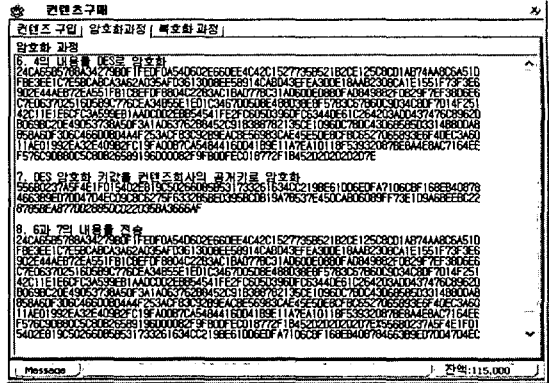


그림 8. 디지털 상품 주문을 위한 자료 암호화 과정 (전송)

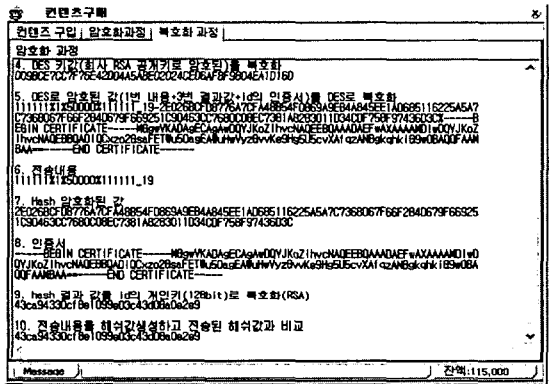


그림 9. 디지털 상품 결제를 위한 자료 복호화 과정 (결제)

### III. 제안된 프로토콜의 특징 및 기존 프로토콜과의 비교

#### 1. 제안된 프로토콜의 특징

제안된 프로토콜을 전자지불 프로토콜의 요구사항 만족도 측면에서 분석해 보았다.

##### ① 익명성

인증서를 첨부하여 인증기관으로부터 인증서의 내용을 통보 받기 전까지는 어느 누구도 계좌 추적과 같은 개인 정보의 외부 누출은 발생하지 않아 개인의 지불 내역이 공개되지 않는다.

실명 정보가 아닌 ID만을 사용하기 때문에 인증기관의 승인 없이는 어떠한 경우라도 전자화폐 사용자의 실명 추적이 불가능하다.

##### ② 위조 불가능성

모든 거래가 일련번호 발행 절차를 거치기 때문에 신청한 인증서와 일련번호 없이는 어떠한 경우라도 권한이 부여된 은행이외의 경우를 제외하고는 전자 화폐 발행이 불가능하며, 은행 또한 개인의 동의 없이 불법적인 전자화폐발행을 할 수 없다.

③ 오프라인성

구매자가 컨텐츠 구입 대금으로는 전자화폐를 지불했을 때 판매자는 은행에 접속하지 않더라도 전자화폐의 공정성, 유효성을 검증할 수 있도록 했다.

④ 이중 사용 및 부인 방지

영수증 발행 및 검증 절차를 수행하여 거래 당사자간에 정보의 전달 내용에 대해 부인할 수 없도록 하였다. 또한, 전자 화폐에 대한 사용도 일련번호를 부여하고, 접속과 동시에 잔액을 계산함으로써 잔액 이상인 초과 금액의 사용이나 이중 사용이 불가능하도록 하였다.

⑤ 속임 방지

당좌 수표의 경우 소지인이 반드시 은행을 통해서만 현금 인출이 가능하듯이, 제안된 프로토콜은 인증서와 일련번호 없이는 거래가 불가능하기 때문에 인증서와 일련번호가 없는 거래는 모두 부정 한 거래로 간주된다.

2. 기존 전자지불 프로토콜과의 비교

대부분의 전자지불 프로토콜이 익명성 제어를 제공하지 못하고 있으며, 제안된 프로토콜과 기존 프로토콜과의 전체적인 특성을 비교하면 [표 1]과 같다.

[표 1] 기존 전자지불 프로토콜과의 비교

비교항목 전자화폐	안전성	이중사용 방지	Vendor의 부정방지	익명성
Millicent	○	○	X	X
MPTP	○	○	X	X
Mini-pay	○	X	○	X
E-cash	○	○	○	○
Cyber-cash	○	-	○	X
Echeck	○	○	○	X
FV	○	-	○	X
NetCheque	○	○	○	X
NetBill	○	○	○	X
제안 방식	○	○	○	○

■ NetBill과의 비교

구매자는 NetBill 서버의 지불승인을 받은 후 상

품을 수령하고, 판매자는 결제가 일어난 후 상품을 전달하기 때문에 구매자와 판매자 모두가 상호 신뢰할 수 있으나, 매 서비스마다 서버에 접속하여 확인 절차를 거쳐야 하고, 거래 단계도 복잡함으로 인하여 다른 지불 프로토콜에 비해서 전자 서명이 많이 쓰이는 단점이 있다.

또한, 판매자는 구매자의 신원을 파악하고, NetBill에 의한 모든 거래 정보는 서버에 기록되므로 거래를 추적할 수 있기 때문에 구매자와 판매자 모두 익명성이 보장되지 않는다. 하지만 새로 제안된 프로토콜의 경우 가상 ID를 사용하여 인증기관의 도움 없이는 실명정보를 알 수 없기 때문에 익명성이 보장되며, 구입과 지불을 동시에 처리함으로써 기존의 지불방식에 비해 지불 단계를 줄일 수 있다.

■ Millcent와의 비교

Millcent는 선불방식으로써 구매자가 판매자의 스크립(scrip)을 구입하여 거래하는 방식으로 암호화를 사용하지 않고 해쉬 연산만을 이용함으로써 구현 비용 및 연산 과정을 현저하게 줄였다. 하지만, 구매자는 각 판매자마다 다른 스크립을 구입해야 하는 번거로움이 있으며, 익명성이 보장되지 않고 판매자가 스크립 생성에 필요한 모든 정보를 알고 있기 때문에 부정한 스크립을 생성할 수 있는 문제가 있다. 그러나 제안된 프로토콜은 가상 ID를 사용함으로써 다른 판매자와의 거래도 언제든지 할 수 있으며, 판매자 독단으로는 구매와 관련된 신규 DB를 생성할 수 없도록 하였고, 영수증을 발행함으로써 판매자가 구매자를 속이고 부정한 거래를 할 수는 없다.

3. 제안된 프로토콜의 안전성 및 효율성

제안된 프로토콜은 안전성과 효율성 측면에서 다음과 같은 특징들을 보여 준다.

① 현금 계좌에서 전자화폐로의 전환, 전자화폐로 결제, 전자화폐에서 현금 계좌로의 전환 등 모든 거래에는 항상 인증서와 일련번호를 함께 제출하여 일상의 당좌 수표처럼 인출 시점마다 금액에 일련번호를 남긴다. 그렇게 함으로써 제한적이거나 필요시에 자금의 흐름을 인증기관의 협조를 얻어 밝혀 낼 수 있다.

② 모든 거래는 인증기관으로부터 할당받은 ID만을 사용하기 때문에 은행이나 상점에서는 거래 당사자의 실명내용을 알 수 없도록 하였다.

③ 당좌 거래에 포함되는 당좌통장처럼 거래 내

역을 본인이 상세하게 알 수 있도록 하였으며, 평소에는 잔액만 보관하기 때문에 자금의 흐름을 알 수 없다.

④ 상품이 모두 디지털로 되어 있기 때문에 상품 제공과 지불 사이에 생기는 공백으로 인한 불신이 발생하지 않는다는 점을 감안하여, 상품 주문과 지불을 동시에 처리함으로써 거래 단계를 단축시킬 수 있었다.

⑤ 전자화폐 발행 및 상품 구매 등의 모든 거래를 서버의 거래 DB에 저장함으로써 구매자가 정당한 접속을 시도할 경우 구매자의 모든 거래내역을 파악할 수 있고, 거래 시점에서 사용 가능한 전자화폐의 금액을 표시 할 수 있다.

⑥ 거래내역을 서버에서 관리하기 때문에 지불 서버의 안전성과 기밀성이 확보된다면, 사용자는 안전한 거래를 할 수 있다.

#### IV. 결 론

인터넷과 웹의 급속한 발전에 힘입어 인터넷 쇼핑물, 온라인 경매와 같은 전자상거래를 통한 상품 거래의 규모가 폭발적으로 증가하고 있다. 보안이 취약한 인터넷과 같은 가상공간에서의 상품 대금 지불 방법으로 기존의 실물화폐가 가지는 특성들을 가지며 보안성이 뛰어난 전자화폐가 중요시될 것으로 기대된다. 본 논문에서는 디지털 콘텐츠 거래를 위해 개발된 NetBill 시스템에서 익명성을 보장하지 못했던 단점을 보완하고 복잡한 지불 과정을 간략화한 네트워크형 전자지불 프로토콜을 제안하였다.

① 제안된 프로토콜은 영수증 발행 및 검증 절차를 수행하여 거래 당사자간에 정보의 전달 내용에 대해 부인할 수 없도록 하였다.

② 전자 화폐에 대한 사용도 일련번호를 부여하고, ID로 정당한 접속이 이루어지면 접속과 동시에 사용내역을 파악하고 잔액을 계산함으로써 잔액 이상인 초과 금액의 사용이나 이중 사용이 불가능하도록 하였다.

③ 거래 당사자들은 실명이 아닌 인증기관으로부터 부여받은 가상 ID만을 사용함으로써 인증기관의 개입이 없다면 완전한 익명성이 제공되도록 하였다.

④ 콘텐츠의 제공도 인증번호를 부여하여 사용

자가 인증번호를 입력하여 다운로드받을 수 있도록 하였다.

⑤ 판매자가 영수증의 발급 및 검증 절차를 수행함으로써 거래의 단계가 다른 시스템에 비하여 줄어들었으며, 전자화폐의 잔액이 허락하는 금액만큼 제약 없이 사용할 수 있다.

이러한 시스템의 발달은 전자적인 거래의 발달을 가져와 전자상거래 뿐만이 아닌 많은 분야에서 이용되리라고 생각되며, 많은 상점과 개인들의 이용과 관심이 있다면 전자상거래가 지금 보다도 발전할 수 있을 것으로 기대된다.

#### 참고문헌

- [1] J.Camenisch, U.Maurer, and M.Stadler, "Digital payment systems with passive anonymity-revoking trustees", In Esorics '96, Italy, 1996.
- [2] David Chaum, Amos Fiat, and Moni Naor, "Untraceable Electronic Cash", Advances in Cryptology-Crypto '88, LNCS 403, Springer Verlag, pp.319-327, 1988.
- [3] David Chaum, "Online Cash Checks", Advances in Cryptology-Eurocrypto'89, LNCS 434, Springer Verlag, pp.288-293, 1989.
- [4] Chaum, D., "Blind Signatures for Untraceable Payments," Advances in Cryptology Proceedings of Crypto '82, pp199-203, 1982.
- [5] O. Toole, "The Internet Billing server Transaction Protocol Alternatives", Carnegie Mellon University Information Networking Institute, 1994.
- [6] B. Cox, J. D. Tygar and M. Sirbu, "NetBill Security and Transaction Protocol", Proceeding of 1st USENIX on Electronic Commerce, 1996.
- [7] Security of Electronicmoney, Bank for International Settlements, 1996.
- [8] William Stallings, Network and Internetwork Security, Prentice Hall, 1995
- [9] 이만영 외, 「전자상거래보안기술」, 생능출판사, 2000.



저자소개



한재균(Jae-kyun Han)

1997년 한국방송통신대학교 정보통계학과 졸업(학사)  
1999년 조선대학교 산업대학원 전자공학과 졸업(석사)  
2003년 조선대학교 대학원 전자공학과(박사수료)

※관심분야 : 전자상거래, 전자지불, 정보통신 보안, 암호프로토콜



한승조(Seung-jo Han)

1980년 조선대학교 전자공학과 졸업  
1982년 조선대학교 전자공학과 석사  
1994년 충북대학교 전자계산학과 박사

1986년 6월~1987년 3월 뉴올리언즈대학 객원교수  
1995년 2월~1996년 1월 텍사스대학 객원교수  
2000년 12월~2002년 3월 버클리대학 객원교수  
1998년 3월~현재 조선대학교 전자정보통신공학부 교수

※관심분야 : 통신보안시스템설계, S/W불법복제 방지시스템, ASIC 설계