# 추적 가능한 공정한 전자화폐 시스템

장석철, 이임영
순천향대학교 정보기술학부

# Traceable Fair Electronic Cash System

Seok-Cheol Jang, Im-Yeong Lee
Division of Information Technology Eng. Soonchunhyang Univ

**요 약**

사이버 공간에서 이루어지는 전자상거래에서 중요하게 여겨지는 전자화폐 시스템은 사용자의 익명성을 기본적으로 제공하고 있다. 하지만 이러한 익명성으로 인해 각종 범죄 활동에 이용하려는 시도가 발생할 수 있다. 따라서 사회적, 경제적인 범죄로의 이용가능성 때문에 익명성 제어에 관한 연구는 필수적이다. 이에 본 논문은 사용자 추적은 물론 동전 추적도 할 수 있는 새로운 프로토콜을 제안한다.

## 1. 서론

컴퓨터 산업의 급속한 발전과 정보화 사회 구현을 위한 각종 전산망이 확대 보급됨으로써 대량의 중요한 정보들이 컴퓨터를 통해 처리 및 저장되고 인터넷을 통하여 신속하게 정보 교환이 이루어지고 있다. 또한 인터넷의 성장으로 인해 보다 많은 기업과 상점 그리고 사용자가 인터넷상에서 전자상거래를 이용하고 있다. 특히 전자상거래에서 가장 중요한 요소중에 하나는 안전하고 효율적인 전자지불 시스템이다.

동전과 지폐로 대별되던 화폐에 신용카드가 나오면서 화폐의 혁명이 시작됐다. 이른바 플라스틱 머니로 불리며 급속한 확산속도를 보이던 신용카드는 국민 1인당 1장 이상을 소유할 정도로 대중화된 화폐로 자리잡고 있다. 최근에는 정보통신 및 컴퓨터 기술의 발달로 신용카드, 전자 자금이체 등 현금대체 결제수단이 보편화되고 있다. 하지만 이러한 현금 대체 결제수단을 인터넷에서 사용할 경우 신용카드 번호 누출 등으로 개인 사생활이 노출될 수 있다. 또한 실물화폐가 갖는 동일한 재질의 입수가 곤란, 투명성 및 고도의 인쇄, 제조기술이 필요 등으로 인해 실물화폐는 정보화사회에 대응하기는 곤란하다. 왜냐하면 실물화폐는 종이와 금속이라는 물리 매체에 의해 실현되기 때문에 실제 사용이 그 물리적 이동을 전제로 하고 정보로써 취급하기 어렵기 때문이다. 따라서 인터넷과 같은 네트워크 상에서 지불수단으로써 전자화폐의 필요성이 증가되고 있다.

네트워크 상에서 사용하는 전자화폐의 가장 일반적인 요구사항으로 Okamoto-Ohta는 독립성(완전정보화, Independence), 보안성(이중사용방지, Security), 오프라인 상에서의 지불(Off-line payment), 양도성(가치이전성, Transferability), 분할성(Dividability), 익명성(추적불가능성, Untraceability)을 제안했다.[1] 이외에도 불추적성에 의한 프라이버시 보호를 강조함으로써 돈세탁이나 탈세 등의 사회적 범죄가 발생할 수 있기 때문에 조건부로 전자화폐나 사용자를 추적할 수 있는 조건부 추적가능성에 대한 요구조건도 필요하다.

본 논문에서는 전자상거래에서 중요한 기술인 전자화폐 시스템 중 사용자 추적 및 동전 추적이 가능한 새로운 전자화폐 시스템에 대해 알아본다.

## 2. 연구동향

1982년 David Chaum이 은닉 서명 기법을 이용하여 사용자의 익명성을 제공하는 전자화폐 시스템[2]을 제안한 이후로 익명성을 제공하는 수많은 제안 방식들이 등장하였다. 하지만 이러한 논문들은 완전한 익명성을 제공함으로써 많은 문제점들이 도출되었다. 1992년 B.von Solms 와 D. Naccache가 익명성 제공

본 연구는 정보통신부의 대학S/W연구센터 지원사업에 의해 수행된 것임.

시 발생할 수 있는 각종 범죄 활동에 대해 처음으로 언급하였다.[3] 1995년 E. Brickell, P. Gemmel 과 D. Krvits는 사용자 추적(Owner Tracing)개념을 제안함으로써 문제점을 해결하려고 했다.[4] 또한 1995년 M. Stadler, J.M. Pivetearu, J.Camenisch에 의해 사용자 추적 개념뿐만 아니라 새로운 추적 개념인 동전 추적(Coin Tracing) 개념을 제안함으로써 이러한 문제점들을 해결하려고 노력하였다.[5] 마찬가지로 1996년 Y. Frankel, Y. Tsiounis와 M. Yung도 사용자 추적과 동전 추적을 통하여 익명성 제어를 제안하였다.[6] 1996년 J. Camenisch, J.M. Piveteau와 M. Stadler는 개인 계좌와 익명 계좌를 이용하여 사용자 추적이 가능한 전자화폐 시스템을 제안하였다.[7] 1996년 M. Jakobson과 M. Yung은 추적 기능을 어느 한 기관에서 담당하는 것이 아니라 은행과 Ombudsman이 분산하여 가지고있는 방식을 제안하였다.[8]

익명성 제어는 사용자가 부정사용 하였을 경우에 거래 내역서에 포함된 추적인자를 통해 사용자 식별자를 나타내거나 또는 화폐 사용시 부가되는 화폐 고유 식별값을 나타냄으로서 이루어진다. 익명성 제어는 크게 두 개의 모델로 구분할 수 있다. 하나는 전자화폐 소유자를 식별하는 사용자 추적과 은행으로부터의 화폐 인출을 식별하기 위한 동전 추적이 있다. 사용자 추적에 있어서 익명성 제어 파라메타는 추적기관에서 지불이 이루어지고 난 후에 화폐의 소유자를 판별해 낼 수 있도록 해준다. 이것의 목적은 지불이 이루어지고 난 후에 많은 화폐 유통들에 대해 합법적인 단속 요구로 이중 사용이나 위·변조와 같은 불법 사용이 일어나지 않았더라도 추적하는 것을 가능하게 해준다. 그러나 사용자 추적은 화폐에 관련된 정보에 기반하기 보다는 구입 시간, 구입량, 구입 가게 등과 같은 것들에 기반하기 때문에 사기와 같은 형태에 유용하지는 못하다. 반면에 화폐의 일련번호를 추적하는 것과 유사한 동전 추적은 물건을 구입하기 전에 추적하는 기능을 제공한다. 동전 추적에 있어서 신뢰기관은 은행으로부터 인출된 화폐를 확인하고 물품 구입에 사용한 것과 인출된 화폐를 연결시킬 수가 있다.

## 3. 제안방식

본 논문에서 제안하고 있는 방식은 전자화폐 시스템에서 요구하는 기본적인 기능뿐만 아니라 익명성 제어 기능을 가지고 있다. 먼저 1996년 J. Camenisch, J.M. Piveteau와 M. Stadler에 의해 제안된 사용자 추적만이 가능한 전자화폐 시스템에 동전 추적을 추가하여 완전한 익명성 제어 전자화폐 시스템을 제안하고 있다. 여기서 동전 추적은 이산 대수 문제를 이용하였고, 사용자 추적은 기존 방식인 개인 계좌와 익명 계좌를 통하여 이루어진다.

### 3.1 시스템 파라메타

- 공동
  - p, q : 소수 ( q|(p-1) )
  - $g_1$, $g_2$, $g_3$ : GF(p)상의 원시근
  - $H$ : 일방향 해쉬함수
  - $z_v \equiv g^{x_v} \pmod p$
  - $h \equiv g^{x_h} \pmod p$
- 사용자(Customer)
  - $P_A$ : 개인계좌
  - $A_A$ : 익명계좌
- 은행(Bank)
  - $(Sig_B, Ver_B)$ : 은행의 서명 scheme
  - $x_h \in Z_q$, $x_v \in Z_q$
- 신뢰기관 (Trustee)
  - $X_T$ : 비밀정보
  - $Y_T = g_2^{X_T} \pmod p$ : 공개정보
  - $(Sig_T, Ver_T)$

### 3.2 개인계좌(Personal Account) 개설 단계

사용자가 은행으로부터 개인 계좌를 개설하는 단계이다.

step1:은행은 $x_p \in Z_q$을 랜덤하게 선택하고 $P_A \equiv g_1^{x_p} h \pmod p$을 계산한다. 또한 $P_A$에 은행이 서명을 한 $S_{P_A} = Sig_B(P_A)$ 와 $x_p$을 사용자에게 보낸다. 그리고 은행은 $x_C \equiv (x_p + x_h)^{-1} \pmod p$을 계산하고 $P_A$와 $x_C$을 저장한다.

Step2:사용자는 은행으로부터 받은 $x_p$을 이용하여 $P_A \equiv g_1^{x_p} h \pmod p$을 계산하고, 다음과 같이 은행의 서명을 확인한다. 또한 $P_A$와 $x_p$을 저장한다.

$$Ver_B(P_A, S_{P_A}) \stackrel{?}{=} 1$$

### 3.3 신뢰기관(Trustee)에 등록

사용자는 신뢰기관에 개인계좌를 등록하고 익명계좌를 개설하기 위한 파라메타를 승인 받는다.

step1:사용자는 $x_A \in Z_q$을 랜덤하게 선택하고, $P_A$, $S_{P_A}$와 같이 신뢰기관에 보낸다.

step2:신뢰기관은 은행의 서명을 다음과 같이 확인한다.

$$Ver_B(P_A, S_{P_A}) \stackrel{?}{=} 1$$

$A_A = (P_A)^{x_A'} \pmod p$를 계산하고, $A_A$에 신뢰기관이 서명을 한 $S_{A_A} = Sig_T(A_A)$ 을 사용자에게 보낸다. 신뢰기관은 $x_A$, $P_A$, $A_A$을 저장한다.

step3:사용자는 $A_A = (P_A)^{x_A^{-1}} \pmod p$을 계산하고 신뢰기관의 서명을 다음과 같이 확인한다.

$$Ver_T(A_A, S_A) \stackrel{?}{=} 1$$

또한 $Cnt_{C,T}=0$으로 하고 $x_A$, $A_A$, $S_{A_A}$와 $Cnt_{C,T}$을 저장한다.

### 3.4 익명계좌 개설

사용자가 은행으로부터 새로운 익명계좌를 개설하는 단계이다.

step1:사용자는 먼저 $r_1, r_2 \in Z_q$을 선택하고 $t=g_1^{r_1}h^{r_2} \pmod p$을 계산하여 은행에게 t, $A_A$와 $S_{A_A}$을 보낸다.

step2:은행은 신뢰기관의 서명을 다음과 같이 확인한다.

$$Ver_T(A_A, S_{A_A}) \stackrel{?}{=} 1$$

또한 $u \in Z_q$을 랜덤하게 선택하여 사용자에게 보낸다.

step3:사용자는 u를 이용하여 다음과 같이 계산하여 $s_1$, $s_2$을 은행으로 보낸다.

$s_1=uP_Ax_A^{-1}+r_1 \pmod p$, $s_2=ux_A^{-1}+r_2 \pmod p$

step4:은행은 $s_1$, $s_2$을 이용하여 다음과 같이 확인을 한다.

$$t(A_A)^u \stackrel{?}{=} g_1^{s_1}h^{s_2} \pmod p$$

또한 $Cnt_{C,B}=0$으로 하고 $A_A$, $Cnt_{C,B}$를 저장한다.

### 3.5 개인계좌로부터 전자면허발행 단계

익명계좌를 개설한 후 실질적으로 쓰이게 될 동전에 일부분이 될 전자면허발행 단계이다.

step1:은행은 다음과 같이 계산을 한 후 사용자에게 보낸다.

$$t'=P_A^{r'} \pmod p \quad r' \in Z_q$$

step2:사용자는 $\alpha, \beta \in Z_q$을 랜덤하게 선택한 다음 다음과 같이 계산하여 $c'$을 은행에게 보낸다.

$$t=t'z_v^{\alpha}P_A^{\beta} \pmod p$$

$$c=H(t \| y_A \| Cnt_{C,T})$$

$$c'=c-\alpha \pmod q$$

step3:은행은 다시 $c'$을 이용하여 다음과 같이 계산하여 $s'$을 사용자에게 보낸다.

$$s'=r'-c'x_Cx_v$$

step4:사용자는 은행으로부터 받은 $s'$을 이용하여 다음과 같이 계산하여 전자면허를 발급 받는다.

$$s''=s'+\beta \pmod p$$

$$t \stackrel{?}{=} P_A^{s'}z_v^c \pmod p$$

$$s=s''x_A \pmod q$$

전자면허 (s, c)를 저장하고 $Cnt_{C,T}$을 하나 증가시킨다.

### 3.6 익명계좌로 전자화폐 예치 단계

개인계좌로부터 발급 받은 전자면허를 은행의 서명을 통하여 사용할 수 있는 전자화폐로 만드는 과정이다.

step1:사용자는 $w \in Z_p^*$을 랜덤하게 선택한 후 추적 파라메타를 계산하여 (s, c), v, $A_A$, $A'_1$, $A'_2$을 은행에 보낸다.

$A'_1=y_T^w \pmod p$, $A'_2=P_Ag_2g_3^w \pmod p$

step2:은행은 $A'_1$, $A'_2$이 올바르게 생성하였는지 확인한다.

$$\log_{g_3}(A'_2/P_Ag_2) \stackrel{?}{=} \log_{A'_1}y_T$$

또한 c가 올바르게 생성되었는지 확인한다.

$$t=P_A^sZ_v^c \pmod p, \quad c \stackrel{?}{=} H(t \| A_A \| Cnt_{C,B})$$

올바르게 생성되었으면 $Cnt_{C,B}$을 하나 증가시킨다.

마지막으로 은행은 (s, c), v, $A_A$, $A'_1$, $A'_2$을 저장하고 c에 은행의 서명을 한 $c'=Sig_B(c)$을 사용자에게 보낸다.

step3:사용자는 은행의 서명을 다음과 같이 확인한다.

$$Ver_B(c, c') \stackrel{?}{=} 1$$

서명 확인이 끝나면 사용자는 전자화폐 EC를 다음과 같이 구성한다.

$EC=\{(s, c) \| A'_1 \| A'_2 \| Sig_C((s, c) \| A'_1 \| A'_2)\}$

### 3.7 지불단계

실제로 구성된 전자화폐를 통해 상품을 사고 상점에 지불하는 단계이다.

step1:사용자는 $\delta \in Z_p^*$을 랜덤하게 선택하여 다음과 같이 계산한 후 EC, (s, c), A, $A_1$, $A_2$를 상점에 보낸다.

$$A \equiv (A'_2)^w \pmod p$$

$$A_1 \equiv g_2^w \pmod p$$

$$A_2 \equiv g_1^{w\delta} \pmod p$$

step2: 상점은 사용자로부터 받은 EC의 사용자 서명을 확인하고 A, $A_1$, $A_2$를 확인한다.

$$A \stackrel{?}{=} A_1A_2g_3 \pmod p$$

확인이 끝난 다음 상점은 EC, (s, c), A, $A_1$, $A_2$를 저장한다.

### 3.8 예치단계

사용자가 지불한 전자화폐 EC를 예치하기 위해 상점은 거래내역 T를 은행에 전송한다. 은행은 T로부터 전자화폐 및 전자면허의 유효성을 확인하고 은행의 DB를 이용하여 이중 사용 여부를 확인한다.

$$T=\{EC, (s, c), A_1, g_1, g_2, g_3, p\}$$

## 4. 제안방식의 고찰

### 4.1 이중사용방지

본 논문에서는 사용자와 신뢰기관 사이의 거래내역을 체크할 수 있는 카운터 $Cnt_{C,T}$와 사용자와 은행 사이의 거래내역을 체크할 수 있는 카운터 $Cnt_{C,B}$는 거래시 항상 증가한다. 따라서 만약 이중 사용이 발생되면 이 카운터들이 불균형을 이루어지므로 이중사용 여부를 알 수 있다.

### 4.2 익명성 제어

가. 동전 추적

동전 추적 기능을 통해 신뢰기관은 법원의 명령으로 사용자가 전자화폐를 사용하기 전에 은행에 추적 기능을 부여 할 수가 있다. 즉, 인출 단계에서 사용자가 은행에 전송한 인출 사본 중 $A'_1$으로부터 추적기관은 $A_1$을 생성하고 이를 은행에 재 전송해 줌으로써 은행측에서는 이를 통해 화폐를 추적한다. 즉, 해당 화폐를 블랙리스트에 올림으로서 상점측에서 인수를 거부하도록 할 수도 있으며, 사용화폐와 인출화폐를 연결함으로써 화폐를 추적할 수가 있다. 화폐 발행 단계에서는 다음 과정을 수행시킴으로서 동전추적 기능을 제공한다.

step 1 : 은행은 사용자가 제시한 인출 사본 중 $A'_1$을 신뢰기관에게 제공한다.

step 2 : 신뢰기관은 $A'_1$로부터 $A_1$을 계산해낸다.

$$(A'_1)^{x_T^{-1}} \equiv (y_T^w)^{X_T^{-1}} \equiv g_2^{X_T \cdot w \cdot X_T^{-1}} \equiv g_2^w \equiv A_1$$

step 3 : 신뢰기관은 $A_1$을 은행에게 전송한다.

이때 은행은 신뢰기관이 전송해 준 $A_1$을 사용자가 생성하여 지불 단계에서 상점에 제공하는 $A_1$과 연결시킴으로서 물품을 구입하기 전에 지불의 적법성과 상관없이 추적 기능을 제공한다.

나. 사용자 추적

신뢰기관은 개인계좌와 익명계좌사이의 관계를 알고 있다. 따라서 법원의 요청이 있을 때 사용자 추적을 할 수 있다.

step1:은행은 익명계좌 $A_A$를 신뢰기관에 전송한다.

step2:신뢰기관은 익명계좌로부터 개인계좌를 계산해낸다.

$$(A_A)^{x_A} = [(P_A)^{x_A^{-1}}]^{x_A} = P_A$$

step3:신뢰기관은 개인계좌( $P_A$)를 은행에게 전송한다.

따라서 은행은 개인계좌를 통하여 사용자를 추적할 수 있다.

## 5. 결론

전자화폐에 있어서 완전한 익명성을 제공함으로써 세금 포탈, 돈 세탁, 범죄에 이용될 가능성이 많았다. 하지만 이러한 문제점을 해결하기 위해 현재는 익명성을 선택적으로 제거할 수 있는 익명성 제어에 많은 연구가 진행중이다. 이에 본 고는 기존에 사용자 추적만이 가능한 방식에 동전 추적기능을 추가함으로써 좀더 낳은 방식을 제안하였다. 동시에 익명계좌생성시 본 방식을 IC카드에 수용함으로써 더욱 효율적으로 사용 가능할 수 있으리라 판단된다.

요즘 급속한 인터넷에 발전으로 전자상거래가 활기를 띠고 있다. 전자상거래에서 가장 중요한 전자화폐 시스템이 보다 실용적이고 효율적인 연구가 계속 되기를 바란다.

## [참고문헌]


[1] T.Okamoto and K.Ohta, "Universal Electronic Cash", In Advances in Cryptology, Crypto'91, pp324-337, 1991

[2] D.Chaum, "Blind Signatures for untraceable payments" Advances in Cryptography, Crypto'82, pp199-203, 1983

[3] B,von Solms and D. Naccache, "Oh blind signatures and perfect crimes", Computers and Security, pp581-583, 1992

[4] E.F.Brickell, P.Gemmell, and D.Kravitz, "Trustee-based tracing extension to anonymous cash and the making of anonymous change", In Symposium On Distributed Algorithms(SODA), Albuquerque, NM.1995

[5] M.Stadler, J.M.Piveteau, and J.Camenisch, "Fair blind signatures", In Advances in Cryptology, Proc, of Eurocryupto '95, pp209-219, 1995

[6] Y. Tsiounis, Y. Frankel, and M. Yung, "Indirect Discourse Proofs: Achieving Fair Off-Line Electronic Cash," Asiacrypt '96, Lecture Notes in Computer Science 1163, pages 286-300, 1996

[7] J. Camenisch, J.-M. Piveteau, and M. Stadlerr, "An Efficient Fair Payment System," Proceedings of 3rd ACM Conference on Computer Communications Security, ACM press, March 1996, pp. 88-94.

[8] ] M. Jakobsson and M. Yung, "Revokable and versatile electronic money," 3rd ACM Conference on Computer and Communications Security, pp. 76-87, 1996

[9] 오형근, 이임영, "익명성 제어 기능을 가지는 전자화폐 프로토콜에 관한 연구", 한국통신 정보보호학회 종합학술발표회 논문집 Vol 8. No 1. pp 109-121, 1998