# VSS와 은닉서명에 기반한 공정한 추적 방식

김병곤, 김광조

한국정보통신대학원대학교, 국제정보보호기술연구소

# Fair Tracing based on VSS and Blind Signature

Byeong-Gon Kim and Kwangjo Kim

International Research center for Information Security(IRIS),

Information and Communications Univ.(ICU), Korea

## 요 약

전자현금에 대한 암호학적 요구사항 중의 하나가 추적성이다. 전자 현금에 대한 무조건적인 익명성은 돈 세탁, 협박등의 완전범죄가 가능하게 하며, 반대로 익명성이 보장되지 않는다면 전자현금 사용에 따른 사생활 보호 문제가 대두되게 된다. 이를 해결하고자 등장한 것이 합법적인 추적성을 보장하는 공정한 추적 방식 이며, 본 논문에서는 제3의 신뢰기관, 은닉서명, VSS(verifiable secre sharing)을 결합한 새로운 공정한 추적 방식을 제안한다.

## I. 서 론

전자상거래가 활성화됨에 따라 전자 현금에 대한 필요성 및 수요가 증가하고 있다. 전자 현금은 고객이 은행에서 전자현금을 인출하여, 오프라인으로 상인에게 지불하고, 상인은 해당 현금을 은행에 예치한다. 고객의 프라이버시를 위한 익명성은 은닉서명을 통하여 해결할 수 있으나, 무조건적인 익명성은 돈세탁, 협박, 강도 등 완전 범죄에 이용될 수 있다.

이런 익명성 문제 때문에 취소 가능한 익명성 방식이 개발되었다[1]. 여기에는 인출된 돈이 예치되었는가를 알아내는 코인 추적과 지금 예치되는 돈의 인출자가 누구인지를 추적하는 소유자 추적 메커니즘이 있다. 이러한 추적 기능은 현실의 현금에서는 없는 전자현금의 장점이나 여기에도 공정한 추적에 대한 문제가 남아 있다. 즉, 어떻게 합법적인 추적을 가능하게 하고 불법 추적을 못하게 할 것인가 하는 문제이다.

합법적인 추적이란 판사나 인출자에 의해서 추적이 허락된 경우를 말하며, 공정한 추적이란 합법적인 추적이 항상 가능하고, 불법적인 추적이 금지되는 경우를 말한다. Kügler 와 Vogt는 은행이 제3의 신뢰기관(TTP) 없이 공정한 추적이 가능하도록 새로운 메커니즘(KV방식)을 제안하였다[2]. 이 인출 기준의 메커니즘은 *'optimistic fair tracing'* 이라고 불렀는데 그 이유는, 돈이 추적될지 여부는 인출시에 결정해야 하며, 불법 추적을 막지 못한다는 점이다. 그러나 불법 추적은 인출자 또는 추적자가 사후에 밝혀낼 수 있으며, 판사에게 증명할 수 있으므로 불법으로 추적한 은행은 기소될 수 있다.

그러나, 본 논문에서는 불법 추적이 아예 불가능한 진정한 의미의 인출 기준 공정한 추적을 제안하며 KV방식에 비해 계산 복잡도도 줄어들었다. 그러나 이것은 TTP를 도입함으로써 달성되었다.

## II. 기본 요소

### 1. KV방식[2]

Kügler 와 Vogt가 제안한 인출되는 코인에 표시하는 메커니즘은 Okamoto-Schnorr 은닉서명[3]과 Chaum-van Antwerpen undeniable

signature[4]를 결합하여 만들어졌다.

1) 기호

$p,q$ : $q|(p-1)$을 만족하는 큰 소수

$g_1,g_2,g_3$ : 위수 $q$의 $Z_p^*$ 원소

$(s_1,s_2) \in_R Z_q$ : 은행의 은닉 서명용 개인키

$v = g_1^{s1} g_2^{s2} \bmod p$ :은행의 은닉 서명용 공개키

$x \in_R Z_q$ : 은행의 부인방지서명용 개인키

$y = g_3^x \bmod p$ :은행의 부인방지서명용 공개키

2) 프로토콜

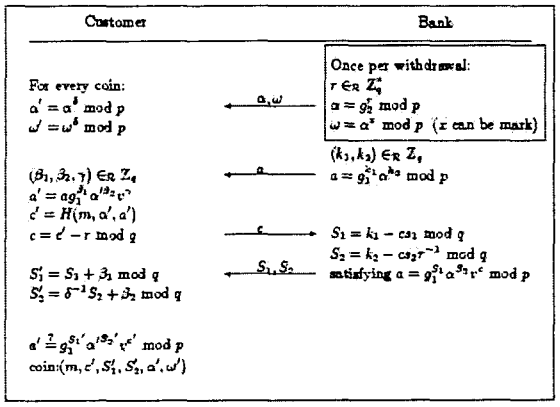


그림1 : KV방식

3) 추적능력

만일 은행이 마킹된 코인을 발행하기로 결정 했다면 단순히 랜덤한 부인방지 서명용 개인키 $x$ 대신에 $x_M$을 선택하여 사용하고 저장해 두면 된다. 그후 코인이 사용되어 은행에 예치될 때 그런 마킹이 검출될 것이다. 이때 은행은 모든 저장된 마킹키 $x_M$에 대하여 $\omega' = ? \alpha^{x_M} \bmod p$ 인지를 검사한다.

만일 고객이 그의 코인이 추적되었는지 여부를 체크하려면 부가적인 정보 $Sig_{bank}$ = $(a,\omega,$ $customerID,$ $coin\ generation)$ 이 필요하다.

4) 약점

이 KV방식의 약점은 합법적인 코인 추적을 위하여 많은 부가적인 정보가 필요하다는 점이다. 왜냐하면 마킹은 판사에 의해 인증 받아야 되고, 은행은 마킹키와 그것에 대한 판사의 서명을 저장해야 한다. 합법적인 추적인지 확인하는 단계에서 은행은 모든 마킹키와 판사의 서명을 공개해야 한다.

또 다른 단점은 코인의 마킹 여부를 체크하는데 많은 컴퓨팅 파워가 필요하다는 점이다. 왜냐하면 고객은 $\omega' = a^{x'} \bmod p$인 점을 이용하여 모든 $x$, $x_M$을 x'과 비교해야 한다. 만일 모든 $x$, $x_M$ 중에서 찾지 못했다면 그 코인은 불법적으로 추적되었다고 주장할 수 있다.

## 2. VSS(Verifiable Secret Sharing)

Feldman은 비 대화형 검증 가능한 비밀 공유 방식을 제안하였고 많은 변형들이 제안되었다. 본 논문에서는 그 중 단순한 한가지를 사용하였다 [5].

1) 기호

$s$ : secret value,

$k$ : threshold

$j$ =(1..n) : 비밀 공유할 사용자

2) 방식

분배자 : random polynomial $f(x) = s + a_1x + a_2x^2 + ... + a_{k-1}x^{k-1} \bmod q$를 선택.

분배자 : 각 사용자 $j$에게 $f(j)$를 배포.

분배자 : $q|(p-1)$을 만족하는 큰 소수 p와 위수 $q$의 $Z_p^*$ 원소에서 랜덤하게 생성자 g를 선택한다. $c_0=g^s \bmod p$, $c_1=g^{a1} \bmod p$,..,$c_{k-1}=g^{ak-1} \bmod p$ 등을 계산.

분배자 : $p,g,c_0,c_1,...c_{k-1}$을 모든 j에게 배포

사용자 $j$ : 비밀이 적절하게 배포되었는지 체크 가능하다. 왜냐하면,

$$g^{f(j)} = ? \ c_0 c_1^{j} c_2^{j^2} \cdots c_{k-1}^{j^{k-1}}$$

$$= g^s g^{a_1 j} g^{a_2 j^2} \cdots g^{a_{k-1} j^{k-1}}$$

$$= g^{s + a_1 j + a_2 j^2 + \cdots + a_{k-1} j^{k-1}}$$

$$= g^{f(j)}$$

사용자 $j$ : 일반적인 비밀 공유 방식에 쓰이는 Lagrange 보간법을 이용하여 비밀값 s 복구 가능.

# III. 제안 방식

## 1. 특징

본 논문에서 제안하는 방식에서는 TTP (Trusted Third Party)를 채택하여 TTP가 마크 x와 부인방지 서명 $\omega = \alpha^x \bmod p$ 를 만든다. 마크 x는 비밀값으로서 은행과 고객간에 VSS를 이용하여 공유된다. 따라서 은행 혼자서는 코인을 추적할 수 없으며 이것은 불법 추적이 아예 불가능함을 의미한다. 그러나 TTP, 은행, 고객 세 주체 중 두 주체가 협동하면 VSS 방식에 따라 비밀값을 알아낼 수 있고, 이것은 언제나 합법적인 추적이 가능함을 의미한다.

부인방지 서명을 드러내거나 수정하는 것은 Okamoto-Schnorr 은닉서명에 영향을 미치지 아니하므로 x가 은행에 의해 주어지지 아니하였다 하여도 코인의 신뢰성은 은행의 은닉서명에 의해 유지 된다.

## 2. Protocol

1) 기호

$p,q$ : $q|(p-1)$을 만족하는 큰 소수

$g_1,g_2$ : 위수 $q$의 $Z_p^*$ 원소인 생성자

$(s_1,s_2) \in_R Z_q$ : 은행의 은닉 서명용 개인키

$\upsilon = g_1^{s1} g_2^{s2} \bmod p$ :은행의 은닉 서명용 공개키

$x \in_R Z_q$ : 비밀 마크

2) 초기단계

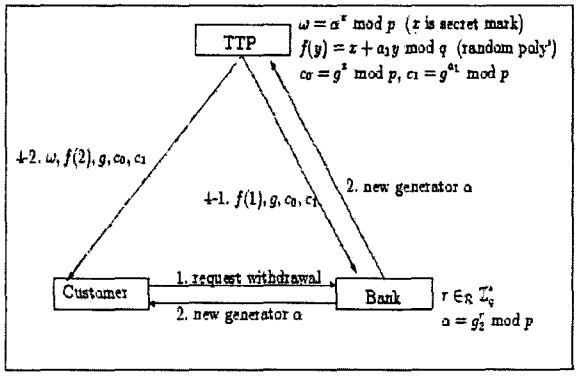


그림2 : 초기단계

step1. 고객이 은행에게 코인 인출 요청

step2. 은행은 난수 $r$을 $Z_q^*$에서 고르고 새로운 무작위 생성자 $\alpha = g_2^r \bmod p$를 계산하여 TTP와 Customer에게 전달.

step3. TTP 는 임의의 다항식 $f(y)=x+a_1y \bmod q$ 를 선택하고, $c_0=g^x \bmod p$, $c_1=g^{a1} \bmod p$를 계산한다.

step4. TTP는 $f(1),g,c_0,c_1$ 을 은행에게 보내고, $\omega = \alpha^x \bmod p$, $f(2)$, $g$, $c_0$, $c_1$을 고객에게 보낸다.

step5. 마크 $x$는 VSS에 따라 $f(1),f(2)$를 이용하여 복구 가능하며, $\alpha$와$\omega$는 KV방식과 동일하게 고객에게 주어진다.

3) 인출단계

이 단계에서는 KV방식과 거의 유사하다. 다시 말해서 변형된 Okamoto-Schnorr 은닉 서명이 적용되었다.

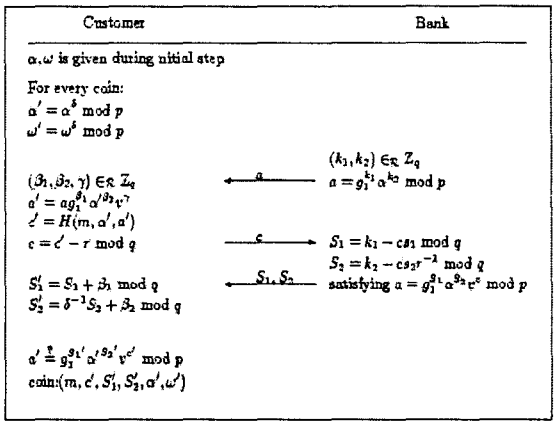


그림3 : 인출단계

step1. 고객은 $Z_q^*$상에서 난수δ를 고르고 $\alpha' = \alpha^\delta \bmod p$, $\omega' = \omega^\delta \bmod p$를 계산한다.

step2. 은행은 $Z_q$상에서 난수$(k_1,k_2)$를 고르고 $\alpha = g_1^{k_1} \alpha^{k_2} \bmod p$ 를 계산하여 고객에게 전달한다.

step3. 고객은 $Z_q$상에서 난수$(\beta_1,\beta_2,\gamma)$를 고르고, $\alpha' = \alpha\, g_1^{\beta_1} \alpha'^{\beta_2} \upsilon^\gamma \bmod p$ 및 $c'=H(m,\alpha',\alpha')$을 계산하고 $c = c'-r \bmod q$를 은행에게 전달한다.

step4. 은행은 $S_1=k_1-cs_1 \bmod q$, $S_2=k_2-cs_2r^{-1} \bmod q$를 계산하여 고객에게 전달한다. 이 계산은

$a = g_1^{S_1} a^{S_2} v^c \bmod p$ 관계를 만족한다.

step5. 고객은 $S_1' = S_1 + \beta_1 \bmod q$, $S_2' = \delta^{-1} S_2 + \beta_2 \bmod q$를 계산한다.

step6. 누구나 $a'$과 $g_1^{s_1'} a'^{s_2'} v^{c'} \bmod p$를 비교함으로써 은닉서명을 검증 가능하다.

코인 : $(m, c', S_1', S_2', a', \omega')$

3) 검증단계

이 단계의 목적은 코인이 추적되었는지, 합법적인 추적인지, 비밀 공유가 잘 되었는지 판단하는 것이다.

만일 고객이 협박에 의한 인출 때문에 코인 추적을 은행에 요청한다면 은행과 고객은 $f(1), f(2)$를 서로 공개함으로써 비밀값 x를 추출할 수 있다.

$f(1) = x + a_1$, $f(2) = x + 2a_1$

예치되는 코인들에서 $w' = a^{\alpha} \bmod p$를 체크한다. 고객은 의심스러우면 VSS를 이용하여 x값의 진실성을 체크할 수 있다.

$$g^{g(2)} = ?\ c_0\ c_1^2 = g^x g^{2a_1} = g^{x+2a_1}$$

## IV. 비교 분석

본 논문에서 제안된 프로토콜은 KV방식과 비교하여 계산 및 데이터 저장소 측면에서 훨씬 효율적이다. 만일 중간 규모의 은행 고객이 백만명이고, 각 고객 당 약 천개의 코인을 인출하고, 고객의 1%가 의심스러운 고객이라 할지라도, 저장해야할 코인과 마킹 정보는 엄청나다($10^9$ 코인, $10^7$ 마크).

또한 추적의 적법성을 체크하기 위하여 기존의 프로토콜은 매 코인마다 비교 연산을 $10^9$번 수행하게 된다. 따라서 제안된 프로토콜은 이러한 비교에서 약 $10^9$배 효율적이다.

그리고 필요한 추가정보도 거의 비슷하거나 오히려 작다. 왜냐하면 기존 프로토콜에서는 마킹키에 대한 판사의 서명이 필요하기 때문이다.

무엇보다도 가장 큰 장점은 제안된 프로토콜이 낙관적인 공정한 추적이 아닌 완벽한 공정 추적을 지원한다는 점이다.

## V. 결론

전자현금 시스템에서의 공정한 추적은 중요한 요구사항임에도 불구하고 현실화된 뛰어난 프로토콜은 거의 없다. 왜냐하면 전자현금 프로토콜을 현실화 하는데는 이 외에도 많은 요구사항이 있기 때문이며, 모든 요구사항을 만족하는 적절한 프로토콜을 설계하기가 쉽지 않기 때문이다.

본 논문에서는 TTP를 가정하지 않는 기존 프로토콜 보다는 TTP를 가정함으로써 더 현실적이고 가벼운 프로토콜이 설계될 수 있음을 보였다. 이것은 현금의 분할, off-line 이체 등 다양한 전자현금 요구사항을 모두 고려한 현실적인 전자현금 프로토콜 구현을 위한 하나의 방편으로서 고려해 볼 수 있을 것이다.

## 참고문헌


[1] G. Davida, Y. Frankel, Y. Tsiounis, and M. Yung. *Anonymity control in e-cash systems*, In Financial Cryptography - FC97, LNCS Vol.1318, pp.1-16. Springer-Verlag, 1997.

[2] D. Kügler and H. Vogt. *Fair tracing without trustees*. In Financial Cryptography -FC2001, LNCS Vol.2339, pp.136, Preproceedings, 2001.

[3] T.Okamoto, *Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes* , Advances in Cryptology-Crypto 92, LNCS Vol.740, pp.31 53, Springer-Verlag,1992.

[4] D.Chaum. *Zero-knowledge undeniable signatures*. Advances in Cryptology - EUROCRYPT 90, LNCS Vol. 473, pp.458-464. Springer-Verlag, 1990.

[5] T.Okamoto, H. Yamamoto, *Modern cryptography*, pp.227, Life & Power press, 1997.