VSS를 이용한 신뢰기관 없는 공정한 추적 방식

김병곤, 김광조

한국정보통신대학원대학교 국제정보보호기술연구소

Fair Tracing based on VSS without trustees

ByeongGon Kim and Kwangjo Kim

International Research center for Information Security(IRIS)

Information and Communications Univ.(ICU)

요 약

우리는 전자화폐의 공정한 추적을 보장할 뿐 만 아니라 계산적으로 비교 연산이 작은 새로운 추적 방식을 제안한다. 다른 많은 추적 방식들이 제3의 신뢰기관을 도입하거나 또는 나중에 불법 추적을 발견하는 방식인데 비하여, 본 방식은 불법 추적이 은행 혼자서는 원천적으로 불가능한 방법으로써 은닉서명과 VSS (verifiable secret sharing)를 결합하여 사용하며, 거래과정에 상인이 개입한다. 이러한 공정한 추적 방식은 무조건적 익명성으로 인한 협박, 납치, 돈세탁 등의 완전 범죄를 막는 역할을 할 수 있다.

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 전자현금 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 낙관적 견해의 공정한 추적(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 불가능한 진정한 의미의 공정한 추적 방식을 제안하며 KV 방식에 비해 계산 복잡도도 줄어들었다.

II. 기본 요소

1. KV방식[2]

Kügler 와 Vogt가 제안한 인출되는 전자현금에 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 q를 갖는 Z_p^* 상의 원소

$(s_1,s_2) \in_R Z_q$: 은행의 은닉 서명용 개인키

$v = g_1^{s1}g_2^{s2}(mod\ p)$:은행의 은닉서명용 공개키

$x \in_R Z_q$: 은행의 부인방지서명용 개인키

$y = g_3^x(mod\ p)$:은행의 부인방지서명용 공개키

2) 프로토콜

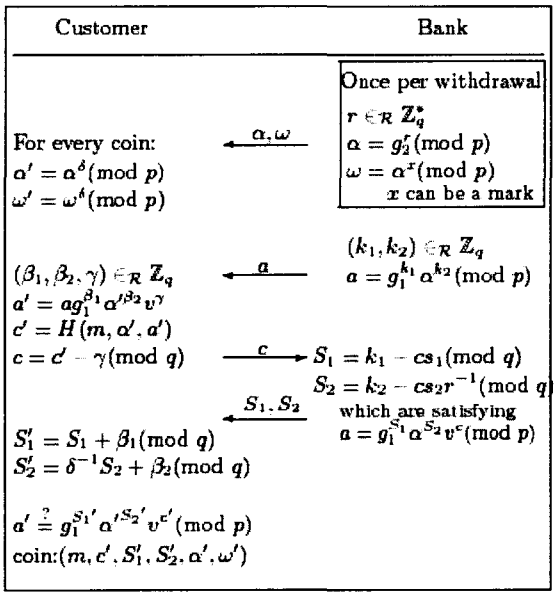

그림 1 : KV방식

3) 추적능력

만일 은행이 표식된 전자현금을 발행하기로 결정했다면 단순히 부인방지서명용 개인키 x 대신에 x_M을 선택하여 사용하고 저장해 두면 된다. 그 후 전자현금이 사용되어 은행에 예치될 때 그런 표식이 검출될 것이다. 이때 은행은 모든 저장된 표식용 키 x_M에 대하여 $\omega' = ?\ \alpha'^{x_M} (\mathrm{mod}\, p)$ 인지를 검사한다.

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

4) 단점

KV방식의 단점은 합법적인 전자현금 추적을 위하여 많은 부가적인 정보가 필요하다는 점이다. 왜냐하면 표식은 판사에 의해 인증 받아야 되고, 은행은 표식용 키와 그것에 대한 판사의 서명을 저장해야 한다. 합법적인 추적인지 확인하는 단계에서 은행은 모든 표식용 키와 판사의 서명을 공개해야 한다.

또 다른 단점은 전자현금의 표식 여부를 체크하는데 많은 컴퓨팅 파워가 필요하다는 점이다. 왜냐하면 고객은 $\omega' = a'^{x_M}(mod\ p)$인 점을 이용하여 모든 x, x_M을 x'과 비교해야 한다. 만일 모든 x, x_M 중에서 찾지 못했다면 그 전자현금은 불법적으로 추적되었다고 주장할 수 있다.

2. VSS(Verifiable Secret Sharing)

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

1) 기호

s : 비밀값

k : 문턱값

j : 비밀을 공유하는 사용자들 (1,...,n)

p,q : $q|(p-1)$을 만족하는 큰 소수

g : 위수 q의 Z_p^* 원소인 랜덤 생성자

2) 방식

분배자 : 임의의 다항식 $f(x) = s + a_1x + a_2x^2 + ... + a_{k-1}x^{k-1}\ (mod\ q)$를 선택한다.

분배자 : 각 사용자 j에게 $f(j)$를 배포한다.

분배자 : $c_0 = g^s\ (mod\ p)$, $c_1 = g^{a1}(mod\ p)$, ..., $c_{k-1} = g^{ak-1}(mod\ p)$ 등을 계산한다.

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

사용자 : 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 : Lagrange 보간법을 이용하여 비밀값 s의 복구가 가능하다.

III. 제안 방식

1. 주요개념

KV방식에서는 고객과 은행만이 주요 참여자였다. 그리고 기 제안된 KK방식[6]에서는 TTP (Trusted Third Party)를 채택하여 TTP가 비밀표식 x와 부인방지 서명 $\omega = \alpha^x (\mathrm{mod}\, p)$ 를 만들어 배포하였고, 이를 통하여 완전한 공정 추적을 보장하였다. 그러나 이는 TTP를 가정하여 이루어진 것이므로 기존의 KV방식보다 우월하다고 볼 수 없다.

본 논문에서 제안하는 방식에서는 TTP대신에 전자화폐의 유통 주체중 하나인 상인이 개입한다. 또한 비밀 표식은 고객이 만들어 VSS를 이용하여 배포함으로써 은행 독자적인 불법 추적을 방지한다. 즉, 은행은 고객이 만들어준 비밀값을 알지 못하나 VSS를 이용하여 그 값이 허위가 아님을 체크할 수 있다. 나중에 고객이 상인과 거래시 동전과 더불어 동일한 비밀값을 VSS를 이용하여 배포하여야 한다.

합법적인 추적을 위해서 두 주체가 협동하여 공유된 비밀값을 알아냄으로써 추적이 가능하다. 즉 고객의 요청에 의한 추적, 법원의 허락하에 은행과 상인이 협조하여 고객의 범죄를 예방하기 위한 추적등이 가능하다. 상인이 은행의 불법 요청에 응할 아무런 이유나 이득이 없는 반면에 법원의 명령에 의해서는 협조가 가능하므로 이는 낙관적인 견해의 공정한 추적보다는 더 공정하다고 볼 수 있다.

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

2. Protocol

1) 기호

p,q : $q|(p-1)$을 만족하는 큰 소수

g_1,g_2 : 위수 q의 Z_p^* 원소인 생성자

$(s_1,s_2) \in_R Z_q$: 은행의 은닉 서명용 개인키

$v = g_1^{s1} g_2^{s2} (mod\ p)$:은행의 은닉서명용 공개키

$x \in_R Z_q$: 비밀 표식

2) 초기단계

이 단계에서는 고객이 비밀 표식을 만들고 분배

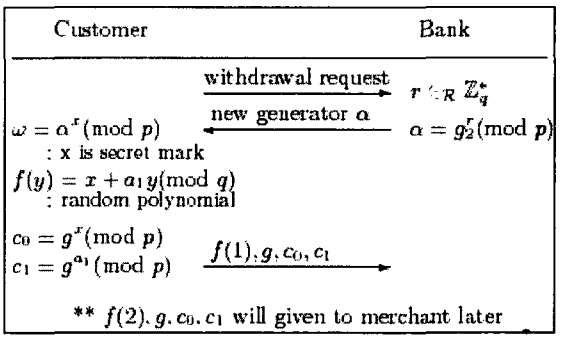

그림 2 : 초기단계

한다.

step1. 고객이 은행에게 전자현금 인출을 요청한다.

step2. 은행은 난수 r을 골라 새로운 생성자 $\alpha = g_2^r (\mathrm{mod}\, p)$를 계산하여 고객에게 전달한다.

step3. 고객은 난수 x를 비밀 표식으로 정하고, $\omega = \alpha^x (\mathrm{mod}\, p)$를 계산한다.

step4. 고객은 임의의 다항식

$f(y) = x + a_1 y (\mathrm{mod}\, q)$

를 선택하고, $c_0 = g^x (\mathrm{mod}\, p)$,

$c_1 = g^{a_1} (\mathrm{mod}\, p)$를 계산한다.

step5. 고객은 $f(1), g, c_0, c_1$ 을 은행에게 보낸다.

step6. 고객은 $f(2), g, c_0, c_1$ 을 향후 거래시 상인에게 보낸다.

step7. 표식 x는 VSS에 따라 $f(1), f(2)$를 이용하여 복구 가능하며, 은행은 x를 모른다. a와 ω는 KV방식과 동일하게 고객에게 주어진다.

3) 인출단계

이 단계에서는 KV방식과 거의 유사하다. 다시 말해서 변형된 Okamoto-Schnorr 은닉 서명이 적용되었으며, 전자현금의 형태와 각 변수들간의 관계식은 동일하다.

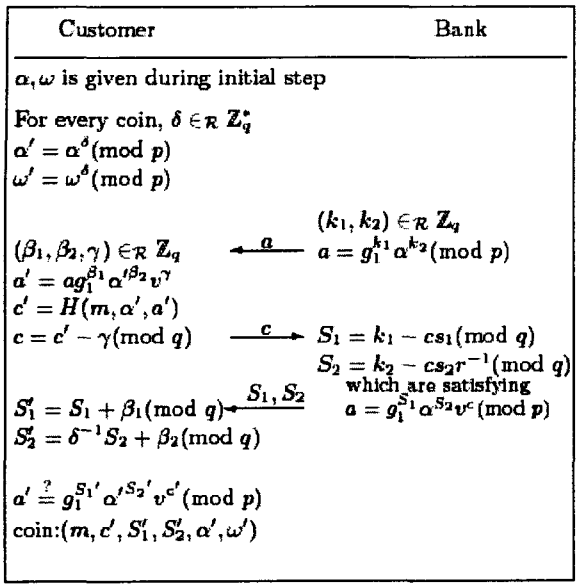

그림 3 : 인출단계

step1. 모든 전자현금에 대하여, 고객은 난수 δ를 고르고 $\alpha' = \alpha^{\delta} (\mathrm{mod}\, p)$, $\omega' = \omega^{\delta} (\mathrm{mod}\, p)$를 계산한다.

step2. 은행은 난수(k_1,k_2)를 고르고, $a = g_1^{k_1} \alpha^{k_2} (\mathrm{mod}\, p)$ 를 계산하여 고객에게 전달한다.

step3. 고객은 난수(β_1,β_2,γ)를 고르고, $a' = a\, g_1^{\beta_1} \alpha'^{\beta_2} v^{\gamma} (\mathrm{mod}\, p)$ 및 $c'=H(m,a',a')$을 계산하고 $c = c'-\gamma \pmod q$를 은행에게 전달한다.

step4. 은행은 $S_1 = k_1-cs_1 \pmod q$, $S_2 = k_2-cs_2r^{-1} \pmod q$를 계산하여 고객에게 전달한다. 이 계산은 $a = g_1^{S_1} \alpha^{S_2} v^{c} (\mathrm{mod}\, p)$ 관계를 만족한다.

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

step6. 누구나 a'과 $g_1^{S_1'} \alpha'^{S_2'} v^{c'} (\mathrm{mod}\, p)$ 를 비교함으로써 은닉서명의 검증이 가능하다.

전자현금 : $(m,c',S_1',S_2',a',\omega')$

4) 지불, 예치 및 검증 단계

고객이 상인에게 돈을 지불할 때 $f(2)$, g, c_0, c_1 도 전달해야 한다. 그때 상인은 공유된 비밀값의 진실성을 아래 수식으로 체크할 수 있다.

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

상인이 받은 전자현금을 은행에 예치할 때 추적 메커니즘이 작동될 수 있다. 은행이 비밀값 x를 안다면 예치되는 전자현금들에서 $w'=a^{\alpha} \pmod p$를 체크한다.

고객이 범죄자로부터 협박을 받아 돈을 범죄자에게 주었다면, 고객은 은행에게 비밀값 x를 알려주어 추적을 요청할 수 있다. 또한 고객의 범죄가 의심스러운 경우 소유자 추적을 위하여, 은행과 상인은 판사의 허락하에 고객의 비밀값 x를 드러낼 수 있다.

IV. 장단점 분석

1) 추적성 및 계산량 비교

본 논문에서 제안된 방식의 가장 큰 장점은 공정한 추적을 완벽하게 지원한다는 점이다. 왜냐하면 은행 혼자서는 비밀 표식을 알 수 없기 때문에 혼자서는 추적 자체가 불가능하다.

또한 계산 및 데이터 저장소 측면에서 훨씬 효율적이다. 만일 중간 규모의 은행 고객이 백만명이고, 각 고객 당 약 천개의 전자현금을 인출하고, 고객의 1%가 의심스러운 고객이라 할지라도, 10^9개의 전자현금이 발행되고, 10^9개의 키 리스트가 저장되어야 하며, 10^7개의 표식 정보가 저장되어야 한다. 그러나 제안된 방식에서는 표식 정보가 저장되지 않는다. 또한 추적의 적법성을 체크하기 위하여 기존의 프로토콜은 매 전자현금마다 비교연산을 10^9번 수행하게 된다. 따라서 제안된 프로토콜은 이러한 비교에서 약 10^9배 효율적이다.

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

2) 변형 가능성

제안된 방식에서 비밀 표식을 생성하고 이를 분배하는 작업은 고객이 담당하지만, 전자화폐의 다른 프로토콜과 결합하여 여러 가지 요구사항을 충족시키고자 할 때 융통성 있게 작업의 전가가 가능하다.

즉, 초기단계에서 비밀 표식 x를 생성하고, 임의

의 다항식을 선택하고, 값을 분배하는 과정은 TTP가 담당할 수 있다[6]. 이때 상인에게 나중에 분배되던 값들은 초기단계에서 은행과 고객에게 주어진다.

또는 TTP대신에 제3의 금융기관이나 현재 거래하는 은행과 이해 관계가 얽혀있지 않은 제3자나 정부기관 등이 담당할 수 있다. 그리고 3개의 기관으로도 비밀값의 은닉을 보장받을 수 없을 때, VSS의 특성에 따라 그 이상의 객체들을 프로토콜에 개입시킬 수 있다. 이때에도 전자현금의 신뢰성은 Okamoto-Schnorr 은닉서명에 의해 유지된다.

V. 결론

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

본 논문에서는 TTP를 가정하지 않고, 거래의 세 주체를 모두 고려함으로써, 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.

[6] 김병곤, 김광조, *VSS와 은닉서명에 기반한 공정한 추적 방식*, CISC2003 하계정보보호학술대회논문집, Vol.13, No.1, pp.53-56, Proceedings, 2003