비밀분산법을 이용한 익명성 보장 핑거프린팅 기법
(Anonymous Fingerprinting Method using the Secret Sharing Scheme)

용 승 림 † 이 상 호 ††
(Seung-Lim Yong) (Sang-Ho Lee)

요 약 디지털 형식으로 저장되어 있는 데이타의 불법적인 복사와 재분배는 전자상거래 상에서 데이타를 판매하는 상점에게 매우 큰 문제가 된다. 핑거프린팅 기법은 암호학적인 기법들을 이용하여 디지털 데이타를 불법적으로 재배포한 사용자를 찾아냄으로써 디지털 데이타의 저작권을 보호한다. 익명성이 보장되는 핑거프린팅 기법은 대칭적인 기법과 달리 사용자만이 핑거프린트가 삽입된 데이타를 알 수 있고 비대칭 기법과 달리 데이타가 재배포되기 전에는 사용자의 익명성이 보장되는 기법이다.

본 논문에서는 비밀분산법을 이용한 익명성이 보장되는 새로운 핑거프린팅 기법을 제안한다. 상점은 이전에 배포되었던 데이타를 찾았을 경우, 데이타로부터 재배포자의 신원정보를 추출하여 재배포자의 배포사실을 증명할 수 있다. 또한 등록시에 Schnorr 서명을 이용하여 고발된 사용자가 범행을 부인할 수 없도록 한다. 제안된 방법은 이산대수문제와 양자간 안전한 계산과정의 안전성에 근거하여 사용자의 익명성이 보장된다.

키워드 : 익명적 핑거프린팅 기법, 비밀분산법, 저작권 보호, 전자서명

Abstract The illegal copying and redistribution of digitally-stored information is a crucial problem to distributors who electronically sell digital data. Fingerprinting scheme is a techniques which supports copyright protection to track redistributors of electronic information using cryptographic techniques. Anonymous fingerprinting schemes, differ from symmetric fingerprinting, prevent the merchant from framing a buyer by making the fingerprinted version known to the buyer only. And the scheme, differ from asymmetric fingerprinting, allows the buyer to purchase goods without revealing her identity to the merchant.

In this paper, a new anonymous fingerprinting scheme based on secret sharing is introduced. The merchant finds a sold version that has been distributed, and then he is able to retrieve a buyer's identity and take her to court. And Schnorr's digital signature prevents the buyer from denying the fact he redistributed. The buyer's anonymity relies on the security of discrete logarithm and secure two-party computations.

Key words : Anonymous fingerprinting, Secret sharing, Copyright protection, Digital signature

1. 서 론

인터넷과 같은 컴퓨터 망과 컴퓨터 이용의 급격한 발달로 전자상거래가 활발해지고 디지털 데이타의 확산 및 보급이 일반화되고 있다. 그러나, 이러한 데이타들은 디지털이라는 속성으로 인하여 누구나 손쉽게 불법적인 복제를 통해서 이들을 획득할 수 있게 되고, 이 때문에 저작권 문제가 야기되고 있다. 따라서 정보기반 전자 상거래에서 디지털 데이타의 저작권 보호는 아주 중요한 문제가 되었다.

핑거프린팅 기법은 디지털 데이타의 저작권을 보호하기 위해 데이타의 복사 자체를 막는 암호학적인 기법이 아니라 암호학적인 기법들을 이용하여 디지털 데이타를 불법적으로 재분배한 사람을 찾아내는 기법이다[1]. 저작권 보호에 관한 규칙을 어기고 데이타를 불법적으로 분배하는 사람을 재배포자(traitor)라 한다. 핑거프린팅 기법은 데이타가 불법적으로 재배포 되었을 때 상점이 그 데이타를 구매한 재배포자를 식별할 수 있게끔 함으로써 디지털 저작권을 보호한다.

† 비 회 원 : 이화여자대학교 컴퓨터학과
dragon@ewha.ac.kr
†† 종신회원 : 이화여자대학교 컴퓨터학과 교수
shlee@ewha.ac.kr
논문접수 : 2003년 5월 19일
심사완료 : 2004년 4월 1일

핑거프린팅 기법은 대칭적인 기법과 비대칭적인 기법, 익명성이 보장되는 비대칭적인 기법의 세 가지 부류로 나뉜다. 대칭적인 기법은 상점이 서로 다른 데이타의 복사본들을 각 사용자에게 나누어주고 데이타가 재배포되었을 경우 그 복사본을 어떤 사람에게 나누어준 것인지를 찾아내어 재배포자를 찾아내는 방법이다[2-4]. 반면 비대칭적인 기법은 핑거프린트가 삽입된 데이타를 알 수 있고 상점은 핑거프린트된 데이타를 알 수 없도록 한다. 그러나 이 기법은 상점이 재배포된 데이타를 찾았을 때 재배포자의 신원을 데이타로부터 찾아내고 제삼자에게 이를 증명할 수 있다. 따라서 상점은 정직한 사용자의 신원도 알아내어 재배포자로 고발할 수 있는 단점이 있다[5]. 익명성이 보장되는 비대칭적인 핑거프린팅 기법은 데이타가 불법적으로 재배포되기 전까지 상점은 핑거프린트된 데이타를 모를 뿐 아니라 사용자가 데이타를 재배포하지 않는 한 사용자의 익명성도 철저히 보장되는 기법이다. 만약 재분배된 데이타가 발견되면 상점은 등록센터의 도움을 받고, 핑거프린트된 데이타에서 사용자 정보를 추출하여 조정자(arbiter)에게 재배포자의 유죄를 입증할 증거로 제시하여 재배포자의 신원을 확인하고 증명할 수 있다[1,6-9].

본 논문에서는 비밀분산법과 Schnorr의 전자서명 기법을 이용한 익명성을 제공하는 핑거프린팅 기법을 제안한다. 비밀분산법을 이용하여 사용자가 데이타를 재배포하기 전까지는 사용자의 익명성을 보장할 수 있으며 전자서명기법을 이용하여 사용자가 재배포자로 증명되었을 때 부인할 수 없다. 또한 기존의 익명성을 제공하는 기법들에 비해 효율적이다.

2. 관련 연구

2.1 핑거프린팅

핑거프린팅은 디지털 컨텐츠의 저작권 보호를 위한 암호학적인 기법으로 디지털 데이타를 불법적으로 재분배한 사람을 찾아내어 불법적 재배포 행위를 막을 수 있다[1]. 일반적으로 핑거프린팅 기법은 대칭 기법, 비대칭 기법 그리고 익명성 보장 비대칭 기법으로 나뉜다. 대칭 기법은 상점이 핑거프린트를 삽입하는 반면, 비대칭 기법과 익명성 보장 비대칭 기법은 상점과 사용자 사이에서의 상호교환 프로토콜에 의하여 핑거프린트를 삽입하게 된다. 따라서 비대칭 기법들은 프로토콜이 수행되는 동안에 사용자가 자신의 비밀 정보를 삽입할 수 있으며 프로토콜이 끝나면 단지 사용자만이 데이타에 삽입된 핑거프린트를 알 수 있다. 익명성 보장 비대칭적 기법은 사용자의 프라이버시를 위하여 삽입된 핑거프린트를 모를 뿐 아니라 사용자가 데이타를 재배포하지 않는 한 사용자의 익명성도 철저히 보장되는 기법이다.

Domingo는 1998년에 양자간 안전한 계산 프로토콜(Secure Two-Party Computation)을 이용하여 사용자의 익명성을 보장하는 핑거프린팅 프로토콜을 설계하였다[10]. 그 후 2000년에 Chung이 Domingo의 방식을 개선하여 프로토콜을 설계하였다[6]. Domingo와 Chung의 방식은 전체적으로 등록, 핑거프린팅, 그리고 식별 프로토콜로 구성된다. 이 방식들은 이산대수 문제의 안전성에 근거하여 안전성이 보장되며 양자간의 안전한 계산 프로토콜에 의하여 사용자의 익명성이 보장된다. 그러나 Domingo의 방식은 등록 프로토콜의 통신회수와 식별 프로토콜에서의 지수 연산 회수, 비교회수가 많은 단점이 있고, 이를 개선한 Chung의 방식은 통신량에서는 Domingo의 방식보다 효율적이나 식별 프로토콜에서 곱셈연산과 비교연산의 회수가 많은 단점이 있다.

2.2 암호학적 기법들

2.2.1 비밀분산법

비밀분산법이란 비밀정보 D를 다수의 비밀조각으로 분할하여 각 참가자들에게 공유시키고 복원 권한을 가진 참가자들의 비밀조각으로부터 복원시킴으로써 원 정보를 안전하게 유지·관리하는 암호 프로토콜이다. 대표적인 비밀분산법으로 Shamir에 의해 제안된 (t, n)-임계치 비밀분산법이 있다[11]. Shamir의 (t, n)-임계치 비밀분산법은 다음과 같다.

비밀정보를 생성·분배하는 분배자는 비밀정보 D를 상수항 $a_0 = D$로 하는 임의의 $t-1$차 다항식 $q(x) = a_0 + a_1x + \ldots a_tx^{t-1}$을 생성하고 비밀조각 $D_i(D_1 = q(x_1), \ldots, D_n = q(x_n))$를 계산하여 각 참가자에게 (x_i, D_i)의 값을 나누어준다. 비밀정보 복원을 위해서는 임의의 t명의 참가자가 자신들의 비밀조각 t개의 값을 이용하여 $q(x)$의 계수의 값들을 보간법을 이용하여 구하고, 다항식에 0을 대입함으로써 비밀정보 $D = q(0)$를 복원한다.

$$q(x) = \sum_{k=1}^{t} D_i \cdot \prod_{i=1, i \neq k}^{t} \frac{(x - x_i)}{(x_k - x_i)}$$

그러나 비밀조각이 $t-1$개만 주어졌을 때는 비밀정보 D를 복원할 수 없다. 이러한 성질을 사용자의 신원을 숨기고, 사용자가 데이타를 재배포할 경우 비밀정보인 아이디를 복원하는데 이용한다.

2.2.2 Schnorr의 전자서명 기법

Schnorr의 전자서명 기법의 안전성은 이산대수 문제의 풀기 어려움에 근거한다. Schnorr 서명을 이용하는 사용자는 임의 난수 g와 두 개의 소수 p, q를 나누어 갖는다. 비밀키, 공개키 쌍을 생성하기 위하여 사용자는 하나의 임의난수 $s(0 < s < q)$를 비밀키로 생성하고, 공개키 $v = g^{-s} \bmod q$를 생성한다. 메시지 m에 서명을 하기 위하여 임의의 수 $r(r \in Z_q)$을 선택하고 다음과 같은 계

산을 수행한다.

$$x = g^r \bmod p,\quad e = h(m|x),\quad y = (r + se) \bmod q$$

함수 $h()$는 충돌 회피 일방향 해쉬함수이다. 메시지 m에 대한 서명은 $\langle e, y\rangle$쌍이 된다. 서명을 확인하기 위하여 $x' = g^y v^e \bmod p$이고 e와 $h(m|x')$가 같은지 확인한다. 확인이 되면 서명은 정당한 것이다[12].

r 값은 다른 메시지에 서명을 생성하기 위하여 반드시 한번만 사용되어야 한다. 만약 하나의 r 값을 두 개의 서로 다른 메시지 m과 m'에 사용하면, 생성된 두 개의 서명값 (c, y)와 (c', y')을 이용하여 비밀값 s를 다음과 같은 식을 이용하여 얻어낼 수 있다.

$$s = \left(\frac{y - y'}{c - c'}\right) \equiv \left(\frac{(r + sc) - (r + sc')}{c - c'}\right) \bmod q$$

전자서명을 이용하여 사용자가 재배포된 데이타에 대하여 부인하는 것을 막을 수 있고 Shnorr 전자서명의 특성으로 인하여 사용자는 서로 다른 데이타에 같은 서명을 붙일 수 없다.

3. 익명성을 보장하는 핑거프린팅 기법의 모델

$item \in \{0,1\}^*$을 몇 개의 비트를 변경하는 방법으로 핑거프린트를 삽입할 수 있는 디지털 데이타라 하자. 핑거프린트가 삽입된 $item'$은 원래의 데이타 $item$과 구별하기 어려워야 하며, 변경된 비트의 위치를 알지 못하는 경우에는 데이타를 못쓰게 만들지 않는 한 변경된 비트를 찾아내어 이를 다시 변경할 수 없다는 "마킹을 위한 가정(marking assumption)"을 따른다[3]. 본 장에서는 익명성을 보장하는 핑거프린팅 프로토콜을 정의하고 핑거프린팅 기법의 안정성에 대하여 정의한다.

정의 1(AF 프로토콜). 익명성을 보장하는 핑거프린팅 프로토콜인 AF 프로토콜은 사용자 B, 상점 M, 등록센터 R, 그리고 조정자 A의 네 구성원으로 구성되어 있다. 핑거프린팅 프로토콜 P는 네 개의 부프로토콜 $P = \{P_{Reg}, P_{Fing}, P_{Iden}, P_{Trial}\}$로 구성된다.

- P_{Reg} : B와 R사이의 확률론적 양자간 프로토콜(probabilistic two-party protocol)이다. B는 R에게 등록을 하고 인증서를 받게 되고 R은 B의 등록레코드를 남긴다.
- P_{Fing}: B와 M사이의 확률론적 양자간 프로토콜이다. B는 M으로부터 데이타를 구매하고 M과 함께 핑거프린트를 생성한다. 프로토콜 수행결과물로 M은 구매내역을 얻고 B는 핑거프린트가 삽입된 데이타를 얻는다.
- P_{Iden} : R과 M사이의 확률론적 양자간 프로토콜이다. 만약 M이 불법적으로 유포된 데이타를 찾게되면 자신의 구매내역을 이용하여 R에게 구매내역에 해당하는 사용자의 등록정보를 요구한다.
- P_{Trial} : M과 A사이의 확률론적 양자간 프로토콜이다. M이 재배포된 데이타로부터 추출한 핑거프린트 정보와 R로부터 받은 사용자의 정보를 A에게 전송하여 재배포자를 추적한다.

이제 AF 프로토콜에 대한 안전성에 대하여 정의한다.

정의 2. 만약 다음의 조건을 만족한다면 프로토콜 $P = \{P_{Reg}, P_{Fing}, P_{Iden}, P_{Trial}\}$는 안전한 AF 프로토콜이다.

1) 정확성(correctness) : 모든 부프로토콜들은 B, M, R, 그리고 A가 정직할 때 언제든지 성공적으로 종료되어야 한다.

2) 익명성 : 재배포된 복사본을 가지게 되는 경우를 제외하고, M은 P_{Fing}이나 P_{Iden}프로토콜을 통하여 사용자의 어떠한 정보도 알아낼 수 없다(M이 R과 공모를 하더라도 재배포된 복사본이 없는 경우는 사용자를 알아낼 수 없다).

3) 무혐의 사용자의 보호(protection of innocent user) : 공모하지 않은 B, M, R은 사용자가 공모에 참여하지 않은 경우 그 사용자가 재배포자라는 것을 증명할 수 있는 정당한 증거를 만들 수 없어야 한다.

정의 3. $item$을 상점만이 가지고 있는 비밀값을 삽입할 수 있는 디지털 데이타라 할 때 $item$에 비밀값 x를 임베딩하고 임베드된 비밀값 x을 추출하는 두 개의 알고리즘은 다음과 같다.

- A_{FING} : 비밀값 x와 $item$을 입력값으로 하여 $item$에 비밀값 x를 임베드하는 알고리즘이다. 알고리즘의 출력값은 비밀값 x가 삽입된 $item'$이 된다.
- A_{EXT} : 비밀값 x가 삽입된 $item'$과 원래의 $item$을 입력값으로 하여 비밀값이 삽입된 $item'$으로부터 비밀값 x를 추출해 내는 알고리즘이다. 알고리즘의 출력값은 비밀값 x가 된다.

위에서 정의한 알고리즘 A_{FING}과 A_{EXT}은 다음의 요구사항들을 만족한다.

1) 정확성 : 모든 $item$과 비밀값 x에 대하여 $x = A_{EXT}(item, item')$이다.

2) 영지식성 : 모든 A_{FING} 알고리즘은 시뮬레이터의 결과값인 $x \in \{0,1\}^*$와 A_{FING} 알고리즘의 뷰를 구별할 수 없는 시뮬레이터가 존재한다.

3) 복원과 공모 회피성 : 사용자가 재배포자가 아닌 경우, 무혐의 사용자를 제외한 사용자들의 공모에 의한 공격으로부터 무혐의 사용자의 어떠한 정보도 재배포된 데이타로부터 추출해 낼 수 있는 다항시간내의 A_{EXT} 알고리즘이 존재하지 않는다.

4. 프로토콜

본 장에서는 익명성을 제공하면서 안전한 핑거프린팅 기법에 대하여 설명한다. 사용자 B는 상점 M으로부터 데이타를 구매하기 전에 R에 등록을 한다. 사용자가 이용하는 Schnorr 서명의 공개키는 공개되어 있다고 가정한다. 본 논문에서 제안하는 핑거프린팅 기법은 등록, 핑거프린팅, 신원확인 및 심리의 4개의 부프로토콜로 구성되어 있다. 각각의 프로토콜은 다음과 같다.

4.1 등록 프로토콜 - P_{Reg}

사용자는 데이타를 구매하기 전에 등록센터에 등록을 한다. 모든 사용자는 Schnorr 전자서명의 공개키와 비밀키 쌍을 가지고 있다. 사용자는 임의난수를 생성하여 Schnorr의 전자서명을 생성하고 서명값을 등록센터에 보낸다. 임의난수 $r'=g^r$의 값은 서명 값으로 이용되고 $x'=g^x$의 값은 사용자의 위탁값으로 이용된다. 이후 등록센터와 사용자는 비밀분산법의 프로토콜을 수행하여 사용자의 비밀정보를 등록센터가 저장하고, 이 정보는 후에 재배포된 데이타가 발견되었을 때 상점의 요청을 받아 재배포자를 찾아내는 정보로 이용된다. 등록에 관한 상세 프로토콜은 다음과 같다.

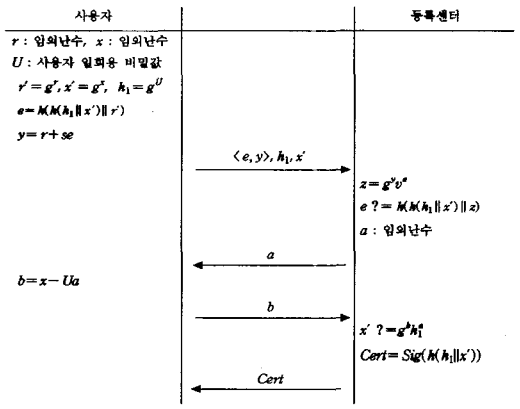

그림 1 등록 프로토콜

1) 사용자는 Schnorr 서명기법을 이용하기 위하여 임의난수 $s(0<s<q)$를 비밀키로, $v=g^{-s} \bmod q$를 공개키로 생성하여 공개키는 공개한다.

2) 사용자는 임의난수 r,x를 선택하여 $r'=g^r$, $x'=g^x$을 계산하고 일회용 비밀값 U를 이용하여 $h_1=g^U$을 계산한다. 임의의 난수 x값은 현재의 거래에 대하여 사용자가 책임이 있음을 나타내는 난수이다. 그리고 r값은 Schnorr 서명기법을 이용하기 위한 임의난수이다.

계산한 h_1, x', r'의 값을 이용하여 $e=h(h(h_1\|x')\|r')$를 계산하고 $y=r+se$을 계산하여 Shnorr의 전자서명 $\langle e,y\rangle$을 생성한다. $\langle e,y\rangle$와 h_1, x'을 등록센터로 보낸다. 사용자는 등록센터에게 영지식 증명을 이용하여 $h_1=g^U$를 만족하는 일회용 비밀값 U를 알고 있음을 증명한다.

3) 등록센터는 사용자로부터 받은 서명값 $\langle e,y\rangle$와 h_1, x'를 이용하여 서명이 올바른지 확인한다. 즉, 사용자의 공개키 v를 이용하여 $z=g^y v^e$ 의 값을 계산하고 사용자로부터 받는 서명값 $\langle e,y\rangle$에 대입하여 서명값과 $h(h(h_1\|x')\|z)$값이 e값과 같으면 서명이 확인되는 것이다.

4) 사용자가 보낸 서명을 확인하고 사용자에게 도전값 a를 보낸다.

5) 사용자는 $b=x-Ua$를 계산하고 응답값 b를 등록센터로 보낸다.

6) 등록센터는 a,b, 받아둔 x'을 이용하여 $x'=g^b h_1^a$ 값이 맞는지 확인하고, 값이 맞는 경우 $Cert=Sig(h(h_1\|x'))$와 같이 서명을 하여 사용자에게 보낸다.

4.2 핑거프린팅 프로토콜 - P_{Fing}

사용자가 상점에서 데이타를 구매할 때 사용자와 상점 사이에서 핑거프린팅 프로토콜이 수행된다. 상점은 비밀분산법을 이용하여 사용자 정보의 일부를 받으며 b''값을 도전값에 대한 블라인드된 응답값으로 받는다. 해쉬함수의 일방향성에 의하여 상점은 도전값에 대한 응답값 b'자체의 값을 알아낼 수는 없고 양자간의 안전한 계산 프로토콜상에서 값이 맞는지의 여부를 확인할 수 있다. 핑거프린트된 데이타를 사용자만이 알고 상점은 어떠한 정보도 알 수 없도록 하기 위하여 양자간의 안전한 계산 프로토콜(secure two-party computation)을 수행한다. 상세한 핑거프린팅 프로토콜은 그림 2와 같다.

1) 상점은 사용자에게 도전값 a'을 보낸다.

2) 사용자는 $b'=x-Ua'$값을 계산하고 $b''=h(b')$을 계산하여 b''과 $Cert$값을 상점에게 보낸다.

3) 상점과 사용자는 동시에 양자간의 안전한 계산과정을 수행한다[4,13]. 사용자는 h_1과 b'을 입력값으로, 상점은 사용자에게서 받은 $Cert$ 값과 b'' 값 그리고 사용자가 구매를 원하는 원래의 데이타 $item$을 입력값으로 입력한다. 그리고 다음의 계산과정을 수행한다.

(a) $ver_1=Verify_1(b', b'')$. b'의 값을 검증하기 위하여 b''의 값을 이용하여 검증을 수행한다. ver_1은 부울변수로서 상점만이 그 값을 볼 수 있으며 $b''=h(b')$인 경우에만 참이 된다.

(b) $ver_2=Verify_2(a', b', h_1, Cert)$. 먼저 $z=g^{b'} h_1^{a'}$ 값

을 계산한다. 계산한 z값을 서명값에 대입하여 $Cert$값과 $h(h_1||z)$의 값이 같으면 검증되는 것이다.

(c) $item' = A_{FING}(item, emb)$. 알고리즘의 수행으로 원래의 데이타 $item$값에 핑거프린트 $emb=(a', b')$가 삽입된 $item'$이 결과값으로 얻어지며 이 값은 사용자만이 볼 수 있는 값이 된다.

위의 양자간의 안전한 계산과정 모두는 상점이 먼저 결과값을 얻어내어 ver_1과 ver_2에 대한 값이 참으로 검증이 된 후에 사용자가 $item'$을 얻을 수 있도록 수행된다. $Verify_1$과 $Verify_2$의 알고리즘은 검증 알고리즘으로써 $Verify_1$ 알고리즘은 해쉬값의 참, 거짓을 검증하고 $Verify_2$ 알고리즘은 서명값의 참, 거짓과 $Cert$값의 참, 거짓을 검증한다.

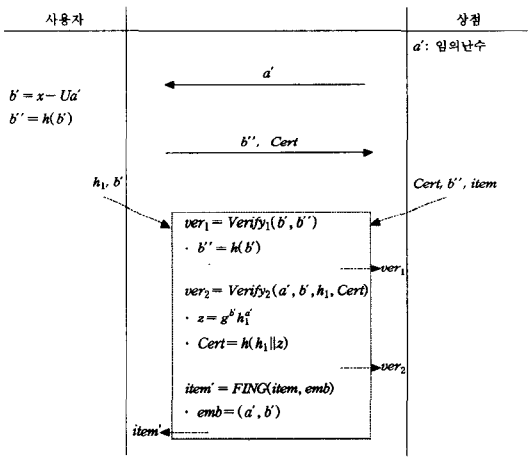

그림 2 핑거프린팅 프로토콜

4.3 신원확인 프로토콜 - P_{Iden}

상점이 불법적으로 재배포된 데이타 $item'$을 발견하였을 때 신원확인 프로토콜을 수행한다. 재배포된 데이타로부터 emb값을 추출해내고 이를 이용하여 조정자에게 재배포된 사용자에 대하여 증거를 제시한다. 상세한 프로토콜은 다음과 같다.

1) 만약 $item'$이 재배포된 것이 발견되면 상점은 $item'$으로부터 핑거프린트를 추출해 내는 알고리즘을 이용하여 $emb = A_{EXT}(item, item')$를 추출해 낸다.

2) 추출해낸 데이타 emb는 (a', b')값이 된다. 추출해낸 값 (a', b')을 등록센터에 보낸다.

3) 등록센터는 $x' ? = g^b h_1^{a'}$을 계산한 후 등록 데이타베이스로부터 해당하는 $(a, b, \langle e, y\rangle)$의 값을 찾아내어 상점에게 보낸다.

4) 상점은 등록센터로부터 받은 값들을 이용하여 사용자의 일회용 비밀값 U를 알아낼 수 있다.

$$U = \frac{b - b'}{a' - a}$$

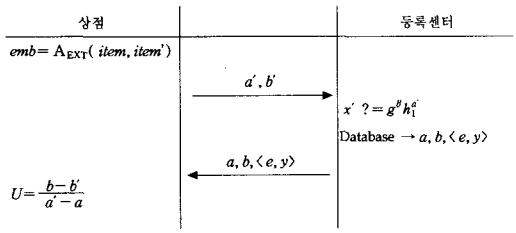

그림 3 신원확인 프로토콜

4.4 심리 프로토콜 - P_{Trial}

분쟁이 발생하였을 경우 상점은 조정자에게 디지털 데이타 $item'$이 재배포되었음을 확인시켜야 한다. 조정자는 상점과의 다음의 프로토콜을 통하여 고발된 사용자가 디지털 데이타를 재배포하였음을 확인한다.

1) 상점은 조정자에게 증거가 되는 값을 보낸다.

$$proof = ((a', b'), (a, b, \langle e, y\rangle))$$

2) 조정자는 $(a, b), (a', b')$값을 이용하여 사용자의 일회용 비밀값 U를 찾아낸다.

$$U = \frac{b - b'}{a' - a}$$

3) U를 이용하여 $h_1 = g^U$와 $x'' = g^{(b+Ua)}$을 계산한다. h_1값과 x''값을 이용하여 인증서 $Cert = h(h_1||x'')$이 맞는지 확인한다. 그리고 사용자의 Schnorr 공개키 v와 $proof$ 안의 값 $\langle e, y\rangle$를 이용하여 $z' = g^y v^e$을 계산하여 사용자의 전자서명 값이 맞는지 검증한다. 만약 인증서의 값이 맞는 경우 사용자는 디지털 데이타를 재배포한 것이 되고, 서명의 검증값에 의하여 이를 부인할 수 없게 된다. 그렇지 않을 경우 사용자는 무죄가 된다.

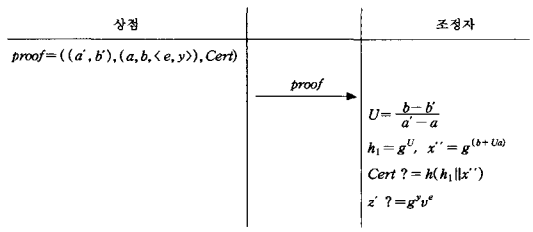

그림 4 심리 프로토콜

5. 결과 및 분석

본 논문에서 상점은 핑거프린트를 삽입하는 삽입 기

법이 공모공격에 안전하고 재배포된 데이타로부터 증거값을 찾을 수 있다는 안전성을 가정한다. 사용자에 대한 안전성은 암호학적 기법들의 안전성에 근거한다.

5.1 정확성

프로토콜 P의 네 개의 부 프로토콜 $P=\{P_{Reg}, P_{Fing}, P_{Iden}, P_{Trial}\}$은 모든 경우의 검사를 통하여 정확하게 수행됨을 증명할 수 있다.

5.2 안전성

제안한 기법의 안전성은 상점, 사용자, 그리고 등록센터의 관점에서 안전성을 분석한다.

5.2.1 상점에 대한 안전성

핑거프린트를 삽입하는 삽입기법의 특성에 근거하여, 최대 공모공격의 크기를 넘지 않거나 공모하여 재배포된 디지털 데이타가 원래의 데이타와 충분히 비슷한 경우에, 상점은 핑거프린트를 추출하는 알고리즘의 정의에 입각하여 *emb*값을 추출해낼 수 있다.

사용자는 상점으로부터 디지털 데이타를 구매하기 전에 등록센터에 자신의 일회용 비밀값을 Schnorr 서명기법을 이용하여 서명해 놓는다. 따라서 상점이 재배포된 데이타를 발견하여 재배포자를 추적하면 재배포자는 이를 회피할 수 없게 된다. 또한 양자간의 안전한 계산과정을 통하여 상점의 도전값에 대한 사용자의 응답값이 틀리거나, 등록센터로부터 받은 *Cert*값이 검증되지 않을 경우 사용자가 디지털 데이타를 얻을 수 없게 된다. 따라서 상점은 사용자로부터 사용자의 정당한 정보를 획득하지 못한 경우 디지털 데이타를 사용자에게 주지 않을 수 있으며, 재배포된 데이타에 대해서는 재배포자를 언제든지 추적할 수 있다.

5.2.2 사용자에 대한 안전성

사용자는 공격자가 다른 참여자들과 공모를 하고 사용자가 구매한 다른 구매내역들을 알고 있다 하더라도 특정한 데이타에 대한 정보가 없는 한 정직한 조정자를 심리 프로토콜과정에서 확신시키지 못한다. 즉, 조정자를 확신시키기 위해서는 사용자의 일회용 비밀값 U를 추출하고 이를 이용하여 인증서 *Cert* 값을 확인하여야 한다. 또한 사용자의 공개키를 이용하여 사용자의 서명이 맞는지도 확인해야 한다. 그러나 공격자는 사용자의 서명에 대한 비밀키를 모르기 때문에 사용자의 정당한 서명을 생성할 수 없다. 그리고 공격자는 이산대수 문제의 안전성에 근거하여 x값과 U값을 알아낼 수 없기 때문에 정당한 인증서값도 만들어낼 수 없다. 따라서 사용자는 제삼의 공격자나 등록센터와 상점의 공모공격으로부터도 안전하다.

5.2.3 등록센터에 대한 안전성

사용자는 등록시에 자신의 Schnorr 서명의 비밀키 값을 이용하여 h_1, x'에 서명을 수행하게 된다. 따라서 사용자 자신이 아닌 다른 사람이 사용자를 가장할 경우 등록 과정의 다음 두 계산에 대하여 등록센터가 올바른 답을 얻을 수 없게 된다.

$$z = g^{y}v^{e},\quad e = h(h(h_1 \| x') \| z)$$

위의 안전성은 Schnorr 서명기법의 안전성에 기반한다. 또한 사용자의 일회용 비밀값에 대하여 사용자가 영지식 증명법을 이용하여 자신의 일회용 비밀값을 알고 있음을 확인받게 되고 이에 서명을 붙이기 때문에, 서명으로 인하여 나중에 재배포 여부를 부인할 수 없다.

5.3 사용자의 익명성

핑거프린팅 프로토콜을 따르는 정직한 사용자는 양자간의 안전한 계산과정의 안전성에 근거하여 상점은 디지털 데이타에 삽입되는 정보를 알 수 없기 때문에 사용자의 익명성을 제공할 수 있다. 사용자는 이산대수문제와 양자간 안전한 계산과정의 안전성에 근거하여 사용자의 신원이 드러나지 않는 상태로 핑거프린트가 삽입된 디지털 데이타를 구매할 수 있다. 상점은 사용자로부터 $h(b')$과 *Cert*값만을 받으며, 양자간 안전한 계산과정의 안전성에 의하여 h_1을 알 수 없고, 만약 알아냈다 하더라도 이산대수 문제의 안전성에 근거하여 일회용 비밀값 U를 알아낼 수 없다.

5.4 효율성

본 논문에서 제안한 기법은 기존의 기법들에 비하여 효율성이 향상되었다. 등록시에는 계산상 효율성의 향상폭이 거의 없지만 사용자와 상점과의 핑거프린팅 프로토콜 수행에는 모듈라 지수연산의 감소가 두드러진다. 또한 신원확인 프로토콜에서는 다른 기법들에 비해서 모듈라 지수연산은 2회로 줄었다. 또한 다른 기법들이 재분배자의 신원을 찾아내기 위해서 데이타베이스 비교를 평균 N/2번 하는데 비하여 본 논문에서는 (a, b),

표 1 기존 방식과의 비교

프로토콜	비교대상	Domingo 기법[6]	Chung 기법 [4]	제안한 기법
등록	계산복잡도	6E + 1M	7E + 2M	6E + 2M
	통신횟수	4회	2회	4회
핑거프린팅	계산복잡도	5E + 1M	4E + 2M	2E + 1M
신원확인	계산복잡도	3E + N/2 + 2M	(3+1)E + 3M	4E + 1M
	비교연산	N/2 (평균)	N/2 (평균)	1

(a', b')의 값만 있으면 쉽게 사용자의 일회용 비밀값 U를 계산해 낼 수 있기 때문에 비밀분산법의 사용자 아이디를 쉽게 계산할 수 있기 때문에 신원확인 프로토콜에서의 데이타베이스 비교연산을 1번만 하면 된다. 표 1은 기존의 기법들과의 비교를 나타낸다. E는 모듈라 지수연산을 나타내며 M은 곱셈연산을 나타낸다.

6. 결 론

본 논문에서는 비밀분산법을 이용하여 사용자의 신원정보를 숨겨두었다가 재배포시 드러나도록 구성하고, Schnorr 서명을 이용하여 고발된 사용자가 범행을 부인할 수 없도록 하는 새로운 익명성을 보장하는 핑거프린팅 기법을 제안하였다.

제안한 방법은 이산대수문제와 양자간 안전한 계산과정의 안전성에 근거하여 사용자의 익명성이 보장되며 암호학적 안전성에 근거하여 프로토콜의 안전성을 증명할 수 있다. 비밀분산법을 이용하여 재분배자의 신원을 빠르게 알아낼 수 있어 신원확인 프로토콜에서의 비교연산횟수를 획기적으로 줄일 수 있었다. 기존의 제안된 기법들에 비하여 등록 프로토콜에서는 비슷한 결과를 보였으나 핑거프린팅 프로토콜에서는 계산상 효율성을, 신원확인 프로토콜의 경우엔 계산상 효율성과 비교연산에서의 효율성이 증대되었다.

참 고 문 헌

[1] B. Pfitzmann and A. R. Sadeghi, "Coin-based anonymous fingerprinting," In Advances in Cryptology-EUROCRYPT '99, LNCS 1592, pp. 150-164, 1999.

[2] G. Blakley, C. Meadow and G. B. Purdy, "Fingerprinting long forgiving messages," In Advances in Cryptology-CRYPTO'85, LNCS 218, pp. 180-189, 1986.

[3] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," In Advances in Cryptology-CRYPTO '95, LNCS 963, pp. 452-465, 1995.

[4] W. Trappe, M. Wu and K. Liu, "Collusion-resistant fingerprinting for multimedia," IEEE International Conference on Acoustics, Speech, and Signal Processing, Vol. 4, pp. 3309-3312, 2002.

[5] B. Pfitzmann and M. Schunter, "Asymmetric fingerprinting," In Advances in Cryptology-EYROCRYPT'96, LNCS 1070, pp. 84-95, 1996.

[6] C. Chung, S. Choi, Y. Choi and D. Won, "Efficient anonymous fingerprinting of electronic information with improved automatic identification of redistributors," ICICS 2000, LNCS 2015, pp. 221-234, 2001.

[7] J. Domingo-Ferrer, "Anonymous fingerprinting based on committed oblivious transfer," PKC 1999, LNCS 1560, pp. 43-52, 1999.

[8] M. Kuribayashi and H. Tanaka, : A new anonymous fingerprinting scheme with high enciphering rate," INDOCRYPT'01, LNCS 22247, pp. 30-39, 2001.

[9] B. Pfitzmann and M. Waidner, "Anonymous fingerprinting," In Advances in Cryptology-EUROCRYPT'97, LNCS 1233, pp. 88-102, 1997.

[10] J. Domingo-Ferrer, "Anonymous fingerprinting of electronic information with automatic identification redistributors," IEE Electronic Letters, Vol. 43, No. 13, 1998.

[11] A. Shamir, "How to share a secret," CACM, 22(11), pp. 612-613, 1979.

[12] C. Schnorr, "Efficient signature generation for smart cards," Journal of Cryptology, 4(3), pp. 161-174, 1991.

[13] D. Chaum, I. B. Damagaard and J. vad de Graaf, "Multiparty computations ensuring privacy of each party's input and correctness of the result," In Advances in Cryptology -CRYPTO'87, LNCS 293, pp. 87-119, 1988.

용 승 림

1998년 2월 이화여자대학교 공과대학 컴퓨터학과 학사. 2000년 2월 이화여자대학교 공과대학 컴퓨터학과 석사. 2000년~현재 이화여자대학교 컴퓨터학과 박사과정. 관심분야는 디지털저작권보호, 전자화폐, 암호학 등임

이 상 호

1979년 서울대학교 계산통계학과 이학사. 1981년 한국과학기술원 전산학과 이학석사. 1987년 한국과학기술원 전산학과 공학박사. 1990년 미국 일리노이대학교 전산학과 방문교수. 현재 이화여자대학교 컴퓨터학과 교수