DOI: 10.3745/KIPSTC.2008.15-C.3.167

모바일 환경에서의 콘텐츠 보호를 위한 핑거프린팅 기법

용 승 림[†] · 이 상 호[††]

요 약

핑거프린팅 기법은 암호학적인 기법들을 이용하여 디지털 데이터를 불법적으로 재배포한 사용자를 찾아냄으로써 디지털 데이터의 저작권을 보호하기 위해 사용된다. 핑거프린팅 기법은 구매자의 프라이버시 보호를 위하여 익명성과 비대칭성을 보장할 수 있어야 하므로, 이산대수 문제나 그래프 동형 문제와 같은 어려운 문제들에 기반하거나 공개키 암호 시스템을 이용한다. 그러나 이러한 기법들은 많은 계산량을 필요로 하기 때문에 계산능력이 낮은 모바일 환경에 적합하지 않다. 본 논문에서는 구매자의 익명성과 비대칭성을 만족하면서 모바일 환경에서 콘텐츠를 보호하기 위한 효율적인 핑거프린팅 기법을 제안한다. 제안한 기법에서는 에이전트의 개념을 이용하고, 콘텐츠 암호화를 위하여 대칭키 암호 시스템을 이용함으로써 효율성을 향상시켰다.

키워드 : 콘텐츠 보호, 핑거프린팅 기법, 대칭키 암호 시스템, 모바일 환경, 에이전트

Fingerprinting Scheme for Contents Protection in Mobile Environment

Seunglim Yong[†] · Sang-Ho Lee[††]

ABSTRACT

Fingerprinting scheme supports the copyright protection to track redistributors of digital content using cryptographic techniques. Fingerprinting schemes should guarantee buyer's anonymity and asymmetry for their privacy. Most of known fingerprinting schemes adopt public-key cryptosystems to achieve asymmetry and discrete logarithm problem or graph isomorphism problem to achieve anonymity. However, these schemes are not suited in mobile environment because of the drawbacks of requiring high computational complexity. In this paper, we propose an efficient fingerprinting scheme for mobile environment to provide not only asymmetry of the protocol but also transaction anonymity of the buyer. By employing symmetric encryption to encrypt the digital content and adopting agent to perform the protocols, the efficiency of the proposed scheme is improved.

Key Words : Contents protection, Fingerprinting scheme, Symmetric encryption system, Mobile environment, Agent

1. 서 론

M-commerce란 휴대폰이나 PDA 등의 이동통신 단말기의 무선 네트워킹으로 이루어지는 모든 비즈니스이다. M-commerce 환경에서 사용자는 이동 단말기를 사용하여 언제, 어디서나 자유롭게 원하는 정보에 접근하여 서비스를 제공받을 수 있다. 최근 보편화된 무선 단말기의 보급과 이동통신 네트워크의 고속화 등에 힘입어 이동통신 사용자의 수가 빠르게 증가하게 됨에 따라 M-commerce 환경에서의 디지털 데이터의 확산 및 보급이 늘어나고 있다. 그러나 디지털 데이터가 갖는 특성으로 인하여 저작권 문제가 야기되어 왔으며 이는 유선 환경에서와 같이 모바일 환경에서도 중요한 문제로 부각되고 있다.

† 정 회 원 : 인하공업전문대학 컴퓨터시스템과 전임강사
†† 종신회원 : 이화여자대학교 컴퓨터학과 교수
논문접수 : 2007년 5월 31일
수 정 일 : 1차 2007년 10월 19일, 2차 2007년 12월 4일, 3차 2008년 3월 3일
심사완료 : 2008년 3월 13일

핑거프린팅 기법은 암호학적인 기법들과 워터마킹 기법을 이용하여 디지털 데이터를 불법적으로 재배포한 구매자를 찾아냄으로써 디지털 데이터의 저작권을 보호할 수 있는 방법이다. 즉 판매자는 재배포한 구매자를 찾아낼 수 있도록 구매자마다 다른 핑거프린트라고 불리는 마크를 디지털 콘텐츠에 삽입한다. 핑거프린팅 기법에서 핑거프린트가 삽입된 콘텐츠들은 동일한 콘텐츠에 구매자마다 다른 핑거프린트를 삽입하여 유일성을 갖는 콘텐츠가 생성되어야 하며 판매자는 구매자에게 콘텐츠를 판매하지만 구매자의 신원은 알지 못해야 하는 비대칭성과 익명성을 만족해야 한다. 이를 위하여 기존의 핑거프린팅 기법들은 이산대수 문제나 그래프 동형 문제와 같은 어려운 문제들을 기반으로 하였다. 그러나 이러한 기법들은 계산 복잡도가 높아 유선 환경에서도 적용하기 힘든 기법들이다. 더구나 유선환경보다 계산능력이 낮은 모바일 환경에는 더더욱 적용하기 힘들다. 최근에 에이전트를 이용한 모바일 환경에서의 핑거프린팅 기법이 제안

되었으나 공개키 암호 시스템으로 콘텐츠를 암호화하기 때문에 효율성이 현저히 떨어지는 단점이 있다.

본 논문에서는 구매자의 이동통신 단말기보다 계산 능력이 나은 에이전트의 개념을 적용하고 콘텐츠를 암호화할 때 대칭키 암호 시스템을 이용함으로써 모바일 환경에서 적용하기에 적합한 핑거프린팅 기법을 제안한다.

2. 관련 연구

2.1 암호학적 기법

2.2.1 교환 암호 시스템

교환 암호 시스템은 교환적인 성질을 만족하는 암호 시스템이다[1]. 즉, 어떤 알고리즘 CE가 교환적이라는 것은 두 개의 키 k_1과 k_2 그리고 어떤 메시지 m이 있을 때 다음과 같은 성질을 만족한다는 것이다.

$$CE(k_1, CE(k_2, m)) = CE(k_2, CE(k_1, m))$$

암호메시지 $c = CE(k, m)$를 복호화하는 것은 $m = CE^{-1}(k, c)$와 같이 쓸 수 있다. 평문 메시지 m은 메시지가 두 개의 서로 다른 키 k_1과 k_2로 암호화 되었을 때 암호문을 k_1으로 먼저 복호화하고, 그 다음에 키 k_2로 복호화하여 얻을 수 있다. 마찬가지로 암호 메시지를 키 k_2를 이용하여 먼저 복호화하고 그 다음에 k_1을 이용하여 복호화해서 얻을 수도 있다. 교환 암호 시스템의 응용 분야는 멘탈 포커 게임(Mental Poker Game)에서 카드를 분배할 때 각각의 게이머가 정당하게 카드를 나누어 갖기 위한 프로토콜을 설계할 때 등이다[2][3].

2.2.2 대리서명

대리서명(Proxy Signature) 방식은 Mambo[4][5]에 의해서 처음 제안되었다. 대리서명은 대리서명자가 원 서명자를 대신하여 원 서명자의 서명과 동일한 효력을 갖는 대리서명을 생성하고 이를 검증하는 암호학적 프로토콜이다. 어떤 조직의 간부가 정보통신망에 접속할 수 없는 지역으로 출장을 가는 경우에 그는 출장 기간 동안 어떤 문서에 대한 결제나 메일 등에 대한 응답을 위하여 그의 권한을 다른 사람에게 부여하여야 한다. 권한을 위임받은 자-대리서명자-는 그에 적절한 직무를 수행하게 되는 것이고 이를 원활하게 수행하도록 하는 개념이 대리서명인 것이다. 이러한 방식은 위조불능, 서명부인방지, 위임부인불가, 대리서명 위조불가, 대리서명의 정당성 검증, 대리서명자를 식별하는 등의 조건을 가져야한다.

대리서명 기법은 원 서명자의 서명 권한을 위임하는 형태에 따라 완전 위임, 부분 위임, 보증 위임 방식으로 나뉜다. 완전 위임 방식은 원 서명자가 대리서명자에게 자신의 비밀키를 주는 경우로 대리서명자의 서명과 원 서명자의 서명이 구분이 되지 않는 방식이다. 부분 위임은 완전 위임 보다 안전한 방식으로 원 서명자가 대리서명용 비밀키를 자신의 비밀키를 이용하여 생성하는 방식이다. 이 때 비밀키는 대리서명용 비밀키로부터 계산이 불가능하여야 한다. 보증 위임 방식은 원 서명자가 대리서명자에게 보증서를 발행함으로써 대리 서명을 구현하는 방식이다.

2.2 기존 연구

J. G. Choi는 에이전트 개념을 이용하여 모바일 환경에서 익명성이 보장되는 핑거프린팅 기법을 제안하였다[6]. 모바일 환경에서 구매자는 계산능력이 떨어지는 모바일 기기를 가지고 있기 때문에 구매자의 기기보다 계산 능력이 좋은 에이전트가 구매자를 대신하여 프로토콜을 수행한다. 핑거프린팅 기법은 다섯 개의 단계 - 등록 단계, 위임단계, 핑거프린트 생성단계, 핑거프린트 삽입단계, 재배포자의 신원확인 - 로 구성된다. 이때 에이전트는 Romao와 Silva[7]가 제안한 대리 인증서를 받음으로써 구매자로부터 권한을 위임받게 된다. 권한을 위임받은 에이전트는 구매자를 대신하여 등록 프로토콜과 핑거프린팅 프로토콜을 수행하며 구매자 대신 구매자의 서명을 생성할 수 있다. 핑거프린팅 프로토콜이 수행되고 나서 에이전트는 핑거프린트가 삽입된 암호화된 콘텐츠를 구매자에게 전송한다. 삽입된 콘텐츠는 판매자가 알 지 못하도록 준동형의 암호(homomorphic encryption) 기법[3]을 적용하여 구매자의 공개키로 암호화된다. 구매자가 에이전트로부터 암호화된 콘텐츠를 전송받고 나면 구매자는 암호화된 콘텐츠를 자신의 비밀키를 이용하여 복호화하게 된다. 그러나 준동형의 암호는 공개키 기반 암호 기법이기 때문에 현실적으로 계산능력이 떨어지는 모바일 기기에서 구매자가 암호화된 콘텐츠를 복호화하기 어렵다.

3. 모바일 환경에서의 핑거프린팅 기법

본 절에서 모바일 환경에 적합한 핑거프린팅 프로토콜에 대하여 기술한다. 먼저 본 논문에서 사용되는 기호를 정의하고 참여자의 역할에 대하여 정의한다.

1) 사용되는 기호

- $item \in \{0,1\}^*$: 핑거프린트가 삽입될 수 있는 콘텐츠
- $item'$: 핑거프린트가 삽입된 콘텐츠.
- F : 구매자의 고유 인식정보인 핑거프린트
- H : 충돌 회피성 해쉬함수
- AE/AD : 공개키 암호시스템, 암호화/복호화 알고리즘
- SE/SD : 대칭키 암호시스템, 암호화/복호화 알고리즘
- CE : 교환 암호 시스템

2) 참여자의 역할

프로토콜의 참여자는 구매자, 에이전트, 판매자, 등록 센터,

그리고 재판관이다. 각각의 참여자의 역할은 다음과 같다.

- 등록 센터(RC): 등록 센터는 구매자와 등록 프로토콜을 수행하여 구매자의 익명 공개키 쌍을 등록받고 익명 공개키 쌍에 대한 인증서를 발급하며 다른 참여자들과의 공모를 행하지 않는 신뢰기관이라 가정한다.
- 에이전트(M): 에이전트는 구매자로부터 대리서명 키 쌍을 받아 권한을 위임받은 후 구매자를 대신하여 콘텐츠를 구매하는 역할을 하고 구매자를 대신하여 서명을 수행할 수 있다. 무선 환경에서 에이전트는 무선통신 사업자가 될 수도 있고, 구매자를 대신하여 프로토콜을 수행할 수 있는 소프트웨어 에이전트나 대리 에이전트(Proxy Agent)가 될 수도 있다. 에이전트는 공개키 쌍 (x_M, y_M)을 가지고 있다.
- 구매자(B): 구매자는 익명 공개키 쌍을 등록 센터에 등록하고 구매 행위를 할 때 등록한 익명 공개키 쌍을 이용한다. 핑거프린팅 프로토콜을 수행할 때 에이전트에게 권한을 위임하고 핑거프린팅 프로토콜이 끝나면 에이전트로부터 콘텐츠를 전송받는다. 구매자는 일반 CA로부터 인증 받은 공개키 쌍 (x_B, y_B)을 가지고 있다.
- 판매자(C): 판매자는 에이전트와 프로토콜을 수행하며, 구매자의 핑거프린트를 임의로 생성하고 이를 콘텐츠에 삽입한다.
- 재판관(J): 재배포가 발생되었을 때 판매자의 요청에 의하여 재배포자를 추적하고 재배포자를 판단하는 제3의 신뢰기관이다.

프로토콜은 등록, 권한위임, 핑거프린트 삽입, 그리고 신원확인의 네 개로 구성된다. 에이전트는 계산능력이 떨어지는 구매자로부터 권한을 위임받은 후 구매자를 대신하여 프로토콜을 수행한다. 에이전트는 구매자를 대신하여 서명을 생성할 수 있고, 핑거프린트 프로토콜이 수행되고 나면 판매자로부터 받은 핑거프린트가 삽입된 암호화된 콘텐츠를 구매자에게 전송한다. 자세한 단계별 프로토콜은 다음과 같다.

3.1 등록 단계

구매자는 먼저 등록 센터에 자신의 익명 공개키를 등록한다. 구매자와 등록 센터는 공개키 쌍을 가지고 있다고 가정한다. 구매자의 비밀키는 x_B이고 공개키는 $y_B = g^{x_B}$이다.

1) 구매자는 $x_1 + x_2 = x_B$를 만족하는 임의의 두 비밀값 x_1, $x_2 \in {}_RZ_p$를 선택하고 구매자의 익명 공개키 $y_1 = g^{x_1}$을 생성한다. 구매자는 비밀값 x_2를 등록 센터의 공개키로 암호화한 $E_{RC}(x_2)$를 생성하고 x_1을 이용하여 서명한 서명값 $Sig(H(x_2))$을 생성한다. 구매자는 y_B, y_1, $E_{RC}(x_2)$ 그리고 $Sig(H(x_2))$를 등록 센터에 보낸다. 서명값을 보냄으로써 구매자가 생성한 익명 공개키에 대한 비밀키를 알고 있음을 증명할 수 있다.
2) 등록 센터는 $E_{RC}(x_2)$값을 자신이 비밀키로 복호화하고 해쉬함수를 적용하여 구매자가 보낸 서명값 $Sig(H(x_2))$을 검증한다. 서명값이 맞으면 구매자는 익명 공개키 y_1에 대하여 비밀키 x_1을 알고 있음이 증명된다. 등록 센터는 $y_2 = g^{x_2}$를 계산하여 y_B의 값이 y_1과 y_2의 곱의 값과 같은지 확인한다. 이 값이 검증되면, 등록 센터는 구매자에게 인증서 $Cert(y_1)$을 보내준다.

3.2 권한 위임 단계

익명 구매자는 에이전트와 권한 위임의 프로토콜을 수행한다.

1) 구매자는 콘텐츠를 구매할 때 필요한 임의의 값 t와 t 비트 문자열 L_B를 생성한다. 그리고 L_B를 재판관의 공개키로 암호화하여 $E_J(L_B)$를 생성한다. 정수 L_B의 각 비트는 $l_j = \{0, 1\}$로 구성되어 있다. 이때 L_B의 비트 패턴은 $\{0, 0, \ldots, 0\}$ 또는 $\{1, 1, \ldots, 1\}$이 되어서는 안된다.
2) 임의의 값 k를 선택하고, (x_1, y_1)과 등록 센터로부터 받은 인증서 $Cert(y_1)$, 암호화한 L_B 값 $E_J(L_B)$를 이용하여 $r = g^k$, $s = x_1 \cdot H(Cert(y_1) \| E_J(L_B) \| r) + k$를 생성한다.
3) 구매자는 t비트 문자열과 2단계에서 생성된 r, s 값을 접합한 $L_B \| r \| s$를 생성하고 에이전트의 공개키 y_M으로 암호화한 $AE_{y_M}(L_B \| r \| s)$, $Cert(y_1)$ 그리고 $E_J(L_B)$를 에이전트에게 보낸다.
4) 에이전트는 식 $g^s = y_1^{H(Cert(y_1) \| E_J(L_B) \| r)} r$을 계산함으로써 s값이 맞는지 확인한다. 구매자가 보내준 (r, s) 쌍이 익명구매자의 위임키로 이용된다.

3.3 핑거프린팅 단계

권한을 위임받은 에이전트는 구매자를 대신하여 핑거프린팅 프로토콜을 수행한다. 에이전트는 구매자의 익명 공개키 y_1과 인증서 $Cert(y_1)$ 그리고 콘텐츠를 나눌 프레임의 개수 t를 판매자에게 보내고 디지털 콘텐츠 $item$을 요구한다. 판매자는 구매자의 두 개의 핑거프린트 F_B^0와 F_B^1를 생성한다.

1) 판매자는 에이전트가 요구한 $item$의 두 개의 복사본 $item^0$, $item^1$을 생성하고 이것을 t개의 프레임으로 나눈다. 판매자는 $item^0$의 t개의 프레임에 핑거프린트

F_B^0를 삽입하고 $item^1$의 t개의 프레임에 핑거프린트 F_B^1을 삽입한다.

$item_B^i = \{item_B^{i,1}, item_B^{i,2}, \ldots, item_B^{i,t}\}$ *where*
$item_B^{i,j} = item^{i,j} \oplus F_B^i,\ i=\{0,1\}, j=\{1,2,\ldots,t\}$

2) 판매자는 임의로 선택된 t개의 키로 구성된 두 개의 비밀키 벡터 K_0과 K_1을 생성한다.

3) (그림 1)과 같이 판매자는 $item_B^i$의 각 프레임을 키벡터의 각 원소로 암호화하고 두 개의 암호화된 콘텐츠 벡터 X_B^0, X_B^1을 생성하고 이들을 에이전트에게 보낸다. 키벡터 K_i는 $item_B^i$를 암호화하는데 이용한다 .

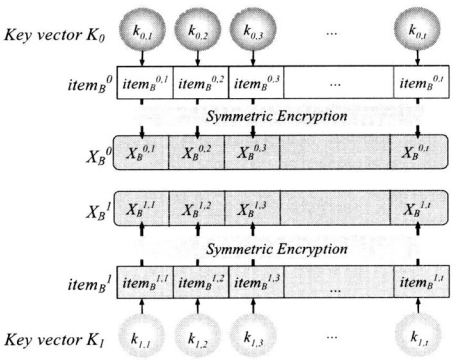
$X_B^i = SE(K_i, item_B^i)$
$= SE(k_{i,j}, item_B^{i,j}),\ where\ i=\{0,1\},\ j=\{1,2,\ldots,t\}$

4) 판매자는 비밀키 mk를 생성한 후 두 개의 암호화된 키벡터 $EK_i = SE(mk, K_i)$를 (그림 2)와 같이 생성한다. 판매자는 비밀키 S를 선택하고 교환 암호 알고리즘 CE를 이용하여 두 개의 암호화된 키벡터 EK_i를 암호화하여 벡터 C_i를 생성하고 에이전트에게 보낸다.

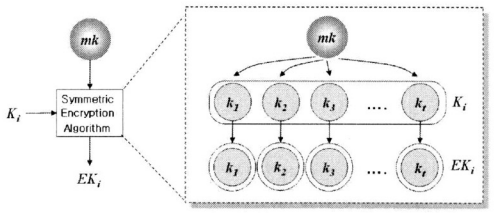
5) 에이전트가 C_i를 받으면 구매자로부터 받은 비트패턴 L_B에 따라 새로운 암호화된 벡터 C'를 구성한다. 비트패턴 L_B가 $l_j=0$이면 $c'_j = c_{0,j}$를, $l_j=1$이면 $c'_j = c_{1,j}$를 선택한다.

6) 에이전트는 임의의 비밀키 R을 선택한 후 암호화된 벡터 $D = CE(R, C')$를 생성하고 판매자에게 보낸다.

7) 판매자는 벡터 D를 자신의 비밀키 S를 이용하여 복호화하여 $U = CE^{-1}(S, D)$인 벡터 U를 구한다. 판매자는 U를 에이전트에게 보낸다.



(그림 1) 콘텐츠 암호화



(그림 2) 키벡터 암호화

8) 에이전트는 $T_B = E_f(L_B)$와 대리 서명키를 이용하여 서명값 $Sig(T_B)$를 생성하고 판매자에게 보낸다. T_B와 $Sig(T_B)$는 나중에 재배포여부를 확인하는데 증거로 활용된다.

9) 판매자는 $Sig(T_B)$의 정당성 여부를 확인한다. 서명이 정당하면 mk를 구매자의 공개키 y_1으로 암호화한 $AE_{y_1}(mk)$와 그의 서명값을 에이전트에게 보낸다.

10) 에이전트는 서명을 확인하고 판매자로부터 받은 벡터 U을 복호화하여 t개의 암호화된 키벡터를 얻어낸다. 에이전트는 이렇게 얻어진 복호키, 단계 9에서 받은 $AE_{y_1}(mk)$과 그의 서명값 그리고 암호화된 콘텐츠를 구매자에게 전송한다.

11) 구매자는 $AE_{y_1}(mk)$를 자신의 비밀키로 복호화하고, mk를 이용하여 암호화된 키벡터 를 복호화하여 키벡터 K_B를 얻는다. 키 벡터 K_B를 이용하여 암호화된 콘텐츠 $item_B^{l_i,j} = SE^{-1}(k_{l_i,j}, X_B^{l_i,j})$를 복호화한다.

3.4 구매자 신원확인

불법적으로 재배포된 콘텐츠가 발견되면 판매자는 그 콘텐츠로부터 핑거프린트를 추출하여 구매자가 누구인지 추적한다.

1) 불법 재배포된 콘텐츠가 발견되면, 판매자는 핑거프린트 패턴을 추출하고 핑거프린트 F_B^0, F_B^1을 이용하여 $item_B^0, item_B^1$을 생성하고 이를 재판관에게 Rec_B의 데이터들과 함께 보낸다.

2) 재판관은 T_B를 검증하고 $item_B$에 핑거프린트 F_B^0, F_B^1이 있는지를 확인하고, 핑거프린트 패턴이 사용자의 비트패턴 L_B와 일치하는지 검증한다.

3) 재판관은 구매자의 익명 공개키 y_1을 이용하여 서명값 $Sig(T_B)$을 검증한다. 만약 검증이 되면 y_1을 등록 센터에 보내서 구매자의 원래의 아이디를 요청하여 재배포자가 누구인지 알아낸다.

4. 안전성 및 효율성

4.1 안전성

4.1.1 추적성

구매자는 어떠한 경우라도 한 개 이상의 정당한 $item_B$을 판매자로부터 얻어낼 수 없다. 구매자가 두 개 이상의 $item_B$을 얻기 위해서는 t개 이상의 키를 얻어내야 하지만 이를 위해서는 판매자가 구매자로부터 받은 암호화된 벡터 D에 두 번 이상의 복호화를 수행해 주어야 하기 때문에 t개의 복호키만을 얻어낼 수 있다.

또한 불법 배포를 위하여 구매자는 에이전트에게 T_B을 틀리게 생성하여 보내도록 할 수 있다. 만약 정당하지 않은 L'_B값을 이용하여 $T'_B = E_f(L'_B)$를 만들었다면, 판매자는 대리서명 공개키를 이용하여 검증할 때 원래의 값과 생성된 값이 서로 다르기 때문에 서명을 검증할 수 없다. 따라서 판매자가 에이전트로부터 받은 값들이 검증이 되었다면, 구매자는 자신이 받을 콘텐츠의 비트벡터를 알고 있으며 에이전트가 위조하지 못했음을 확신할 수 있다.

4.1.2 부인 봉쇄

핑거프린팅 단계에서 에이전트는 $Sig(T_B)$을 생성한다. 대리서명 키는 구매자만이 생성할 수 있고, 대리서명 키를 생성할 때 만들어진 값 s안에 T_B의 값이 들어 있기 때문에 불법 재배포된 콘텐츠가 발견되었을 때 $item_B$에 대한 구매자는 재배포된 콘텐츠가 구매자의 것임을 부인할 수 없다.

4.1.3 비대칭성

판매자는 구매자의 핑거프린트 패턴을 알아내기 위해서는 에이전트가 선택한 c'_i의 값을 알아내기 위야 하고 이를 위해서 d_i를 계산해내야 한다. 그러나 이 계산은 암호알고리즘 CE를 공격하는 방법만큼이나 어렵다. 또한 구매자가 모든 t프레임에 대하여 선택한 c'_i를 알아낼 수 있는 확률은 $1/2^t$와 같다. 따라서 판매자는 비밀키 R을 알지 않고서 에이전트가 선택한 정보를 찾아내기는 계산상 불가능하다.

또한 판매자는 같은 핑거프린트를 $item_B^i$에 삽입하여 동일한 콘텐츠를 생성하여 정직한 구매자를 재배포자로 만들고자 할 수 있다. 그러나 삽입된 핑거프린트가 동일할 경우 핑거프린팅 단계에서 구매자가 선택한 임의의 패턴 L_B가 핑거프린트 패턴과 다르게 되어 신원확인 단계에서 구매자가 생성한 비트 패턴값과 핑거프린트 패턴값이 다르게 된다. 따라서 판매자는 동일한 두 개의 콘텐츠를 생성하고 서로 다른 콘텐츠를 생성한 것처럼 구매자를 속일 수 없다.

4.1.4 조작 봉쇄

판매자가 구매자의 핑거프린트를 알고 있지만 핑거프린트가 삽입된 콘텐츠는 t개의 프레임으로 나뉘어 있기 때문에 모든 가능한 조합의 수는 2^t가지가 되므로 판매자는 구매자가 어떤 프레임을 선택했는지 알 수 없다. 또한 악의적인 판매자는 L''_B과 $item''_B$를 생성하여 구매자가 배포한 것처럼 구매자를 고발할 수 있다. 이 경우에 판매자는 $T''_B = E_f(L''_B)$에 대한 정당한 서명 $Sig(T''_B)$값을 생성해 낼 수 없고 따라서 신원확인 단계에서 재판관을 확신시킬 수 없다.

4.1.5 구매자의 익명성

핑거프린팅 단계에서 판매자는 구매자의 익명 공개키 y_1을 알고 있다. 하지만 에이전트로부터 구매자의 다른 비밀정보나 구매자의 공개키를 알아낼 수 없다. 따라서 판매자가 구매자의 공개키 y_B를 알기 위해서는 x_2의 값을 알아야만 한다. 만약 암호 알고리즘이 안전하다면 판매자와 등록센터가 공모공격을 하지 않는 한 판매자는 x_2값을 알아낼 수 없다. 또한 비록 판매자가 구매자의 핑거프린트는 알고 있지만 구매자의 핑거프린트 패턴은 알 수 없기 때문에 구매자의 익명성은 보장된다.

4.2 효율성

모바일 환경에서 구매자는 계산 능력이 낮은 모바일 기기를 가지고 프로토콜을 수행해야 한다. 따라서 제안한 기법에서는 모바일 기기보다 계산능력이 좋은 에이전트를 이용하여 복잡한 프로토콜은 대신 수행하도록 하였다. 구매자는 에이전트에게 대리서명 키 쌍을 생성하여 줌으로써 권한을 위임하여 주고, 에이전트는 구매자를 대신하여 핑거프린팅 프로토콜을 수행한다. 핑거프린팅 프로토콜이 수행된 후 구매자는 에이전트가 전송한 키와 콘텐츠만 복호화하면 된다.

<표 1>은 기존에 제안된 [6]의 기법과 본 논문에서 제안한 기법의 수행시간 비교표이다. 핑거프린트가 삽입된 콘텐츠를 구매자가 구매자의 단말기로 복호화할 때 걸리는 시간을 측정하였다. 공개키 암호 기반 핑거프린팅 기법을 이용하였을 경우 콘텐츠가 공개키 암호 알고리즘으로 암호화되어 있기 때문에 구매자가 콘텐츠를 복호화하는데에 많은 시간이 걸린다. 반면 제안한 대칭키 기반 핑거프린팅 기법은 콘텐츠를 복호화하는데 걸리는 시간이 매우 적다. 비록 핑

〈표 1〉 모바일 핑거프린팅 수행시간 비교표

기법 \ 콘텐츠크기 (byte)		100	500	1,000	10,000	100,000
공개키 기반	콘텐츠 복호화	5,351	14,775	29,389	299,567	x
대칭키 기반	콘텐츠 복호화	47	78	94	656	2,125
	키 복호화	159	159	159	159	159
	합계	206	237	253	805	2,284

거프린팅 단계에서 콘텐츠를 암호화한 키를 구매자의 공개키로 암호화하여 전송하기 때문에 키를 공개키 암호 시스템을 이용하여 복호화하기 위한 시간이 추가적으로 든다 하더라도 구매자가 키를 복호화하고 콘텐츠를 복호화하는 합계 시간이 공개키 암호 기반의 기법에 비하여 현저히 낮음을 볼 수 있다. 그러나 [6]의 경우 에이전트는 암호화된 콘텐츠만 구매자에게 전송하면 되지만 제안한 기법에서는 콘텐츠를 암호화한 키도 전송해야 하기 때문에 (대칭키 암호 시스템의 키 사이즈 × t) 비트만큼 전송해야 할 메시지의 양이 늘어나게 된다. 구현은 Bouncy Castle 암호 라이브러리와 sun사의 WTK 2.5.2 에뮬레이터를 이용하였고 공개키 암호 시스템으로 160bit ECC 알고리즘을, 대칭키 기법으로 AES 알고리즘을 이용하였다.

5. 결 론

모바일 환경에서 구매자는 계산 능력이 떨어지는 모바일 기기를 가지고 있다. 본 논문에서는 모바일 환경에 적합한 에이전트를 이용한 익명성을 제공하는 핑거프린팅 기법에 대하여 제안하였다. 구매자는 에이전트에게 대리 서명키 쌍을 제공함으로써 권한을 위임하고 에이전트는 복잡한 모든 프로토콜을 구매자 대신 수행한 후 콘텐츠를 구매자에게 전송한다. 제안한 기법에서 콘텐츠는 대칭키 암호 시스템을 이용하여 암호화하고, 콘텐츠를 암호화할 때 이용되는 키벡터만 공개키 암호 시스템을 이용하도록 설계되어 기존의 기법보다 시간적인 효율성이 향상되었다. 또한 판매자는 비록 권한을 위임받은 에이전트와 핑거프린팅 단계를 수행하지만, 불법 재배포된 콘텐츠의 구매자를 찾을 수 있고 구매자는 익명성이 보장되며 프로토콜의 비대칭성도 만족하였다. 그러나 $2t$개의 복호화 키를 생성해야 하고, 기존의 기법과 비교하여 에이전트가 구매자에게 암호화된 콘텐츠 이외에 복호화 키를 추가적으로 전송해야 하는 단점이 있다.

참 고 문 헌

[1] F. Bao, R. H. Deng and P. Feng, "An Efficient and Practical Scheme for Privacy Protection in the E-commerce of Digital Goods," International Conference on Information and Communication Security(ICICS'00), LNCS 2836, pp.162-170, 2001.

[2] S. Goldwasser and S. Micali, "Probabilistic Encryption and How to Play Mental Poker Keeping Secret All Partial Information," ACM Symposium on Theory of Computing (STOC'82), pp.365-377, 1982.

[3] W. Zhao, V. Varadharajan and Y. Mu, "A Secure Mental Porker Protocol over the Internet," Australasian Information Security Workshop(AISW'03), Vol.21, pp.105-109, 2003.

[4] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signature for delegating signing operation", Proc. Third ACM Conference on Computer and Communications Security, pp.48-57, 1996.

[5] M. Mambo, K. Usuda and E.Okanmoto, "Proxy signature: delegation of the power to sign messages," IEICE Transaction on Fundamentals, Vol. E79-A, No.9, pp.1338-1353, 1996.

[6] J. G. Choi and J .H. Park, "A generalization of an anonymous buyer-seller watermarking protocol and its application to mobile communication," IWDW'04, LNCS 3304, pp.232-242, 2004.

[7] A. Romao and M. M da Silva, "Secure Mobile Agent Digital Signature with Proxy Certificates," E-Commerce Agents, LNCS 2033, pp.206-220, 2001.

[8] E. F. Brickell and Y. Yacobi, "On Privacy Homomorphisms," Advances in Cryptology - EUROCRYPT'87, LNCS 304, pp.117-125, 1987.

용 승 림

e-mail : slyong@inhatc.ac.kr

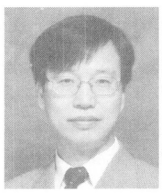
1998년 이화여자대학교 컴퓨터학과 (공학사)

2000년 이화여자대학교 대학원 컴퓨터학과 (공학석사)

2006년 이화여자대학교 과학기술대학원 컴퓨터학과(공학박사)

2008년~현 재 인하공업전문대학 컴퓨터시스템과 전임강사

관심분야 : 암호프로토콜, 저작권 보호, RFID 보안 등



이 상 호

e-mail : shlee@ewha.ac.kr

1979년 서울대학교 계산통계학과 (이학사)

1981년 한국과학기술원 전산학과 (이학석사)

1987년 한국과학기술원 전산학과 (공학박사)

1983년~현 재 이화여자대학교 컴퓨터학과 교수

관심분야 : 알고리즘 설계, 정보보호, 바이오인포매틱스 등