通信情報保護學會論文誌
第 10 券 第 4 號, 2000. 12

재분배자의 자동 식별기능을 갖는 효율적인 익명성을 제공하는 핑거프린팅*

정 찬 주**, 오 수 현**, 양 형 규***, 원 동 호**

Efficient Anonymous Fingerprinting with Improved Automatic Identification of Redistributors

Chanjoo Chung**, Soohyun Oh**, Hyungkyu Yang***, Dongho Won**

요 약

본 논문에서는 디지털 컨텐츠의 전자상거래에서 사용될 수 있는 재분배자의 개선된 자동 식별기능을 갖는 효율적인 익명성을 제공하는 핑거프린팅 방식을 제안한다. Domingo가 Electronic Letters에서 제안한 방식[1]은 등록 프로토콜의 통신 회수와 식별프로토콜에서 지수 연산 회수가 너무 많아 전자상거래에서 비효율적이다. 제안하는 방식은 등록 프로토콜에서 통신 회수를 2-pass로 줄였고, 식별 프로토콜에서는 평균적으로 공개키 디렉토리 상에 있는 공개키 수에 반정도의 지수 연산의 회수가 필요했던 것을 단지 1번의 지수 연산으로 줄였다. 따라서, 디지털 컨텐츠의 전자상거래가 일상 생활에서 쓰이게 됨에 따라 제안하는 방식의 이용 가치는 증대될 것이다.

ABSTRACT

This paper proposes efficient anonymous fingerprinting with improved automatic identification of redistributors in electronic commerce of digital contents. The proposed scheme by Domingo's in Eletronic Letters is inefficient in electronic commerce, because of pass numbers in registration protocol and exponential computations in identification protocol. Our scheme is reduced 2-pass in registraton protocol and is required only 1 time exponential computation than his in identification protocol. According to electronic commerce of digital contents used in ordinary life, our scheme's values are increased.

keyword : *fingerprinting, copyright marking, anonymous, automatic identification, traitor tracing*

Ⅰ. 서 론

컴퓨터 네트워크와 멀티미디어 관련 기술의 발전에 따라 디지털 컨텐츠의 지적소유권을 보호하기 위한 방법들이 대두되기 시작하였다. 이러한 기술로 기존에 쓰인 방식은 암호화 방식과 접근제어 방식이 있었지만, 이 방식은 디지털 컨텐츠에 적법한 허가를 얻은 후에는 불법복제가 가능하다는 문제점을 가지고 있다.

이에 새롭게 대두된 방식이 카피라이트 마킹 방식(copyright marking)이다[2]. 카피라이트 마킹 방식은 디지털 컨텐츠에 소유권자의 정보를 삽입함으로써 디지털 컨텐츠의 불법복제 자체는 막지는 못하지만, 이후에 저작권 관련 분쟁이 발생하였을 경우

* 본 연구는 한국 과학 재단의 특정기초연구(97-01-00-13-01-5) 지원 사업에 의해 수행하였습니다.
** 성균관대학교 전기전자 및 컴퓨터공학과 ({cjchung, shoh, dhwon}@dosan.skku.ac.kr)
*** 강남대학교 이공대학 산업·전산·전자공학부 (hkyang@kns.kangnam.ac.kr)

에 저작권자를 밝혀낼 수 있기 때문에 불법복제를 예방하는 효과를 기대할 수 있다. 카피라이트 마킹 기술의 하위 분류로 워터마킹 기술과 핑거프린팅 기술이 있다. 워터마킹 기술은 동일한 컨텐츠에 대하여 동일한 소유권 정보를 삽입하여 소유권 인증 기능만을 제공하는 반면에, 핑거프린팅은 동일한 컨텐츠에 대하여 서로 다른 소유권 정보를 삽입하여 소유권 인증 기능뿐만 아니라 구매자를 식별하는 기능까지 제공한다. 따라서, 전자상거래의 발전에 따라 디지털 컨텐츠의 지적 소유권 보호를 위한 방법으로 핑거프린팅 기술에 대한 관심은 증대될 것이다.

핑거프린팅 기술의 하위 분류로 소유권 정보가 사용된 키에 의하여 식별 기능을 제공하는 불법자 추적(traitor traicing) 기술이 있다[3]. 이 기술은 pay-TV와 같은 방송 시스템에서 방송업자가 영상을 암호화하여 전송한 경우에 영상 복호시 사용되는 키를 재분배하는 구매자를 추적하는 기술이다.

핑거프린팅은 디지털 컨텐츠의 저작권 보호와 데이터 베이스의 고속 검색 방법, 그리고 pay-TV와 같은 방송 시스템 등의 많은 응용분야를 가지고 있으며, 이는 전자상거래 활성화와 더불어 응용 범위는 더욱 넓어질 것이다.

본 논문의 구성은 다음과 같다. 2장에서는 핑거프린팅 기술의 분류와 핑거프린팅의 요구사항에 대하여 알아본다. 3장에서는 Domingo가 제안한 방식에 대하여 알아보고, 4장에서는 제안하는 방식의 프로토콜을 자세히 기술한다. 5장에서는 제안하는 핑거프린팅 방식의 안전성을 분석하고, Domingo가 제안한 방식과 비교한다. 끝으로 6장에서는 결론을 내리고자 한다.

II. 기술 분류 및 요구사항

핑거프린팅은 판매자가 불법 복사된 디지털 컨텐츠를 발견했을 경우, 재분배자를 사후 검출하는 기능을 제공하기 때문에 불법 복사 자체를 막지는 못하지만 불법적인 사용을 검출할 수 있는 기능을 제공함으로써 불법 복사를 방지하는 효과를 기대할 수 있다. 핑거프린트는 판매자가 디지털 컨텐츠를 구별하기 위하여 원본 컨텐츠에 삽입하는 정보이다.

2.1 핑거프린팅 기술의 분류

핑거프린팅은 핑거프린팅되는 데이터, 검출 감도, 핑거프린팅 방법, 생성된 핑거프린트 그리고 식별정보를 아는 개체에 따라 분류될 수 있다.[4] 이러한 분류는 상호 배타적이지 않고 서로 연관되어 있는 경우가 많다. [표 1]은 핑거프린팅의 분류 방법과 그에 따른 종류를 나타낸 것이다.

[표 1] 핑거프린팅의 분류

분류 방법	종류
삽입 대상 객체 (Object)	· Digital fingerprint · Physical fingerprint
검출 감도 (Detection Sensitivity)	· Perfect fingerprint · Statistical fingerprint · Threshold fingerprint
핑거프린트 방법 (Fingerprint-Method)	· Recognition fingerprint · Deletion fingerprint · Addition fingerprint · Modification fingerprint
삽입되는 정보 형태 (Fingerprint)	· Discrete fingerprint · Continuous fingerprint
식별정보 노출수준 (Identification Information)	· Symmetric fingerprinting · Asymmetric fingerprinting

2.1.1 삽입 대상 객체에 따른 분류

삽입 대상이 되는 객체는 디지털 컨텐츠에 핑거프린트하는 방법을 제공하기 때문에, 기본적인 분류 방법이 된다. 이 분류에는 디지털 핑거프린트와 물리적 핑거프린트로 나뉜다. 전자는 핑거프린트되는 객체가 디지털 형식으로 컴퓨터에서 핑거프린트를 처리할 수 있는 경우이고, 후자는 객체가 다른 데이터를 구별하기 위하여 사용될 수 있는 물리적인 특징을 갖고 있는 경우이다. 후자의 예로는 인간의 지문, 홍채 형태, 목소리 형태 등이 있다.

2.1.2 검출 감도에 따른 분류

불법적인 사용에 대한 핑거프린팅 방식의 검출 감도 수준에 따른 기준이다. 불법 복사에 대한 검출 감도에 따라서, 핑거프린팅을 완전, 통계적, 그리고 한계치 핑거프린트로 나뉜다. 완전(perfect) 핑거프린트는 핑거프린트된 컨텐츠에 핑거프린트를 인식할 수 없도록 변형을 가하는 경우에, 컨텐츠를 사용할 수 없게 만드는 방식이고, 통계적(statistical) 핑거프린트는 불법 복사된 컨텐츠가 아무리 많이 주어진다 할지라도 공모한 컨텐츠로부터 공모에 가담한 구매자를 식별할 수 있는 방식이다. 다음으로 한계치(threshold) 핑거프린트는 완전 핑거프린트와 통계적 핑거프린트를 혼합한 방식으로 한계치를 두어 한계치

이전까지의 불법적인 복사는 허용하지만 한계치 이후의 불법적인 복사에 대해서는 식별하는 방식이다.

2.1.3 핑거프린트 삽입 방법에 따른 분류

핑거프린트를 어떻게 삽입하는지에 따른 분류로서, 인식, 삭제, 첨가, 그리고 수정 형태로 삽입된다. 인식 형태는 컨텐츠의 부분에 존재하는 핑거프린트를 인식 및 기록하는 것으로 구성되는 방식이고, 삭제 형태는 원본 컨텐츠의 임의의 부분이 삭제되어 핑거프린트되는 방식이다. 첨가 형태는 원본 컨텐츠에 임의의 부분에 핑거프린트를 첨가하는 방식이고, 어떤 특정한 부분을 변화시키는 방식이 수정 형태이다

2.1.4 삽입되는 정보 형태에 따른 분류

핑거프린트 방식에 의하여 컨텐츠에 삽입된 핑거프린트의 특성에 따른 분류로서, 연속과 이산 핑거프린트가 있다. 생성된 핑거프린트가 불연속한 값을 갖는 경우가 이산(discrete) 핑거프린트이고, 연속적인 값을 갖는 경우가 연속(continuous) 핑거프린트이다. 대부분의 물리적 핑거프린트는 연속 핑거프린트에 포함된다.

2.1.5 식별정보 노출 수준에 따른 분류

이 분류 기준은 핑거프린트된 컨텐츠를 아는 개체가 누구인가에 따른 분류로서, 대칭 핑거프린팅과 비대칭 핑거프린팅이 있다. 핑거프린트된 컨텐츠를 판매자와 구매자 둘 다 알고 있는 경우가 대칭(symmetric) 핑거프린팅이고, 판매자는 알지 못하고 구매자만이 핑거프린트된 컨텐츠를 알게되는 경우가 비대칭 핑거프린팅이다.

2.2 핑거프린팅 시스템의 요구사항

핑거프린팅 시스템의 요구사항은 카피라이트 마킹에 포함되는 디지털 워터마킹 시스템의 요구사항과 비슷하지만 다른 몇 가지 요구사항이 부가적으로 필요하다. 이는 디지털 워터마킹이 소유권에 대한 인증기능만을 제시하는 반면에, 디지털 핑거프린팅은 소유권에 대한 인증뿐만 아니라 식별기능까지 제공하기 때문에 필요한 요구사항들이다.

2.2.1 공모 허용 오차

공모 허용 오차에 대한 요구사항은 핑거프린트를 불법적으로 재분배 받은 공격자에게 많은 컨텐츠가 주어지더라도, 공격자는 컨텐츠를 비교하여 핑거프린트를 찾거나 삭제할 수 없어야 하고, 새로운 핑거프린트를 생성할 수 없어야 한다는 요구사항이다.

2.2.2 컨텐츠 품질 허용 오차

컨텐츠 품질 허용 오차는 삽입된 마크들이 데이터의 유용성 또는 품질을 감소시키지 않아야 한다는 요구사항이다. 이는 핑거프린트를 삽입한 후에도 지각적으로 감지될 수 없도록 핑거프린트를 삽입하여야 한다.

2.2.3 컨텐츠 조작 허용 오차

컨텐츠 조작 허용 오차는 공격자가 컨텐츠를 변경한다 할지라도 너무 많은 잡음으로 인하여 컨텐츠를 사용할 수 없도록 만들지 못하도록 해야 함을 나타낸다. 이것은 공격자가 조작 공격을 컨텐츠에 가하더라도 핑거프린트를 컨텐츠에 존재하게 함으로서, 조작 후에도 컨텐츠로부터 핑거프린트를 추출하여 불법 복사자를 추적하기 위함이다.

Ⅲ. Domingo가 제안한 핑거프린팅 방식

최근의 연구들은 다양한 방법으로 핑거프린팅 방식의 기능성을 강화하고 있다. 대칭 핑거프린팅 방식의 경우 판매자와 구매자 모두가 핑거프린트된 데이터를 알고 있기 때문에, 제3자에게 누가 복사본을 만들어 재분배했는지를 증명할 수 없다는 문제점이 있다. 이를 해결하기 위해, Pfitzmann과 Schunter는 [5]에서 비대칭 핑거프린팅 방식을 제안하였다. Pfitzmann은 또한 비대칭 핑거프린팅 방식을 이용하여, 불법자 추적(traitor tracing) 방식을 제안하였고[6], 은닉 서명을 이용하여, 익명성을 제공하는 핑거프린팅 방식을 제안하였다[7]. 또한 Pfitzmann과 Sadeghi는 동전 던지기에 기반한 익명성을 제공하는 핑거프린팅 방식을 또한 제안했다[8].

익명성을 제공하는 핑거프린팅 방식은 판매자가 재분배자를 식별하기 위하여 추출된 핑거프린트를 이용하며, 등록센터와 상호작용을 통하여 재분배자를 식별하게된다. 이 경우에, 등록센터의 작업량이 증가되는 문제를 가지게 된다. Domingo는 이를 개선하여 판매자 스스로 재분배자를 자동식별하는 핑거프린팅 방식을 제안하였다[1].

3.1 시스템 설정

p를 소수 $q=(p-1)/2$를 만족하는 커다란 소수라

하자. G를 위수 $(p-1)$를 갖는 그룹이라 하고, g를 그룹 G의 원시원소라 하자.

구매자 B와 등록센터 R은 ElGamal 공개키와 비밀키 쌍을 갖는다[9]. 구매자 B의 비밀키는 x_B이고 공개키는 $y_B = g^{x_B} \bmod p$ 이다. 등록센터 R은 비밀키를 이용하여 인증서를 발급하고, 인증서는 등록센터의 공개키를 이용하여 검증된다. 모든 구매자들의 공개키는 알려지고 인증 되었다고 가정한다.

3.2 등록 프로토콜

구매자는 다음과 같은 순서로 등록센터에 등록하게된다.

먼저, 등록센터 R은 랜덤 비밀값 $x_r \in Z_p$를 선택하고, $y_r = g^{x_r} \bmod p$를 계산하여 구매자 B에게 y_r를 전송한다.

구매자 B는 $x_1 + x_2 = x_B$를 만족하는 랜덤한 비밀값 x_1, x_2를 선택하고, $S_1 = y_r^{x_1} \bmod p$와 $S_2 = y_r^{x_2} \bmod p$를 계산하여, 등록센터에 S_1과 S_2를 전송한다. 그러한 후에, 구매자 B는 자신이 x_1, x_2의 알고 있다는 사실을 영지식 증명을 이용하여 등록센터 R에 증명한다[10]. 구매자 B는 핑거프린팅에서 공개키로 사용할 $y_2 = g^{x_2} \bmod p$를 계산하여, 등록센터 R에게 전송한다. 핑거프린팅 프로토콜에서 S_1은 익명성을 제공하기 위한 인증 정보로 사용된다.

등록센터 R은 구매자 B로부터 받은 S_1, S_2이 $S_1 S_2 = y_B^{x_r}$를 만족하고, 익명성을 제공하는 공개키 y_2가 $y_2^{x_r} = S_2$를 만족하는지 검증한다. 2번의 검증이 성공한다면, 등록센터는 인증서 $Cert(S_1 \| y_r)$과 $Cert(S_2 \| y_r)$를 생성하고, 처음에 선택한 랜덤한 비밀값 x_r과 함께 인증서를 구매자 B에게 전송한다. [그림 1]은 등록 프로토콜을 도식화한 것이다.

이상의 과정을 반복 수행하여, 구매자 B는 인증서 쌍 (S_1, S_2)를 얻게된다.

3.3 핑거프린팅 프로토콜

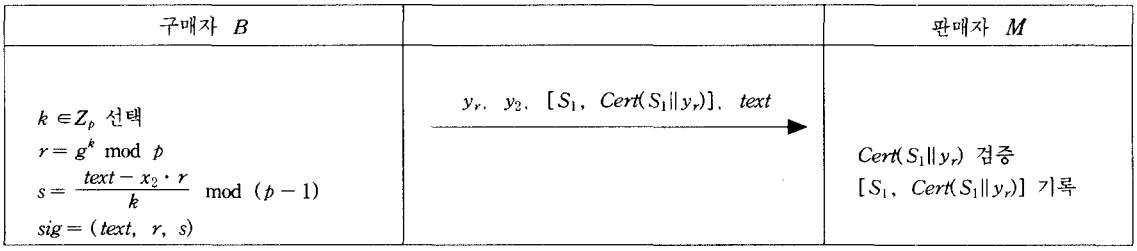
구매자 B는 디지털 컨텐츠를 구매하기 위하여 판매자와 핑거프린팅 프로토콜을 수행한다.

구매자는 y_r, y_2, $[S_1, Cert(S_1 \| y_r)]$ 그리고 구매하고자 하는 디지털 컨텐츠를 나타내는 문자열 *text*를 판매자 M에게 전송하고, *text*를 자신의 비밀키 x_2를 사용하여 ElGamal 서명 *sig*를 생성한다[9]. *sig*는 판매자 M에게 전송되지 않는다.

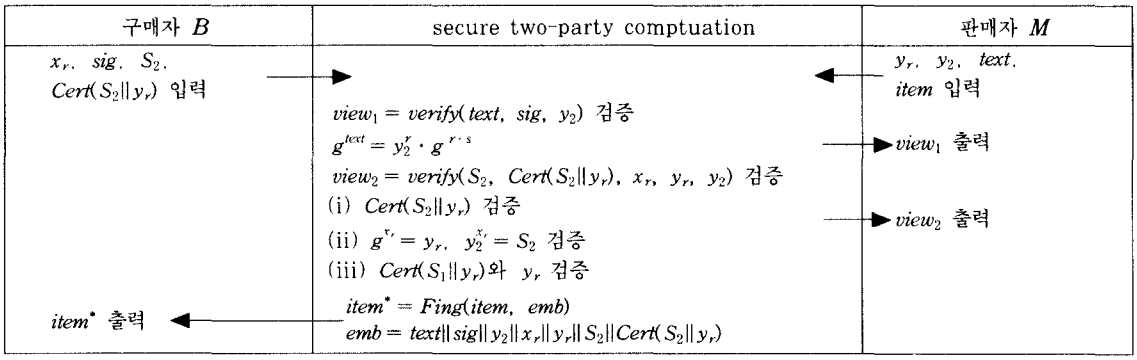
판매자 M은 구매자 B로부터 전송 받은 인증서 $Cert(S_1 \| y_r)$를 검증한다. [그림 2]는 구매자 인증 과정을 도식화 한 것이다. 검증이 성공할 경우에, 구매자 B와 판매자 M은 안전한 양자간 계산(two-party computation)를 수행한다. 판매자 M의 입력은 y_r, y_2, *text*와 구매자가 구매하고자 하는 디지털 컨텐츠 *item*이고, 구매자 B의 입력은 x_r, *sig*, S_2 그리고 인증서 $Cert(S_2 \| y_r)$이다. 안전한 양자간 계산(secure two-party computation)[11]은 다음과

등록센터 R		구매자 B
선택 $x_r \in Z_p$ $y_r = g^{x_r} \bmod p$를 계산		$y_B = g^{x_B} \bmod p$
	y_r →	$x_1 + x_2 = x_B \in Z_p$ 선택 $S_1 = y_r^{x_1} \bmod p$, $S_2 = y_r^{x_2} \bmod p$를 계산
	← S_1, S_2	
	(x_1, x_2를 알고 있음을 영지식으로 증명)	$y_2 = g^{x_2} \bmod p$
	← y_2	
$S_1 S_2 = y_B^{x_r}$ 검증, $y_2^{x_r} = S_2$ 검증 $Cert(S_1 \| y_r)$, $Cert(S_2 \| y_r)$ 생성		
	$Cert(S_1 \| y_r)$, $Cert(S_2 \| y_r)$, x_r →	(S_1, S_2)

[그림 1] Domingo's 등록 프로토콜



〔그림 2〕 Domingo's 핑거프린팅 프로토콜의 구매자 인증 과정



〔그림 3〕 Domingo's 안전한 양자간 계산(two-party computation)

같이 이루어진다.

먼저, $view_1 = verify(text, sig, y_2)$를 검증한다. $text$에 관한 서명 sig는 공개키 y_2를 사용하여 검증된다. 출력 $view_1$은 서명 검증이 성공하는 경우에, 판매자 M에게만 보여지는 불린(Boolean) 변수이다.

$view_2 = verify(S_2, Cert(S_2 \| y_r), x_r, y_r, y_2)$를 검증한다. 먼저, S_2에 관한 인증서를 검증하고 $g^{x_r} = y_r$ 그리고 $y_2^{x_r} = S_2$ 인지 검증하고 마지막으로 판매자에 의하여 이전에 검증된 S_1에 관한 인증서에서 y_r 값을 검증한다. 출력 $view_2$는 이전의 3가지 검증이 성공하는 경우에, 판매자 M에게만 보여지는 불린 변수이다.

$item^* = Fing(item, emb)$. 전통적인 핑거프린팅 알고리즘이 원본 컨텐츠 $item$에 emb를 삽입하기 위하여 사용된다. 여기서 emb는 다음과 같이 구성된다.

$$emb = text \| sig \| y_2 \| x_r \| y_r \| S_2 \| Cert(S_2 \| y_r)$$

핑거프린트된 정보 $item^*$는 구매자 B에게만 보여지고 출력으로서 주어진다.

이전의 안전한 양자간 계산에서, 판매자 M이 먼저 $view_1$과 $view_2$ 둘 다가 참이라면, 출력을 얻고 둘 중에 하나만 거짓이어도 구매자 B는 출력 $item^*$를 얻을 수 없다. 〔그림 3〕 양자간 계산을 도식화 한 것이다.

3.4 재분배자 식별 프로토콜

판매자 M은 재분배된 복사본이 발견된다면, 복사본으로부터 emb를 추출한다. 그리고 추출된 emb안에 y_r 값과 같은 인증서를 판매기록으로부터 찾아 식별 프로토콜에 들어간다. 식별 프로토콜은 다음과 같이 진행된다.

먼저, 익명성을 제공하는 공개키 y_2를 사용하여 $text$에 관한 서명 sig를 검증한다. y_r값은 인증서 S_1과 S_2에 관련된 값이다. 즉, 인증서의 일부분이기 때문에 변경될 수 없다. x_r값은 익명성 공개키 y_2의 소유자와 S_2의 소유자가 같다는 것을 증명한다. 이는 등록 프로토콜에서, 구매자 B가 $y_2^{x_r} = S_2$를 만족하는 y_2를 제공한 후에, 등록센터 R이 $\log_g y_r = x_r$를 구매자 B에게 제공했기 때문이다. 만약 Diffie-Hellman 키분배가 안전하면, 구매자 B는 $\log_g y_2 = x_2 = \log_{y_r} S_2$를 알지 못하고 정확한 y_2를 생성할 수 없다.

판매자 M은 재분배한 구매자를 식별하기 위하여, $S_1 S_2 = y_B^{x_r}$를 만족하는 공개키 y_B가 발견될 때까지 공개키 디렉토리의 공개키에 x_r 지수 연산을 수행한다. 이러한 연산을 수행한 후에, 부정직한 구매자 B가

식별된다. y_r이 인증되었기 때문에 x_r를 모르는 판매자 M은 y_r를 위조할 수 없고 구매자를 고발할 수 있게 된다.

Ⅳ. 제안하는 핑거프린팅 방식

앞 장에서 설명한 Domingo의 방식은 익명성을 제공하고 재분배자의 자동 식별을 제공한다는 장점이 있지만, 재분배자를 식별하는 과정에서 만족하는 공개키가 발견될 때까지 지수 연산을 반복해야 하므로, 평균 $N/2$번의 지수 연산을 요구한다는 단점이 있다. N은 공개키 디렉토리에 있는 공개키들의 수이다. 따라서, 본 논문에서는 1번의 지수 연산만으로 재분배자의 신분을 확인할 수 있는 효율적인 핑거프린팅 방식을 제안하고자 한다.

또한, 제안하는 방식은 구매자 등록과정이 2-pass 프로토콜로 구성되므로 4-pass 프로토콜인 Domingo 방식에 비해 통신 회수면에서도 효율적인 방식이다.

4.1 시스템 설정

시스템 설정은 Domingo가 제안한 방식 같다. p를 $p=2q+1$ (단, q는 큰 소수)를 만족하는 큰 소수라 하자. G를 위수 $(p-1)$를 갖는 그룹이라하고 g를 그룹 G의 원시원소라 하자.

구매자 B와 등록센터 R은 ElGamal 공개키와 비밀키 쌍을 갖는다. 구매자 B의 비밀키는 x_B이고 공개키는 $y_B=g^{x_B} \bmod p$ 이다. 등록센터 R은 비밀키를 이용하여 인증서를 발급하고, 인증서는 등록센터의 공개키를 가지고 검증된다. 모든 구매자들의 공개키는 알려지고 인증되었다고 가정한다.

4.2 등록 프로토콜

구매자 B는 $x_1 \cdot x_2 = x_B \pmod p$를 만족하는 비밀 랜덤값 x_1과 x_2를 선택한다. $t=g^{x_1} \bmod p$와 등록센터의 공개키 pk_R를 사용하여 x_2를 암호화한다. 암호화 결과는 $E_{pk_R}(x_2)$이다. t와 $E_{pk_R}(x_2)$을 등록센터 R에게 전송한다. 구매자 B는 비밀 랜덤값 x_1을 알고 있다는 것을 영지식 증명을 이용하여 등록센터 R에게 증명한다[10]. 여기서, Domingo 방식에서와 같은 구매자의 익명성을 제공하기 위한 공개키로 t가 사용된다.

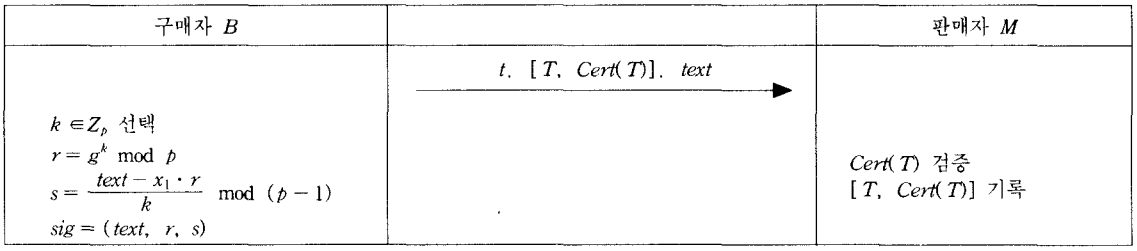
등록센터 R은 암호화된 $E_{pk_R}(x_2)$를 복호화 하여 x_2 얻고, t에 x_2 지수 연산을 하여, $t^{x_2} \bmod p = y_B$인지 검증한다. 검증이 성공하면, 랜덤값 $x_r \in Z_p$를 선택하고, $T=g^{x_2 \cdot x_r} \bmod p$를 계산한다. T는 핑거프린팅 프로토콜에서 구매자가 등록된 구매자를 나타내는 인증정보로 사용된다. 등록센터 R은 t와 T에 대한 인증서 $Cert(t\|x_r)$과 $Cert(T)$를 계산하여, 랜덤 비밀값 x_r과 함께 구매자 B에게 전송한다. 구매자 B는 등록센터 R로부터 전송받은 T와 x_r를 사용하여 $T=g^{x_2 \cdot x_r} \bmod p$를 검증한다. [그림 4]는 등록 프로토콜을 도식화 한 것이다. 이상의 과정을 반복적으로 수행함으로써, 구매자 B는 여러 개의 인증서 쌍 $(t,\ T)$을 얻게된다.

4.3 핑거프린팅 프로토콜

구매자 B는 판매자에게 자신의 정당한 사용자임을 밝

구매자 B		등록센터 R
$x_1 \cdot x_2 = x_B \in Z_p$ 선택 $t=g^{x_1} \bmod p$, $E_{pk_R}(x_2)$ 계산		
	$t=g^{x_1} \bmod p$, $E_{pk_R}(x_2)$ →	
		$D_{sk_R}(E_{pk_R}(x_2))=x_2$ 계산 $t^{x_2}=y_B$ 검증 $x_r \in Z_p$ 선택 $T=g^{x_2 \cdot x_r} \bmod p$ 계산 $Cert(t\|x_r)$, $Cert(T)$ 생성
	(x_1을 알고 있음을 영지식 증명)	
	← $Cert(t\|x_r)$, $Cert(T)$, x_r	
$T=g^{x_2 \cdot x_r} \bmod p$ 검증, $(t,\ T)$쌍 획득		

[그림 4] 제안하는 등록 프로토콜



〔그림 5〕 제안하는 핑거프린팅 프로토콜의 구매자 인증 과정

히기 위하여 등록센터로부터 받은 인증서 $[T, Cert(T)]$와 익명성을 제공하는 공개키 t, 그리고 구매자가 구매하고자하는 디지털 컨텐츠를 나타내는 문자열 *text*를 판매자에게 전송한다. 그리고 *text*에 관한 ElGamal 서명 *sig*를 비밀 랜덤값 x_1을 이용하여 생성한다.

판매자 M은 구매자 B로부터 전송 받은 인증서 $Cert(T)$를 등록센터의 공개키를 사용하여 검증한다. 〔그림 5〕는 구매자 인증과정을 도식화 한 것이다.

검증이 성공한다면, 구매자 B와 판매자 M은 안전한 양자간 계산(two-party computation)[11]을 수행한다. 안전한 양자간 계산은 다음과 같다. 판매자 M의 입력은 T, t, *text*와 구매자 B가 구매하고자 하는 원본 디지털 컨텐츠 *item*이고, 구매자 B의 입력은 x_r, x_2, *sig* 그리고 $Cert(t||x_r)$이다.

먼저, $view_1 = Verify(text, sig, t)$을 검증한다. 서명 *sig*는 구매자 B의 익명성을 제공하는 공개키 t를 사용하여 검증된다. 출력 $view_1$은 서명 검증이 성공할 경우에, 판매자 M에게만 보여지는 불린 변수이다.

두 번째로, $view_2 = Verify(t, Cert(t||x_r), x_2, x_r, T)$를 검증한다. 인증서 $Cert(t||x_r)$를 검증한다. 여기서는 구매자의 안전한 양자간 계산의 입력 값 중에서 x_r의 정당성도 검증된다. 즉, 인증서 안에 있는 x_r 값과 입력 값 x_r 이 같은지를 검증하는 단계도 포함된다. 그리고 구매자가 처음에 제공한 T가 정당한지를 $T = g^{x_2 \cdot x_r} \bmod p$를 검사한다. $view_2$는 이전의 인증서 검증과 T값 검증이 성공할경우에, 판매자 M에게만 보여지는 불린 변수이다.

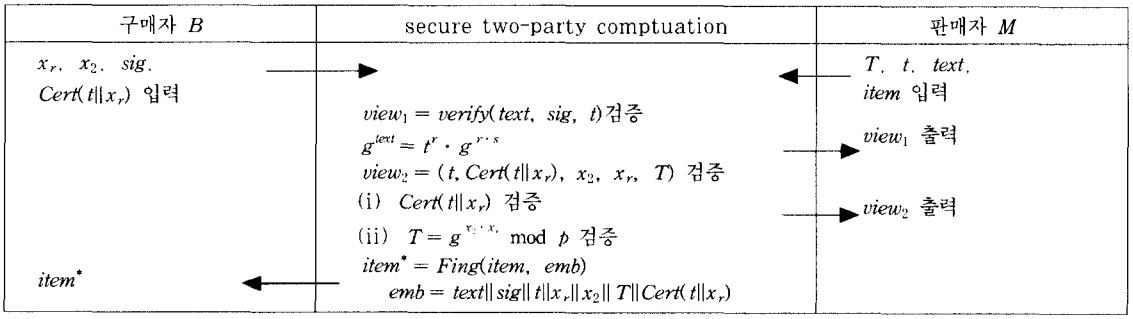
$item^* = Fing(item, emb)$은 핑거프린트 *emb*를 원본 컨텐츠 *item*에 삽입하여 $item^*$ 출력하는 알고리즘이다. 여기서도 Domingo의 방식과 마찬가지로, 전통적인 핑거프린팅 알고리즘이 원본 컨텐츠에 삽입정보 *emb*를 삽입하기 위하여 사용된다. 삽입 정보 *emb*는 다음과 같이 구성된다.

$$emb = text||sig||t||x_r||x_2||T||Cert(t||x_r)$$

핑거프린트된 정보 $item^*$는 구매자 B에게만 보여지고 출력으로 주어진다. 판매자 M은 $view_1$과 $view_2$ 둘 다가 참일 경우에, 먼저 출력으로 얻고 $item^*$는 출력으로 얻을 수 없다.

4.4 식별 프로토콜

판매자 M은 재분배된 복사본을 발견하게 되면, 복사본으로부터 *emb*를 추출하고, *emb* 안에 T값과 같은 인증서 $Cert(T)$를 판매기록으로부터 찾아, 이를 가지고 식별 프로토콜을 수행한다.



〔그림 6〕 제안하는 안전한 양자간 계산(two-party computation)

먼저, *text*에 관한 서명 *sig*를 익명성을 제공하는 공개키 t를 사용하여 검증한다. 등록센터가 만들어 준 x_r 값은 인증서 $Cert(T)$와 $Cert(t\|x_r)$의 일부분이기 때문에 위조될 수 없다.

x_2값은 익명성 공개키 t의 소유자와 T의 소유자가 같다는 것을 증명한다. 이것은 등록프로토콜에서 구매자가 먼저 x_2를 제공한 후에, 등록센터가 선택한 x_r을 이용하여, $T = g^{x_2 \cdot x_r}$를 생성했기 때문이다. 구매자 B가 새로운 $T = g^{x_2' \cdot x_r}$를 생성한다고 할지라도, 인증서 $Cert(T)$를 구성할 수 없기 때문에 안전하다. 따라서, 구매자 B는 정당한 T를 생성할 수 없다.

판매자 M은 재분배한 구매자 B를 식별하기 위하여 구매자의 익명성 공개키 t에 대하여 *emb*로부터 추출한 x_2를 지수 연산함으로써, 다음과 같은 *id*를 얻을 수 있다.

$$id = t^{x_2} \bmod p$$

따라서, 판매자는 식별된 *id*값과 같은 공개키 y_B를 공개키 디렉토리로부터 찾으면 된다. 즉, $id = y_B$이다. T와 t는 등록센터의 비밀키를 사용하여 인증 되었고, T와 t에 연관된 정당한 x_r를 판매자는 위조할 수 없다. 그래서, 공개키 y_B의 소유자를 재분배한 구매자로 고발할 수 있다.

V. 제안하는 방식의 안전성 분석 및 비교

이장에서는 등록 프로토콜의 안전성과 구매자의 익명성에 대한 안전성을 알아보고, Domingo 방식과 비교하여 본다.

제안하는 핑거프린팅 방식은 이산대수 문제에 기반하고 있다.

5.1 등록 프로토콜에서 안전성

등록 프로토콜은 구매자 B의 비밀키 x_B의 노출없이 구매자 인증을 제공한다.

등록센터 R은 등록 프로토콜에서 구매자가 전송한 t, x_2와 영지식 증명의 증거만을 알 수 있다. 영지식 증명은 어떠한 정보도 노출하지 않는다. 등록센터 R은 구매자 B의 비밀키 x_B를 알지 못하고, $t'^{x_2} = y_B$를 만족하는 t'를 찾을 수 없다. 구매자 B의 비밀키 x_B를 알지 못하는 공격자가 $t^{x_2} = y_B$를 만족하는 x_1를 계산할 수 있다면, 공격자는 이산대수 x_B를 계산할 수 있다. 만약 공격이 가능하다면, 이산대수 문제를 풀 수 있다. 일반적으로, 이산대수 문제는 푸는 다항식 시간 알고리즘이 존재하지 않기 때문에, 등록센터 R은 $t'^{x_2} = y_B$를 만족하는 t'를 만들 수 없다. 따라서, 등록 프로토콜은 정당한 구매자만이 성공할 수 있다.

5.2 구매자의 익명성

핑거프린팅 프로토콜에서, 판매자 M이 알고 있는 정보는 t, $[T, Cert(T)]$ 그리고 안전한 양자간 계산의 불린 변수 $view_1$과 $view_2$이다. 판매자 M이 구매자 B의 공개키 y_B를 알기 위해서는 x_2를 알아야 한다. 그러나, 만약 안전한 양자간 계산이 가능하다면, 판매자 M이 x_2를 알기 위한 유일한 방법은 인증서 $Cert(T)$를 통하여, $\log_g T$를 계산하여야 한다. 하지만, 이것도 등록 프로토콜의 안전성에서 설명한 바와 같이 $T = g^{x_2 \cdot x_r}$를 만족하는 이산대수 $x_2 \cdot x_r$를 계산하여야 한다. 그러나, 이산대수 문제를 푸는 다항식시간 알고리즘이 존재하지 않으므로, $x_2 \cdot x_r$를 계산할 수 없다. 따라서, 구매자의 익명성은 보장된다.

5.3 Domingo의 방식과 비교

계산량과 통신수의 관점에서, 이전의 프로토콜 중에서, 등록 프로토콜과 식별 프로토콜만 비교한다.

5.3.1 등록 프로토콜 비교

Domingo의 방식에서, 등록센터가 y_r값을 계산하면서 1번의 지수 연산이 필요하다. 구매자는 S_1과 S_2를 계산하면서 2번의 지수 연산이 필요하고, 익명성을 제공하기 위한 공개키 y_2를 생성하면서 1번의 지수 연산이 더 필요하다. 다시 등록센터는 $S_1 S_2 = y_B^{x_r}$를 검증하면서 1번의 지수 연산이 필요하고, $y_2^{x_r'} = S_2$를 검증하면서 1번의 지수 연산이 더 필요하다. 총 6회의 지수 연산이 필요하며 통신 회수는 4-pass이다.

제안하는 방식에서는 구매자가 t를 생성하면서, 1번의 지수 연산를 필요로 하고, x_2를 암호화 하면서 2번의 지수 연산이 필요하다. 등록센터는 x_2를 복호화 하면서 1번의 지수 연산을 필요로 하고, $t^{x_2} = y_B$를 검증하면서 1번의 지수 연산과 T를 생성하면서 1번의 지수 연산을 필요로 한다. 다시 구매자는 전송

〔표 2〕 Domingo 방식과 비교

프로토콜	비교 대상	Domingo's 방식	제안하는 방식
등록	지수 연산	6	7
	통신 수	4	2
식별	지수 연산	3+ $N/2$(평균)	3+1
	곱셈 연산	2	3
	비교 연산	$N/2$(평균)	$N/2$(평균)

받은 T값을 검증하는데 1번의 지수 연산을 필요로 한다. 총 7회의 지수연산이 필요하며 통신 회수는 2-pass이다.

따라서, 제안하는 방식의 등록 프로토콜은 Domingo가 제안한 방식보다 지수 연산은 1회 증가되었지만, 통신수는 2-pass로 간소화 되었다.

5.3.2 식별프로토콜 비교

Domingo의 방식에서, 서명 sig를 검증하기 위하여 2번의 지수 연산이 필요하고, x_r값이 정당성 검증을 위하여, $y_2^{x_r'} = S_2$, 1번의 지수 연산이 필요하고, 부정직한 구매자의 공개키 y_B를 찾기 위하여, 공개키 디렉토리에 있는 공개키의 수를 N이라 하면, 평균적으로 $N/2$번의 지수 연산이 추가로 필요하다.

제안하는 방식에서는 서명 sig를 검증하기 위하여 마찬가지로 2번의 지수 연산이 필요하고, x_2의정당성을 검증하기 위하여, $T = g^{x_2' \cdot x_1}$, 1번의 지수연산이 필요하고, 부정직한 구매자를 찾기 위하여, $t^{x_2} = id$ 단지 1번의 지수 연산만을 필요로한다.

따라서, 제안하는 방식은 Domingo가 제안한 방식보다 재분배자를 식별하는 과정이 평균적으로 ($N/2$-1) 번이 줄어들어 디지털 컨텐츠의 전자상거래시에 훨씬 효율적이다.

Ⅵ. 결 론

핑거프린팅은 디지털 컨텐츠에 식별 정보를 삽입하여 디지털 컨텐츠를 재분배하는 구매자를 식별하는 방법이다. 즉, 불법 복사는 가능하지만, 불법 복사가 발생한 후에 복사된 디지털 컨텐츠로부터 식별 정보를 추출하여 재분배한 구매자를 식별함으로써 구매자가 불법 복사하는 것을 방지하는 방식이다.

Domingo가 제안한 방식은 등록 프로토콜이 4-pass로 구성되어 있고 식별 프로토콜에서 평균적으로 공개키 디렉토리에 있는 공개키 수의 반에 달하는 연산을 한 후에 재분배자를 식별할 수 있는 단점이 있다. 이는 전자상거래에 적용할 경우 통신 회수와 계산량적인 면에서 매우 비효율적이다.

본 논문에서는 전자상거래에서 효율적으로 사용될 수 있도록 등록 프로토콜을 2-pass로 간소화하여 구성했고, 식별 프로토콜에서 지수 연산을 1번하여 재분배자를 식별하는 매우 효율적인 핑거프린팅 방식을 제안했다. 제안한 방식은 앞으로 전자상거래를 통하여 이미지, 오디오 그리고 동영상과 같은 디지털 컨텐츠의 전자상거래시에 구매자의 익명성을 보장하고, 판매자의 지적 소유권을 보호하는데 적용할 수 있을 것으로 기대되고, 이용가치가 무척 크다고 할 수 있다.

참 고 문 헌

〔1〕 J. Domingo-Ferrer, "Anonymous Fingerprinting of Electronic Information with Automatic Identification of Redistributors", Electronics Letters 34/13, pp. 1303~1304, 1998.

〔2〕 Peticolas, F. A. P., R. J. Anderson, and M. G. Kuhn, "Information Hiding-A Survey", Proceedings of the IEEE, Vol. 87, No. 7, pp. 1062~1078, 1999.

〔3〕 Chor, B., A. Fiat, and M. Naor, "Tracing Traitors", in Advances in Cryptology, Proceeding of CRYPTO '94, Vol. 839 of Lecture Notes in Computer Science, Springer-Verlag, pp. 257~270, 1994.

〔4〕 Katzenbeisser, S., Peticolas, F. A. P., "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House, 2000.

〔5〕 Pfitzmann, B., and M. Schunter, "Asymmetric Fingerprinting", in Advances in Cryptology, Proceedings of EUROCRYPT '96, Vol. 1070 of Lecture Notes in Computer Science, Springer-Verlag, pp. 84~95, 1996.

〔6〕 Pfitzmann, B., "Trials of Traced Traitors", in Information Hiding: First International Workshop, Proceedings, Vol. 1174

of Lecture Notes in Computer Science, Springer-Verlag, pp. 49~64, 1996.

[7] Pfitzmann, B., and M. Waidner, "Anonymous Fingerprinting", in Advances in Cryptology, Proceedings of EUROCRYPT '97, Vol. 1233 of Lecture Notes in Computer Science, Springer-Verlag, pp. 88~102, 1997.

[8] Pfitzmann, B., and A. Sadeghi, "Coin-Based Anonymous Fingerprinting", in Advances in Cryptology, Proceedings of EUROCRYPT '99, Vol. 1592 of Lecture Notes in Computer Science, Springer-Verlag, pp. 150~164, 1999.

[9] ElGamal, T., "A public-key cryptosystem and signature scheme based on discrete logarithms", IEEE Tran. Inf. Theory, IT-31, pp. 469~472, 1985.

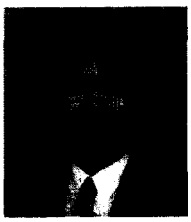
[10] Chaum, D., Evertse, J. H., and Van De Graaf, J., "An improved protocol for demonstrating possession of discrete logarithms and some generalization", in Advances in Cryptology, Proceedings of EUROCRYPT '87, Vol. 304 of Lecture Notes in Computer Science, Springer-Verlag, pp. 127~141, 1987.

[11] Chaum, D., Damgaard, I. B., and Van De Graaf, J., "Multiparty computation ensuring privacy of each party's input and correctness of the result", in Advances in Cryptology, Proceedings of CRYPTO '87, Vol. 293 of Lecture Notes in Computer Science, Springer-Verlag, pp. 87~119, 1987.

〈著者紹介〉

정 찬 주 (Chanjoo Chung)
1999년 2월 : 강남대학교 전자계산학과 졸업
1999년 3월~현재 : 성균관대학교 전기전자 및 컴퓨터공학부 석사과정
※ URL : http://dosan.skku.ac.kr/~cjchung

오 수 현 (Soohyun Oh)
1998년 2월 성균관대학교 정보공학과 졸업(공학사)
2000년 2월 성균관대학교 전기전자 및 컴퓨터 공학과 대학원 졸업(공학석사)
2000년 3월~현재 : 성균관대학교 전기전자 및 컴퓨터 공학과 박사 과정
※ URL : http://dosan.skku.ac.kr/~shoh



양 형 규 (Hyungkyu Yang)
1983년 2월 :성균관대학교 전자공학과 졸업(학사)
1985년 8월 :성균관대학교 전자공학과 석사(공학석사)
1994년 8월 :성균관대학교 정보공학과 박사(공학박사)
1984년 12월~1990년 2월 : 삼성전자 컴퓨터부문 선임연구원
1995년 3월~현재 :강남대학교 이공대학 전자계산학과전공 조교수
〈관심 분야〉 네트워크 보안, 암호화 프로토콜

원 동 호 (Dongho Won)
성균관대학교 전자공학과 졸업(학사, 석사, 박사)
1978년 4월~1980년 3월 : 한국전자통신연구소 연구원
1985년 9월~1986년 8월 : 일본 동경공대 객원 연구원
1996년 4월~1998년 4월 : 정보화 추진위원회 자문위원
1982년 3월~현재 : 성균관대학교 전기 전자 및 컴퓨터 공학부 교수
1999년~현재 : 한국통신정보보호학회 부회장
1999년~현재 : 성균관대학교 전기전자 및 컴퓨터공학부 학부장
1999년~현재 : 성균관대학교 정보통신대학원 원장
2000년 7월~현재 : 정보통신부 지정 정보보호 인증기술 연구센터 센터장
※ URL : http://dosan.skku.ac.kr/~dhwon
〈관심 분야〉 암호 이론, 정보 이론