情報保護學會論文誌
第14券 第3號, 2004. 6

공모 공격에 안전한 불확정 전송 프로토콜 기반의 디지털 핑거프린팅 기법*

최 재 귀[a)†], 박 지 환[a)‡], 김 태 석[b)]
부경대학교[a)], 동의대학교[b)]

Secure Oblivious Transfer Protocol-based Digital Fingerprinting Against Conspiracy Attack

Jae-Gwi Choi[a)†], Ji-Hwan Park[a)‡], Tai-Suk Kim[b)]
Pukyong National University[a)], DongEui University[b)]

요 약

디지털 핑거프린팅(digital fingerprinting)은 멀티미디어 컨텐츠에 구매자의 정보를 삽입함으로 컨텐츠를 불법적으로 재분배하는 부정자를 추적하는 방법이다. Domingo가 최초로 제안한 COT(committed oblivious transfer) 기반의 핑거프린팅 방식은 핑거프린팅 단계의 계산적 복잡도를 완전히 분석하여 기존의 MDPK(minimum disclosure proof of knowledge)나 SMPC(secure multi-party computation)등에 기반한 방식들에 비해 구현 가능성을 높였다는 의의를 지닌다. 그러나 이 방식은 판매자의 부정에 안전하지 못하다는 문제점이 있다. 본 논문에서는 첫째, 두 가지 COT기반의 디지털 핑거프린팅 방식의 문제점을 지적하고, 둘째, 이것의 해결을 위해 이중 잠금 암호(two-lock cryptosystem) 시스템을 사용한 불확정 전송 프로토콜 기반의 디지털 핑거프린팅 기법을 제안한다. 제안방식은 기존의 COT 기반 방식에서 안전성과 식별 단계의 효율성을 개선하였다.

ABSTRACT

Digital fingerprinting schemes are cryptographic methods that a seller can identify a traitor who illegally redistributed digital contents by embedding it into buyer's information. Recently, Josep Domingo-Ferrer suggested an anonymous digital fingerprinting scheme based on committed oblivious transfer protocol. It is significant in the sense that it is completely specified from a computation point of view and is thus readily implementable. But this scheme has the serious problem that it cannot provide the security of buyers. In this paper, we first show how to break the existing committed oblivious transfer-based fingerprinting schemes and then suggest secure fingerprinting scheme by introducing oblivious transfer protocol with two-lock cryptosystem based on discrete logarithm. All computations are performed efficiently and the security degree is strengthened in our proposal.

Keywords : *Digital fingerprinting, conspiracy attack, oblivious transfer, two-lock cryptosystem*

Ⅰ. 서 론

네트워크를 이용한 정보의 공유가 증대되고 있는 상황에서 불법 복사와 같은 행위로부터 저작권자의

접수일 : 2004년 4월 19일 ; 채택일 : 2004년 6월 5일
† 주저자 : jae@mail1.pknu.ac.kr
‡ 교신저자 : jpark@pknu.ac.kr

권리를 보호하고 건전한 정보 사회를 창출하기 위해 정보 보호의 중요성이 한층 증대되고 있다. 지금까지 정보보호를 위한 방법으로 이용되어 온 데이터의 암호화는 디지털 데이터에 대한 접근은 어느 정도 제한할 수 있었으나, 불법 배포로 인한 저작권(copyright) 침해는 해결할 수 없었다. 이러한 제한적인 암호화 방식을 보완하기 위하여 컨텐츠 자체에 구매자가 인지할 수 없도록 저작권 정보를 삽입하는 디지털 워터마킹(digital watermarking)이 연구되어졌다. 디지털 워터마킹 기법은 인간의 의식 체계 또는 감지 능력으로는 검출할 수 없게 저작권자 또는 판매자의 정보를 멀티미디어 컨텐츠 내에 삽입해 둠으로써 이후에 발생하게 될 지적 재산권 분쟁에서 정당함을 증명하는 데 사용되어진다. 그러나 만약 불법적으로 배포되고 있는 디지털 컨텐츠를 발견하였을 때, 디지털 워터마킹 기법을 사용한 컨텐츠의 저작권자나 판매자는 누구인지 알 수 있지만, 누가 불법적으로 배포하였는지는 알 수가 없다. 그래서 새롭게 연구된 분야가 디지털 핑거프린팅(digital fingerprinting)이다. 디지털 핑거프린팅은 기밀 정보를 디지털 컨텐츠에 삽입하는 측면에서는 디지털 워터마킹과 동일하나, 삽입 정보의 내용에 있어서는 다르다. 디지털 워터마킹이 저작권자나 판매자의 정보가 삽입되는 반면, 디지털 핑거프린팅은 디지털 컨텐츠를 구매하는 사용자의 정보가 삽입되는 것이다. 따라서 디지털 워터마킹을 사용하였을 때는 하나의 컨텐츠에 삽입되는 정보가 동일한 반면, 핑거프린팅을 사용하였을 때는 조금씩 다른 정보가 삽입된다. 따라서 핑거프린팅 기술이 적용된 컨텐츠가 불법적으로 배포된다면, 해당 컨텐츠 내에서 핑거프린팅된 정보를 추출하여 어떤 구매자에게 판매된 컨텐츠임을 식별할 수 있으므로 법적인 조치를 가할 수 있게 된다. 이러한 핑거프린팅 기술은 소유권에 대한 인증뿐만 아니라 개인 식별까지 제공해야 하므로 기존의 워터마킹이 갖춰야 할 요구사항인 비가시성, 견고성, 유일성과 더불어 공모 허용, 비대칭성, 익명성, 조건부 추적성들이 부가적으로 필요하게 된다.

최근의 핑거프린팅에 대한 연구는 공모 (collusion)에 대한 방지를 효과적으로 구현하는 공모 보안 코드에 관한 연구와 계산량과 안전성을 개선하여 디지털 핑거프린팅의 실현 가능성을 높이는 연구에 중점을 두고 진행되고 있다. 특히 Domingo가 처음으로 제안한 COT(committed oblivious transfer) 기반의 핑거프린팅 방식[1]은 기존의 MDPK(minimum disclosure proof of knowledge)나 SMPC(secure multi-party computation) 또는 일반적인 영지식 증명 프로토콜을 이용하던 핑거프린팅 프로토콜에서 명확히 분석하지 못했던 계산적 복잡도를 완전 분석함으로 핑거프린팅의 실현 가능성을 보여주었다. 그 후, Sadeghi등에 의해 Domingo방식의 문제점이 지적되고, 개선되어졌으나, 이 방식 또한 구매자의 부정에 안전하지 못하다는 단점이 있다[2]. 본 논문에서는 두 가지 COT 기반의 핑거프린팅 방식[1][2]의 문제점을 지적하고, 새로운 해결 방안을 제시하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서 COT기반의 방식에 대하여 알아보고, 이의 안전성을 분석한다. 3장에서는 제안 방식의 방법론과 프로토콜에 대해 기술하고, 4장에서 제안 방식의 안전성 및 특성을 비교·분석하고 끝으로 5장에서 결론을 내리고자 한다.

II. COT 기반의 디지털 핑거프린팅

구매자의 익명성을 보장하는 익명 핑거프린팅 기법은 Pfitzmann등에 의해 처음으로 제시된 후, 그룹 서명, verifiable encryption등의 다양한 방법을 사용하여 그 기능성을 강화하는 방식들이 제안되어졌다[3][4][5]. 이는 비대칭형 핑거프린팅 개념을 포함하는 방식으로 판매자는 구매자에게 컨텐츠를 판매하지만, 프로토콜 진행과정에서 구매자의 신원을 알지 못하도록 하는 기법이다. 그러나 대부분의 익명 핑거프린팅 방식은 핑거프린팅 단계에서 이산 대수 문제 또는 그래프 동형 문제와 같은 어려운 문제에 기반한 MDPK나 SMPC 프로토콜을 블랙박스 형태로 삽입하여 구현함으로 높은 계산적 복잡도를 가지는 단점이 있다. 일반적으로 워터마킹은 미리 오프라인에서 계산한 후, 판매할 때 워터마킹된 컨텐츠를 제공하면 된다. 이에 반해 핑거프린팅의 경우에는 구매자마다 삽입 정보가 달라지므로 임의의 구매자가 인터넷상으로 판매자의 서버에 접속하여 실시간으로 핑거프린팅 프로토콜을 거쳐야 판매가 이루어지므로 복잡도가 높은 계산은 실제 구현에 불합리하다. 아래에 기술할 COT기반의 핑거프린팅 방식은 등록단계에서는 기존의 방식을 그대로 유지하나, 계산적 복잡도가 가장 높은 핑거프린팅 단계에서 명백하게 계산적 복잡도가 분석되어 있는 COT를 사용하였기 때문에 익명 핑거프린팅 프로토콜의 실제 적용 가능성을

높였다고 평가된다. 본 장에서는 제안 방식의 기초가 되는 Doming방식[1]과 이를 개선한 Sadeghi방식[2]에 대해 알아본다.

2.1 Domingo-Ferrer 방식[1]

Step1. 시스템 초기화

n비트 길이의 디지털 컨텐츠를 $content$라 표기한다.

(1) 판매자는 $content$의 각 비트($content_i$)에 2가지 version(marked version과 unmarked version)을 준비한다. 이를 각각 $content_i^0$, $content_i^1$이라 표기한다.

(2) 판매자는 XOR속성의 bit commitment를 사용하여 $content_i^0$,$content_i^1$의 출력 값으로 com_i^0, com_i^1를 만들어 둔다.

Step2. 구매자 등록

(1) 등록 센터는 랜덤 값 x_r를 선택한 후, $y_r = g^{x_r}$를 구매자에게 전달한다.

(2) 구매자는 비밀 값 s_1, s_2를 선택한 후 식(1)과 같이 S_1, S_2를 계산하여 등록 센터에 보내고, 영지식 증명을 통해 x_1, x_2를 알고 있음을 등록 센터에게 증명한다. 여기서 x_B는 구매자의 비밀키이고, $y_B = g^{x_B}(modp)$는 이에 대응되는 공개키이다.

$$s_1 + s_2 = x_B(modp),\ S_1 = y_r^{s_1}, S_2 = y_r^{s_2} \quad (1)$$

(3) 구매자는 y_1 ($y_1 = g^{s_1}$)을 계산하여 등록 센터에 보낸다.

(4) 등록 센터는 식(2)처럼 구매자로부터 받은 정보를 검증하고, 식이 검증되면 인증서 $Cert(y_1)$를 생성하여 구매자에게 보내준다.

$$S_1 S_2 = y_B^{x_r},\ y_1^{x_r} = S_1 \quad (2)$$

Step3. 핑거프린팅

(1) 컨텐츠의 각 비트별로 판매자와 구매자는 COT 프로토콜을 수행하는데, 이 때 판매자는 입력 값으로 com_i^0,com_i^1을 넣고, 구매자는 그 중 하나를 가지게 된다. COT 프로토콜을 수행함으로 판매자는 구매자에게 어떤 컨텐츠가 선택되어 전달되었는지 알 수 없고, 구매자 역시 자신이 받지 않은 다른 컨텐츠는 알 수 없게 된다.

(2) 구매자는 선택한 값을 다시 commitment하고, 이 값과 자신의 비밀키 s_1으로 서명한 값을 판매자에게 보낸다.

Step4. 식별

불법 배포된 컨텐츠 $content^{red}$가 발견되었다면

(1) 판매자는 $content^{red}$와 관련된 컨텐츠에 해당하는 모든 서명된 commitment 값을 검색한 후, 해당 구매자를 찾는다. 이 때의 구매자는 익명 구매자이므로 판매자는 등록 센터의 도움을 얻는다.

(2) 부정자가 식별될 때까지 해당 컨텐츠를 구매한 모든 구매자에게 구매자의 commitment값의 공개를 요구한다.

(3) 공개된 컨텐츠와 $content^{red}$의 각 비트가 일정 수준 이상 일치하면 해당 구매자를 부정자로 추적한다. 이 때, 공개할 비트의 위치 선정은 동전 던지기 프로토콜을 이용한다.

2.2 Sadeghi 방식[2]

Sadeghi방식은 Domingo방식에서 COT 프로토콜을 수행할 때 판매자의 부정에 대한 가능성을 지적하였으며, 이에 대한 해결책을 제시하였다. Sadeghi 등이 지적한 Domingo 방식의 가장 큰 문제는 COT 프로토콜을 수행할 때, 만약 판매자가 서로 다른 2개의 값 즉 com_i^0,com_i^1 ($content_i^0$,$content_i^1$)을 입력하지 않고, 같은 값을 입력한다면 판매자는 구매자에게 어떤 컨텐츠가 전달되었는지 쉽게 알 수 있다는 것이다.

이에 대한 해결책으로 Sadeghi등은 핑거프린팅 단계에서 구매자가 판매자에게 특정 비트들에 대해서는 2개의 commitment값 모두를 요구하도록 하였다. Sadeghi방식은 핑거프린팅 단계를 제외한 나머지 단계에서는 Domingo의 방식을 그대로 유지하나, 핑거프린팅 단계에서 판매자의 입력 값을 요구함으로 판매자의 동일한 값 입력이라는 부정을 방지하고자 하였다.

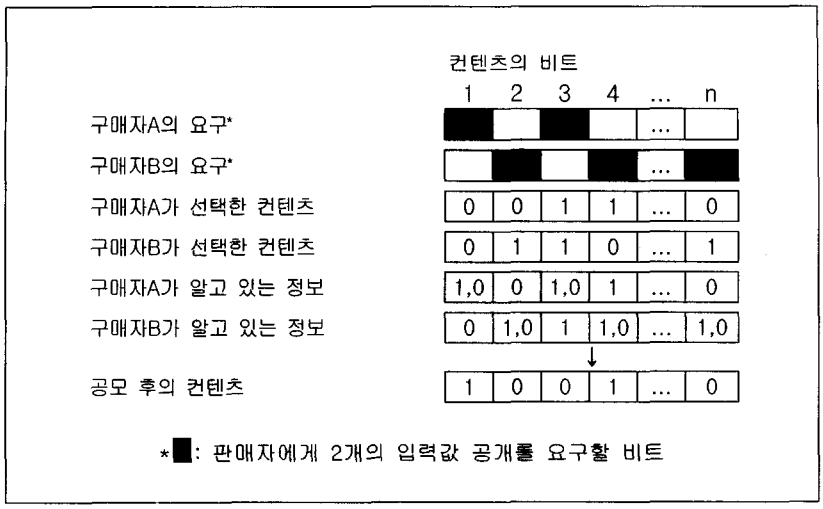


그림 1. 공격자 A, B에 의한 공모 공격(conspiracy attack)

2.3 COT 기반 핑거프린팅 방식의 분석

2.3.1 Domingo-Ferrer방식 분석

이 방식은 판매자가 컨텐츠의 각 비트마다 서로 다른 2개의 비트를 준비하고, 이를 COT의 입력 값으로 설정함으로써 판매자는 후에 구매자가 어떤 비트를 선택하는 지 알 수 없도록 하고, 구매자는 자신이 선택한 정보 이외는 알 수 없도록 하여 핑거프린팅의 비대칭을 제공한 방식이다. 그러나 이 방식은 Sadeghi방식에서 지적되었듯이 COT프로토콜을 수행할 때 판매자가 2개의 입력 값을 같은 값으로 한다면, 판매자는 구매자가 어떤 컨텐츠를 선택하는 지를 쉽게 알 수 있으므로 프로토콜의 안전성에 큰 취약점을 가지게 된다. 또한 식별단계가 비효율적이라는 문제와 핑거프린팅 수행시 컨텐츠의 비트 수만큼 COT를 수행해야 하는 통신량의 문제도 여전히 남아 있다. 실제로 식별 단계에서는 해당 컨텐츠를 구매한 다수의 구매자들 각각에 대해서 모두 식별 프로토콜을 진행해야 하는 비효율성을 지니고 있다.

2.3.2 Sadeghi 방식의 분석

Sadeghi방식은 Domingo방식에서 판매자의 부정을 방지하기 위해 판매자로 하여금 컨텐츠의 일부 비트에 대한 2개의 commitment값을 공개하도록 하였다. 그러나 이 해결 방법은 역으로 구매자의 부정을 가능하도록 만들고 있다. 다음의 상황을 고려해 보자. 만약 구매자 A와 구매자 B가 공모하여, 같은 컨텐츠에서 구매자 A는 판매자에게 홀수 비트를, 구매자 B는 짝수 비트의 공개를 요구한다면, 구매자 A는 홀수 비트의 모든 정보를 알 수 있고, 구매자 B는 짝수 비트의 모든 정보를 알 수 있게 되어, 공모한 구매자는 자신들이 소유하지 않은 다른 컨텐츠를 생성할 수 있게 된다. 그리고 이 컨텐츠를 불법 배포할 경우에는 어떤 부정자(traitor)도 추적할 수 없게 되든지 아니면 다른 정직한 구매자가 부정자로 식별되어질 것이다. 본 논문에서는 이러한 공격 방법을 기존의 '공모 공격(collusion attack)'[2]과 같은 결과를 가지나, 방법적인 차이가 존재하므로 또 다른 '공모공격(conspiracy attack)'이라 명시한다. 만약 판매자에게 요구할 수 있는 비트 수가 적다면, 더 많은 공모자의 참여로 공모 공격을 성공할 수 있을 것이다. 그림 1은 2명의 공격자의 공모 방법을 나타낸다.

III. 제안 방식

3.1 Two-Lock 암호체계를 이용한 불확정 전송 프로토콜

본 논문에서는 기존의 COT방식에서 가능한 판매자와 구매자의 부정을 방지하기 위해 이산 대수 문제

1) 공격자는 여러 개의 컨텐츠를 비교하여 핑거프린팅 위치가 파악되면, 핑거프린팅 비트를 지운다든지 아니면 전혀 상관없는 핑거프린팅 비트를 만들어 삽입하여 컨텐츠를 재구성하여 이를 배포할 수 있게 된다. 이러한 공격을 '공모공격(collusion attack)'이라 부른다[6].

에 기반한 two-lock 암호 시스템을 이용한 불확정 전송 프로토콜을 사용한다[7]. 아래에 two-lock 암호 시스템을 이용한 불확정 전송 프로토콜에 대해 간략히 기술한다.

(1) Alice→Bob:
$Y_1 = A_k(m_1), ..., Y_n = A_k(m_n)$

(2) Bob→Alice:
$Z_1 = B_{s_1}(Y_i), ..., Z_t = B_{s_t}(Y_{i+t-1})$

(3) Alice→Bob:
$C_1 = A_k^{-1}(Z_1), ..., C_t = A_k^{-1}(Z_t)$

(4) Bob:
$m_i = B_{s_1}^{-1}(Y_i), ..., m_t = B_{s_t}^{-1}(Y_t)$

Alice의 n개의 비밀 값 $m_1, m_2, ..., m_n$ 중에 Bob은 t개만 알 수 있게 되고, Alice는 Bob이 어떤 값들을 선택하였는지 알 수 없다. 여기에서 $A_k(.), B_s(.)$는 키 k, s를 이용한 암호 알고리즘이고, $A_k^{-1}(.), B_s^{-1}(.)$는 $A_k(.), B_s(.)$의 복호 알고리즘이다. 특히 알고리즘 A와 B가 같은 경우를 commutative 속성 암호 알고리즘이라고 한다.

위 방식은 Alice가 불확정 전송 프로토콜 수행시 같은 입력 값을 넣었는지 아닌지, Bob이 확인할 수 있으므로 제안 방식에서는 핑거프린팅 단계에서 이 프로토콜을 사용한다.

3.2 불확정 전송 프로토콜 기반의 디지털 핑거프린팅 방식 제안

[매개변수 및 시스템 설정]

- G : 위수 $p-1$를 갖는 그룹
- p : $q=(p-1)/2$를 갖는 그룹
- g : 그룹 G의 원시 원소
- $F=\{F_0, F_1, ..., F_t\}$: $F_i=\{f_{i_1}, f_{i_2}, ..., f_{i_k}\}$ 인 핑거프린트
- $content$: 컨텐츠
- $content_i^*$: F_i가 삽입된 컨텐츠
- $A_a(.), B_b(.)$: 키 a, b를 이용한 암호 알고리즘
- $A_a^{-1}(.), B_b^{-1}(.)$: $A_a(.), B_b(.)$에 대한 복호 알고리즘
- x_B/y_B : 구매자의 비밀키/공개키
- $Alcie, Bob, Ron$: 판매자, 구매자, 등록(신뢰) 센터

Step1. 등록 (Registration)

(1) Bob은 $x_1 \cdot x_2 = x_B$를 만족하는 랜덤 값 x_1, x_2를 선택한 후, $y_B, y_B^*(=g^{x_1})$와 Ron의 공개키로 암호화한 $A_{y_{Ron}}(x_2)$을 Ron에게 보내고, 영지식 증명을 통해 자신이 x_1을 소유하고 있음을 Ron에게 증명한다.

(2) Ron은 식(3)과 같이 Bob에게 받은 정보를 확인하고, 식이 검증되면 인증서 $Cert(y_B^*)$를 생성하여 Bob에게 보내준다.

$$y_B = (y_B^*)^{x_2} \tag{3}$$

Step2. 핑거프린팅 (Fingerprinting)

(1) Bob은 구매하고자 하는 컨텐츠에 대한 내용과 자신의 인증서 $Cert(y_B^*)$를 $Alice$에게 보낸다.

(2) Bob의 인증서가 검증되면, $Alice$는 n개의 핑거프린트 $F_0, F_1, ..., F_{n-1}$를 생성하여 각 핑거프린트를 삽입한 n개의 복사본 $content_i^*$ $(i=\{0,1,...,n-1\})$을 만든다. 이 때 핑거프린팅(워터마킹) 알고리즘은 공모 공격(collusion attack)에 안전하다고 평가된[8] Cox의 방식[9]을 사용한다. $Alice$은 자신의 레코드에 y_B^*, $Cert(y_B^*)$와 $F_0, F_1, ..., F_{n-1}$를 저장해두고, Bob과 다음 단계를 수행한다.

(3) $Alice$는 핑거프린트된 n개의 컨텐츠를 k를 이용하여 식(4)와 같이 암호화하여 보낸다. 이 때, 판매자는 구매자가 어떤 값을 선택하였는지 $\frac{1}{n}$의 확률로 알 수 있다.

$$\begin{aligned} Y_0 &= A_k(content_o^*), ..., \\ Y_{n-1} &= A_k(content_{n-1}^*) \end{aligned} \tag{4}$$

(4) *Bob*은 이 n개 중에서 하나를 선택하고, 랜덤 값 s를 선택한 후, 이것을 식(5)와 같이 재 암호화하여 다시 *Alice*에게 보낸다. 이 때, *Bob*이 선택한 값이 재 암호화되어 *Alice*에게 전달되므로 *Alice*는 *Bob*이 어떤 컨텐츠를 선택하였는지 알 수 없다. 여기에서는 *Bob*이 Y_2를 선택했다고 가정하자.

$$Z = B_s(Y_2) \tag{5}$$

(5) *Alice*는 Z를 자신의 레코드 내 *Bob*의 필드에 저장해두고 C를 *Bob*에게 재전송한다.

$$C = A_k^{-1}(Z) \tag{6}$$

(6) *Bob*은 식(7)과 같이 C를 복호한 후 컨텐츠 $(content_2^*)$를 이용한다.

$$\begin{aligned} content_2^* &= B_s^{-1}(C) = B_s^{-1}(A_k^{-1}(Z)) \\ &= B_s^{-1}(A_k^{-1}(B_s(Y_2)) \\ &= B_s^{-1}(B_s(content_2^*)) \\ &= content_2^* \end{aligned} \tag{7}$$

Step3. 식별 (Identification)

불법 배포된 컨텐츠 $content^{red}$가 발견되면

(1) *Alice*는 핑거프린팅(워터마킹) 추출 알고리즘을 통해 삽입된 정보를 추출한다. $content^{red}$에서 추출된 정보를 F_{red}라 두면, 자신의 레코드에 저장된 핑거프린트에서 F_{red}와 가장 상관계수가 높은 구매자 필드를 검색한 후, 해당 필드안의 구매자의 인증서와 (익명)공개키, 핑거프린트, Z와 불법 배포된 $content^{red}$를 재판관에게 보낸다.

(2) 재판관은 *Alice*에게 받은 정보에서 F_{red}와 해당 구매자의 핑거프린트의 상관도를 확인하고, 이것이 확인되면 *Ron*에게 해당 구매자의 신원을 요청한다. 이 구매자가 불법 배포자(traitor)로 식별된다.

(3) 만약 불법 배포자로 식별된 구매자가 재판관의 판단에 이의가 있을 경우, 자신의 컨텐츠 또는 Y_i를 재판관에게 보내어 여기에서 검출된 F_i와 F_{red}의 상관관계, 그리고 판매자의 레코드 내 자신의 필드에 저장된 핑거프린트 내에 F_i가 존재하는 지를 조사한다. 만약 불법 배포자로 식별된 구매자가 보내온 정보와 *Alice*가 보내온 정보가 같지 않다면 해당 구매자는 불법 배포에 대한 책임을 질 필요가 없으며, 그렇지 않다면 불법 배포자로 재확인 식별된다.

Ⅳ. 제안 방식의 고찰

4.1 제안 방식의 특성 및 안전성 분석

■ 익명성(Anonymity)

제안 방식에서는 기존의 익명 핑거프린팅의 방식에서처럼 등록 센터(*Ron*)는 정직한 구매자의 신원을 어떤 누구에게도 노출시키지 않는다는 가정을 둔다. 제안 방식의 핑거프린팅 단계에서 판매자가 구매자에 대해 알고 있는 것은 구매자의 (익명)공개키 y_B^* 에 관한 정보뿐이다. x_2 역시 등록 센터의 공개키로 암호화되어서 전송되므로 이산대수 문제를 풀지 않고서는 판매자는 구매자의 신원을 전혀 알 수 없으므로 제안 방식은 구매자의 익명성을 보장한다.

■ 비연결성(Unlinkability)

익명의 구매자라도 같은 공개키 (y_B^*)를 이용하여 컨텐츠를 계속 구매한다면, 공개키 y_B^*와 구매한 컨텐츠간에는 연결성이 존재하게 되는데, 제안 방식에서는 구매자가 컨텐츠를 살 때마다 등록 프로토콜을 수행하므로 익명의 구매자와 컨텐츠 간에는 어떤 연결성도 존재하지 않는다.

■ 추적성(Traceability)

제안 방식에 사용되는 암호 알고리즘 및 핑거프린팅(워터마킹) 알고리즘은 안전하다는 가정을 두고 있다. 따라서 구매자는 자신의 컨텐츠에 삽입된 정보를 아무 의미가 없도록 변경하거나 추출할 수 없으므로, 판매자는 불법 배포된 컨텐츠 내에서 특정 구매자를 규정할 수 있는 핑거프린트 정보를 높은 확률로 추출할 수 있다.

■ 위조 불가(No Framing)

구매자의 특정 핑거프린트 F_i가 삽입된 컨텐츠를 알기 위해서, 판매자는 반드시 구매자의 비밀키 s를

알거나, 구매자가 선택한 컨텐츠(핑거프린팅된 컨텐츠)를 알아야 한다. 제안 방식에서는 구매자만이 자신의 비밀키 s를 알고 있으며, two-lock 암호 시스템을 이용한 불확정 전송 프로토콜 수행함으로 판매자 역시 구매자가 어떤 핑거프린트를 선택하였는지 알 수 없다. 따라서 정직한 구매자는 불법 배포자로 식별되지 않으며, 구매자 이외의 다른 사람들은 구매자와 똑같은 컨텐츠를 생성할 수 없다.

■ 부인 불가(No Repudiation)

불법 배포자로 식별된 구매자는 해당 컨텐츠($content_{red}$)가 자신이 아닌 판매자 혹은 다른 사람이 배포하였다고 주장할 수 없다. 왜냐하면 해당 구매자만이 비밀키 s와 자신만의 핑거프린트된 컨텐츠를 알고 있으므로 다른 사람들은 그 컨텐츠를 생성할 수 없기 때문이다. 아울러 구매자는 핑거프린팅 단계에서 판매자가 n개의 입력 값으로 동일한 값을 넣지 않았음을 확인할 수 있으므로, 구매자의 부인은 허용되지 않는다.

■ 공모 공격 안전성(Collusion Tolerance)

공모 공격(collusion attack)에 안전하기 위해서 제안 방식에서는 핑거프린팅(워터마킹) 알고리즘으로 공모 공격(collusion attack)에 강인하다고 평가된 Cox의 알고리즘[9]을 사용한다.

4.2 기존 방식과의 비교 분석

Domingo방식[1]이 판매자의 부정에, Sadeghi방식[2]이 구매자의 공모 공격(conspiracy attack)에 안전하지 못한 반면, 제안 방식은 판매자의 부정과 구매자의 공모 공격(conspiracy attack)에 안전하다. 따라서 전자의 방식들[1][2]에서는 판매자의 위조와 구매자의 부인이 가능한 반면 제안 방식은 위조와 부인이 불가능하다. 또한 Domingo방식은 공모 보안 코드(C-secure code)[6]를 사용하지 않아, 공모 공격(collusion attack)에 약하고, Sadeghi방식 역시 이에 대한 해결책을 제시하지 못한 반면 제안 방식은 Cox의 알고리즘[9]을 이용함으로 공모 공격에 대한 안전성을 추가하였다.

그리고 불법 배포자를 추적하기 위해 2가지의 방식에서는 모든 구매자(불법 배포된 컨텐츠와 같은 컨텐츠를 구매한)가 식별 단계를 수행해야 되나, 제안 방식은 판매자와 등록센터, 분쟁이 발생할 시 해당 구매자만이 참여하면 되므로 식별 과정의 비효율성도 개선하였다. 표 1은 제안 방식과 기존 방식과의 특성을 비교한 것이다.

V. 결 론

COT(committed oblivious transfer) 기반의 핑거프린팅 방식은 핑거프린팅 단계의 계산적 복잡도를 완전 분석함으로서 기존의 방식들에 비해 구현 가능성을 높였다는 의의를 가지나, 판매자의 부정과 구매자의 공모 공격(conspiracy attack)에 안전하지 못하며 식별 단계에서도 모든 구매자가 참여해야 하는 비효율성을 가진다. 제안 방식에서는 이중 잠금 암호 알고리즘 (two-lock cryptosystem)을 사용한 불확정 전송 프로토콜 기반의 디지털 핑거프린팅 기법을 제안함으로 기존 방식의 문제점을 해결하였다. 그러나 제안 방식은 핑거프린팅 단계에서 구매자와 판매자 사이에 전달되는 정보량이 많다는 문제가 있으므로 이에 대한 연구를 향후 진행할 예정이다.

참 고 문 헌

[1] J.Domingo-Ferrer, "Anonymous Finger

표 1. 제안 방식과 기존 방식의 비교

	[Domingo99]	[Sadeghi01]	제안방식
익명성	○	○	○
비연결성	○	○	○
위조불가	×	×	○
부인불가	×	×	○
공모공격 안전성 (Collusion Tolerance)	×	×	○
식별단계 참가 개체	판매자, 전 구매자, 등록 센터	판매자, 전 구매자, 등록 센터	판매자, 등록 센터 (분쟁 시: 구매자 참가)

printing Based on Committed Oblivious Transfer", *PKC99, LNCS 1560, Springer-Verlag*, pp.43-52, 1999.

[2] Ahmad-Reza Sadeghi, "How to Break a Semi-anonymous Fingerprinting Scheme", *IH2001, LNCS2137, Springer-Verlag*, pp.384 -394, 2001.

[3] B.Pfitzman and W.Waidner, "Anonymous Fingerprinting" , *Eurocrypto97, LNCS 1233, Springer-Verlag*, pp. 88-102, 1997.

[4] Jan Camenisch, "Efficient Anonymous Fingerprinting with Group Signatures", *Asicacrypt2000, LNCS 1976, Springer-Verlag*, pp. 415-428, 2000.

[5] B.Pfitzmann and Ahmad-Reza Sadeghi, "Anonymous Fingerprinting with Direct Non-Repudiation", *Asiacrypt2000, LNCS 1976, Springer-Verlag*, pp.401-414, 2000.

[6] D.Boneh and J.Shaw, "Collusion-secure Fingerprinting for Digital Data", *Crypto95, LNCS 963, Springer-Verlag*, pp.452-465, 1995.

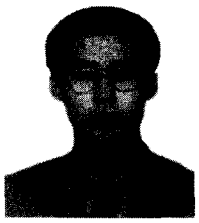
[7] Qian-Hong Wu, Jian-Hong Zhang, and Yu-Min Wang, "Practical t-out-n Oblivious Transfer and Its Applications", *ICICS2003, LNCS 2836, Springer-Verlag*, pp.226-237, 2003.

[8] Joe Killian, F.Thomson Leighton, Lasely R. Matheson, Talal G. Shannon, Rovert E. Tarjan and Francis Zane, "Resistance of Digital Watermarks to Collusive Attacks", *Proceedings of 1998 ISIT*, pp.271, 1998.

[9] I.J. Cox, J.Kilian, T.Leighton, and T. Shamnon, "Secure Spread Spectrum Watermarking for Image, Audio and Video", *IEEE Transactions on Image Processing, vol.6, no 12*, pp.1673-1678, 1997.

〈著者紹介〉

최 재 귀 (Jae-Gwi Choi) 준회원
1998년 2월 : 부경대학교 전자계산학과 졸업
2001년 8월 : 부경대학교 전산교육전공 석사
2002년 3월~현재 : 부경대학교 정보보호학과 박사과정
2002년 10월~2003년 8월 : Kyushu Univ. 교환학생, JSPS지원
2004년 4월~현재 : Tokyo Univ. Internship, KOSEF지원
〈관심분야〉 정보보호, 저작권 보호



박 지 환 (Ji-Hwan Park) 정회원
1990년 : 요코하마국립대학 전자정보공학 졸업
1990년~현재 : 부경대학교 전자컴퓨터정보통신공학부 교수
1994년~1995년 : 동경대학 생산기술연구소 방문연구
1998년~1998년 : 일본 전기통신대학 방문연구
1999년~1999년 : Monash University, Australia, 방문연구
2001년, 2003년 : Communication Research Lab. Japan, JSPS Fellowship
1996년~현재 : 동경대학 생산기술연구소 협력연구원
1997년~현재 : 정보보호학회 이사, 논문지 편집위원
2002년 3월~2004년 2월 : 정보보호학회 영남지부장
1998년~현재 : 멀티미디어학회 운영위원, 논문지 편집위원
1999년~현재 : 정보처리학회 논문지 편집위원
2004년~현재 : 방송공학회 논문지 편집위원
〈관심분야〉 정보보호, 암호학, 멀티미디어 압축 및 응용

김 태 석 (Tai-Suk Kim) 정회원
1992년 3월 : 일본KEIO대학 이공학부 계산기과학전공 졸업
1993년 3월~현재 : 동의대학교 컴퓨터·소프트웨어공학부 교수
2000년 3월~2003년 7월 : 동의대학교 전산정보원장
2000년 3월~2003년 9월 : (재)부산테크노파크 운영위원(동의대분소장)
2003년 8월~현재 : 동의대학교 교무처장
〈관심분야〉 인터넷응용 및 보호, 원격강의, 자연어 처리