2000년 한국정보처리학회 추계 학술발표논문집 제7권 제2호

향상된 자동식별기능과 익명성을 제공하는 핑거프린팅

정찬주*, 유희종*, 원동호*
*성균관대학교 전기전자 및 컴퓨터 공학부
e-mail:cjchung@dosan.skku.ac.kr

Improved Automatic Identification and Anonymous Fingerprinting

Chan-Joo Chung*, Hui-Jong Yu**, Dong-Ho Won*
*Dept of Electrical & Computer Engineering, Sung-Kyun-Kwan University

요약

최근에 네트워크와 하드웨어 기술의 발달에 따라 디지털 컨텐츠의 지적소유권에 관한 분쟁이 많이 발생하고 있다. 본 논문에서는 디지털 컨텐츠의 전자상거래에서 지적소유권에 대한 분쟁을 해결하는데 사용될 수 있는 익명성을 제공하는 핑거프린팅 방식을 제안한다. 제안하는 방식은 판매된 디지털 컨텐츠를 재분배하는 구매자를 판매자가 등록센터의 도움 없이 재분배자를 식별하는 향상된 자동식별기능을 갖는다.

1. 서론

컴퓨터 네트워크와 하드웨어 기술의 발달에 따라 디지털 컨텐츠의 지적소유권을 보호하기 위한 방법이 대두되기 시작하였다. 이러한 기술로 기존에 사용된 방식은 암호화 방식과 접근제어 방식이다. 그러나, 위의 방식들은 디지털 컨텐츠에 적법한 허가를 얻은 후에는 디지털 컨텐츠의 특성상 불법복사가 가능하다는 문제점을 갖고 있다.

불법복사를 해결하기 위하여 제안된 방식이 카피라이트 마킹(copyright marking) 방식이다. 카피라이트 마킹 방식은 디지털 컨텐츠에 소유권자의 정보를 삽입하는 방식이다. 카피라이트 마킹 방식도 불법복사 자체는 막지 못하지만, 지적소유권에 관한 분쟁이 발생 시에 지적소유권자를 밝혀낼 수 있기 때문에 불법복사를 방지하는 효과가 있다. 카피라이트 마킹를 분류하면 워터마킹과 핑거프린팅 기술이 있다 워터마킹 기술은 동일한 디지털 컨텐츠에 대하여 동일한 소유권 정보를 삽입하여 소유권에 대한 인증기능만을 제공하는 반면에, 핑거프린팅 기술은 동일한 디지털 컨텐츠에 대하여 서로 다른 소유권 정보를 삽입하여 소유권에 대한 인증기능 뿐만 아니라 구매자를 식별하는 기능을 제공한다. 전자상거래가 활성화되어 감에 따라 디지털 컨텐츠의 지적소유권 보호를 위한 방법으로 핑거프린팅 기술에 대한 관심은 크게 증대될 것이다.

2. 연구배경

Wagner에 의하여 처음으로 제안된 핑거프린팅 방식[1]은 가설검정에 기반하여 재분배자를 식별하는 방식이다. [1]은 구매자들이 공모하여 디지털 컨텐츠를 만들 수 있다는 문제점을 갖고 있었다. 이를 해결하기 위하여 Boneh는 공모에 안전한 코드를 핑거프린트로 사용하는 방식[2]을 제안하였다. [1, 2]은 판매자와 구매자가 핑거프린팅된 디지털 컨텐츠를 알기 때문에 대칭 핑거프린팅이라 불리고, 불법복사본이 발견된 경우 불법복사를 한 사람이 누구인지를 제삼자에게 증명할 수 없다는 문제점을 갖고 있다.

이런 문제점을 해결하기 위하여, Pfitzmann과 Schunter는 핑거프린팅된 데이터는 구매자만이 알 수 있고, 판매자는 알지 못하는 비대칭 핑거프린팅 [3]을 제안하였다. Pftizmann은 또한 비대칭 핑거프린팅 방식을 이용하여, 불법자 추적(traitor tracing) 방식[4]을 제안하였고, 은닉 서명을 이용하여, 구매 Computer Engineering, Dae-sung자의 익명성을 제

공하는 핑거프린팅 방식[5]을 제안하였다. 익명성을 제공하는 핑거프린팅 방식은 판매자가 재분배자를 식별하기 위하여 추출된 핑거프린트를 이용하여, 등록센터와 상호통신을 통하여 재분배자를 식별하게된다. 등록센터의 작업이 구매자의 등록업무 이외에 재분배자 식별이 추가되는 문제점이 있다. Domingo는 이를 개선하여 판매자 스스로 재분배자를 자동식별하는 핑거프린팅 방식[6]을 제안하였다. 최근의 연구들은 다양한 방법으로 디지털 핑거프린팅 방식의 기능성을 강화하고 있다.

본 논문에서는 [6]에서 제안한 방식보다 향상된 자동식별 기능과 구매자의 익명성을 보장하는 핑거프린팅 방식을 제안한다.

3. 제안하는 핑거프린팅 방식

[6]의 방식은 익명성을 제공하고 재분배자의 자동 식별을 제공한다는 장점이 있지만, 재분배자를 식별하는 과정에서 만족하는 공개키가 발견될 때까지 평균 $N/2$번의 지수 연산을 요구한다는 단점이 있다. N은 공개키 디렉토리에 있는 공개키의 수이다. 따라서, 본 논문에서는 1번의 지수 연산만으로 재분배자의 신분을 확인할 수 있는 효율적인 핑거프린팅 방식을 제안하고자 한다. 제안하는 방식은 구매자 등록과정이 2-pass 프로토콜로 구성되므로 4-pass 프로토콜인 [6]의 방식에 비해 통신 회수측면에서도 효율적인 방식이다.

[시스템 설정]

시스템 설정은 다음과 같다. p는 $p=2q+1$ (단, q는 큰 소수)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. 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 인증 되었다고 가정한다.

3.1 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 $E_{pk_R}(x_2)$를 계산하고, 각각을 등록센터 R에게 전송한다. t는 구매자의 익명성을 제공하기 위한 공개키이다.

등록센터 R은 암호화된 $E_{pk_R}(x_2)$를 등록센터의 비밀키를 사용하여 복호화하여 x_2 얻고, $t^{x_2} = y_B$인지 검증한다. 검증이 성공할 경우, 랜덤값 $x_r \in Z_p$를 선택하고, $T = g^{x_2 \cdot x_r} \bmod p$를 계산한다. T는 핑거프린팅 프로토콜에서 인증정보로 사용된다. 등록센터 R은 t와 T에 대한 인증서 $Cert(t \| x_r)$과 $Cert(T)$를 계산하여, 랜덤값 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. 이상의 과정을 반복적으로 수행함으로써, 구매자 B는 여러 개의 인증서 쌍 (t, T) 을 얻게된다.

3.2 핑거프린팅 프로토콜

구매자 B는 판매자에게 자신의 정당한 사용자임을 밝히기 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 sig를 비밀 랜덤값 x_1을 이용하여 생성한다.

판매자 M은 구매자 B로부터 전송 받은 인증서 $Cert(T)$를 등록센터의 공개키를 사용하여 검증한다. 검증이 성공할 경우 판매자 M은 판매기록으로 $[T, Cert(T)]$를 기록한다. 그리고, 구매자 B와 판매자 M은 안전한 양자간 계산(two-party

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	$t, E_{pk_R}(x_2)$ →	
		$D_{sk_R}(E_{pk_R}(x_2))$ 계산
		$t^{x_2} = y_B$ 검증
		$x_r \in Z_p$ 선택
		$T = g^{x_2 \cdot x_r} \bmod p$ 계산
	$Cert(t \| x_r)$, $Cert(T)$, x_r ←	$Cert(t \| x_r)$, $Cert(T)$ 생성
$T = g^{x_2 \cdot x_r} \bmod p$ 검증		
(t, T) 쌍 획득		

[그림 1] 제안하는 등록 프로토콜

computation)[7]을 수행한다. 안전한 양자간 계산은 다음과 같다. 판매자 M의 입력은 T, t, $text$ 그리고 구매자 B가 구매하고자 하는 원본 디지털 컨텐츠 $item$이고, 구매자 B의 입력은 x_r, x_2, sig 그리고 $Cert(t||x_r)$이다.

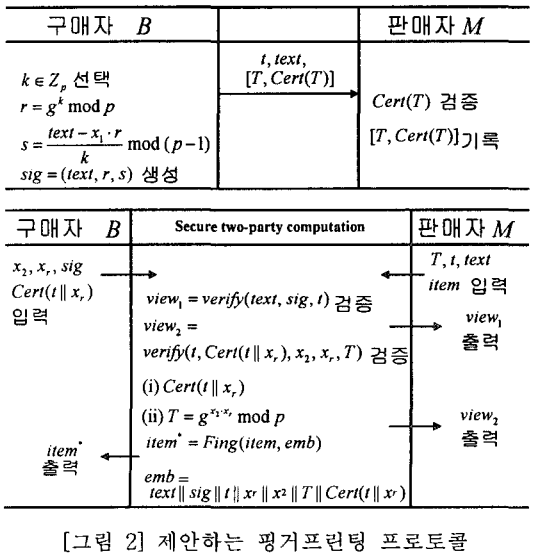
먼저, $view_1 = Verify(text, sig, t)$을 검증한다. 서명 sig는 구매자 B의 익명성을 제공하는 공개키 t를 사용하여 검증된다. 출력 $view_1$은 서명 검증이 성공할 경우에, 판매자 M에게만 보여지는 불린 변수이다.

두 번째로, $view_2 = Verify(t, Cert(t||x_r), x_2, x_2, T)$를 검증한다. 먼저 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_r이 같은지를 검증하는 단계도 포함된다. 그리고 구매자가 처음에 제공한 인증정보 T가 정당한지를 $T = g^{x_2 \cdot x_r} \bmod p$를 검사한다. $view_2$는 이전의 인증서 검증과 T값 검증이 성공할 경우에, 판매자 M에게만 보여지는 불린 변수이다.

$item^* = Fing(item, emb)$은 핑거프린트 emb를 원본 컨텐츠 $item$에 삽입하여 $item^*$ 출력하는 알고리즘이다. 핑거프린팅 알고리즘이 원본 컨텐츠에 삽입 정보 emb를 삽입하기 위하여 사용된다. 삽입 정보 emb는 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.



[그림 2] 제안하는 핑거프린팅 프로토콜

3.3 식별프로토콜

판매자 M은 재분배된 불법복사본을 발견하게 되면, 불법복사본으로부터 emb를 추출하고, emb 안에서 추출한 T값과 같은 인증서 $Cert(T)$를 판매기록으로부터 찾아, 이를 가지고 식별 프로토콜을 수행한다. 먼저, $text$에 관한 서명 sig는 익명성을 제공하는 공개키 t를 사용하여 검증한다. 등록센터가 만들어준 x_r 값은 인증서 $Cert(T)$와 $Cert(t||x_r)$의 일부분이기 때문에 위조될 수 없다. x_2값은 익명성을 제공하는 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 emb로부터 추출한 x_2를 지수 연산함으로써, 다음과 같은 id를 얻을 수 있다.

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

따라서, 판매자는 식별된 id값과 같은 공개키 y_B를 공개키 디렉토리로부터 찾으면 된다. $id = y_B$이다. T와 t는 등록센터의 비밀키를 사용하여 인증되었고, T와 t에 연관된 정당한 x_r를 판매자는 위조할 수 없다. 그래서, 공개키 y_B의 소유자를 재분배한 구매자로 고발한다.

4. 제안하는 방식의 안전성

이장에서는 등록 프로토콜의 안전성과 구매자의 익명성에 대한 안전성을 알아본다. 제안하는 핑거프

린팅 방식은 이산대수 문제에 기반하고 있다.

[등록 프로토콜에서 안전성]

등록 프로토콜은 구매자 B의 비밀키 x_B의 정보 공개 없이 구매자 인증을 제공한다. 등록센터 R은 등록 프로토콜에서 구매자가 전송한 t와 x_2에 대해서만 알 수 있다. 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 t와 x_B를 계산할 수 있다면, 공격자는 이산대수 x_1를 계산할 수 있다. 만약 공격이 가능하다면, 이산대수 문제를 풀 수 있다. 일반적으로, 이산대수 문제는 푸는 다항식 알고리즘이 존재하지 않기 때문에, 등록센터 R은 $t^{x_2} = y_B$를 만족하는 t를 만들 수 없다.

[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. 구매자 B의 공개키 y_B를 알기 위해서는 x_2를 알아야 한다. 그러나, 만약 안전한 양자간 계산이 가능하다면, 판매자 M이 x_2를 찾기 위한 유일한 방법은 인증서 T를 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 계산하여한다. 그러나, 이산대수 문제를 푸는 다항식 알고리즘이 존재하지 않으므로, $x_2 \cdot x_r$를 계산할 수 없다. 따라서, 구매자의 익명성은 보장된다.

5. 결론

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 불법 복사를 방지하는 방식이다.

본 논문에서는 전자상거래에서 효율적으로 사용될 수 있도록 등록 프로토콜을 2-pass로 구성했고, 식별 프로토콜에서 지수 연산을 1번만하여도 재분배자를 식별하는 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 기대된다.

참고문헌

[1] Wagner, N. R., "Fingerprinting", in Proceeding of the 1983 IEEE Symposium on Security and Privacy, Oakland, California, USA, pp.18-22, 1983.

[2] Boneh, D., and J. Shaw, "Collusion-secure Fingerprinting for Digital Data", in Advances in Cryptology, Proceedings of CRYPTO '95, vol. 963 of Lecture Notes in Computer Science, Springer-Verlag, pp.452-465, 1995.

[3] 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.

[4] 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.

[5] 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.

[6] J. Domingo-Ferrer, "Anonymous Fingerprinting of Electronic Information with Automatic Identification of Redistributors", Electronics Letters 34/13, pp.1303-1304, 1998.

[7] 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.