익명적 비대칭 핑거프린팅 기법의 보안 취약성 분석 및 개선 방안

(Security Analysis and Improvement of an Anonymous Asymmetric Fingerprinting Scheme with Trusted Third Party)

권 세 란 †

(Saeran Kwon)

요 약 워터마킹 기법을 기반으로 하는 익명적 비대칭 핑거프린팅 기법은, 판매자와 익명을 사용하는 구매자간의 프로토콜에 다양한 암호 기술을 적용하여, 판매자로 하여금 콘텐츠에 구매자마다 다른 신호 즉 핑거프린트를 삽입하게 하지만 실제로 구매자가 얻게 되는 (핑거프린트가 삽입된) 컨텐츠가 정확히 어떤 것인지 모르게 하는, 판매자와 더불어 구매자의 권리도 지켜주는 저작권 보호 기술이다. 이 기법에서 정직한 구매자는 익명성이 유지될 수 있지만, 콘텐츠의 불법 재배포가 발생하면 판매자는 삽입된 핑거프린트를 증거로 확인하는 분쟁 조정을 거쳐 익명의 재배포자가 실제로 누구인지를 추적할 수 있다.

2007년에 Yong 등은 신뢰기관을 이용한 익명적 비대칭 핑거프린팅 기법을 제안하였는데, 본 논문에서 우리는, 그들의 기법이 중간자 공격에 의해 핑거프린트 값이 노출되는 취약점이 있어 의도를 가진 구매자가 구입한 콘텐츠에서 핑거프린트를 제거할 수 있으며, 또한 구매자가 불법 행위를 하지 않았더라도, 판매자가 저장된 판매 관련 정보를 이용해 익명 구매자의 실제 이름을 알 수 있는 취약점이 있음을 보인다. 덧붙여서, 우리는 이와 같은 취약점을 보완하면서 전체적인 통신회수를 줄이며 구매자 입장에서 복잡한 절차를 거치지 않고 간편하게 상품 구매를 할 수 있는, 효율성에서 개선된 익명적 비대칭 핑거프린팅 기법을 제안한다.

키워드 : 비대칭 핑거프린팅, 워터마킹, 익명성, 중간자 공격

Abstract An anonymous asymmetric fingerprinting protocol combined with watermarking techniques, is one of the copyright protection technologies keeping both right of a seller and that of a buyer, where a seller and an anonymous buyer perform such a protocol that employs various cryptographic tools in order that the seller does not know the exact watermarked copy that the buyer receives, while inserting an invisible non-removable fingerprint i.e., each different unique watermark, into each copy of the digital content to be sold. In such a protocol innocent buyers are kept anonymous during transactions, however, the unlawful reseller is unambiguously identified with a real identity as a copyright violator.

In 2007, Yong and Lee proposed an anonymous asymmetric fingerprinting scheme with trusted third party. In this paper we point out the weakness of their scheme such as: the buyer with intention can remove the fingerprint in the watermarked content, because he/she can decrypt the encrypted fingerprint with a symmetric key using man-in-the-middle-attack; a real identity of a buyer can be revealed to the seller through the identification process even though he/she is honest. Furthermore, we propose an improved secure and efficient anonymous asymmetric fingerprinting scheme which enables to reduce the number of communication between the participants.

Key words : Asymmetric Fingerprinting, Watermarking, Anonymity, Man-in-the-middle-attack

† 정 회 원 : 대림대학 컴퓨터정보계열 교수
sranie@ewhain.net
논문접수 : 2009년 2월 18일
심사완료 : 2009년 5월 20일

정보과학회논문지: 시스템 및 이론 제36권 제5호(2009.10)

1. 서 론

최근 인터넷 관련 기술의 발전과 인터넷상의 다양한 웹 서비스의 확산으로 언제 어디서나 전자상거래 등을 통하여 손쉽게 멀티미디어 컨텐츠, 이미지 파일, 비디오 스트림, 그리고 소프트웨어 프로그램 등의 디지털 자료를 전송 및 다운 받아 편리하게 이용할 수 있게 되었다. 하지만 동시에 디지털 정보 처리 기술의 발전으로 비록 암호화한 상태로 전송 및 다운받은 자료라 할지라도 이를 복호화한 후에는 이에 대한 복제, 변환, 편집 등의 조작을 쉽게 할 수 있어, 이런 자료들을 경제적 이득을 얻을 목적으로 다시 불법적으로 재배포 하는 것 또한 가능하다. 따라서 이들 디지털 자료에 대한 지적 소유권 확립 및 저작권 보호 문제가 인터넷상의 건전한 전자상거래가 이루어지기 위해 해결되어야 할 주요 과제로 떠오르게 되었다.

지금까지 디지털 자료의 지적 소유권 확립 및 저작권 보호에 대한 다양한 방법들이 연구되어 왔는데 그중 디지털 워터마킹 기법[1,2] 및 이를 기반으로 한 핑거프린팅 기법[3-6]이 많은 연구자들에 의해 가장 효과적으로 저작권을 보호할 수 있는 기술로 받아들여지고 있다. 디지털 워터마킹 기법은 컨텐츠 안에 어떤 첨가적인 신호 즉 마크를 삽입하여 분쟁 발생시 컨텐츠 안에 삽입 된 마크를 확인하여 디지털 컨텐츠의 법적인 소유권을 주장할 수 있게 하는 기법인데, 이 기법이 가능하기 위해서는 콘텐츠에 삽입하는 신호가 불법 배포자가 의도적으로 신호 즉 워터마크를 제거하거나 변형하기 위해 시행하는 여러 종류의 이미지 변환 공격에 견딜 수 있도록 만들어져있어야 된다. 다시 말하면 콘텐츠의 이미지를 손상하지 않고는 워터마크를 없애는 것이 불가능하여야 한다. 일반적인 워터마크 기법이 같은 컨텐츠 판매시 모든 복사본에 동일한 워터마크를 삽입하는 반면에, 핑거프린팅 기법은 컨텐츠 복사본에 구매자 마다 다른 워터마크를 보이지 않게 삽입하는데, 일정시간이 지나 판매자가 시장에서 불법적으로 재배포 된 해적판을 발견할 경우, 그 안에 눈으로 지각하긴 어렵지만 구매자에 따라 다르게 삽입된 워터마크를 워터마크 추출 알고리즘으로 확인하여, 어떤 구매자가 불법적으로 해적판을 재배포 했는지 확인하여 법적인 대응을 할 수 있게 해주는 기법이다.

지금까지 워터마킹을 기반으로 하는 여러 핑거프린팅 프로토콜이 제안되었는데[4-10], Qian and Nahrstedt [5]는, 판매자 단독으로 워터마크를 삽입하는 전통적인 방식의(워터마킹 기반의) 핑거프린팅 기법은 구매자에 대한 공정성 문제가 발생할 수 있다는 사실을 처음으로 제기하였다. 이것은 악의적인 판매대행업자가 구매자를 가장하여 컨텐츠를 불법 배포한 후, 오히려 정직한 구매자를 불법배포자로 고발할 수 있기 때문이다. 따라서 판매자만에 의한 워터마크 삽입 방식이 아닌, 판매자-구매자 간의 상호프로토콜을 통하여, 후에 판매자가 구매자를 가장할 수 없도록 판매자는 실제로 구매자가 받게 되는 복사본안에 정확히 어떤 워크마크가 삽입되었는지를 모르게 신호를 삽입하는 비대칭적(asymmetric) 방식이 제안되었다[4-6]. 그러나 위 방식[4-6]의 판매자-구매자 간의 상호프로토콜은 판매자가 구매자를 확인하는 과정에서 구매자의 신원이 노출되기 때문에, 일반적인 전자상거래나 전자 지불 방식에서 요구되어지는 구매자의 익명성이 보장되지 않는다. 따라서 구매자가 불법재배포를 하지 않는 한 구매자의 익명성을 보장해줄 수 있는 익명적 워터마킹 프로토콜들이 Lei[7], Ju[8], Choi[9], Goi[10] 등에 의해 제안되었다.

2007년에, Yong[11]은 신뢰기관을 이용한 익명적 비대칭 핑거프린팅 기법을 제안하였다. 그들의 스킴은 익명 공개키 생성과 이것을 등록하는 단계에서 Ju[8]나 Goi[10]처럼 계산 복잡도가 높은 영지식 증명을 사용하지 않고, Lei[7]처럼 인증서 이름에 실명 대신에 익명(예: 익명 공개키)을 사용한다는 점만 다를 뿐 신뢰기관(CA)이 요청자의 신원을 직접 확인하며 제출된 익명 공개키가 임의로 선택한 익명 비밀키를 사용해 올바르게 만든 것인지를 검증해야 하는 등의 복잡한 절차를 필요로 하는 전통적인 전자인증서 제공방식을 사용하지 않으며, Choi[9]의 스킴처럼 높은 계산량과 많은 통신량이 필요한 익명적 핑거프린팅 생성 과정을 사용하지 않아 효율성에서 개선된 면이 있다. 하지만 구매자가 핑거프린트 인증센터(FCA)에 핑거프린트 등록을 요청한 후 제공받은 두 번 암호화된 핑거프린트를 가지고 판매자에게 상품구매를 신청하면, 판매자는 다시 FCA에게 구매자로부터 받은 자료에 해당하는 대칭키 암호시스템의 핑거프린트 복호화 키를 요청해서 제공받아야 하므로, 스킴의 전 과정을 고려하면, 기존의 스킴들[8-10]에서 적용되던 방식 -즉, 구매자가 FCA(혹은 워터마크 인증센터)에게서 구매자의 익명 공개키로 한번 암호화된 핑거프린트와 그것에 대한 FCA의 서명을 제공받거나[8,9] 구매자 본인이 핑거프린트를 생성해서 CA에게 인증을 받거나[10]해서 얻은 핑거프린트와 서명을 판매자에게 직접 제공하는 방식- 에 비해, Yong[11]의 스킴은 복호화키 취득을 위해 다시 판매자와 FCA 사이의 2번의 통신이 더 필요한 단점이 있다. 또한 이 과정에서 공격자(악의적인 구매자)가 중간자 공격(man-in-the-middle-attack)을 시행할 수 있어, 이 공격을 시행하면, (신원확인과정에서 본인임을 부인할 수 없게 만드는) 콘텐츠 속의 워터마크를 없앨 수 있어, 콘텐츠를 재배포하고도

증거가 없어 추적당하지 않는다. 결과적으로 Yong의 스킴[11]은, 중간자공격에 의해, 핑거프린팅 기법의 기본요구사항인 추적성(traceability)이나 부인방지(no repudiation) 등의 요건을 만족시키지 못하게 된다.

본 논문에서, 우리는 Yong[11]이 제안한 신뢰기관을 이용한 익명적 비대칭 핑거프린팅 기법의 보안 취약점을 분석한다. 다음으로, 이와 같은 취약점을 보완하면서 좀 더 효율적으로 개선된 익명적 비대칭 핑거프린팅 기법을 제안한다.

2. Yong의 핑거프린팅 기법

Yong[11]에 의해 제안된 신뢰기관을 이용한 익명적 비대칭 핑거프린팅 기법은 Cox[1]의 워터마킹 기법과 El-Gamal type의 공개키 시스템 그리고 준동형의 성질을 만족하는 암호시스템 등을 기본 building block으로 하고 있다. Yong[11]의 기법에서 등록과 핑거프린팅 프로토콜 과정을 간단히 설명하면 다음과 같다.

2.1 용어정의

프로토콜의 참여자와 사용기호는 다음과 같다.

□ 참여자

- 핑거프린트 인증센터(FCA) : 핑거프린트를 생성, 관리하는 제3의 신뢰기관
- 등록센터(RC) : 구매자의 익명키를 등록하고 그에 대한 인증서를 생성해주는 제3의 신뢰기관
- 판매자(S) : 디지털 콘텐츠 판매 개체
- 구매자(B) : 디지털 콘텐츠 구매 개체
- 재판관 : 신원확인 프로토콜에서 불법재배포자의 신원을 제공된 증거들을 기반으로 하여 확인시켜주는 개체

□ 사용되는 기호

- F : 구매자의 고유 인식정보인 핑거프린트
- M : 핑거프린트가 삽입될 구매하고자 하는 원본
- $\overline{M}$: 구매자의 핑거프린트가 삽입된 콘텐츠
- H : 충돌 회피성 해쉬함수
- AE/AD : 공개키 암호시스템 암호화/복호화 알고리즘
- SE/SD : 대칭키 암호시스템 암호화/복호화 알고리즘
- HE/HD : 준동형 성질을 만족하는 암호시스템

2.2 구매자 등록하기

구매자와 핑거프린트 인증센터는 모두 공개키와 개인키 쌍을 가지고 있다. 구매자의 개인키는 x_B이고 공개키는 $y_B = g^{x_B}$이다.

• 익명 공개키 등록

1) 구매자는 $x_1 + x_2 = x_B$ 인 임의의 두 수 x_1, x_2를 선택한 후 x_1과 $y_1 = g^{x_1}$을 익명 개인키, 익명 공개키 쌍으로 이용한다. 구매자는 y_B, y_1, $AE_{RC}(x_2)$ 그리고 익명 개인키 x_1을 사용해 서명한 서명 $Sig_{x_1}(H(x_2))$을 등록 센터(RC)에 보낸다.

2) RC는 자신의 개인키로 $AD_{RC}(AE_{RC}(x_2)) = x_2$ 값을 구한 후 $y_1 \cdot g^{x_2} = y_B$인지 확인하여 값이 맞으면 익명 y_1의 인증서 $Cert(y_1)$을 구매자에게 전송한다.

• 핑거프린트 등록

1) 구매자는 핑거프린트 인증센터(FCA)에게 익명 공개키 y_1과 인증서 $Cert(y_1)$를 전송한다. FCA는 y_1에 대한 인증서의 검증이 맞으면 핑거프린트 F를 생성한 후 y_1을 이용하여 암호화시켜 $HE_{y_1}(F)$을 구한다.

2) FCA는 대칭키 암호시스템을 위한 키 k를 임의로 택하여 $C = SE_k(HE_{y_1}(F))$와 서명 $Sig(H(C))$를 생성하여 구매자에게 보내고, 자신의 데이터베이스에 y_1, F, $Sig(H(C))$, 그리고 비밀키 k를 저장한다.

2.3 상품 구매하기

• 핑거프린팅 프로토콜 (그림 1 참고)

1) 구매자는 판매자에게 y_1, C, $Sig(H(C))$를 보낸다.

2) 판매자는 C에 해쉬함수를 적용한 값 $H(C)$에 대한 FCA의 서명 $Sig(H(C))$이 맞는지 확인하여 정당한 서명으로 검증되면 y_1과 $Sig(H(C))$를 FCA에게 보낸다.

3) FCA는 y_1과 관련된 대칭키 암호시스템의 키 k를 찾아 이것을 판매자 S의 공개키로 암호화하여 $AE_S(k)$를 구한 후, $Sig(H(C))$와 함께 판매자에게 보낸다.

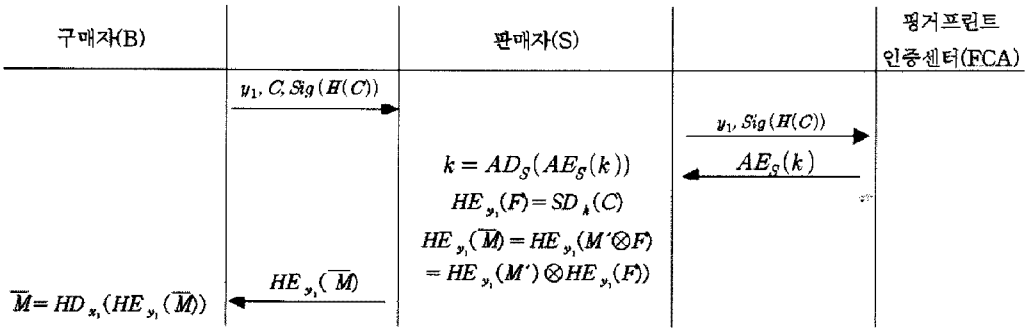

그림 1 핑거프린팅 프로토콜 (Yong[11])

4) 판매자 S는 자신의 개인키를 이용하여 비밀키 $k=AD_S(AE_S(k))$ 값을 구한 후 이 복호화 키 k를 사용해 C를 복호화하여 아래처럼 $HE_{y_1}(F)$을 얻는다.

$$SD_k(C)=SD_k(SE_k(HE_{y_1}(F)))=HE_{y_1}(F)$$

5) 판매자는, 재배포시 특정한 구매자를 찾을 수 있는 도구로 사용하기 위해, 유일한 핑거프린트 V를 생성하여 콘텐츠 M에 삽입하여 $M'=M\otimes V$을 생성한다.

6) 판매자는 y_1으로 M'을 암호화하여 $HE_{y_1}(M')$을 구해 여기에 $HE_{y_1}(F)$을 삽입하면, HE의 준동형성에 의해 $HE_{y_1}(M')\otimes HE_{y_1}(F)=HE_{y_1}(M'\otimes F)=HE_{y_1}(\overline{M})$이 얻어지는데, 이것을 구매자에게 보내고, y_1, V, k, C, $Sig(H(C))$의 값들은 자신의 데이터베이스에 저장한다.

7) 구매자는 y_1에 대한 개인키 x_1을 사용해 $HE_{y_1}(\overline{M})$을 복호화하여 $\overline{M}=M'\otimes F=M\otimes V\otimes F$를 얻는다.

2.4 재배포자의 신원확인

• 신원확인 프로토콜

불법적으로 재배포된 M의 복사본 $\overline{M}$ 또는 $\hat{M}$이 발견되었을 때, 판매자는 다음의 프로토콜을 수행한다.

1) 판매자는 재배포된 콘텐츠에서 핑거프린트 U를 추출하여 자신의 데이터베이스(DB)에 저장되어 있는 핑거프린트들 중에 유사도가 높은 핑거프린트를 찾아서 그 핑거프린트에 해당하는 정보들을 찾아낸다. 판매자는 불법 복제의 증거 pf를 추출된 핑거프린트, 구매자의 익명 공개키, 복호화 키, 암호화된 핑거프린트로 구성하여 재판관에게 보낸다. $pf=<U, y_1, k, C, Sig(H(C))>$

2) 재판관은 pf 값들과 FCA의 공개키를 이용하여 서명 $Sig(H(C))$을 확인하여 올바르면, FCA에게 y_1에 대한 인증서와 핑거프린트를 요청한다. 재판관은 인증서를 검증한 후, 핑거프린트를 y_1으로 암호화 한 값과 C를 k로 복호화한 값이 일치하면, 등록 센터에게 익명 공개키 y_1에 대한 구매자의 실제 아이디를 요청한다.

3. Yong의 핑거프린팅 기법의 취약점 분석

• 중간자 공격(man-in-the-middle-attack)

Yong등은 그들이 제안한 스킴에 대해 다음처럼 안전성 분석을 하였다[11]: 구매자는, 핑거프린트 인증센터(FCA)가 생성한 핑거프린트 F를 알 수 없으며, 또한 이 핑거프린트는 Cox[1]의 워터마킹 기법처럼 공격에 안전한 방식으로 삽입되기 때문에, 핑거프린팅 프로토콜의 최종단계에서 익명 비밀키를 가지고 복호화 해서 얻게 된, 핑거프린트가 삽입된 콘텐츠 $\overline{M}=M\otimes V\otimes F$에서 핑거프린트 F를 제거할 수 없다고 주장하였다. 하지만 다음처럼 중간자 공격(man-in-the-middle-attack)을 시행하면 구매자가 핑거프린트 F를 알 수 있고, 따라서 $\overline{M}$에서 핑거프린트 F를 제거할 수 있다.

Yong의 스킴의 핑거프린팅 프로토콜 단계(그림 1 참고)를 살펴보면, 판매자 S는 구매자로부터 받은 y_1과 $Sig(H(C))$를 FCA에게 보내고, FCA는 단지 데이터베이스에서 y_1과 관련된 대칭키 암호시스템의 복호화 키 k를 찾아 자료를 보낸 S의 공개키로 암호화하여 $AE_S(k)$를 구하여 정보를 요청한 S에게 보내기만 할 뿐, (여기서 S의 공개키 인증서 검증은 당연히 할 것이므로 그것을 제외한다면) 키 요청 판매자 본인에 관한 어떤 검증 작업도 하지 않으며, 요청처리결과를 저장하지도 않는다.

사실 FCA가 키 요청 판매자가 올바른 판매자인지를 검증하는 작업은 많은 정보 처리시간과 과도한 저장용량을 필요로 한다. 왜냐하면 현실에서 시장에서 판매되고 있는 상품의 종류들은 수시로 변화하며 또한 어떤 판매업자들이 어떤 상품을 판매하는지 등은 언제든지 변경될 수 있으므로, FCA는 이처럼 변화하는 시장 정보를 파악하기 위해 판매자들에 대한 신원확인을 거쳐 수시로 그들이 판매하는 상품 정보들을 업데이트해서 저장하고 있어야 되기 때문이다. 더구나, 스킴[11]에서의 FCA는, 구매자의 요청에 의해 생성된 핑거프린트가 어떤 상품의 구매에 이용되는지를 모르므로, 자신에게 복호화 키를 요청하는 판매자가 현재 구매자가 거래를 진행 중인 상품의 올바른 판매자인지를 검증하기가 사실상 어렵다.

한편, 전자 상거래나 일반적인 상거래에서 비록 현재는 상품의 구매자라 할지라도 자신이 권리를 갖고 있는 다른 상품에서는 판매자도 될 수 있는 다양한 상황을 고려한다면, Yong의 핑거프린팅 프로토콜은, 특정 콘텐츠의 판매자임을 검증하는 과정이 없기 때문에, 누구라도 자신이 상품 판매자임을 주장하면서, 공개키 인증서(: 인증서 제공이 Yong의 스킴에서 구체적으로 명시되어 있진 않지만, FCA가 판매자 S의 공개키로 키 k를 암호화해야 하므로, 먼저 S의 공개키에 대한 인증이 필요함)와 y_1과 $Sig(H(C))$를 FCA에게 보내면, FCA는 복호화 키 k를 인증서의 공개키로 암호화하여 보내주게 된다. 따라서 악의적인 구매자 B가 판매자 S에 대한 중간자 공격을 할 수 있는데, 이것은 B가 네트워크 상에서 현재 거래 상품의 판매자 S가 FCA에게 보내는 y_1, $Sig(H(C))$를 보게 되면, 그때 B는 S의 공개키 인증서 $Cert(S)$ 대신 자신의 공개키 인증서 $Cert(B)$로 인증서를 바꾸어 보낸다. 만약 프로토콜이 인증서를 직접 보내지 않고 판매자 신원만을 알려주는 방식으로 진행되는 경우라면, S의 전송을 중간에서 가로채여 판매자 신원을 B로 바꾼 다음 y_1, $Sig(H(C))$를 FCA에게 보낸다.

FCA는 익명 공개키 y_1과 실제이름 B의 관련성을 모르기 때문에, 위의 어떤 방식으로 요청하던지 간에, B가 판매자인 것처럼 해서 복호화 키를 요청하게 되면, 제출된 신원 B의 공개키로 키 k를 암호화하여 $AE_B(k)$를 보내준다. 다시 중간에서 B가 이것을 가로채어 자신의 개인키 x_B를 가지고 복호화하여 $k=AD_B(AE_B(k))$값을 구한 후, 이것을 다시 S의 공개키로 암호화한 $AE_S(k)$를 계산하여, S에게 도로 보낸다. 판매자 S는 중간에서 B가 k에 대한 정보를 가로챘는지 모른 채 그림 1에서처럼 프로토콜을 계속 진행하므로 이 프로토콜의 마지막 단계에 B는 핑거프린트가 삽입된 콘텐츠 $\overline{M}=M\otimes V\otimes F$를 얻게 된다. 이때 B는, 위의 중간자 공격을 통해 얻은 복호화 키 k를 사용해, 갖고 있던 C를 다음처럼 복호화하여 $SD_k(C)=SD_k(SE_k(HE_{y_1}(F)))=HE_{y_1}(F)$를 얻을 수 있고, 이것을 자신의 익명 개인키 x_1으로 다시 복호화하여 $F=HD_{x_1}(HE_{y_1}(F))$를 얻을 수 있다. 결과적으로, B는 핑거프린트 F의 값을 알기 때문에 $\overline{M}$에서 F를 제거 할 수 있다. 따라서 콘텐츠의 불법 재배포시 재배포자에 대한 신원확인 프로토콜을 수행하더라도 B가 콘텐츠에서 F를 제거했기 때문에 판매자는 재판관에게 B의 불법재배포를 증명할 수 없다. 또한 FCA가 자료 쌍 y_1, $Sig(H(C))$에 연계된 복호화 키 k를 어떤 판매자가 요청했는지를 보관하지 않기 때문에 B에 의한 중간자 공격도 추적당하지 않는다.

지금까지 우리는 스킴[11]이 중간자 공격에 취약함을 기술하였다. 하지만, 판매자가 FCA에게 y_1, $Sig(H(C))$를 보내면서 k값을 요청하는 프로세스에서, FCA가 k값을 암호화시켜 제공한 후, 제공에 대한 기록을 데이터베이스에 따로 저장하거나 표시하지 않기 때문에, 굳이 구매자 B가, 네트워크를 계속 감시해야 되는 중간자 공격까지 시행하지 않더라도, 판매자 S로부터 구입한 콘텐츠에서 핑거프린트 F를 제거할 수 있다. 구체적으로, 콘텐츠의 구매요청 전일지라도, 암호화된 핑거프린트를 이미 FCA로부터 제공받은 B는, 판매자인척하면서 자신의 인증서와 함께 y_1, $Sig(H(C))$를 FCA에게 보내면서 k값을 요청하면, FCA는 익명 공개키 y_1의 실제신원이 B인 것을 모르므로, 판매자인척하는 B에게 $AE_B(k)$를 제공할 것이고, 따라서 B는 앞에서 설명한 같은 방법으로 핑거프린트 F를 얻을 수 있다. 또한 B의 구매요청에 의해 판매자 S 역시 자신의 인증서와 함께 y_1, $Sig(H(C))$를 보내면서 k값을 요청하면, FCA는 B에게 $AE_B(k)$를 제공했던 것을 기억하지 못하기 때문에 S에게 다시 $AE_S(k)$를 제공하게 된다. 따라서 S는 그림 1처럼 프로토콜을 계속 수행하게 되고, 결국 이 프로토콜의 마지막 단계에서 B는 핑거프린트 F가 삽입된 콘텐츠 $\overline{M}$를 취득하게 되어 이 콘텐츠에서 F를 제거할 수 있다.

• 익명성 관련 문제

재배포자 신원확인 프로토콜 단계(2.4절 참고)에서, 불법 재배포된 복사본 $\hat{M}$에서 추출하여 재판관에게 (연관된 정보와 함께) 증거로 제출하는 핑거프린트 U는, 판매자가 임의로 만들어 삽입한 (또는 노이즈 등으로 인해 원래 값에서 약간 변화된) 핑거프린트로써 FCA 등에 의해 검증된 값은 아니다. 따라서 실제로 해적판이 시장에 재배포된 상황이 아니더라도, 판매자가 의도적으로 콘텐츠 M에 U를 삽입하여, 자신의 DB에 저장되어 있는 $y_1, k, C, Sig(H(C))$와 함께 U를 재판관에게 제출하면서 신원확인을 요청할 수 있다. Yong 스킴[11]에서의 재판관은, 판매자가 제출한 자료 y_1 ,k, C와 FCA에게 요청해서 제공받은 핑거프린트 F를 가지고, F를 y_1으로 암호화 한 값과 C를 비밀키 k로 복호화한 값이 맞는지 계산하여 값이 일치하면 RC에게 y_1의 실제 이름을 요청한다. 그런데 위의 경우에 두 값은 당연히 일치하므로, 판매자는 필요하면 언제나 가지고 있는 자료를 이용해 익명 공개키의 실소유자를 재판관에게 요청하여 알 수 있다. 따라서 구매자가 불법 행위를 하지 않은 경우에도, 구매자의 익명성이 보장되지 않는다.

4. 개선 방안

Yong[11] 스킴의 핑거프린팅 등록과 상품구매는, 판매자, 구매자, 핑거프린트 인증센터(FCA)의 참여로 이루어지는데, 이들 간의 업무 수행 절차는 그림 2와 같다. 그림에서 보듯이, 이들의 기법은, 구매자가 FCA와 판매자 양쪽과 접촉해야하며, 관련 참여자들 사이에서 6번의 통신을 해야 하는 복잡함이 있다. 스킴의 진행 과정(그림 2 참고)을 개략적으로 살펴보면 다음과 같다: 구매자의 핑거프린팅 등록요청에 대해 핑거프린팅 인증센터(FCA)는 두 번 암호화된 핑거프린트 C를 제공해주고, 구매자는 이 C를 가지고 판매자에게 상품구매를 신청한다; 판매자는 다시 FCA에게 구매자로부터 받은 자료 C에 해당하는 복호화 키를 요청한다. 즉 일반적인 핑거프린팅 스킴[8-10]이 핑거프린트 생성을 위해 FCA와 한번 접촉 하는 것에 비해, Yong의 기법은 복호화 키 취득을 위해 다시 (판매자가) FCA와 접촉해야하는 단점이 있다.

또한 신원확인 프로토콜에서는, 재판관이, 고발된 해적판 안에 FCA가 생성해서 인증해 준 핑거프린트의 존재를 확인하는 과정이 없기 때문에, 결과적으로 앞의 3장의 예에서 보는 것처럼, 구매자의 익명성이 깨어진다.

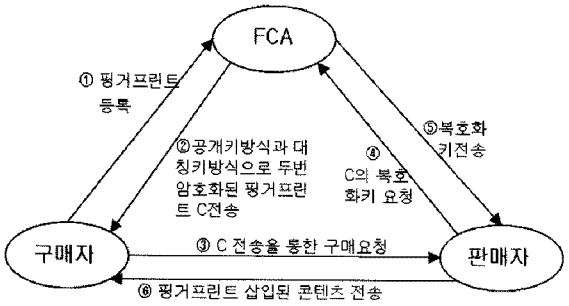

그림 2 Young[11] 스킴의 흐름도

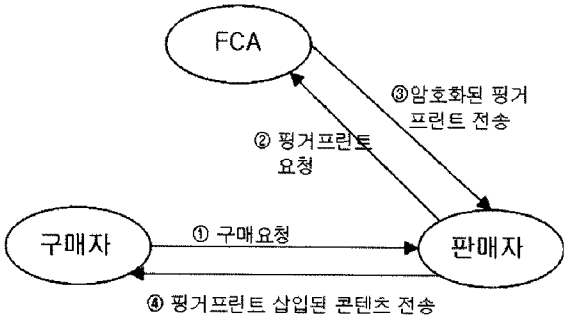

그림 3 개선된 스킴의 흐름도

일반적으로 전자 상거래에서 구매자는 복잡한 절차를 어려워하며 되도록 간편하게 상품 구매를 하기를 원한다. 따라서 개선 방안(그림 3)은, 상품 구매 과정에서 구매자는 상품 요청만 수행하며, 콘텐츠에 삽입될 핑거프린트의 요청은 판매자가 직접 하도록 하여 효율성을 증진시키고 동시에 중간자 공격에 대한 취약성 문제를 제거할 수 있도록 설계된다. 또한 신원확인 프로토콜에서, 재판관이 불법 재배포로 고발된 해적판에 실제로 FCA가 만들어준 핑거프린트가 존재하는지 확인하는 과정을 첨가한다.

개선안은 다음과 같다(여기서 구매자의 익명키 등록 프로토콜은 Yong[11]의 스킴과 같으므로 생략한다).

• 개선된 핑거프린팅 프로토콜(그림 3)

1) 상품을 구매하기 위해 구매자와 판매자는 먼저 구입할 상품에 대한 정보와, 구입에 관련한 의무와 권리 관계, 판매자 정보를 기술한 상품 협약서(ARG)에 동의한다. 구매자가 협약서(ARG)에 익명적으로 동의하는 방법으로, 판매자가 판매 상품 설명과 협약 관련 정보를 홈페이지에 게시해 놓으면 구매자는 익명으로 이것을 사용하는 방안이 있다[7,12]. 상품 협약서에 대한 동의는, 판매자가 부당한 이득을 취할 목적에서 어떤 상품에 이전의 핑거프린트를 사용하는 것을 못하게 하며, 판매자를 명시하여 침입자의 위장 공격을 어렵게 한다. 구매요청 시 구매자는 판매자에게 익명키 y_1의 인증서 $Cert(y_1)$, ARG, $Sig_{x_1}(ARG)$를 보낸다. y_1은 인증서 $Cert(y_1)$ 안에 포함되어 있으므로 따로 보낼 필요가 없다.

2) 판매자 S는 인증서 $Cert(y_1)$와 y_1의 ARG에 대한 서명 $Sig_{x_1}(ARG)$이 옳은 것으로 검증되면 핑거프린트 요청을 위해, $Cert(y_1)$, ARG, $Sig_{x_1}(ARG)$를 자신의 실명 인증서 $Cert(S)$와 함께 FCA에게 보낸다.

3) (i) FCA는 $Cert(y_1)$과 y_1의 서명 $Sig_{x_1}(ARG)$이 옳은 것으로 검증되고, ARG 안에 표시된 판매자와 $Cert(S)$의 S가 같은 이름의 판매자인지 확인되면, ARG에 표시된 상품에 적합한 유일한 핑거프린트 F를 생성하여 y_1을 사용하여 암호화시켜 $HE_{y_1}(F)$을 구한다. (ii) FCA는 대칭키 암호시스템의 키 k를 임의로 택하여 $C = SE_k(HE_{y_1}(F))$를 계산하고, 판매자 S의 공개키로 k를 암호화한 $AE_S(k)$를 구한다. 다음으로 서명 $Sig(H(C, ARG, y_1, S))$를 생성하여 C, $AE_S(k)$와 함께 판매자 S에게 보내고, 데이터베이스에 판매자 S, F, ARG, $Sig_{x_1}(ARG)$, y_1 그리고 비밀키 k를 저장한다.

4) (i) 판매자는 C, ARG, y_1, S에 해쉬 함수를 적용한 값에 대한 FCA의 서명 $Sig(H(C, ARG, y_1, S))$이 맞는지 확인하여 정당한 서명으로 검증되면, 자신의 개인키를 이용하여 비밀키 $k = AD_S(AE_S(k))$값을 구한 후, 이렇게 얻어진 복호화 키 k를 이용해 C를 복호화하여 $HE_{y_1}(F)$을 얻는다. (ii) 판매자는, 후에 자신이 저장한 구매자 정보를 검색할 때 검색키로 사용하기 위해, 먼저 임의의 핑거프린트 V를 생성하여 콘텐츠 M에 삽입하여 $M' = M \otimes V$을 생성한다. 다시 M'를 y_1으로 암호화하여 $HE_{y_1}(M')$을 구한 후 여기에 $HE_{y_1}(F)$을 삽입하면 $HE_{y_1}(M') \otimes HE_{y_1}(F) = HE_{y_1}(M' \otimes F) = HE_{y_1}(\overline{M})$이 얻어지는데, 이것을 구매자에게 보낸 후 V, k, C, ARG, $Sig_{x_1}(ARG)$, $Cert(y_1)$, $Sig(H(C, ARG, y_1, S))$들은 자신의 데이터베이스에 저장한다.

5) 구매자는 y_1에 대한 익명 개인키 x_1을 사용하여 $HE_{y_1}(\overline{M})$을 복호화하여 $\overline{M} = M \otimes V \otimes F$를 얻는다.

• 재배포자 신원확인 프로토콜

콘텐츠 M의 해적판 $\hat{M}$이 시장에서 발견되면, 판매자는, 앞의 4)항 (ii)에서 검색키로 사용하기 위해 콘텐츠에 자신만이 아는 핑거프린트를 삽입했었는데, 해적판 $\hat{M}$에서, 그때 적용한 핑거프린팅 기법의 추출 알고리즘과 원본 M을 사용해 핑거프린트 U를 추출해낸다. U가 데이터베이스에 있는 검색키 용의 어떤 핑거프린트 V와 미리 계산된 신뢰임계 값을 넘을 정도로 유사하면, V를 색인 키로 한 연관된 정보를 찾아, 해적판 $\hat{M}$와 함께, 재판관에게 증거 $pf = <M' = M \otimes V, k, C, ARG,$

$Sig_{x_1}(ARG)$, $Cert(y_1)$, $Sig(H(C,ARG,y_1,S))$>로 제출한다. 재판관은 판매자 S가 보낸 증거에 포함된 인증서와 서명들이 모두 검증되면, ARG, $Sig_{x_1}(ARG)$, y_1을 FCA에게 보내 대응하는 핑거프린트 F를 요청한다. 재판관은 제공받은 F를 y_1으로 암호화 한 값과 C를 비밀키 k로 복호화한 값이 일치하면, M', $\hat{M}$, F를 가지고, F에 적용되는 핑거프린트 추출 알고리즘을 사용해서 $\hat{M}$ 안에 F가 있는지 확인한다. $\hat{M}$안에 F의 존재성이 확인되면 재판관은 등록 센터(RC)에게 익명 y_1에 대응하는 실제 소유자의 이름을 요청한다.

5. 분 석

제안된 기법의 상품구매 과정은, 구매자는 상품 요청만 수행하며, 콘텐츠에 삽입될 핑거프린트를 요청하는 일은 판매자가 직접 함으로써, 구매자는 핑거프린트 요청 단계를 거치지 않고 간편하게 판매자에게 상품 구매 요청을 할 수 있다. 판매자 입장에서는, 의도를 가진 침입자의 중간자 공격이 성공할 수 없어 악의적 구매자가 구매한 콘텐츠에서 핑거프린트를 제거할 수 없으므로, 콘텐츠의 불법적인 재배포시, 컨텐츠 속의 핑거프린트가 재배포자를 추적할 수 있게 해주므로, 안심하며 상품판매를 할 수 있다.

판매자 입장에 대해 구체적으로 살펴보면, 제안된 기법은 FCA로부터 직접, 두 번 암호화된 핑거프린트 C, 판매자의 공개키로 암호화된 복호화 키, 그리고 C와 판매자 이름(예: 공개키 인증서 상의 이름) 등에 대한 FCA의 서명을 함께 제공받기 때문에, 만약 FCA에게 관련 메시지를 전송 중인 네트워크 상에서 공격자(예 구매자 B)가 중간에서 자신이 판매자(B)인척하면서, 협약서ARG 안의 판매자를 B로 바꾸고, 동시에 자신의 익명 개인키 x_1을 사용해 변경된 협약서ARG'의 서명을 새로 만들어, $Cert(B)$, $Cert(y_1)$과 함께 FCA에게 보내면서 중간자 공격을 시도하여 결국 복호화 키 k와 핑거프린트 F 값을 알게 되더라도, 원본 콘텐츠를 갖고 있는 진정한 판매자 S에게 중간에 가로챈 메시지를 다시 전해줄 때, 기반으로 하는 서명 스킴의 안전성을 가정한다면, B를 S로 바꾸고 ARG'를 ARG로 바꾼 메시지에 대한 FCA의 서명을 만들 수 없기 때문에, 프로토콜은 중단된다. 만약 응답을 기다리던 S가, 판매자가 S인 원래의 협약서 ARG를 가지고 다시 FCA에게 핑거프린트 요청을 한다면, FCA는 판매자가 S인 새로운 거래로 생각하므로 새로운 핑거프린트 F'을 생성해서 이것을 새로운 비밀키 k'으로 암호화하여 C'을 제공해 주므로, B가 앞에서 중간자 공격으로 얻은 정보는 소용이 없게 된다.

또한 개선된 기법에서는 상품 협약서(ARG)를 통해, 익명 구매자가 구매상품과 구매 관련 사항 그리고 판매자 등에 관한 사항을 판매자와 동의하는 과정을 첨가하였는데, FCA는 협약서의 서명을 통해 이 정보가 동의된 것을 확인한 후 핑거프린트 제공 시에 관련 협약서, 익명 구매자, 판매자, 그리고 (암호화 시킨) 제공 핑거프린트 등에 대해 서명을 하므로, 특정 핑거프린트는 FCA의 서명을 통해 특정구매자, 특정상품, 특정판매자 등과 연관성을 갖고 있음을 보여준다. 따라서 이것은 판매 대행을 하는 판매자가, 어떤 불법 재배포된 상품에 대한 신원확인 재판을 통해 알게 된 이전 상품에 사용된 핑거프린트를, 그 구매자의 새 구매 상품에 삽입하여 재배포해 놓고는, 구매자가 새 상품 역시 불법 재배포한 것처럼(unbinding problem) 재판관에게 증명할 수 없다.

또한 신원확인 프로토콜에서, 재판관이, 제출된 해적판에 실제로 FCA가 만들어준 핑거프린트가 존재하는지를 확인하기 때문에, 반드시 구매자가 불법재배포를 했을 경우에만 그에 대한 신원이 알려지게 된다.

6. 결 론

본 논문에서, 우리는 Yong[11]이 제안한 신뢰기관을 이용한 익명적 비대칭 핑거프린팅 기법이, 핑거프린팅 프로토콜 단계의 복호화 키 취득을 요청하는 과정에서 중간자 공격에 대한 보안 취약점이 나타날 수 있으며, 신원확인 프로토콜 단계에서는, 재판관이 재배포된 해적판에서 FCA가 생성해서 제공해준 핑거프린트의 존재를 확인하는 과정이 없기 때문에, 판매자는 필요하면 언제나 데이타베이스에 저장된 판매 관련 정보를 이용해 익명 구매자의 실제 이름을 재판관에게 요청할 수 있어, 구매자의 익명성을 유지하기 어렵다는 것을 보였다.

다음으로, 이와 같은 취약점을 보완하면서, 전체적인 통신회수를 줄이며 구매자 입장에서 복잡한 절차를 거치

표 1 Yong의 기법 [11]과 제안된 개선 기법의 비교

	중간자 공격에 대한 안전성		정직한 구매자의 익명성	unbinding problem	익명키 등록 통신회수	핑거프린트를 사용한 상품구매 과정의 참여자 간 전체통신회수
	재배포자 추적성	부인 방지				
개선 기법	○	○	○	해결	2	4
Yong의 기법	×	×	×	발생 가능	2	6

지 않고 간편하게 상품 구매를 할 수 있는, 효율성에서 개선된 익명적 비대칭 핑거프린팅 기법을 제안하였다.

참 고 문 헌

[1] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Processing*, vol.6, pp. 1673-1687, Dec. 1997.

[2] M. Swanson, M. Kobayashi, and A. Tewfik, "Multimedia data embedding and watermarking technologies," *Proc. IEEE*, vol.86, pp.1064-1087, June 1998.

[3] N.R. Wanger, "Fingerprinting," *IEEE Symposium on Security and Privacy*, pp.18-22, 1983.

[4] B. Pfitzmann and M. Schunter, "Asymmetric fingerprinting," *Eurocrypt'96, LNCS 1070*, pp.84-95, Springer-Verlag, 1996.

[5] L. Qian and K. Nahrstedt, "Watermarking schemes and protocols for protecting rightful ownership and customer's rights," *J. Vis. Commun. Image Representation*, vol.9, pp.194-210, Sept. 1998.

[6] N. Memon and P.W. Wong, "A buyer-seller watermarking protocol," *IEEE Trans. Image Processing*, vol.10, pp.643-649, Apr. 2001.

[7] C.L Lei, P.L. Yu, P.L. Tsai, and M.H. Chan, "An efficient and anonymous buyer-seller watermarking protocol," *IEEE transactions on Image Processing*, **13**(12), pp.1618-1626, 2004.

[8] H.S. Ju, H.J. Kim, D.H. Lee, and J.I. Lim, "An anonymous buyer-seller watermarking protocol with anonymity control," In: P.J. Lee, C.H. Lim (eds.) *ICISC 2002, LNCS 2587*, pp.421-432, 2003.

[9] J.G. Choi, K. Sakurai, and J.H. Park, "Does it need trusted third party? Design of buyer-seller watermarking protocol without trusted third party," In: J. Zhou M. Yung, Y. Han (eds.) *ACNS 2003, LNCS 2846*, pp.265-279, 2003.

[10] B.M Goi, R.C.-W. Phan, Y. Yang, F. Bao, R.H. Deng, and M.U. Siddiqi, "Cryptanalysis of two anonymous buyer-seller watermarking protocols and an improvement for true anonymity," In: M. Jakobsson, M. Yung, J. Zhou (eds.) *ACNS 2004, LNCS 3089*, pp.369-382, 2004.

[11] 용승림, 이상호, "신뢰기관을 이용한 익명적 비대칭 핑거프린팅 기법", *정보과학회논문지 : 시스템 및 이론*, 제 34 권 제 7 호, pp.288-295, 정보과학회 (2007.8).

[12] Min-Hua Shao, "A Privacy-preserving buyer-seller watermarking protocol with semi-trust third party," *TrustBus 2007, LNCS 4657*, pp.44-53, Springer-Verlag, 2007.

권 세 란

서울대학교 수학교육과(학사). 서울대학교 수학과(석사). 데이콤 연구원. 1993년 서울대학교 수학과(박사). 2007년 이화여자대학교 컴퓨터학과 석·박사통합과정(박사). 1998년~현재 대림대학 컴퓨터정보계열 부교수. 관심분야는 정보보호, 암호프로토콜, 저작권 보호