情 報 保 護 學 會 誌
第 11 券 第 3 號, 2001. 6

디지털 컨텐츠의 지적 재산권 보호를 위한 익명 핑거프린팅의 연구 동향

여 상 수*, 윤 훈 기*, 김 성 권*

요 약

디지털 컨텐츠의 지적 재산권 보호를 위한 디지털 워터마킹 기술이 많이 연구되어져 왔다. 핑거프린팅은 디지털 컨텐츠 지적 재산권 보호를 위한 또 다른 기술로서, 디지털 워터마킹에서는 컨텐츠 내부에 소유권자나 판매권자의 정보가 삽입되는 반면에, 핑거프린팅에서는 구매자의 정보가 삽입이 된다. 따라서, 핑거프린팅을 이용하면 불법적으로 컨텐츠를 재분배한 구매자가 누구인지 밝혀낼 수 있기 때문에, 구매자들로 하여금 불법적인 재분배하려는 의욕을 저하시킬 수 있다. 이러한 핑거프린팅 프로토콜 중에서 익명 핑거프린팅 프로토콜은 합법적인 구매자에 대해서는 익명성을 보장해 주며, 불법적인 재분배자에 대해서만 신원을 밝혀낼 수 있도록 하는 프로토콜이다. 이 논문에서는 현재까지 연구된 익명 핑거프린팅 프로토콜에 대해서 비교 분석하고, 익명 핑거프린팅 프로토콜에서 충족되어야 하는 요구사항들을 살펴본다.

Ⅰ. 서 론

전자상거래를 통해서 디지털 컨텐츠가 판매되는 것이 활성화되기 위해서는 지적 재산권 보호에 대한 연구가 선행되어야 한다. 디지털 컨텐츠는 일반적인 오프라인 컨텐츠와는 달리 쉽게 복사 및 배포가 가능하다는 특성이 있다. 따라서, 합법적인 구매자가 판매자로부터 디지털 컨텐츠를 구입한 후, 이것을 불법적으로 재분배(redistribution)하는 것을 막아주는 방법이 고려되어야만 한다. 현재까지 이에 대한 해결책으로 디지털 워터마킹(digital watermarking)에 대한 연구가 진행되어져 왔다.

디지털 워터마킹 기법은 디지털 컨텐츠 내에 저작권자 또는 판매권자에 대한 정보를 삽입해 놓음으로써, 이후에 발생하게 되는 지적 재산권 분쟁에서 정당성을 증명하는데 사용되어질 수 있다. 이를 위해서는 디지털 컨텐츠의 저작권자나 판매권자가 컨텐츠를 판매하기 이전에 자신의 정보를 컨텐츠 내에 삽입을 해야 한다. 컨텐츠에 워터마킹 정보를 삽입하는 방법도 크게 두 가지로 구분하여 볼 수 있는데, 첫 번째는 삽입되는 정보를 사람의 감각(시각 또는 청각)으로 감지가 가능하도록 삽입하는 인지 가능(perceptible) 워터마킹 기법이다. 이미지의 한쪽 편에 소유권자의 정보를 표시한 것이나 음악파일 내에 삽입되어 있는 저작권 정보 안내 음성 등을 주위에서 쉽게 접할 수 있는데, 이것들이 바로 인지 가능 워터마킹 기법이라 할 수 있다. 이것은 매우 기초적인 워터마킹 기술이라고 할 수 있다. 이 기법의 단점은 워터마킹 정보가 감지가 되기 때문에 삭제하기가 용이하다는 점이다. 다시 말해서, 감지되는 부분만 삭제해 버리면 더 이상 워터마킹의 목적을 이룰 수 없게 된다. 이를 보완하기 위해 연구된 기법은 사람이 감지할 수 없도록 워터마킹 정보를 삽입하는 인지 불가능(imperceptible) 워터마킹 기법이다. 이 기법에서는 각각의 디지털 컨텐츠의 구조에 적절하게 워터마킹 정보를 삽입하게 되고, 그것을 사람이 감지 할 수 없게 만든다. 이렇게 되면 앞의 경우와는 달리 어떤 것이 워터마킹 정보인지를 구분해 내는 것이 어렵게 된다. 워터마킹에 사용된 알고리즘과 알고리즘의 인자로 들어가는 비밀

* 중앙대학교 컴퓨터공학과 (ssyeo,hkyun@alg.cse.cau.ac.kr, skkim@cau.ac.kr)
** 본 연구는 정보통신부 출연 대학정보통신연구센터(ITRC)육성·지원과제 지원으로 수행하였습니다.

키를 아는 경우에만, 워터마킹 정보를 추출하여 낼 수 있다. 따라서, 워터마킹을 제거하려면, 비밀키를 알아내야 하는 암호학적인 공격이 이루어져야 하기 때문에 인지가능 기법에 비해서 효율적인 지적 재산권 보호 효과를 가져 올 수 있다. 그러나, 만약 인터넷 상에서 불법적으로 배포되고 있는 디지털 컨텐츠를 발견하였을 때, 디지털 워터마킹 기법을 사용한 컨텐츠라면, 그 컨텐츠의 원래 저작권자는 누구인지 알 수 있겠지만, 누가 합법적으로 구매한 후에 불법적으로 배포하였는지는 알아낼 수는 없다.

그래서, 새롭게 연구가 시작된 분야는 핑거프린팅(fingerprinting)이라는 분야이다.[20][21]

디지털 컨텐츠에 정보를 삽입하는 방법은 디지털 워터마킹과 동일하다고 할 수 있다. 그러나, 삽입하는 정보의 내용에 있어서는 다르다. 디지털 워터마킹에서는 저작권자나 판매권자의 정보가 삽입되지만, 핑거프린팅에서는 디지털 컨텐츠에 대한 사용권을 구입한 구매자의 정보가 삽입이 되는 것이다. 따라서, 디지털 워터마킹을 사용했을 때는 판매되는 모든 컨텐츠에 삽입되는 정보가 모두 동일한 반면에, 핑거프린팅을 사용하였을 때에는 판매되는 컨텐츠들이 구매한 사용자들마다 조금씩 다른 삽입정보를 가지게 된다. 만약, 불법 재분배된 디지털 컨텐츠에서 핑거프린팅 정보를 추출하게 되면, 그 컨텐츠가 어떤 구매자에게 판매된 컨텐츠인지를 식별(identification)할 수 있게 되고, 법적인 조치를 가할 수 있게 된다.

따라서, 일반적인 구매자들로 하여금 불법적인 재분배에 대한 의욕을 저하시키는 효과를 가져올 수 있게 되며, 디지털 컨텐츠 산업의 발전에 좋은 영향을 줄 수 있으리라 생각된다.

본 논문에서는 지적 재산권 보호를 위한 핑거프린팅 프로토콜의 현재까지의 연구동향을 분석하고, 그 중에서 특히 익명 핑거프린팅이라는 분야를 살펴본다. 익명 핑거프린팅 프로토콜은 최근 연구되어진 분야인데, 대표적인 몇 가지 익명 핑거프린팅 프로토콜을 제시하고, 각각의 장단점과 개선 방안을 고려해 보고자 한다. 또한, 익명 핑거프린팅 프로토콜에 있어서 중요한 요구사항들인 구매자의 익명성(anonymity) 보장, 강건성(robustness), 조건부 추적성(conditional traceability), 공모 허용(collusion tolerance) 등과 같은 사항에 대해서도 언급하고자 한다.

II. 핑거프린팅 프로토콜의 연구 동향

앞 절에서 언급한 디지털 워터마킹에 대한 연구에 있어서는, 원래의 컨텐츠의 품질에 손상이 덜 가면서도, 압축이나 변형 등의 외부적인 요인에도 잘 견디도록 하기 위해서는 정보를 어떤 방법으로 어떤 부분에 삽입을 해야 하는지에 대한 연구가 진행이 되어지고 있다. 디지털 컨텐츠 종류에 따른 내부 구조나 프로세싱 절차 등에 많이 의존적인 연구라고 할 수 있다. 반면에 핑거프린팅 프로토콜에 대한 연구는 일반적으로 디지털 컨텐츠들의 실제적인 구조 차원과는 독립적으로 암호학적인 프로토콜의 차원에서 연구되어지는 경우가 많다. 이것은 핑거프린팅에서는 암호학적인 프로토콜 자체가 차지하는 비중이 크기 때문이라고 생각되어진다. 또한, 암호학적인 프로토콜만 완성되면, 실제의 구현(정보의 삽입)에 있어서는 기존의 연구되어진 디지털 워터마킹 기술을 그대로 핑거프린팅에도 적용할 수 있기 때문이라고도 생각되어진다.

앞으로 언급할 핑거프린팅 프로토콜의 효과적인 설명을 위하여 몇 가지 용어들을 다음과 같이 정의한다. 먼저, 지적 재산권을 보호하고자 하는 대상 디지털 컨텐츠를 C라고 하고, 컨텐츠에 삽입되어지는 핑거프린팅 정보를 E라고 한다. E가 삽입되어서 새롭게 생성된 컨텐츠를 EC라고 한다. 디지털 컨텐츠를 판매하고자 하는 판매자를 M이라고 하고, M으로부터 합법적으로 컨텐츠 C를 구입하는 구매자를 B라고 한다. 컨텐츠 C의 내부에 구매자 B에 해당하는 핑거프린팅을 삽입하여 새롭게 구성된 컨텐츠를 $EC(B)$라고 한다. 특정 구매자 B가 판매자 M의 동의 없이 불법적으로 $EC(B)$를 배포하는 것을 재분배(redistribution)라고 하고, 이렇게 불법적으로 재분배하는 합법적인 구매자 B를 계약위반자(traitor)라고 한다. 그리고, EC를 공격하여서 핑거프린팅 정보를 없애거나 변형하려고 시도하는 공격자를 A라고 한다. 또한, 두 명 이상의 A가 다수의 EC를 비교하여, 핑거프린팅 정보의 삽입 위치나 유형 등을 분석하고 공격하는 형태를 공모(collusion)라고 한다.

핑거프린팅에 대한 개념이 대두된 것은 Wagner의 논문[1](1983년)에서부터라고 할 수 있다.

그 후 여러 명의 공모에 의한 공격에 대해서도 연구되어 왔다[13]. 이를 보완하여 대규모 공모(larger collusion)에 대한 해결책이 Boneh 등의 논문[2](1995)에서 연구되어졌다. 핑거프린팅에서의 공모에 대한 연구는 지금도 계속 연구되고 있는 분야이다.

계약위반자 추적(tracing traitors)은 주문형 TV 방송이나 주문형 Video방송 등에서 사용되는 암호학적인 키(key)들에 대한 핑거프린팅 기법이라고 할 수 있는데, 이에 대한 연구는 Chor 등[3]에 의해서 연구가 시작되었고, Noar, Pinkas[4]와 Kurosawa[5], Pfitzmann[6]등에 의해서 연구가 진행되고 있다.

Pfitzmann은 비대칭형 핑거프린팅(asymmetric fingerprinting)이라는 새로운 핑거프린팅 개념을 도입하였다[7]. 기존의 핑거프린팅 프로토콜을 이 개념을 기준으로 재고해보면, 대칭형 핑거프린팅(symmetric fingerprinting)이 된다. 대칭형 핑거프린팅이란 의미는 구매자 B가 판매자 M에게서 C를 구입하려고 할 때, 핑거프린팅이 삽입된 컨텐츠 $EC(B)$를 판매자 M도 알고 구매자 B도 안다는 의미이다. 이것은 나중에 불법적으로 배포된 컨텐츠를 발견하고 이에 대한 구매자를 식별해 냈을 때, 지적 재산권 침해에 대한 완벽한 증명이 불가능함을 내재하고 있다. 왜냐하면, 구매자 B가 $EC(B)$를 구입하였다는 사실을 판매자 M도 알고있기 때문에, 구매자 B가 실제로 불법 재분배를 하였는지, 아니면 판매자 M이 구매자 B를 가장(masquerading)하여 불법 재분배를 하였는지를 구별해 낼 수 없기 때문이다. 반면에 비대칭형 핑거프린팅은 구매자 B가 $EC(B)$를 구매하는 과정에서, 판매자 M은 $EC(B)$를 알지 못하도록 하는 핑거프린팅 프로토콜이다. 따라서, 불법적인 재분배물(redistributed copy)로부터 핑거프린팅을 추출하여 구매자를 식별하는 것이 가능하다면, 그것 자체가 지적 재산권 침해의 완벽한 증거가 된다. 비대칭형 핑거프린팅에서도 역시 공모를 통한 공격에 대비하는 것이 중요한 연구 방향 중에 하나이다. 이에 대한 연구가 많이 진행되고 있다.

그 후, Pfitzmann 등은 구매자의 익명성을 보장하는 익명 핑거프린팅(anonymous fingerprinting) 프로토콜을 제시하였다[8]. 이것은 비대칭형 핑거프린팅의 개념을 포함하는 프로토콜로서, 판매자 M은 구매자 B에게 컨텐츠를 판매하지만, 프로토콜 진행 과정에서 구매자 B의 신원을 알지 못하도록 하는 프로토콜이다. 이것은 구매자 B가 사전에 제 3자 T에게 임시 ID를 등록하고 진행하는 프로토콜이기 때문에, 판매자는 재분배자 식별 프로토콜을 진행할 때 제 3자 T의 도움을 받음으로써 구매자 B의 신분을 밝혀낼 수 있다. 익명 핑거프린팅에 대한 연구는 Pfitzmann과 Domingo-Ferrer에 의해서 활발하게 진행되어지고 있다[8][9][10][11][12]. 익명 핑거프린팅 프로토콜은 인터넷에서 디지털 컨텐츠 거래를 활성화하는데 긍정적인 영향을 줄 수 있는 것으로 보여진다.

III. 익명 핑거프린팅 프로토콜의 비교 분석

여기서는 Pfitzmann과 Domingo-Ferrer가 연구 발표한 익명 핑거프린팅 프로토콜들을 발표된 순서대로 비교 분석해 보고자 한다.

1. Pfitzmann 프로토콜A,B[8]

Pfitzmann은 처음으로 익명 핑거프린팅의 개념을 소개하면서, 공모가 없는 상황을 가정한 프로토콜을 먼저 제시하였다.(이 프로토콜을 편의상 프로토콜A라 한다) 그리고, 이 프로토콜A를 공모 허용성을 가지는 프로토콜로 발전시키기 위한 프로시저에 대한 연구도 하였다.(이 프로시저를 포함하는 프로토콜A를 편의상 프로토콜B라 한다)

프로토콜A에 대한 설명은 다음과 같다.

1단계-등록(registration) : 구매자 B는 임시 공개키/비밀키쌍을 만들어 등록 센터(registration center) R에 본인확인 절차와 키 검증 절차를 거친 후, 임시 공개키에 대한 등록 센터 R의 인증서를 받는다. 이 과정에서 임시로 만든 공개키와 실제 본인의 신원이 등록 센터 R에 저장되게 된다.

2단계-핑거프린팅 : 구매자 B는 컨텐츠 C를 구입한다는 내용의 문장 *text*를 만들고, 여기에 자신이 등록 센터에 등록한 공개키에 해당하는 비밀키로 서명을 한다. 그리고, 서명과 *text*, 구매자의 임시 공개키, 그리고, 공개키에 대한 인증서를 연결(concatenate)하여 삽입정보 E를 만든다. 이제 만들어진 E는 Brassard 등[16]에 의해서 연구된 Minimum

Disclosure Proof of Knowledge(MDPK) 프로토콜을 사용하여 컨텐츠 C에 삽입하는 절차를 밟는다. 여기서, 판매자 M은 삽입정보 E의 내용은 알 수 없지만, 구매자의 임시 공개키와 그에 대한 인증서를 영지식 증명을 통해서 확인할 수 있으며, 구매자의 서명의 유효성에 대해서도 영지식 증명을 통해서 의해서 확인 받게 되기 때문에 삽입정보의 유효성에 대해서는 확신할 수 있게 된다.

3단계-식별(identification) : 불법으로 재분배된 컨텐츠 EC를 발견하게 되었을 때, 이 식별과정을 통하여 EC에 삽입된 정보 E를 추출해내게 된다. 이것이 지적 재산권 침해에 대한 첫 번째 증거(proof)가 된다. 그리고, 이것을 등록 센터에 보내고, 임시 공개키에 해당하는 사람의 신원을 알려주도록 요청하거나 유죄를 입증해 주도록 요청하게 된다. 이 요청에 대한 등록 센터의 응답 내용이 두 번째 증거가 된다.

4단계-재판(trial) : 재판 과정에서 3단계에서 추출된 두 가지의 증거를 보이면, 재판관은 이것과 재분배한 것으로 고소된 구매자 B의 서명을 비교하여 최종적인 판결을 하게 된다.

Pfitzmann 프로토콜A의 단점은 다음과 같다.

첫째로, 핑거프린팅 단계에서 MDPK 프로토콜을 블랙 박스 형태로 삽입하여 구현하였는데, 이 프로토콜은 내부적으로 이산 대수 문제 또는 그래프 동형 문제와 같은 어려운 문제를 기반으로 구현되어 있다. 일반적으로 워터마킹은 미리 오프라인에서 계산한 후, 판매 시에는 워터마킹된 컨텐츠를 제공하면 된다. 그러나, 핑거프린팅의 경우에는 구매자마다 삽입정보가 달라지기 때문에, 임의의 구매자가 인터넷 상으로 판매자의 서버에 접속하여 실시간으로 핑거프린팅 프로토콜을 거치며 판매가 이루어져야만 한다. 따라서, 위와 같이 복잡도가 높은 계산을 하는 것은 실제 구현에 불합리하다는 결론을 내릴 수 있다. 핑거프린팅 과정에서의 계산적 복잡도는 앞으로의 프로토콜 비교에서 중요한 기준이 된다.

둘째로, 식별 단계에서 판매자는 추출해낸 증거를 등록 센터에 보내고 결과를 기다려야 한다. 이것은 등록센터가 소수이고 판매자는 다수일 때, 등록센터가 처리할 일이 많아진다는 문제가 있으며, 등록센터의 신뢰성이 높아져야 한다는 가정이 전제되어야만 한다.

Pfitzmann 프로토콜B는 공모 허용성을 가지는 프로토콜이지만, Pfitzmann 프로토콜A보다 더 높은 계산적 복잡도를 가지기 때문에 실제적인 적용은 어려울 것으로 보인다.

2. Domingo-Ferrer 프로토콜A[10]

Domingo-Ferrer의 첫 번째 프로토콜은 다음과 같은 절차를 거친다.

가정 : p는 매우 큰 소수, $q=(p-1)/2$도 소수, G는 Z_p^*군, g는 이산 대수 문제를 풀기가 어려운 수로써, G의 생성자이다.

1단계-등록 : 구매자 B의 실제 공개키/비밀키는 x_B와 $y_B=g^{x_B}$이다. 등록 센터 R은 구매자 B를 위하여 임시 공개키/비밀키쌍 x_r, $y_r=g^{x_r}$을 생성하고, y^r을 구매자 B에게 보낸다. 구매자 B는 $s_1+s_2\equiv x_B \pmod{p}$이 되는 s_1과 s_2를 선택하고, $S_1=y_r^{s_1}$과 $S_2=y_r^{s_2}$를 계산한다. 구매자 B는 등록센터 R에게 자신이 s_1과 s_2를 소유하고 속이지 않고 있다는 사실을 증명한다. 이때, Chaum 등[15]에 의해서 연구된 이산대수의 소유를 영지식으로 증명해 주는 프로토콜을 사용하여 증명한다. 그리고 나서, $y_2=g^{s_2}$를 계산하여 등록 센터 R에게 보내준다. 등록센터 R은 $S_1S_2=y_B^{x_r}$이 성립하는 것과 $y_2^{x_r}=S_2$이 성립하는 것을 검증(verify)해본다. 만약, 이것이 모두 정확한 값이면, 두 가지의 인증서 $Cert(y_r\|S_1)$과 $Cert(y_r\|S_2)$를 생성해서, 처음에 만들었던 x_r과 함께 구매자 B에게 보내주게 된다.

2단계-핑거프린팅 : 구매자 B는 컨텐츠 C를 구입한다는 내용의 문장 *text*를 만들고, 여기에 등록 단계에서 설정한 s_2로 서명 *sig*를 생성

한다. 그리고, y_r, y_2, [S_1, $Cert(y_r||S_1)$], *text*를 판매자 M에게 보낸다. 이때, 서명 *sig*는 보내지 않는다. 판매자 M은 S_1의 인증서를 검증해서, 이상 유무를 파악한다. 만약, 이상이 없으면, 구매자 B와 판매자 M은 Chaum 등[14]에 의해서 연구된 Secure Multi-Party Computation(SMPC) 프로토콜을 시작한다. SMPC 프로토콜은 서로의 입력을 보여주지 않으면서, 올바른 입력을 하였는지는 서로가 확인할 수 있는 기능을 제공한다. 그리고, 계산된 결과값도 양측에 비밀리에 전달해주는 기능을 지원한다. 이 프로토콜에 따라서 구매자 B는 SMPC의 입력으로 x_r, *sig*, S_2, $Cert(y_r||S_2)$을 넣는다. 판매자 M은 y_r, *text*, y_2와 판매할 컨텐츠 C를 SMPC의 입력값으로 넣는다. 결과값은 세 가지가 나오게 되는데, 그중 처음 두개의 결과값은 판매자 M에게만 전달되는 값으로써, 구매자 B가 올바른 입력을 제공하였는지를 검증할 수 있는 참, 거짓 출력이다. 만일 이 두 개의 출력 중 하나라도 거짓값이 출력되면, 다음 세 번째의 결과값은 계산되지 않는다. 세 번째 결과값은 아래 수식으로 표현된 핑거프린팅 E가 삽입된 컨텐츠 $EC(B)$이다.

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

이것은 구매자 B에게만 전달되어진다. SMPC가 끝난 후에 판매자 M은 자신의 판매 기록에 [S_1, $Cert(y_r||S_1)$]을 기록해 놓는다.

3단계-식별 : 재분배된 컨텐츠가 발견되면, 판매자 M은 그 컨텐츠로부터 E를 추출해낸다. 그리고, E값을 참고하여, 판매 기록에서 [S_1, $Cert(y_r||S_1)$]를 찾는다. 판매자는 E를 구성하고 있는 요소들의 무결성을 검증해 본다. 그리고 나서, $S_1S_2 = y_B^{x_r}$을 만족하는 y_B가 나올 때까지 공개키 디렉토리를 검색한다. 찾아지는 y_B가 계약위반자의 공개키가 된다.

Domingo-Ferrer 프로토콜A에 대한 평가는 다음과 같다.

첫째로, 식별단계에서 등록 센터의 도움을 받지 않고 판매자가 스스로 재분배자를 찾아낼 수 있다는 점은 장점이라고 할 수 있다. 그러나, 이것은 비효율성을 내포하고 있다. 식별 단계에서의 공개키 디렉토리를 검색하는데 드는 비용을 고려해본다면, 매우 비효율적임을 알 수 있다. 공개키 디렉토리에 등록된 사람의 수를 n이라고 한다면, y_B가 찾아질 때까지 평균적으로 수행되는 지수 연산(exponential computation)의 횟수는 평균적으로 $\frac{n}{2}$ 번이다.

셋째로, Pfitzmann 프로토콜A와 마찬가지로 핑거프린팅 단계에서 SMPC라는 블랙 박스 형태의 프로토콜을 도입하여 익명성을 구현하였다는 것이다. 이 SMPC의 계산적 복잡도는 MDPK 프로토콜의 계산적 복잡도와 비슷하다. 따라서, 핑거프린팅 단계에서 높은 계산적 복잡도가 필요하다는 단점은 극복되지 못했다고 할 수 있다.

3. Domingo-Ferrer 프로토콜B[11]

Domingo-Ferrer가 두 번째로 제시한 핑거프린팅 프로토콜B는 구매자 B가 하는 모든 계산이 스마트카드 상에서 가능하도록 하는 프로토콜이다. 기존 Domingo-Ferrer 프로토콜A를 수정하였다. 다음과 같은 절차를 거치며 가정은 Domingo-Ferrer 프로토콜A의 가정과 같으며, 추가적으로 $l < u < n$의 성질을 만족하는 l, u, n의 값이, 안전성에 관계된 매개변수로써, 신중하게 미리 정해져야 한다는 조건이 있다.

1단계-컨텐츠 초기화 : 구매자가 판매할 컨텐츠를 초기화한다. 컨텐츠 C를 비트 스트림으로 간주하고, n개의 서브 컨텐츠들로 나눈다.

$$C = C_1||C_2||C_3||.....||C_n$$

그리고, 서브 컨텐츠들 중 i = 1부터 u까지의 서브 컨텐츠들에 대해서 두 가지 변형된 형태 C_i'와 C_i''를 구성한다. C_i'는 m개(m은 1보다 큰 홀수)의 0으로 이루어진 벡터를 정해진 위치에 삽입해서 구성하고, C_i''는 m개의 1로 이루어진 벡터를 정해진 위치에 삽입하여 구성한다. 결국은 C_i', C_i''는 각각 한 비트의 E값을 저장하는 것이 된다. 0이나 1을 한 비트만 삽입하지 않고 m개의 0의 또는 1의 벡터를 삽입하는 이유는 공모나 변형에 의한 공격으

로 인해 비트값이 소멸되거나 역전되는 것을 막기 위한 방법으로서의 의미가 있다. 따라서, 나중에 재분배된 컨텐츠에서 각 서브 컨텐츠별로 정해진 위치에서 벡터를 추출하고, 벡터들마다 0이 과반수인지 1이 과반수인지를 계산하여서 각 서브 컨텐츠가 포함하는 비트값이 0인지 1인지를 결정하고 전체 삽입정보 E를 구성하게 되는 것이다.

2단계-등록 : 구매자 B가 등록 센터 R을 통해 자신의 신원을 증명한 후, S_1과 S_2에 대한 인증서를 등록 센터로부터 발급받게 된다. 세부적인 과정은 Domingo-Ferrer 프로토콜A의 등록 단계와 동일하다.

3단계-핑거프린팅 : 구매자 B는 컨텐츠 C를 구입한다는 내용의 문장(text)을 만들고, 여기에 등록 단계에서 설정한 s_2로 서명 sig를 생성한다. 그리고, y_r, y_2,[S_1, $Cert(y_r \| S_1)$], $text$를 판매자 M에게 보낸다. 이때, 서명 sig는 보내지 않는다. 판매자 M은 S_1의 인증서를 검증(verify)해서, 이상 유무를 파악한다. 여기까지는 Domingo-Ferrer 프로토콜A와 동일하다.

다음 과정은 판매자 M이 i = 1부터 l까지에 해당하는 서브 컨텐츠를 보내되 C_i'이나 C_i'' 중에서 하나를 보낸다. 이때 판매자는 Berger 등[17]에 의해서 연구되어진 1-2 provably Secure Oblivious Transfer Scheme (1-2 SOTS)을 사용한다. 따라서, 판매자 M은 구매자 B에게 어떤 서브 컨텐츠들이 선택되어져서 전달되었는지 알지 못한다. 구매자 B는 l개의 서브 컨텐츠 $C_1^*, \ldots, C_l^*$를 받은 후, 그것을 모두 연결한 값 $C_{(l)}^* = C_1^* \| \ldots \| C_l^*$를 미리 약속되어진 해쉬함수 H를 통해서 해쉬하고, 해쉬값 $H(C_{(l)}^*)$값을 구한다. 그리고, $H(C_{(l)}^*)$에 구매자가 서명하여 sig_l^*를 구성한다. 그 후, 생성된 $H(C_{(l)}^*)$와 sig_l^*를 판매자 M에게 전달해준다. 이 시점에서 구매자 B는 판매자 M에게 $H(C_{(l)}^*)$가 올바르게 계산되었다는 것을 일반적인 영지식 증명(Zero-Knowledge Proof, ZKP) 프로토콜을 사용하여 증명해야 한다. 만약, 구매자 B가 $H(C_{(l)}^*)$의 정당성에 대해서 증명하지 못하면, 프로토콜을 멈춘다. 단지 l개의 서브 컨텐츠만 전달되고 끝나게 된다. 따라서, l값은 n에 비해 많이 작은 값이어야 한다.

만약, 구매자 B가 $H(C_{(l)}^*)$에 대한 증명을 하게 되면, 다시 $i = l+1$부터 u까지에 해당하는 서브 컨텐츠를 보내되 C_i'이나 C_i'' 중에서 하나를 1-2 SOTS을 통해서 보낸다. 역시, 판매자 M은 구매자 B에게 어떤 서브 컨텐츠들이 선택되어져서 전달되었는지 알지 못한다. 구매자 B는 $u-l$개의 서브 컨텐츠 $C_{l+1}^*, \ldots, C_u^*$를 받은 후, 그것을 모두 연결한 값 $C_{(u)}^* = C_{l+1}^* \| \ldots \| C_u^*$를 해쉬함수 H를 통해서 해쉬값 $H(C_{(u)}^*)$값을 구하고, 거기에 서명하여 sig_u^*를 구성한다. 구매자 B는 $H(C_{(u)}^*)$와 sig_u^*를 판매자 M에게 전달해주고, 판매자 M에게 $H(C_{(u)}^*)$가 올바르게 계산되었다는 것을 일반적인 영지식 증명 프로토콜을 사용하여 증명해야 한다. 만약, 구매자 B가 $H(C_{(u)}^*)$의 정당성에 대해서 증명하지 못하면, 프로토콜을 멈춘다. 여기까지 전송된 서브 컨텐츠의 개수는 u개이다. u값의 크기는 n에 비해 너무 작아서도 안 된다. 왜냐하면, 모든 핑거프린팅 단계가 정상적으로 종료한 후에 구매자 B가 u까지의 서브컨텐츠를 제외한 $n-u$개의 서브 컨텐츠만을 재분배할 여지가 있기 때문이다. 또 한편으로 u값이 n에 비해 크다면, 구매자 B는 이 시점에서 $H(C_{(u)}^*)$값을 제대로 증명하지 않고 프로토콜을 종료하고, 값을 지불하지 않은 채로 지금까지 받은 u개의 서브 컨텐츠로 컨텐츠를 구성하려는 시도를 하게 되기 때문이다. 따라서, u값을 신중하게 정해주어야만 하고, 또 남은 $n-u$개에 구매자 B가 중요하게 생각하는 정보가 들어 있도록 하는 것이 필요하다.

Domingo-Ferrer 프로토콜B의 장단점을 평가하면 다음과 같다.

첫째로, 구매자 B측에서 하게 되는 연산이 스마트 카드에서도 가능할 수 있음을 보여주고 있다는 점은 장점으로 평가될 수 있다.

둘째로, Pfitzmann 프로토콜A의 핑거프린팅 단계에서나 Domingo-Ferrer 프로토콜A에서 사용된 MDPK나 SMPC를 이용하지 않았다. 그러나, 큰 발전은 없다고 볼 수 있다. 일반적인 ZKP를 사용하는 것도 계산적 복잡도가 높기 때문이다.

4. Pfitzmann 프로토콜C[9]

Pfitzmann은 기존의 자신의 논문[8]에서 제시한 익명 핑거프린팅 프로토콜을 크게 두 부분으로 나누어서 보고 있다. 첫 번째 부분은 등록센터에 구매자 B가 자신의 임시 공개키를 등록하고 인증서를 발급 받아서, 이것이 나중에 식별 단계에서의 B의 신분을 밝혀 내는 중요한 요소로 작동하게 하는 부분(등록 및 식별 단계)이며, 두 번째 부분은 실제적으로 삽입정보 E를 컨텐츠 C에 삽입하여 $EC(B)$를 만들어 내는 부분(핑거프린팅 단계)으로 나누었다. Pfitzmann의 새로운 논문[9] 에서는 이 두 부분 중에서 첫 번째 부분의 효율성을 높이기 위한 시도를 하였다.(이를 프로토콜C라 한다) 기존의 Pfitzmann 프로토콜A, B에서는, 첫 부분의 설계를 등록센터 R에 구매자 B가 임시 공개키를 등록하는 것으로 했지만, Pfitzmann 프로토콜C에서는 이것을 전자 화폐(electronic coins)의 개념을 응용하는 것으로 대체하였다. 여기서 사용되는 전자 화폐는 단순히 등록 및 식별 단계에서 사용될 뿐이지 화폐적인 가치는 지니지 않는다. 등록 및 식별 단계를 제외하고는 원래의 Pfitzmann 프로토콜A를 사용하였다.

이러한 접근 방식은 전자 화폐가 기본적으로 내포하고 있는 특성을 이용하여, 사용자의 익명성을 유지하면서도, 조건부 추적성(conditional traceability)을 이용한 재분배자 식별이 가능하게 만들었다. 그러나, 핑거프린팅 단계에서의 계산적 복잡도는 역시 해결되지 못한 상태로 남아 있다. 단지, 첫 번째 부분을 명백하게 분석이 가능한 암호학적 요소들을 사용했다는 측면이 장점이라고 본다.

5. Domingo-Ferrer 프로토콜C[12]

Domingo-Ferrer는 최근 Committed Oblivious Transfer(COT)[18] 기법을 응용하여, 기존 Domingo-Ferrer 프로토콜B를 개선하였다. COT는 명백하게 계산적 복잡도가 분석되어 있는 기법으로서, 기존의 MDPK나 SMPC 또는 일반적인 영지식 증명 프로토콜을 이용하던 핑거프린팅 프로토콜보다 훨씬 더 구현 가능한 복잡도를 가진다고 볼 수 있다.

이 프로토콜을 Pfitzmann이 나눈 첫 번째 부분과 두 번째 부분으로 나누는 기준으로 볼 때, 분석하면 다음과 같다.

첫 번째 부분은 여전히 등록센터 R에 임시 공개키를 등록하는 방식을 취하고 있다. 그러나, 계산적 복잡도는 분석되어 있다.

계산적 복잡도가 가장 높은 두 번째 부분(핑거프린팅 단계)에서는 앞에서 언급한 COT를 사용하였기 때문에 익명 핑거프린팅 프로토콜의 실제 적용 가능성을 매우 높였다고 평가된다.

이 프로토콜의 단점으로 볼 수 있는 한가지는 식별단계가 비효율적이다는 것이다. 실제로 식별 단계에서는 예상되는 다수의 구매자들 각각에 대해서 모두 식별 프로토콜을 진행해야 하는 번거로움이 있다.

6. 현재까지의 프로토콜들에 대한 요약

현재까지 제안된 익명 핑거프린팅 프로토콜에 대해서 짧게 결론을 내려본다면 다음과 같다.

첫 번째로, Pfitzmann 프로토콜C는 전자 화폐 개념을 기반으로 하여서, 사용자의 등록 및 식별단계의 계산적 복잡도를 낮춘 프로토콜이라 할 수 있다.

두 번째로, Domingo-Ferrer 프로토콜C는 COT를 사용하여서 컨텐츠에 정보를 삽입하는 단계에서의 시간적 복잡도를 명백하고 실제적으로 낮춘 프로토콜이라 할 수 있다.

세 번째로, 공통적인 단점은 디지털 컨텐츠 자체에 대한 공격으로 인해 핑거프린팅 정보가 손상되는 것에 대해서는 적극적으로 고려하지 않았다는 점이다. 앞에서 언급하지는 않았지만, 이 문제점은 지금까지 분석해 본 익명 핑거프린팅 프로토콜에 모두 다 존재하는 단점이라고 할 수 있다. 그러나, 디지털 컨텐츠의 지적 재산권 보호를 위한 익명 핑거프린팅 프로토콜이 실효를 거두기 위해서는 컨텐츠에 대한 공격을 고려하는 프로토콜로 발전해야 된다고 본다.

이 외에도 식별단계의 효율성 문제와 공모에 대한 방지를 효과적으로 구현하는 것에 대한 연구는 지속되어야 할 것으로 보인다. 구체적인 요구사항에 대한 것은 다음 장에서 다룬다.

IV. 핑거프린팅에 필요한 요구사항 분석

이 장에서는 디지털 컨텐츠에 핑거프린팅 프로토콜을 적용하기 위해 만족되어야 하는 일반적인 요구사항을 살펴보고, 효과적인 익명 핑거프린팅 프로토콜은 어떠해야 하는 지를 고찰해 보고자 한다.

익명 핑거프린팅 프로토콜에 필요한 요구사항은 일반적으로 디지털 워터마킹 프로토콜에 필요한 요구사항을 모두 포함하며, 몇 가지 요구사항이 추가적으로 만족되어야 한다.

일반적으로 디지털 워터마킹과 익명 핑거프린팅에서 공통적으로 만족되어야 하는 요구사항들은 아래와 같다.

1. 컨텐츠 품질 보장성

컨텐츠에 정보를 삽입하게 되면, 원래 컨텐츠에 노이즈(noise)가 삽입되는 것과 같은 양상이 된다. 따라서, 어떻게, 어디에, 얼마나 많은 정보를 삽입하느냐에 따라 정보가 삽입된 컨텐츠의 품질이 차이가 나게 된다. 컨텐츠의 품질에는 손상을 주지 않으며 정보를 안전하게 삽입하려는 연구는 계속 진행되어져 오고 있다. 일반적인 비트맵 이미지를 예를 들자면, 각 픽셀을 표현하는 비트들 중에서 LSB(least significant bit)를 정보 삽입에 이용하는 것이 바로 컨텐츠의 품질에 손상을 최소한으로 줄이기 위함이다. 물론, 이것은 아주 기초적인 것으로써, 큰 실효성은 없다. 왜냐하면, JPEG과 같은 이미지 압축(compression)을 수행할 때에는 LSB는 거의 모두 제거되어지기 때문이다. 압축 과정을 고려한 정보 삽입에 대한 연구는 계속해서 이루어지고 있다.

2. 강건성(robustness)

컨텐츠를 재분배하려고 하는 공격자는 컨텐츠에 들어있는 워터마킹 정보나 핑거프린팅 정보에 손실을 주기 위해서, 컨텐츠를 변형하거나 일부를 잘라내거나, 축소 또는 확대하는 등의 조작을 가할 수 있다. 강건성은 이러한 컨텐츠 조작에 대한 공격에 대해서 삽입된 정보가 얼마나 잘 견뎌내어서, 컨텐츠로부터 다시 삽입 정보를 추출해 내려고 할 때, 성공을 거둘 수 있느냐를 평가하는 부분이라고 할 수 있다.

디지털 워터마킹과 달리, 익명 핑거프린팅 프로토콜에서 추가적으로 필요한 요구사항은 아래와 같다.

3. 비대칭성(asymmetry)

핑거프린팅된 컨텐츠를 구매자만이 알고, 판매자는 알지 못하도록 하는 것을 비대칭성이라고 한다. 비대칭성을 갖는 핑거프린팅 프로토콜은 재분배자 식별과정을 거쳐서 나온 결과물이 완벽한 법적인 증거물로 사용될 수 있다. 비대칭성을 갖지 않는 핑거프린팅 프로토콜은 판매자가 핑거프린팅 컨텐츠를 알고 있다는 사실 때문에 지적 재산권 침해에 대한 완벽한 증거물 제시가 불가능하다.

4. 익명성(anonymity)

익명 핑거프린팅 프로토콜에서 중요한 요구사항은 바로 구매자의 익명성 보장이다. 일반적으로 인터넷에서의 전자 상거래의 특징중의 하나는 익명으로 물건을 구입할 수 있다는 점이다. 실제로 익명 핑거프린팅 프로토콜이 최근 연구가 활발히 이루어지고 있는 이유도 구매자들이 자신의 프라이버시를 보호받으며 컨텐츠를 구입하려는 의도를 반영한 것이라고 할 수 있다. 실제로 앞 절에서 분석된 프로토콜들은 다양한 방법으로 구매자의 익명성을 보장하려고 시도하였다.

5. 조건부 추적성(conditional traceability)

앞에서 언급된 비대칭성 및 익명성 보장과 더불어 불법적으로 재분배된 컨텐츠에 대한 구매자를 식별해 낼 수 있는 조건부 추적성이 제공되어야지만, 구매자들이 컨텐츠를 재분배 하고자 하는 생각을 단념시킬 수 있다. 비대칭성 및 익명성, 추적성이 함께 고려되어져야 하기 때문에 익명 핑거프린팅 프로토콜이 쉬운 문제만은 아니다. 대부분의 익명 핑거프린팅 프로토콜에 있어서 전체적인 계산적 복잡도는 이 세 가지 조건을 동시에 만족시키기 위한 단계에서의 계산적 복잡도에 의해서 좌우되어진다.

6. 공모 허용(collusion tolerance)

디지털 워터마킹이 삽입된 컨텐츠와는 달리 핑거프린팅이 삽입된 컨텐츠는 삽입되는 내용이 구매자에 따라서 모두 다르다. 따라서, 다수의 구매자들이 서로 공모하여 핑거프린팅이 삽입된 다수의 컨텐츠를 서로 비교하여 핑거프린팅이 삽입된 위치를 파악할 가능성이 높아지게 된다. 핑거프린팅 위치가 파악되면, 핑거프린팅 비트를 지운다든지, 아니면 전혀 상관없는 핑거프린팅 비트를 만들어 삽입하여 컨

텐츠를 재구성할 수 있으며, 이를 재분배하게 된다.

이와 같은 공모를 대비하여서, 핑거프린팅 프로토콜에서는 공격자에게 많은 컨텐츠가 주어졌다할지라도 핑거프린팅 정보를 찾아낼 수 없어야 한다는 요구사항이 만족되어야 한다. 공모 허용성을 높이기 위해서도 많은 연구가 되어 왔지만, 아직도 높은 계산적 복잡도를 가지고 있는 수준이다.

V. 결 론

본 논문에서는 지금까지 연구된 익명 핑거프린팅 프로토콜들을 비교 분석하였고, 효과적인 익명 핑거프린팅 프로토콜이 갖추어야 할 요구사항을 고려해 보았다. 전자 화폐를 기반으로 한 익명 핑거프린팅 프로토콜과 COT를 기반으로 하는 익명 핑거프린팅 프로토콜이 현재까지의 최선의 해결책이라 볼 수 있다. 그러나, 컨텐츠에 대한 공격을 대비한 연구가 추가적으로 이루어져야 한다. 익명 핑거프린팅 프로토콜에 대한 연구는 디지털 컨텐츠 산업의 발전에 있어서 중요한 역할을 수행하리라 전망된다.

참 고 문 헌

[1] N. R. Wagner, "Fingerprinting", *IEEE Symposium on Security and Privacy*, 1983

[2] D. Boneh and J. Shaw, "Collusion-secure Fingerprinting for Digital Data", *Crypto '95*, LNCS 963, Springer-Verlag, pp. 452-465, 1995

[3] B. Chor, A. Fiat and M. Naor, "Tracing Traitors", *Crypto '94*, LNCS 839, Springer-Verlag, pp. 257-270, 1994

[4] M. Naor and B. Pinkas, "Threshold Traitor Tracing", *Crypto '98*, LNCS 1462, Springer-Verlag, pp. 502-517, 1998

[5] K. Kurosawa and Y. Desmedt, "Optimum Traitor Tracing and Asymmetric Schemes", *Eurocrypt '98*, LNCS 1403, Springer-Verlag, pp. 145-157, 1998

[6] B. Pfitzmann, "Trials of Traced Traitors", *The first International Information Hiding Workshop*, LNCS 1174, Springer-Verlag, pp. 49-64, 1996

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

[8] B. Pfitzmann and M. Waidner, "Anonymous Fingerprinting", *Eurocrypt '97*, LNCS 1233, Springer-Verlag, pp. 88-102, 1997

[9] B. Pfitzmann and A. Sadeghi, "Coin-Based Anonymous Fingerprinting", *Eurocrypt '99*, LNCS 1434, Springer-Verlag, pp. 150-164, 1999

[10] J. Domingo-Ferrer, "Anonymous Fingerprinting of Electronic Information with Automatic Identification of Redistributors", *IEE Electronics Letters*, vol. 34, no. 13, 1998

[11] J. Domingo-Ferrer, "Efficient Smart-Card Based Anonymous Fingerprinting", *CARDIS '98*, 1998

[12] J. Domingo-Ferrer, "Anonymous Fingerprinting Based on Committed Oblivious Transfer", *PKC '99*, LNCS 1560, Springer-Verlag, pp. 43-52, 1999

[13] G. R. Blakley, C. Meadows and G. B. Purdy, "Fingerprinting Long Forgiving Messages", *Crypto '85*, LNCS 218, Springer-Verlag, pp. 180-189, 1985

[14] D. Chaum, I. B. Damgaard and J. van de Graaf, "Multiparty Computations Ensuring Privacy of Each Party's Input and Correctness of the Result", *Crypto '87*, LNCS 293, Springer-Verlag, pp. 87-119, 1987

[15] D. Chaum, J. H. Evertse, and J. van de Graaf, "An Improved Protocols for Demonstrating Possession of Discrete Logarithms and some Generalizations", *Eurocrypt '87*, LNCS 304, Springer-Verlag, pp. 127-141, 1987

[16] G. Brassard, D. Chaum, C. Crepeau, "Minimum Disclosure Proofs of Knowledge", *Journal of Computer and System Sciences*, vol. 37, pp. 156-189, 1998

[17] R. Berger, R. Peralta and T. Tedrick, "A Provably Secure Oblivious Transfer Protocols", *Eurocrypt '84*, LNCS 209, Springer-Verlag, pp. 408-416, 1984.
[18] C. Crepeau, J. van de Graaf and A. Tapp, "Committed Oblivious Transfer and Private Multi-party Computation", *Crypto '95*, LNCS 963, Springer-Verlag, pp. 110-123, 1995
[19] S. Brands, "Untraceable Off-line Cash in Wallet with Observers", *Crypto '93*, LNCS 773, Springer-Verlag, pp. 302-318, 1994
[20] S. Katzenbeisser and F. A. P. Petitcoals (editors), *Information Hiding: techniques for steganography and digital watermarking*, pp. 175-190, Artech House, 2000
[21] R. Oppliger, *Security Technologies for the World Wide Web*, pp. 307-320, Artech House, 2000

〈著者紹介〉

여 상 수(Sang-soo Yeo)
1997년 2월 : 중앙대학교 컴퓨터공학과 졸업
1999년 2월 : 중앙대학교 컴퓨터공학과 석사
2000년 3월~현재 : 중앙대학교 컴퓨터공학과 박사과정
관심분야 : 컴퓨터 이론, 암호 응용 및 정보보호, 생물정보학

윤 훈 기 (Hun-ki Yun)
2000년 2월 : 중앙대학교 컴퓨터공학과 졸업
2000년 3월~현재 : 중앙대학교 컴퓨터공학과 석사과정
관심분야 : 암호 응용 및 정보보호, 디지털 워터마킹

김 성 권 (Sung-kwon Kim)
1981년 2월 : 서울대학교 계산통계학과 졸업
1983년 2월 : 한국과학기술원 전산학과 석사
1990년 6월 : University of Washington 전산학 박사
1991년 3월~1996년 2월 : 경성대학교 전산통계학과 조교수
1996년 3월~현재 : 중앙대학교 컴퓨터공학과 부교수
관심분야 : 암호 응용 및 정보보호, 계산기하학, 생물정보학