韓國 컴퓨터情報學會 論文誌
第10卷 第4號, 2005. 9.

2005-10-4-1-8

디지털 콘텐츠 저작권 보호를 위한 CDN에서 다중서명

신 승 수*, 김 덕 술**

Multisignature Suitable for Digital Contents Copyright Protection on CDN

Seung-Soo Shin*, Duck-Sool Kim**

요 약

디지털 저작권 보호는 저작자의 지적인 재산권과 그에 기울인 노력의 보호 측면에서 중요하며 디지털 콘텐츠 산업의 발전을 위해 매우 중요하다. 하지만 디지털 콘텐츠는 복제가 용이하고 원본과 복사본이 동일하다는 특성으로 인해 저작권의 보호와 대량 불법 복제 및 불법 유통 방지에 어려움을 겪고 있는 실정이다. CDN에서 디지털 콘텐츠 제공자들은 공동으로 저작된 디지털 콘텐츠에 대한 저작권 보호 방안이 필요하다. 본 논문에서는 공동으로 저작된 디지털 콘텐츠에 대한 저작권 보호를 위하여 부인방지 다중기법을 사용하였다. 부인방지 다중기법에 대한 효율성을 입증하였다.

Abstract

Digital copyright protection is important in the protective side of effort to have leaned to in property right and it which are intelligent of an author and is very important for development of digital contents industry. It is the misgovernment that a reproduction is easy as for the digital contents, and the original and a copy have the same characteristic, and it is so, and is experiencing what is hard for protection of copyright and large quantity illegal copy and illegal distribution prevention. CDN needs a copyright protective plan about the digital contents that digital contents providers were written jointly.

The paper used a non-repudiation multi-technique for copyright protection about the digital contents which were written jointly. The Non-repudiation multi-technique proved efficiency about this.

▸ Keyword : CDN, El-Gamal, Multi-signature, Digital Contents

• 제1저자 : 신승수
• 접수일 : 2005.06.09, 심사완료일 : 2005.07.20
* 동명정보대학교 정보보호학과 교수, ** 동명정보대학교 정보보호학과 교수

Ⅰ. 서 론

초기 인터넷 연구의 대부분은 네트워크 인프라 즉, 데이터 링크, 네트워크, 트랜스포트 계층에 집중되었다. 그러나 웹, 스트리밍 등의 새로운 대표적 응용분야가 발생하고, 이에 대한 수요가 기하급수적으로 증가함에 따라 인터넷 인프라는 한계에 다다랐다. 인터넷 인프라의 확충은 기본적으로 고비용을 요구하기 때문에 연구자들은 애플리케이션 계층에서 해결을 시도하였다. 이로 인해 나온 기술이 콘텐츠 네트워킹 기술이다. 기존 연구들이 네트워크 대역폭 증가, 전송의 효율화에 중점을 두었다면, 콘텐츠 네트워킹 기술은 네트워크에 지능을 부여한다. 사용자와 보다 인접한 위치에 콘텐츠를 준비하고, 사용자에게 가장 인접한 위치에 콘텐츠로 안내함으로써 보다 고품질의 콘텐츠 서비스가 가능하도록 한다.

콘텐츠 네트워킹의 가장 대표적인 기술은 CDN (Contents Delivery Network)이다. CDN은 콘텐츠를 사용자와 보다 인접한 위치로 이동시켜 네트워크 상에서 콘텐츠 전송 비율을 줄인다. 뿐만 아니라, CDN은 지능적 전송과 체계적 관리를 부여함으로써 관리자가 한 지점에서 전체 콘텐츠 전송을 완벽하게 제어할 수 있도록 한다[1].

아무리 좋은 CDN을 갖추고 있어도, 인터넷 자체는 보안을 고려하지 않은 전송매체이기 때문에 보안 문제가 발생한다. 또한 ISP(Internet Services Provider)의 서버 시스템은 불법침입 및 데이터 파괴의 위협에 노출되어 있으며, 해킹이나 크래킹의 위협이 더욱 심해지고 있다. 따라서 서버 시스템 보호를 위한 보안 대책이 요구된다. 디지털 콘텐츠의 안전한 분배를 위해서는 전송되는 디지털 콘텐츠의 보안 기술이 필요하다. 일반적으로 멀티미디어 고품질 콘텐츠는 품질의 손상 없이 불법복제가 가능하다. 또한 인터넷에서 불법 복제된 콘텐츠의 배포는 디지털 콘텐츠 제공자들에게 커다란 경제적 손실을 주고 있다. 불법적인 콘텐츠의 배포를 방지하기 위해서는 디지털 서명이 유용하고 안전하다. 이러한 성질은 다음을 만족시켜야 한다[2].

- 위조 불가(Unforgeable) 조건으로 합법적인 서명자만이 디지털 서명을 생성할 수 있어야 한다.
- 서명자 인증(User Authentication) 조건으로 디지털 서명의 서명자를 누구든지 검증할 수 있어야 한다.
- 부인 불가(Nonrepudiation) 조건으로 서명자는 후에서 명한 사실을 부인할 수 없어야 한다.
- 변경 불가(Unalterable) 조건으로 서명한 문서의 내용을 변경할 수 없어야 한다.
- 재사용 불가(Not Reusable) 조건으로 문서의 서명을 다른 문서의 서명으로 사용할 수 없어야 한다.

본 논문의 구성은 다음과 같다. 2장에서는 서명 및 부인방지에 관련된 연구에 대하여 알아보고 3장에서는 CDN상에서 부인 방지 다중기법을 적용한 기법에 대하여 제안한다. 4장에서 결론 및 향후 연구를 제시한다.

Ⅱ. 기존 연구

공개키 암호 방식을 이용한 디지털 서명 방식은 공개 검증 정보를 공개함으로 누구나 그 서명의 진위를 검증할 수 있어 제한적으로 디지털 서명을 사용하려고 하는 경우 제한할 방법이 없다. 또한 개인적으로나 상업적으로 민감한 응용 분야에서의 서명의 사본이 개인의 이익이나 사생활 노출 위험이 있어 문제점으로 지적되고 있다. 따라서 수신자 자신만이 서명을 확인할 수 있는 경우 혹은 서명자의 동의가 있어야 서명을 확인할 수 있는 경우 등의 다양한 형태의 디지털 서명이 필요할 수 있다.

D. Chaum에 의해서 처음으로 제안된 부인방지 서명기법은 서명자의 동의 없이는 서명을 검증할 수 없는 기법으로 많은 응용 분야를 갖는다[5]. 일반 디지털 서명기법으로 해결할 수 없었던 많은 사회적 영역에 적용될 수 있다. 기업 내의 기밀 전자문서와 같은 경우에 서명된 문서가 복제에 의해서 경쟁 관계에 있는 기업으로 유출될 경우에 기업의 손익에 큰 영향을 미칠 수 있다. 특히 일반 서명기법으로 서명된 경우에 그 특성상 모든 사용자가 서명의 타당성을 검증할 수 있으므로, 경쟁 기업에서 쉽게 해당 전자문서의 서명을 검증할 수 있게 된다. 따라서 서명자의 동의 없이는 해당 문서의 서명을 검증할 수 없도록 하는 방법이 필

ㄴ하게 되며, 원하는 수신자만 서명검증을 할 수 있도록 하
ㄴ 특성을 갖는 부인방지 서명기법의 적용이 필수적이다.

El-Gamal 서명기법은 1985년 발표된 디지털 서명으로 ㄴ 안전성은 이산대수문제를 기반으로 하고 있다. El-Gamal 디지털 서명은 정보보호 기능 없이 서명만을 위해 고안된 방식이다[4].

.1 El-Gamal 서명기법

El-Gamal 서명기법은 $GF(p)$상에서의 이산대수문제의 ㅣ려움에 기반 한 서명방식이다. p는 큰 소수로 유한체 $GF(p)$상에서 법 p에 대한 이산대수를 구하는 것이 계산 ㅏ 불가능할 때 $GF(p)$를 암호학적으로 안전한 유한체라 ㅣ의하고 g는 $GF(p)$상에서 정의된 생성자(Generator) ㅣ다[6].

서명자의 비밀키 x, 공개키 y, 서명 대상 메시지 m ㄴ 다음과 같다.

$$x, m \in Z_{p-1},\ y \equiv g^x \bmod p$$

El-Gamal 디지털 서명방식의 구성은 서명 생성 프로토 ㄹ과 서명 검증 프로토콜로 (그림 1)과 같다.

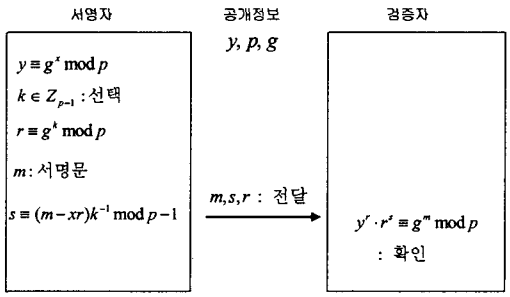

그림 1. El-Gamal 디지털 서명 생성과 검증
Fig 1. EL-Gamal digital signature and verification

서명 생성 프로토콜 순서는 다음과 같다. 서명자는 $\gcd(k, p-1) = 1$을 만족하는 $k \in Z_{p-1}$을 선택하여 r ㅏ s을 다음과 같이 계산한다.

$$r \equiv g^k \bmod p$$
$$s \equiv (m - xr) \cdot k^{-1} \bmod (p-1)$$

그리고 검증자에게 m, s과 r를 전송한다. 검증자은 m, s과 r를 수신한 다음, 공개목록에서 서명자의 공개정보 y, p, g로부터

$$g^m \equiv y^r \cdot r^s \equiv g^{x \cdot r + k \cdot s} \bmod p$$

의 성립여부를 조사한다. 위 식이 성립하면 서명자의 서명임을 확인하게 된다. 검증자은 m, s과 r를 수신한 다음 공개 목록의 서명자의 공개정보 y로부터

$$y^r \cdot r^s \equiv g^m \bmod p$$

의 성립 여부를 조사한다. 식이 성립하면 서명자의 서명임을 확인하게 된다. 검증식은 다음과 같다.

$$y^r \cdot r^s \equiv (g^x)^r \cdot g^{k(m-xr)k^{-1}} \bmod p$$
$$\equiv g^{xr} \cdot g^m \cdot g^{-xr} \bmod p$$
$$\equiv g^m \bmod p$$

2.2 D. Chaum의 부인방지 서명기법

서명자는 암호학적으로 안전한 유한체(Finite Field) $GF(p)$와 군(Group) G_q를 선택한다. g는 군(Group) G_q의 원소로 위수(Order) q를 갖는 생성자이다. 서명자의 비밀키 x와 공개키 y는 다음과 같다[5].

$$x \in Z_q,\ y \equiv g^x \bmod p$$

D. Chaum의 부인방지 서명 방식의 구성은 서명 생성 프로토콜, 서명 확인 프로토콜 그리고 부인 프로토콜로 구성되며 (그림 2)와 같다.

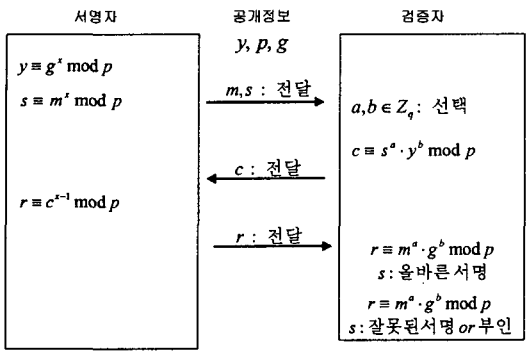

그림 2. D. Chaum의 부인방지 서명
Fig 2. Undeniable signature of D. Chaum

서명 생성 프로토콜 순서는 다음과 같다. 서명자는 메시지 m에 대한 부인방지 서명 s을 생성한다.

$$s \equiv m^x \bmod p,\ m \in G_q$$

그리고 서명자는 m, s을 검증자에게 전송한다. 검증자는 확인 과정을 통하여 서명의 정당성을 확인한다. 서명확인 프로토콜은 다음과 같다. 먼저 검증자는 Z_q상에서 임의의 두 난수 $a, b \in Z_q$를 선택하고 다음과 같이 도전(Challenge) c를 생성한다. 검증자는 도전 c를 서명자에게 전송한다.

$$c \equiv s^a \cdot y^b \bmod p,\ a,b \in Z_q$$

서명자는 다음과 같이 응답(Response) r을 생성하여 검증자에게 전송한다.

$$r \equiv c^{x^{-1}} \bmod p,\ x \cdot x^{-1} \equiv 1 \bmod p$$

검증자는 다음 식을 통해서 서명을 검증한다.
만약

$$r \equiv m^a \cdot g^b \bmod p$$

이면 s는 올바른 서명이고
만약

$$r \neq m^a \cdot g^b \bmod p$$

이면 서명 s이 잘못됐거나, 서명자가 올바른 서명에 대해서 부인을 하는 경우이다.

다음은 부인 프로토콜(Disavowal Protocol)에 관한 설명이다. 임의의 두 난수 $c, d \in Z_q$를 이용한 두 번째 도전 ch'과 응답 $resp'$은 다음과 같다.

$$ch' \equiv s^c \cdot y^d \bmod p,\ resp' \equiv w'^{x^{-1}} \bmod p$$

검증자은 다음 식을 생성해서 서명자의 부정 여부를 검증한다.
만약

$$(r \cdot g^{-b})^c \equiv (resp' \cdot g^{-d})^a \bmod p$$

이면 서명 s가 잘못된 것이고
만약

$$(r \cdot g^{-b})^c \neq (resp' \cdot g^{-d})^a \bmod p$$

이면 서명자가 올바른 서명에 대해서 부인하는 것이다.

III. CDN에서 부인방지 다중서명

CDN(Contents Delivery Network)이란 인터넷 사용자들로부터 멀리 떨어져 있는 CP(Contents Provider)의 웹 서버에 집중되어 있는 콘텐츠 중 그림, 배너, 비디오, 또는 오디오와 같은 용량이 크거나 사용자들의 요구가 잦은 콘텐츠를 여러 ISP의 POP(Point of Presence)들에 설치한 CDN 서버에 미리 저장해 놓고, 콘텐츠 요구 발생시 가장 최적의 CDN 서버로부터 사용자에게 콘텐츠를 전달해

주는 신 개념의 대용량 데이터 전송방식이다. 즉, 대용량의 콘텐츠를 인터넷 사용자 근처에 미리 옮겨놓고, 그곳에서 그 콘텐츠를 인터넷 사용자들에게 신속하게 배달하는 서비스로, 인터넷 사용자는 HTML 텍스트와 같은 용량이 작은 콘텐츠는 CP의 웹 서버에서, 동영상 같이 용량이 큰 콘텐츠는 CDN 서버에서 받아보게 되는 것이다[7].

다음 (그림 3)은 CDN 방식의 서비스를 나타낸 것이다.

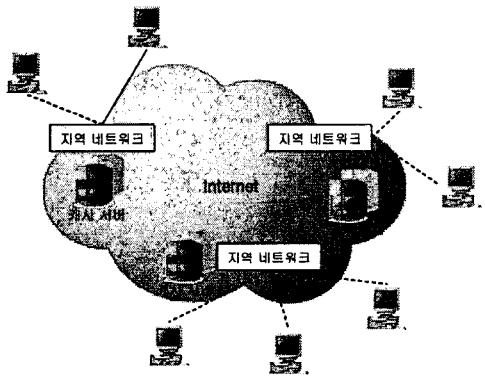

그림 3. CDN 의 구성
Fig 3. Configuration of CDN

CDN 서비스를 받게 되면 인터넷 사용자들은 콘텐츠를 받아보는 과정은 다음과 같이 이루어진다.

[1단계] : URL 입력 즉, 사용자가 브라우저 상에서 방문 하고자 하는 사이트의 URL을 입력하면 인터넷을 통해 CP의 웹 서버로 request가 전달된다.

[2단계] : CDN 서버를 가리키는 embedded URL을 포함하고 있는 HTML 전송 즉, request를 받은 CP의 웹 서버는 CDN 서버를 가리키고 있는 embedded URL을 포함하고 있는 HTML을 사용자에게 전송 하여 준다.

[3단계] : CDN 서버는 embedded object 요청 즉, Subscriber의 브라우저는 HTM에 포함된 embedded URL의 주소, 즉 CDN 서버로 object를 요청하게 된다.

[4단계] : Local CDN 서버로부터 콘텐츠 전달 즉,CDN 서버에 복제되어 있던 콘텐츠가 사용자의 웹 브라우저로 전송된다.

위와 같은 과정을 CDN 서비스는 최종사용자들에게 신속하고 안정된 콘텐츠를 제공하게 된다. 다음 (그림 4)는 CDN 서비스의 제공과정을 나타낸 그림이다.

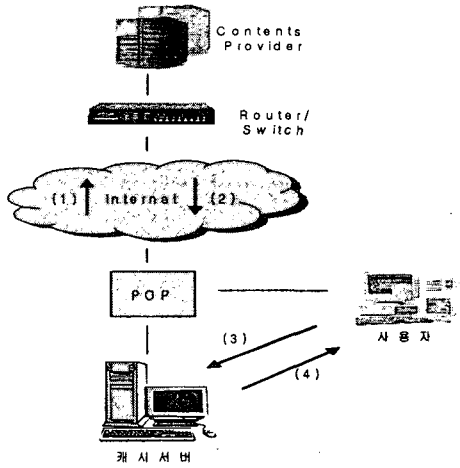

그림 4. CDN 서비스의 제공과정
Fig 4. Process course of CDN service

디지털 콘텐츠를 서비스 하는 전자상거래가 늘어나고 있다. 인터넷 자체는 보안을 고려하지 않은 전송매체이기 때문에 보안 문제가 발생한다. 또한 기업의 서버시스템은 불법 침입 및 데이터 파괴의 위협에 노출되어 있으며, 해킹이나 크래킹의 위협이 더욱 심해지고 있다. 다라서 서버시스템의 보호를 위한 보안 대책이 요구 된다. 디지털 콘텐츠의 안전한 분배를 위해서는 전송되는 디지털 콘텐츠의 보안 기법이 필요하다. 일반적으로 멀티미디어 고품질 콘텐츠는 품질의 손상 없이 불법복제가 가능하다. 또한 인터넷에서 불법 복제된 콘텐츠의 배포는 디지털 콘텐츠 제공자(Digital Contents Provider)에게 커다란 경제적 손실을 주고 있다[8].

디지털 콘텐츠 제공자에서 디지털 콘텐츠를 제공받는 디지털 콘텐츠 사용자 그룹에 속한 인가된 사용자에게 효율적으로 디지털 콘텐츠를 전송하여야 한다. 온라인으로 판매되는 디지털 콘텐츠를 여러 저작자가 만든 경우에, 해당 콘텐츠에 대한 저작권을 저작자들이 함께 공유할 수 있어야 한다. 또한, 콘텐츠 판매에 있어서 모든 저작자들의 동의 하에서만 결제가 가능하도록 함으로써 해당 콘텐츠에 대한 공동의 권리를 실질적으로 보장할 수 있다. 공동 저작권과 관련된 분쟁이 발생했을 경우에 부인 프로토콜을 수행하여 공동 저작권이 변조된 것인지 저작자들이 올바른 저작권에 대해서 부인하는 것인지 식별할 수 있는 특성을 갖는다[9].

본 논문에서는 여러 서명자의 서명이 필요한 다중서명 기법에서 부인방지 성질을 만족하는 부인방지 다중서명 기법을 사용한다. 이 방법은 El-Gamal 서명식을 변형하여 다중서명의 특성을 포함하고 D. Chaum이 제안한 부인방지 성질을 만족한다. 또한, 서명자들에 의한 다중서명 부인 및 다중서명 변조에 대해서 안전하다.

디지털 콘텐츠 저작은 개별적으로도 이루어질 수 있지만 대부분 여러 사람의 공동 노력으로 진행된다. 공동 저작물인 경우에 해당 디지털 콘텐츠에 대한 저작권을 저작자들이 함께 공유하여 권리를 똑같이 행사할 수 있도록 해 주는 공동 저작권 생성 및 보호 기법이 필요하다.

부인방지 다중서명 기법은 서명자들 모두의 동의 없이는 다중서명을 검증할 수 없는 기법이다. 제안한 다중서명 기법은 다중서명 생성, 다중서명 확인, 부인 프로토콜로 구성된다.

3.1 다중서명 생성 프로토콜

(그림 5)는 제안한 다중서명 기법에서 다중서명을 생성하는 과정이다. 메시지 작성자는 서명 대상 메시지를 서명자들에게 전송한다. 서명자들은 다중서명에 필요한 공통키를 생성하고 메시지 m에 대한 부인방지 서명을 만들어 메시지 작성자에게 전송한다. 메시지 작성자는 각 서명자의 부인방지 서명을 조합하여 부인방지 다중서명을 생성한다.

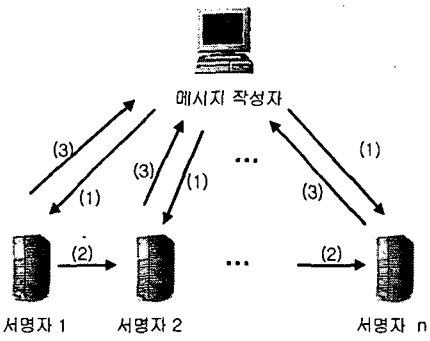

그림 5. 부인방지 다중서명의 생성 단계
Fig 5. Creation step of undeniable multi signature

(그림 5)에서 (1)는 서명대상 메시지, (2)는 공동키 및 공개키 생성, (3)은 공동키를 이용한 서명자들의 서명, (4)은 메시지 작성자의 다중서명 생성이다.

암호학적으로 안전한 유한체 $GF(p)$는 다음을 만족하는 유한체이다. p는 큰 소수로 유한체 $GF(p)$상에서 법 p에 대한 이산대수를 구하는 것이 계산상 불가능할 때 $GF(p)$를 암호학적으로 안전한 유한체라 정의하고 g는 법 p에 대한 위수 $p-1$을 갖는 생성자이다. 서명자들의 수가 n명일 때 각 서명자의 비밀키 및 공개키는 다음과 같다.

$$\text{서명자 } i\text{의 비밀키 : } x_i \in Z_{p-1},\ 1 \le i \le n$$

$$\text{서명자 } i\text{의 공개키 : } y_i \equiv g^{x_i} \bmod p$$

3.1.1 서명자의 공통키 생성

메시지 기안자는 서명 대상 메시지 m과 해시 파라미터 hpr을 서명자들에게 전송한다. 메시지 m에 대한 해쉬값 m_h가 법 p에 대한 원시근(Primitive Root)이 되도록 hpr을 설정한다.

$$m_h = h(m, hpr)$$

(그림 6)은 서명자들의 공동키 R와 대표 공개키 Y를 구하는 과정을 나타낸 것이다.

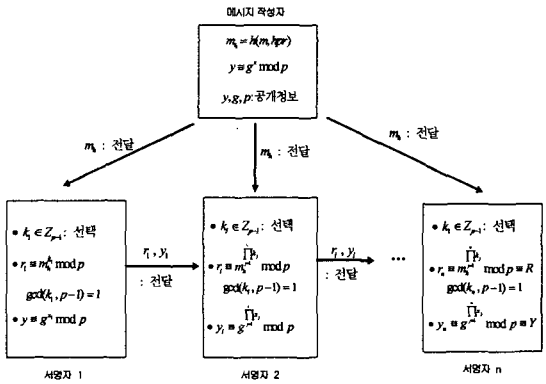

그림 6. 공동키와 공개키 생성 과정
Fig 6. Process course of session key and public key

(그림 7)에서 마지막 서명자는 서명자들의 공통키 R과 서명자들의 대표 공개키 S를 구해서 모든 서명자들과 메시지 기안자에게 R과 S를 전송한다.

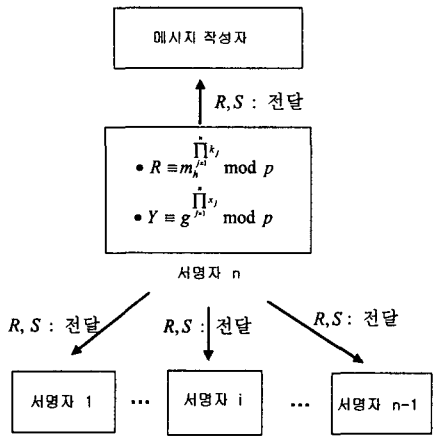

그림 7. 공동키와 공개키 전달
Fig 7. Transmission session key and public key

3.1.2 부인 방지 다중서명 생성 과정

각 서명자는 공통키 R을 이용하여 다음 식을 만족하는 s_i를 구한다. k_i와 $p-1$은 서로소이므로 s_i에 대한 유일한 해가 존재한다.

$$k_i \cdot s_i \equiv x_i \cdot R - k_i \cdot m_h \pmod{p-1}$$

부인 방지 다중서명 생성 과정은 다음 (그림 8)과 같다.

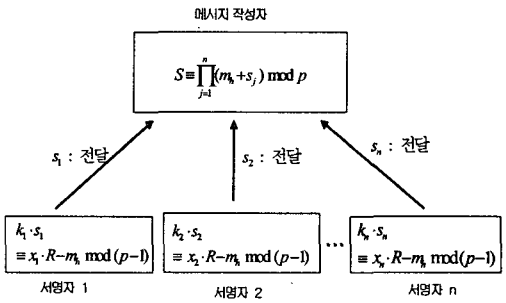

그림 8. 부인 방지 다중서명의 생성 과정
Fig 8. Creation course of undeniable multi signature

.2 다중서명 확인 프로토콜

메시지 작성자는 R, S가 메시지 m에 대한 올바른 다중서명인지 확인하기 위해서 순차적으로 다음과 같은 다중서명 부인 프로토콜을 수행한다.

3.2.1 메시지 작성자의 도전 생성과 서명자의 응답 생성

(그림 9)는 메시지 작성자의 도전(Challenge) 생성과 n명의 서명자의 응답(Response) 생성 과정을 나타낸 것이다.

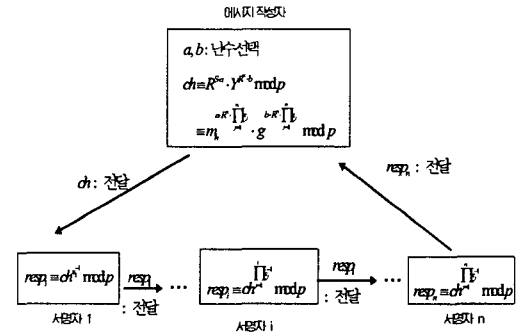

그림 9. challenge과 response 생성 과정
Fig 9. Creation course of challenge and response

(그림 9)에서 x_1^{-1}는 법 $p-1$에 대한 x_1의 모듈러 곱셈의 역이다.

3.2.2 메시지 작성자의 다중서명 검증

메시지 작성자는 다음과 같이 전체 서명자들의 응답을 검증한다.

만약

$$resp_n \equiv m_h^{R^a \cdot a} \cdot g^{R^a \cdot b} \pmod{p}$$

이면 메시지 작성자는 R, S가 메시지 m에 대한 올바른 다중서명임을 확인한다.

만약

$$resp_n \neq m_h^{R^a \cdot a} \cdot g^{R^a \cdot b} \pmod{p}$$

이면 다중서명이 잘못된 경우와 서명자들 중 적어도 한 서명자 이상이 부정을 하는 경우이다.

메시지 작성자는 부인 프로토콜을 이용해서 다중서명이 잘못된 것인지 서명자들이 부정하는 것인지 확인한다.

3.3 부인 프로토콜

메시지 작성자는 다중서명 확인 프로토콜에서 응답 $resp_n$ 에 대한 인증에 실패할 경우에 부인 프로토콜을 통해서 서명자들이 부정하는 것인지 다중서명이 잘못된 것인지 확인한다. (그림 10)은 다른 challenge과 response을 생성 하는 과정을 나타낸 것이다.

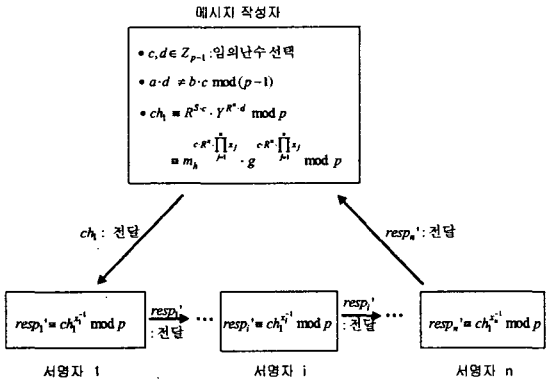

그림 10. 다른 challenge 과 response 생성 과정
Fig 10. Another creation course of challenge and response

다중서명 검증에 실패할 경우에 메시지 작성자는 $resp_n$ 과 $resp_n'$을 이용해서 다음 식을 만든다.

$$R_1 \equiv (resp_n \cdot g^{-R^* \cdot b})^c \bmod p$$
$$R_2 \equiv (resp_n' \cdot g^{-R^* \cdot d})^a \bmod p$$

R_1과 R_2를 비교함으로써 서명자들의 부정인지 또는 다중 서명이 잘못된 것인지 확인한다.

만약

$$R_1 = R_2$$

이면, 다중서명이 잘못된 경우이다.

만약

$$R_1 \neq R_2$$

이면, 서명자들이 올바른 다중 서명에 대해서 부인하는 경우이다.

임의의 난수를 선택할 때, 처음의 challenge와 같은 숫자로 challenge를 선택하고 싶지 않기 때문에 메시지 작성자는 매우 큰 숫자 그룹에서 랜덤 숫자를 선택한다. 이 숫자는 모래 중에서 한 알을 선택한 다음 그것을 다시 더미에 다가 다시 넣고, 그런 다음 더미를 섞고 또 다시 모래알을 선택한다. 두 번 선택해서 같은 모래알이 나오는 것은 매우 희박하다.

Ⅳ. 결 론

디지털 저작권 보호는 저작자의 지적인 재산권과 그에 기울인 노력의 보호 측면에서 중요하며 디지털 콘텐츠 산업의 발전을 위해 매우 중요하다. 하지만 디지털 콘텐츠는 복제가 용이하고 원본과 복사본이 동일하다는 특성으로 인해 저작권의 보호와 대량 불법 복제 및 불법 유통 방지에 어려움을 겪고 있는 실정이다. 또한 유료화 된 디지털 콘텐츠가 인터넷을 통해 전자적으로 거래되는 콘텐츠 전송 시스템이 안정된 수익 모델로서 발전하기 위해서는 적절한 저작권 보호 기술이 필요하다. 디지털 콘텐츠에 대한 불법 복제를 방지하기 위해서 저작권 정보를 생성하고 이를 디지털 콘텐츠 파일에 워터마킹을 이용하여 정보보호 기법의 적용은 필수적이다.

이러한 디지털 콘텐츠의 저작권들을 보호하고 안전하게 디지털 콘텐츠를 전송하기 위하여 본 논문에서는 디지털 콘텐츠 저작권 보호를 위한 CDN에서 다중서명을 제안하였다. 인터넷과 디지털 콘텐츠를 만드는 저작자들에게 유용하고 효과적인 활용이 가능할 것이다.

참고문헌

[1] 최승락, 양철웅, 이중식, "CDN의 핵심 구성 기술들과 경향", 정보과학회지, 제 20권 제 9호, 2002.9

[2] Spectral Lines, "Talking about Digital Copyrights," IEEE Spectrum, Vol.38, Issue 6, p.9, Junc, 2001.

[3] A. O. Freier, P. Karlton and P. C. Kocher, "The SSL Protocol Version 3.0," www.netscape .com/eng/ssl3, Nov., 1996.

[4] 원동호, "현대 암호학," 도서출판그린.

[5] D. Chaum, "Undeniable Signatures," Advances in Cryptology, Proceedings of CRYPTO'89, pp. 212-216, 1990.

[6] T. Elgamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Transactions on Information Theory, Vol .IT-31, No. 4, pp. 469-472, 1985.

[7] 지경용, 조은진, 고중걸, "콘텐츠 유통기술의 혁명", 진한도서,

[8] 고일석, 나윤지, 조동욱, "공개 키 기반의 계층 구조를 갖는 디지털콘텐트 분배 시스템의 설계, 제 11-A권 제 2호, pp. 175-180, 2004.

[9] 고병수, 장재혁, 최용락, "디지털 콘텐츠 유통 및 보호를 위한 인증 시스템 설계 및 구현". OA학회, 제8권 3호, 2003.

[10] 이성진, "인터넷 쇼핑몰의 구매모델에 관한 연구", 한국컴퓨터정보학회 논문지, 제10권 제2호, pp.199-204, 2005.

저 자 소 개

신 승 수

2001년 2월 충북대학교 수학과 (이학박사)

2004년 8월 충북대학교 컴퓨터공학과(공학박사)

2005년 3월~현재 동명정보대학교 정보보호학과 교수

〈관심분야〉 암호학, 무선 PKI, 네트워크보안, 콘텐츠보호

김 덕 술

1992년 2월 동아대학교 화공학과 (공학석사)

1996년 3월 일본 오사카대학 생체제어학과(공학박사)

1999년 3월~현재 동명정보대학 정보보호학과 교수

〈관심분야〉 생체인식, 정보보호, 네트워크보안