DOI : 10.5392/JKCA.2011.11.1.042

RSA 문제와 위임장에 기반한 안전한 대리서명 기법

Secure Proxy Signature Schemes based on RSA Problems and Warrants

서문석*, 장필식**, 최출헌***
대불대학교 컴퓨터응용기술학과*, 대불대학교 컴퓨터교육과**, 대불대학교 디자인학과***

Moon-Seog Seo(msseo@db.ac.kr)*, Phil-Sik lang(phil@db.ac.kr)**,
Chool-Heon Choi(ch1342@db.ac.kr)***

요약

대리서명기법은 대리서명자로 하여금 원서명자를 대신해서 대리로 서명할 수 있도록 구성한 서명 방식을 말한다. 대리서명의 기본 요구조건으로는 위조 불가능성 및 위임 검증 가능성이 있다. 현재까지 다양한 대리서명기법들이 제시되어 왔으나 기본 요구조건들의 복합적인 공격유형에 대해서 안전성 검증이 이루어지지 못하였다. 특히 RSA 문제에 기반 한 대리서명기법들은 위임 검증 가능성 측면에서 가장 공격(Impersonating Attack)에 취약함이 제시되어 공격자가 자신의 개인키로 원서명자의 동의나 인증 없이 유효한 대리서명의 생성이 가능하다. 본 논문에서는 복합적 공격유형인 가장 공격에서의 안전성 검증이 가능한 새로운 대리서명기법으로 RSA문제와 인증서 기반의 위임장을 활용한 대리서명기법을 제안하였으며 타 대리서명기법들과 효율성 측면에서 비교해 보았다.

■ 중심어 : | 전자서명 | 공개키기반구조 | 대리서명 | 위임장 | RSA 문제 |

Abstract

Proxy signature schemes are configured as proxy signers on behalf of their original signers can be allowed to sign messages. Basic security requirements of proxy signature schemes include the strong unforgeability and the verifiability of delegation. So far, a variety of proxy signature schemes that proved on individual basic security terms but not proved on compounded security terms are proposed. Especially the proposed proxy signature schemes based on RSA problem are proved vulnerable to an attacker with his own private key in terms of the impersonating attack. A unauthorized attacker can generate the proxy signature without the appointee's consent or authorization. In this paper, we propose a proxy signature scheme based on RSA problems and warrants that can be proved the security against the impersonating attack. The proposed proxy signature scheme is analyzed on the safety and compared in terms of efficiency with other proxy signature schemes.

■ keyword : | Digital Signature | Public Key Infrastructure | Proxy Signature | Warrants | RSA Problem |

I. 서 론

전자무역, 전자결재 등과 같은 인터넷 기반의 IT서비스 활성화를 위해서는 보안서비스의 이용이 필수적으로 요구되어진다. 이러한 보안서비스 중 비대면 개체식별을 위한 인증(Authentication) 서비스 및 송수신 사

* 본 논문은 2010학년도 대불대학교 교내연구비 지원에 의해 작성되었습니다.
접수번호 : #100914-002
접수일자 : 2010년 09월 14일
심사완료일 : 2010년 12월 23일
교신저자 : 서문석, e-mail : msseo@db.ac.kr

실의 부인을 방지하기 위한 부인방지(Non-Repudiation) 서비스는 핵심 보안 기법으로 전자서명기술을 이용한다. 전자서명기법에는 그 활용 목적에 따라 다양한 변형이 존재하는 데 서명자의 익명성 확보가 가능한 은닉 서명(Blind Signature), 서명을 해야 할 사람이 부재중에 자신을 대리해서 서명할 수 있는 대리 서명(Proxy Signature) 등이 있다.

대리서명방식은 대리서명자(Proxy Signer)로 하여금 원서명자(Original Signer)를 대신해서 대리로 서명할 수 있도록 구성한 서명 방식을 말한다[7]. 대리서명이 그 의미를 갖기 위한 기본 요구조건으로는 첫째 대리서명을 생성할 수 있는 사람은 원서명자로부터 대리 서명자로 지정된 사람만 가능해야하며 제삼자는 대리서명을 생성할 수 없어야 한다는 위조불가능성과 둘째, 대리서명을 확인하는 검증자는 대리서명을 위임한 서명자의 동의가 있었음을 확인할 수 있어야 하는 위임 검증 가능성이 있다. 이러한 대리서명기법은 이산대수문제에 기반 한 대리서명기법으로 M. Mambo와 E. Okamoto에 의해 처음으로 제안되었으며 RSA와 소인수분해문제에 기반 한 대리서명기법들도 추가로 제시되어 왔다[6][8][12]. 그러나 기존 대리서명기법들은 대리서명이 만족해야하는 기본적인 안정성에 대해 각각 개별적으로 증명하였으며 복합적인 환경 하에서의 공격유형에 대한 안전성은 정확히 검증하지 못하였다. 특히 [4]에서는 Zhou. Cao 그리고 Lu에 의해 제안된 RSA와 소인수분해 문제에 기반 한 대리서명기법들이 위임검증 가능성 측면에서 일종의 복합적 공격 유형인 가장공격(Impersonating Attack)에 의해 공격자가 자신의 개인키로 원서명자의 동의나 인증 없이 유효한 대리서명 생성이 가능함을 보였다.

본 논문에서는 RSA 문제에 기반 한 대리서명기법으로 개별 안전성 항목과 더불어 [4]에서 제시한 가장 공격에 대한 안전성 검증이 가능하고 공개키 기반구조(PKI : Public Key Infrastructure) 하에서 X.509v3 인증서 규격을 기반으로 새로 정의한 위임장을 사용하는 새로운 대리서명기법을 제안하였다. 2장에서는 제안된 대리서명 기법들과 이들 대리서명 기법들이 만족해야 하는 안전성에 대한 관련 연구들에 대해 살펴보고 3장에서 안전하고 실용적인 대리서명기법으로서 위임장을 활용한 RSA 문제 기반 대리서명기법을 제안한다. 4장에서는 본 논문에서 제안한 대리서명기법의 안전성을 분석해보고 타 대리서명기법들과 효율성 측면에서 비교하였다.

II. 관련연구

1. 대리서명기법의 안전성

대리서명기법은 그 위임 방법에 따라 전체 위임(full delegation), 부분 위임(partial delegation), 그리고 보증위임(delegation by certificate(warrant))으로 나눌 수 있다[1]. 대리자 보호 서명(proxy-protected signature)은 일종의 부분위임 대리서명 기법으로, 위임받은 대리서명자 이외에는 원 서명자라도 유효한 대리서명을 생성하는 것이 불가능한 방법이다. 최근의 대리서명 연구에 있어서 이러한 성질은 기본적으로 만족해야할 안전성 중 하나로 인정받고 있으며, 이를 강한 위조 불가능성 (Strong unforgeability) 으로 정의하고 있다[11]. 이를 포함하여 대리서명기법이 기본적으로 만족해야할 안전성은 다음과 같다[5][9][10].

- 위임 검증 가능성 (Verifiability of delegation) : 주어진 대리서명으로부터 검증자는 서명된 메시지에 대한 원 서명자의 동의를 확인할 수 있다.
- 강한 신원 확인성 (Strong identifiability) : 누구나 주어진 대리서명으로부터 서명을 생성한 대리서명자의 신원을 확인할 수 있다.
- 강한 부인 방지성 (Strong undeniability) : 대리서명자는 자신이 생성한 대리서명을 부인할 수 없다.
- 오용 방지 (Prevention of misuse) : 대리서명 키는 유효한 대리서명을 생성하는 것 이외의 용도로 사용될 수 없다. 대리서명 키의 오용이 확인될 경우, 대리서명자의 책임이 정확하게 결정되어야 한다.

대리서명기법은 이러한 기본적인 안전성들을 모두 충족하여야 하며, 검증자가 원서명자의 위임 검증을 수

행하지 않는 경우 공격자가 대리서명자로 가장하여 위조된 대리서명을 생성하는 복합적인 공격 유형인 가장 공격에 대해서도 안전성이 검증되어야 한다.

2. 기존 대리서명기법의 분석

M. Mambo와 E. Okamoto에 의해 제안된 이산대수문제에 기반 한 대리서명기법은 다음과 같다[6].

1) 대리서명 준비과정
원서명자는 자신의 개인키 및 공개키 준비
p: 선정
$y \equiv g^x \bmod p$

2) 대리서명 위임과정
원서명자는 위임서명키를 생성하여 대리서명자에게 안전한 채널을 통해 전송

원서명자의 위임서명키 생성
$k \in_R Z_p$: 난수
$K \equiv g^k \bmod (p-1)$
$\sigma \equiv x + kK \bmod (p-1)$
위임서명키 σ, K를 대리서명자에게 비밀전송

대리서명자의 검증
$g^\sigma \equiv yK^K \bmod p$

3) 대리서명 생성 및 검증과정
대리서명자의 대리서명
M: 전자문서
$r \in_R Z_q$
$R \equiv g^r \bmod p \bmod q$
$H = h(M)$
$S_\sigma \equiv r - R\sigma H \bmod q$
전자문서 M과 서명값 S_σ, R, K 전송

검증자의 대리서명 검증
$H = h(M)$
$v \equiv yK^K \bmod p$
$R \equiv g^{S_\sigma} v^{RH} \bmod p \bmod q$

[6]에서 제안한 대리서명기법은 이산대수문제에 기반 한 대리서명기법으로 현재 공개키 기반구조 하에서 대부분 RSA 전자서명 알고리즘을 사용하고 있어 이중의 서명알고리즘을 사용해야하는 불편함이 있으며 안전성 측면에서도 대리서명이 난수 r 과 원서명자가 생성한 σ 에만 의존하고 있어 원서명자도 대리서명을 생성할 수 있어 기본적인 안전성인 강한 위조 불가능성을 충족하고 있지 못하다.

다음은 Zhou, Cao 그리고 Lu에 의해 제안된 RSA와 소인수분해 문제에 기반 한 대리서명기법은 아래와 같다[8].

1) 대리서명 준비과정
원서명자(U_o)의 키
개인키 : (p_o, q_o, d_o), 공개키 : (N_o, e_o)
대리서명자(U_p)의 키
개인키 : (p_p, q_p, d_p), 공개키 : (N_p, e_p)

2) 대리서명의 위임과정
원서명자는 권한의 제한이나 유효기간과 같은 대리서명과 관련있는 정보를 포함하는 위임장 m_w를 생성하고 이를 공개

서명자는 위임장에 다음과 같이 서명
$s_o = H(m_w)^{d_o} \bmod N_o$

원서명자는 서명된 위임장 (m_w, s_o)을 안전한 경로로 대리서명자에게 전송

대리서명자는 $s_o^{e_o} = H(m_w) \bmod N_o$를 확인하여 서명이 유효하면 s_o를 대리서명키로 사용

3) 대리서명 생성 및 검증
대리서명자의 대리서명
대리서명자 U_p는 원서명자 U_o를 대신해 메시지 m에 대해 서명하기 위해 임의의 정수 r을 생성하고 다음을 계산한다.
$R = r^{e_o} \bmod N_o$
$r_1 = s_o \cdot r \bmod N$
$r_2 = H(m, R)^{d_p} \bmod N_p$
메시지 m에 대한 대리서명은 (r_1, r_2)이다.

검증자의 대리서명 검증
$R' = r_1^{e_o} \cdot H(m)^{-1} \bmod N_o$ 를 계산하고
$r_2^{e_o} \equiv H(m, R') \bmod N_p$가 성립하는지 확인

위의 대리서명기법은 [4]에서 대리서명 키 s_o가 실제 대리서명자의 서명 절차에서 제 역할을 수행하지 못함으로써 위임받지 않은 공격자의 서명위조가 가능함을

보였다. 인증서가 직접 대리 서명키로 사용되기 때문에 검증자에게 공개되지 않고 결국 검증자는 위임장에 대한 직접적인 검증을 할 수 없게 된다. 그러므로 위임받지 않은 사용자가 자신의 위임장을 스스로 생성해서 이를 이용하여 대리서명을 할 수 있다. 또한 여기서 제시된 위임장은 일반 메시지에 원서명자가 서명한 전자문서 형태로 이 대리서명기법에만 특화된 것으로 기존 공개키 기반 구조와는 별도로 정의 되어져야 한다.

Ⅲ. 위임장 기반 대리서명기법 제안

본 논문에서 제안하는 대리서명기법에서 사용하고 있는 인증서 기반의 위임장 구조 및 처리방법과 알고리즘을 설명한다.

1. 위임장의 정의 및 처리

제안하고자 하는 대리서명기법에서는 PKI 기반의 X.509v3 인증서규격을 활용한 위임장을 사용한다. PKI는 공개키 암호시스템과 공개키에 대한 인증서를 기반으로 보안서비스를 제공하는 정보보호 기반구조이다. 보안서비스 중 인증서비스의 기반 기술로는 현재 사실상의 표준으로 받아들여지고 있는 ITU-T의 X.509가 있으며 X.509를 이용한 PKI 시스템 구성은 [그림 1]과 같다[13].

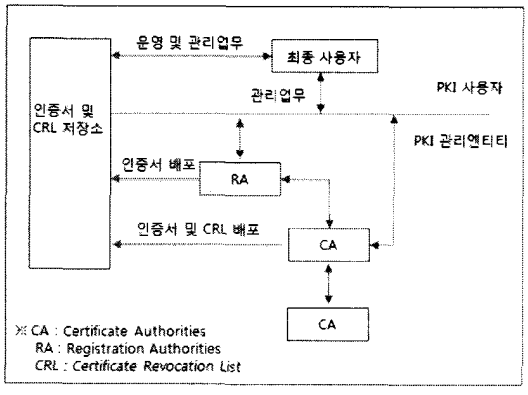

그림 1. PKI 시스템 구성

PKI는 개방형 네트워크에서 안전한 서비스가 이루어질 수 있도록 통신정보의 비밀성, 인증, 무결성 및 부인방지 등의 기본적인 보안서비스를 가장 효과적으로 제공하는 기반 구조이다. 공개키 암호기술의 문제점은 공개키의 가용성을 훼손하는 경우에 발생 하는데 공개키의 가용성이란 어느 누구든지 다른 사용자의 공개키가 필요한 경우에 이를 사용할 수 있는 서비스이다. 공개키가 위·변조되지 않았음을 보장하는 문제 즉, 공개키의 무결성을 보장하기 위해 공개키 대신 공개키와 그 공개키의 소유자를 강하게 연결하여 주는 인증서(Certificate)를 공개하고 인증서는 신뢰할 수 있는 제3자인 인증기관이 자신의 개인키로 서명하여 공개키를 인증하는 시스템을 PKI 시스템이라 한다. 이는 공개키 암호기술이 안전하게 적용될 수 있는 기반구조로써 공개키와 그 소유자를 연결해 주는 인증서, 키와 인증서를 안전하게 관리해주는 서비스 그리고 인증서의 유효성 여부를 확인할 수 있는 구조라고 정의 할 수 있다.

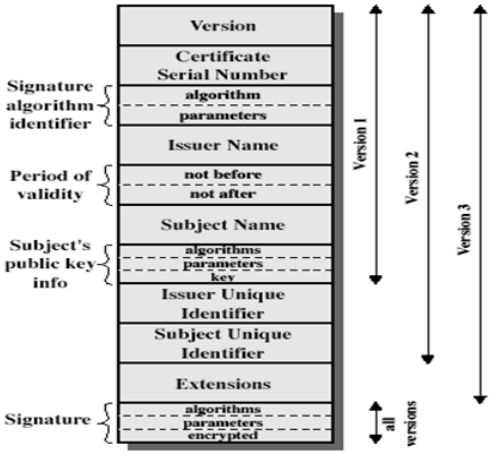

그림 2. X.509v3 인증서

공개키의 진정성 문제를 해결하기 위해서 도입된 인증서는 사용자의 공개키 정보와 함께 그 사용자의 이름, 전자우편 주소 등과 같은 신원 정보를 같이 붙여서 인증기관이라는 신뢰된 제3자가 전자서명을 한 것이다. 현재 X.509라는 표준에 의하여 규정되어 있으며 버전 3까지 발표되어 있다. 인증서에 들어가는 항목은 크게 기본 영역 필드와 확장영역 필드로 나뉘며 [그림 2]의

항목들로 구성되어져 있다[13].

이러한 PKI 기반 구조 하에서 인증서를 위임장으로 활용함으로써 원서명자의 위임 사실을 제3 신뢰기관인 인증기관의 서명을 통해 생성하고 대리서명의 검증자는 인증서 검증과 동일한 방식으로 위임장의 검증이 가능하다. 인증서의 기본필드 중 위임장에서 적용 가능한 항목과 그 내용은 다음과 같다.

- 버전 : 위임장 정의 프로파일 버전번호.
- 일련번호 : 위임장의 일련번호.
- 위임장 발급기관 : 위임장을 발행한 발급기관으로 위임장에 대한 서명자.
- 유효기간 : 위임장의 유효기간으로 특별한 단서가 없는 한 대리서명의 유효기간과 일치.
- 위임 공개키 : 대리서명의 검증에 이용하는 공개키로 이 공개키를 기반으로 원서명자가 대리서명자에게 전달하는 위임 서명키를 생성하고 검증자는 대리서명의 검증에 이 공개키를 사용.
- 키 사용 : 공개키가 사용되는 목적 명시.
- 서명 : 위임장 발급기관이 위임장의 정당성을 입증하는 서명생성.
- 위임장에서 추가로 정의되어져야 하는 항목들로 확장필드 영역에 정의되어져야 하는 항목들은 다음과 같다.
- 대리서명자 : 위임장을 활용하여 대리서명을 생성할 수 있는 대리서명자의 식별 값.
- 위임기간 : 공개키의 유효기간과는 별도로 대리서명의 위임기간을 별도로 명시.
- 권한의 제한 : 위임장을 적용하여 대리서명 가능한 업무범위 등 권한의 제한을 설정.

위임장은 원서명자가 생성하여 인증기관의 서명 후 인증기관의 배포목록을 통해 서명 검증자 및 대리서명자 등 참가자에게 배포되어진다. 대리서명자 및 대리서명 검증자는 위임장의 검증이 필요한 시점에서 위임장에 서명한 제3 신뢰기관의 공개키를 사용하여 위임장의 정당성 여부를 검증할 수 있으며 기존 PKI 시스템에서 실시간 인증서 상태 검증에 사용하는 OCSP(Online Certificate Status Protocol)의 기능을 확대하여 적용하는 것도 가능하다[14].

2. 제안하는 대리서명기법의 알고리즘

본 대리서명기법에서는 원서명자와 대리서명자는 각각 자신의 RSA 알고리즘의 공개키와 개인키를 가진다. 이는 기존 PKI 기반의 인증서를 변경 없이 사용 가능하며 이를 이용한 대리서명 알고리즘은 [그림 3]과 같다.

```
Original Signer
 Public Key : No, eo;
 Private Key : po, qo, do;
Proxy Signer
 Public Key : Np, ep;
 Private Key : pp, qp, dp;
/* Prepare proxy signature */
generateWarrantKey()
{ pt = random_prime_number();
  qt = random_prime_number();
  Nt = pt*qt;
  et = 0f100001;
  dt = (exponet(et, -1) % (pt-1)(qt-1); }
sendWarrantDataToCA(DelegationData).....①
deployWarrantByCA(Mw)

/* Delegation of proxy signature key */
k = ds + et*dt;
sendToProxy(k);
if (verifyByProxy(Mw)) use(k);.....②
else destroy(k);

/* Proxy signature generation by
   proxy signer */
Input message : M;
S1 = exponent(H(M), dp) % Np;
temp = (exponent(H(M), k)/H(M) % Nt);
S2 = temp % No;
sendToVerifier(M, S1, S2);.....③

/* Verify proxy signature by receivers */
Input : M, S1, S2, Mw;
if(verifyByReceiver(Mw)) { .....④
   h1 = exponent(S1, ep) % Np;
   h2 = (exponent(S2, eo) % Nt) % No;
   h3 = H(M);
   if (h1 == h3 && h2 == h3) success;
   else fail; } else fail;
```

그림 3. 대리서명기법 알고리즘

위 알고리즘에서 원서명자가 위임의 내용, 기간 및 대리서명자 등을 포함하여 생성한 위임장 자료는 ①에서 인증기관으로 전송되며 인증기관의 전자서명이 추가되어 위임장 M_w로 변환된 후 인증기관의 디렉토리를 통해 배포되어진다. 인증기관이 전자서명을 수행하는 동안 1회의 지수승 연산이 추가되어진다. 인증기관에서 서명, 배포한 위임장은 ②에서 대리서명자가 위임 서명키의 정당성을 확인하기 위하여 검증되어지며, ④에서는 메시지와 대리서명 (M, S_1, S_2)를 수신한 검증자에 의해 대리서명의 정당성을 확인하기 위해 위임장이 검증되어진다.

위 알고리즘에서 서명위조가 없다면 오일러정리에 기반하여 다음과 같은 수식에 의해 h_2가 계산되어 서명의 정당성이 검증되어질 수 있다.

$$
\begin{aligned}
& S_2^{e_o} \bmod N_t \bmod N_o \\
&= (H(M)^k / H(M))^{e_o} \bmod N_t \bmod N_o \\
&= H(M)^{ke_o} / H(M)^{e_o} \\
&= H(M)^{(d_o + e_t d_t)e_o} / H(M)^{e_o} \\
&= H(M)^{(d_o e_o + e_t d_t e_o)} / H(M)^{e_o} \\
&= H(M)^{(1+e_o)} / H(M)^{e_o} \\
&= H(M)
\end{aligned}
$$

Ⅳ. 제안하는 대리서명기법의 타당성 분석

본 장에서는 제안한 대리서명기법이 기 제시된 안전성 기준에 부합하는지 분석해 보고 기존 대리서명기법들과 효율성 측면에서 비교하여 실세계에 적용 가능한지 타당성 여부를 검토하고자 한다.

1. 안전성 분석

- 위임 검증 가능성 : 검증자는 주어진 대리서명 S_1으로부터 서명 검증을 수행하기 위해 위임장의 위임 공개키 (N_t, e_t)를 사용하여야 하기 때문에 위임장 검증이 요구되어지며 이를 통해 원서명자의 위임 정당성을 확인할 수 있다.
- 강한 위조 불가능성 : 대리서명자가 생성한 서명은 메시지 M과 대리서명자의 개인키 d_p 그리고 위임 서명키 k를 이용하고 있고 이를 바탕으로 (S_1, S_2)를 생성하므로 대리서명자를 제외한 누구도 유효한 대리서명 을 생성할 수 없다.
- 강한 신원 확인성 : 대리서명의 검증을 위해서는 대리서명자의 공개키 (N_p, e_p)의 확보가 필수적으로 요구되어진다. 이는 대리서명자의 인증서를 통해 확보할 수 있으므로 PKI 하에서 누구나 주어진 대리서명자의 신원을 확인할 수 있다.
- 강한 부인 방지성 : 대리서명자는 자신의 개인키 d_p를 이용하여 생성한 대리서명을 부인할 수 없다.
- 오용 방지 : 대리서명을 생성하기 위해서는 키의 용도가 명확히 표시되어 있고 위임자의 서명이 부가되어 있는 위임장을 기반으로 하고 있기 때문에 대리서명자는 유효한 대리서명을 생성하는 것 이외의 용도로 사용할 수 없다.

[4]에서 제기한 복합적 공격유형인 가장 공격은 공격자가 대리서명자로 가장하여 원서명자로부터 위임받은 위임 서명키를 임의로 생성하여 대리서명자로 가장하여 대리서명을 생성하는 것으로 본 논문에서 제시한 대리서명기법의 경우 대리서명 검증자가 대리서명을 검증하는 과정에서 위임장 검증을 통해 원서명자, 대리서명자 및 위임내용 등을 확인한 후 대리서명 검증이 이루어지고 있기 때문에 공격자가 원서명자로부터 위임 없이 임의로 생성한 k를 사용하여 위조된 서명을 생성한 경우 검증자는 위임 검증을 통한 서명 위조 여부의 판단이 가능하다. 또한 위임 서명키 k와 위조된 위임장 소유가 가능한 원서명자라도 대리서명자의 개인키 d_p를 알 수 없으므로 위조된 대리서명의 생성은 불가능하여 위임 검증 가능성과 강한 위조 불가능성을 동시에 충족하여 가장 공격에 대해 안전하다고 할 수 있다.

2. 타 대리서명기법과의 효율성 비교

대리서명 기법은 위임 준비과정, 대리서명 생성과정 및 검증과정으로 구성된다. 대리서명 기법의 효율성을 검증하기 위해서 전자서명 알고리즘의 연산에서 가장 많은 부하를 차지하는 지수승 연산 횟수와 서명 값의 길이를 비교하였으며 대리서명 과정에서 처리 지연이 예상되는 원서명자의 메시지 전송 횟수도 비교하였다.

표 1. 대리서명기법의 효율성 비교

구 분	Mambo&Okamoto (1)	Zhou, Cao&Lu(2)	제안방법(3)
지수승연산 횟수	(3+1+3)*	(2+2+3)*	(2+2+2)*
서명값 길이	3|p|**	2|N|**	2|N|**
송수신 횟수	1	1	2
실용성	○	◎	◎

* (위임준비과정+서명생성과정+검증과정)
** |p|, |N| : 공개 파라미터 및 공개키 길이(1024bit)

[표 1]의 항목 중 지수승 연산 횟수의 경우 위임 준비 과정에서 (1)의 방법이 1회 더 많은 연산을 필요로 하며 대리서명 생성 과정에서는 (2)와 (3)의 방법이 2회로 (1)보다 1회 더 많은 연산을 수행하고 있다. 대리서명의 검증 과정에서는 본 논문에서 제안한 (3)의 방법이 1회 적게 수행하였다. 일반적으로 전자서명 알고리즘의 경우 서명의 생성보다는 검증이 많이 수행되고 있어 서명 검증이 효율적인 경우가 유리하다고 할 수 있어 검증과정이 효율적인 (3)의 방법이 우수하다고 할 수 있다. 서명 값의 길이는 동일한 키 길이(1024bit)를 가정할 경우 (1)의 방식이 1024bit 정도 길어 무선 환경 등 통신 속도에 영향을 받을 경우 비효율적이라 할 수 있다[2]. 대리서명 과정에서 참여자들간의 온라인 송수신 횟수의 경우 본 논문에서 제시한 (3)의 방법은 대리서명의 검증 시 위임장 검증이 요구되어 송수신 횟수가 증가하는 단점이 있다. 실용성 측면에서 (1)의 방법은 이산대수 문제에 기반한 서명 알고리즘으로 기존 PKI 에서 주로 사용하고 있는 RSA 알고리즘과 구별되어 서명 알고리즘이 2원화되는 문제가 있어 실용성이 떨어진다고 할 수 있다. 본 논문에서 제안한 대리서명 기법은 전반적인 효율성 측면에서 기존 제안 방법들과 유사한 정도의 효율성을 확보하고 있다고 할 수 있다.

V. 결론

인터넷기반의 업무환경에서 대리서명의 요구가 증가하는 추세이다. 정보보안 분야에서 다양한 대리서명 기법들이 제안되어 왔고 대리서명이 갖춰야하는 기본 요건뿐만 아니라 필수적으로 요구되는 안전성 등이 추가로 제안되어 이에 부합하는 대리서명기법의 연구가 활발한 실정이다. 지금까지 제안된 대리서명 기법들이 개별 안전성 항목에 대해 검증하는 방법으로 안전성을 증명하여 왔으나 [4]에서와 같이 복합적인 공격 유형에 대해 안전하지 못함이 증명되곤 한다. 그러나 실세계에 적용하기 위해서는 안정성이 증명된 실용적인 대리서명 기법이 필수적으로 요구되어진다.

본 논문에서는 안전한 대리서명기법으로 기존의 PKI 환경 하에서 주로 사용되는 전자서명 알고리즘과 같은 RSA문제와 인증서에 기반 한 위임장을 사용한 새로운 대리서명기법을 제시하였으며 지수승 연산 횟수, 서명값 길이 및 메시지 송수신 횟수 등과 같은 항목으로 기존 대리서명기법들과 비교하여 효율성 측면에서 실세계에 적용 가능성을 검증하였다. 지금까지 제시된 대리서명의 안전성 기준 항목들에 대한 충족여부에 대해 분석하였고 [4]에서 제기된 가장 공격에 대해서도 안전함을 보였다.

제안된 대리서명기법의 실현을 위해서는 위임장이 인증기관을 통해 배포됨을 전제로 하고 있기 때문에 위임장의 표준 프로파일 정의, 위임장 저장 및 배포 방법 그리고 효율적인 위임장 검증방법 등에 대한 추가적인 연구가 필요하다.

참 고 문 헌

[1] 김승주, 박상준, 원동호, “보증 부분 위임과 역치 위임에 의한 대리서명 방식”, 정보보호학회논문지, Vol.8, No.2, pp.69-81, 1998.
[2] 박희운, 이임영, “이동 통신에서 적용 가능한 수신자 지장 대리 서명 방식”, 정보보호학회논문지, Vol.11, No.2, pp.18-27, 2001.
[3] 김소진, 이명희, 최재귀, 박지환, “대리서명방식의 확장에 관한 연구”, 한국멀티미디어학회 춘계발표 논문지, 제5권, 제1호, pp.844-848, 2002.
[4] 박제홍, 강보경, 한재우, “RSA와 소인수분해문제에 기반한 대리서명 기법의 안전성 분석”, 정보보호학회논문지, 제15권, 제2호, pp.65-72, 2005.

[5] 박해룡, 신용녀, 최은영, 강연정, 전길수, 원유재, “대리서명기법의 보안 요구사항”, 20회 정보보호와 암호에 관한 학술대회(WISC2008), pp.83-90, 2008.

[6] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures for delegating signing operation," Proc. Third ACM Conf. on Computer and Communications Security. pp.48-57, 1996.

[7] S. Kim, S. Park, and D. Won, "Proxy Signatures, revisited", Information and Communications Security ICICS'97, LNCS Vol.1334, pp.223-232, 1997.

[8] Y. Zhou, Z. Cao, and R. Lu, "Provably secure proxy-protected signature schemes based on factoring," Appl. Math. Comput. Vol.164, No.1, pp.83-98, 2005.

[9] G. Wang, F. Bao, J. Zhou, and R. H. Deng, "Security analysis of some proxy signatures," Information and Communications Security ICICS 2003, LNCS Vol.2971, pp.305-319, 2004.

[10] A. Boldyreva, A. Palacio, and B. Warinschi, "Secure proxy signature schemes for delegation of signing rights," Cryptology ePrint Archive, Report 2003/096.

[11] D. Pointcheval, J Stern, "Security proofs for signature schemes," Advanced in Cryptology:Eurocrypt'96, LNCS Vol.1070, pp.387-398, 1996.

[12] K. Shim, "An Identity-Based Proxy Signature Schemes from Parings," ICICS'06, LNCS Vol.4307, pp.60-71, 2006.

[13] W. Stallings, *Cryptography and Network Security (3rd Ed),* Prentice Hall, 2003.

[14] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*, RFC2560, 1999.

저 자 소 개

서 문 석(Moon-Seog Seo) 정회원

- 1988년 2월 : 단국대학교 전자계산학과
- 2000년 2월 : 한국정보통신대학원대학교 정보보안전공
- 2002년 9월 ~ 현재 : 대불대학교 컴퓨터응용기술학과 교수

<관심분야> : 전자금융, 공개키기반구조, 암호이론

장 필 식(Phil-Sik Jang) 정회원

- 1990년 2월 : 서울대학교 조선공학과
- 1992년 2월 : KAIST 산업공학과(공학석사)
- 1998년 8월 : KAIST 산업공학과(공학박사)
- 1997년 9월 ~ 현재 : 대불대학교 컴퓨터교육과 교수

<관심분야> : HCI, 감성공학, 음성분석

최 출 헌(Chool-Heon Choi) 정회원

- 1982년 2월 : 홍익대학교 공업디자인학과
- 1995년 2월 : 서울산업대학교 공업디자인(미술학석사)
- 2007년 3월 : NTU(영국) 제품디자인(디자인 박사)
- 2008년 3월 ~ 현재 : 대불대학교 디자인 학과 교수

<관심분야> : 운송기기 디자인