이동통신 환경에 적합한 효율적인 Proxy-Signcryption 방식

김동우[†] · 박지환[††]

요 약

이동통신의 발전에 따라 향후 이동통신 시스템은 많은 사용자들에게 고품질의 멀티미디어 서비스를 제공할 것이다. 따라서 이와 관련된 많은 기술적 응용 분야들이 고려되고 있으며, 특히 보안 관련 분야의 도입을 통해 기밀성 및 안전성을 획득하려 하고 있다. 본 논문에서는 이와 관련하여 이동통신 환경에서 상대적으로 계산 능력이 뛰어난 에이전트(agent)의 도움을 통해 디지털 서명 및 암호화를 수행 할 수 있는 효율적인 Proxy-Signcryption 방식을 제안한다. 제안방식은 대리 서명을 수행할 경우 발생할 수 있는 사용자와 대리서명 에이전트의 부정 서명 생성 및 부인행위를 방지하도록 구성하였으며, 동시에 정당한 수신자가 서명을 확인하도록 함으로서 이동 통신상에서 기밀성과 안전성을 유지하도록 하였다.

An Efficient Proxy-Signcryption Scheme for Mobile Communications

Dong-Woo Kim[†] and Ji-Hwan Park[††]

ABSTRACT

According to the development of mobile communications, the future mobile communication systems are expected to provide high quality multimedia service to users. Therefore, many technical factors are needed in these systems. Especially the confidentiality and the security would be obtained through the introduction of the security for mobile communications. In this paper, we propose an efficient Proxy-Signcryption scheme, which can be performed digital signature and encryption by using the proxy agent who has more computational power under mobile communications environment. The proposed scheme provides non-repudiation and prevents creating illegal signature by the origin and proxy agent in a phase of proxy signature processing. This scheme also keeps the confidentiality and the security in mobile communication by means of confirming the signature by right receiver.

Key words: Mobile Communication, Proxy-Signcryption, Agent, Confidentiality, Non-Repudiation

1. 서 론

최근 네트워크의 발전과 정보통신 분야의 급속한 발전에 따라 사용자들은 네트워크에 직접 연결된 컴퓨터를 사용하지 않고도 이동 중에 소형 노트북이나 휴대폰, PDA 등과 같은 휴대용 단말기를 이용, 인터넷에 접속 가능하게 되었다. 이동통신 분야는 산업계에서 가장 빨리 성장하는 분야 중의 하나로서 많은 사람들이 이동통신 서비스를 통해 그 편리성과 유용성을 인지하고 있다. 그러나 이러한 이동 통신 관련 서비스들은 많은 보안상 문제점들에 노출될 수 있다. 즉, 이동통신에서 신호 교환은 무선 채널을 통해 수행되므로 도청자나 그 밖의 신뢰되지 못한 요소들로부터 위조나 불법적 변경 등과 같은 위협들에 대해서는 취약성을 지니고 있다. 뿐만 아니라 사용자 인증 및 부인봉쇄

접수일 : 2002년 8월 27일, 완료일 : 2002년 12월 23일
[†] 준회원, 부경대학교 전산정보학과
[††] 종신회원, 부경대학교 컴퓨터멀티미디어공학전공 교수

등과 같은 여러 가지 문제가 발생할 수 있게 된다. 따라서 불법 가입자들로부터 기밀성과 안전성을 확보하고, 사용자의 인증성을 제공하기 위한 방법 중에 하나로서 수신자 지정 서명 기법[1]이 제시되었다. 이 기법은 네트워크 상에서 기밀성과 사용자 인증성을 동시에 제공하기 위해서 디지털 서명을 수행한 결과에 공개키 암호 방식을 사용하여 전송하게 된다. 그러나 디지털 서명이나 공개키 암호 방식은 모두 모듈라 멱승과 같은 많은 계산량을 요구하므로 상대적으로 계산 능력이 떨어지는 휴대용 단말기에 사용하기에는 어려운 점이 있다.

이러한 문제점을 해결하기 위해 Y. Zheng은 디지털 서명과 암호화의 기능을 동시에 만족하면서 요구되는 계산량이나 확장면에서 효율적인 Signcryption 방식[2,3]을 제안하였다. 그 후, Signcryption 방식과 서명 생성과 암호화에 요구되는 계산을 상대적으로 능력이 뛰어난 서버에 의뢰하는 대리 서명 방식[4,5]을 이용하여 휴대용 단말기가 수행해야 할 계산량을 더욱 감소시킨 Proxy-Signcryption 방식[6]이 제안되었다. Proxy-Signcryption방식은 대리인 비 보호형 대리 서명방식을 이용하므로 Alice가 임의의 메시지에 대해 Proxy- signcryption을 생성한 후 proxy agent가 생성한 것이라고 주장하는 경우에 제3자는 이를 판단할 수 없다는 문제점이 있다. 이를 해결하기 위해 대리인 보호형 Proxy-Signcryption 방식[7]이 제안되었으나, Proxy agent와 Bob사이에 forward secrecy를 제공하지 않으므로 메시지의 안전성 유지가 어렵다는 문제점이 있다. 여기서 forward secrecy란 송신자의 개인키를 알게 되는 사람이 이전에 송신자가 이 키를 사용하여 생성했던 Signcrypt된 문서로부터 원본 문서를 복구해 낼 수 없는 것을 말한다. 따라서 본 논문에서는 적은 계산량으로 디지털 서명을 수행하면서 기존의 Proxy-Signcryption이 가지고 있는 문제점을 해결하고, proxy agent에서 forward secrecy를 제공하는 개선된 Proxy-Signcryption을 제안한다. 2장에서는 기존 방식인 Proxy-Signcryption과 대리인 보호형 Proxy-Signcryption 문제점을 분석하고, 3장에서 이를 해결한 개선된 Proxy-Signcrypion을 제안한다.

2. 기존 방식의 분석

본 장에서는 C. Gamage 등[6]이 제안한 Proxy-Signcryption 방식과 오수현 등[7]이 제안한 대리인 보호형 Proxy-Signcryption 방식에 대해 분석한다. Proxy-Signcryption이란 사용자가 지정한 대리인이 자신을 대신하여 정당한 Signcryption 메시지를 생성할 수 있도록 하는 방식으로 Signcryption을 생성하는데 요구되는 계산을 상대적으로 계산 능력이 뛰어난 proxy agent에 의존하는 것이다.

2.1 Proxy-Signcryption[6]

Proxy-Signcryption에 사용되는 시스템 설정 파라메터는 다음과 같다.

[시스템 설정]

- p : 512비트 이상의 큰 소수
- q : $q \mid p-1$인 큰 소수
- g : 위수가 q인 Z_p상의 원소
- x_A : $x_A \in Z_q$, Alice의 비밀키
- y_A : $y_A \equiv g^{x_A} \bmod p$, Alice의 공개키
- x_B : $x_B \in Z_q$, Bob의 비밀키
- y_B : $y_B \equiv g^{x_B} \bmod p$, Bob의 공개키
- x_P : $x_P \in Z_q$, proxy agent의 비밀키
- y_P : $y_P \equiv g^{x_P} \bmod p$, proxy agent의 공개키
- $KH()$: Keyed 해쉬 함수
- $E()$ / $D()$: 관용암호/복호 알고리즘

1) 대리서명용 키 생성

Alice는 $x \in Z_q$를 선택하고 $K \equiv g^x \bmod p$를 계산하여 대리 서명용 키 $x_{AP} \equiv x_A + x \cdot K \bmod q$ 를 생성하여 (x_{AP}, K)를 전송한다.

2) 대리서명용 키의 검증

Proxy agent는 $y_{AP} = g^{x_{AP}} = y_A \cdot K^K \bmod p$를 이용하여 자신이 받은 대리 서명용 키가 정당한지 확인한다.

3) Proxy agent에 의한 Signcryption 생성 Proxy agent는 비밀 랜덤수 $x' \in [1,2,\cdots q-1]$ 를 선택하여 $k = y_B^{x'} \bmod p$를 계산한다.

$k = k_1 \parallel k_2$ 로 나누고 다음과 같은 메시지 m에 대한 Signcryption을 생성한다.

$r' = KH_{k_1}(m)$

$s' = x' / (r' + x_{AP}) \bmod q$

$c = E_{k_1}(m)$

메시지 m에 대한 Signcryption된 메시지 (c, r', s', K)를 Bob에게 전송한다.

4) Proxy-Signcryption 의 검증

Bob은 $y_{AP} \equiv y_A \cdot K^K \bmod p$를 계산한 후, 자신의 비밀키를 이용하여 $k=(y_{AP} \cdot g^{r'})^{s' \cdot x_B} \bmod p$ 를 구한다. $k = k_1 \parallel k_2$로 나누고 다음과 같은 메시지를 복호한다.

$$m = D_{k_1}(c)$$

단, $KH_{k_2}(m) = r'$인 경우에만 정당한 Signcryption으로 받아들인다.

그림 1에 제시한 Proxy-Signcryption 방식[6]은 이동통신에서 요구되는 기밀성, 인증성 및 유효성을 확보하고 있다. 그러나 이 방식은 서명 메시지 송신시 서명자와 대리 서명 에이전트간의 대리 서명용 키를 이용하게 된다. 따라서 서명자가 원할 경우 자신이 대리 서명 에이전트를 대신하여 정당한 서명을 생성할 수 있고 대리 서명 에이전트 역시 서명자의 동의 없이 임의로 서명을 생성할 수 있다. 또한 이 방식은 서명자가 메시지 서명에 대한 부인봉쇄가 불가능하기 때문에 전자 상거래 등의 여러 분야에 적용하기에는 문제가 발생 될 수 있다.

2.2 대리인 보호형 Proxy-Signcryption 방식[7]

Proxy-Signcryption방식은 대리인 비 보호형 대리 서명방식을 이용하므로 Alice가 임의의 메시지에 대해 Proxy-Signcryption을 생성한 후, proxy agent가 생성한 것이라고 주장하는 경우에 제3자는 이를 판단할 수 없다는 문제점이 있다. 이를 해결하기 위하여 대리인 보호형 대리 서명 방식을 이용하고, Alice가 전송한 메시지에 대해 부인봉쇄를 제공하기 위해 N. Asokan 등이 제안한 S^3(Server Supported Signatures)방식[8,9]을 이용하여 해결한 방식이 제안되어 있다[7]. 이 방식은 다음과 같은 4개의 구성요소로 이루어진다.

• Alice : 계산 능력이 적은 단말기를 이용하여 인터넷을 통해 전자 상거래를 하려는 사용자

• 서명서버 G : 송신자 부인봉쇄를 제공하기 위해 후보 NRO(Non-Repudiation of Origin) 토큰을 생성하는 서버

• Proxy agent : 사용자의 위임에 의해 Proxy-signcryption을 생성하는 대리인

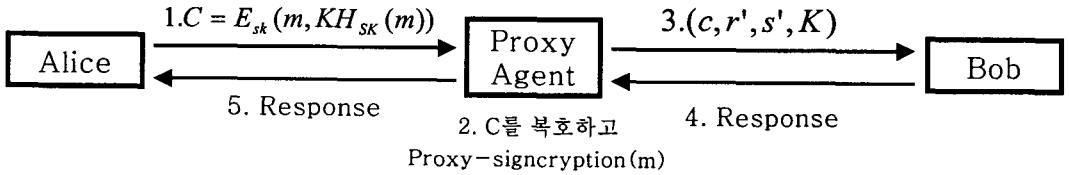
• Bob : 인터넷 쇼핑몰

[시스템 설정] 2.1의 파라메터에 추가되는 항목들

- PK_A : 부인 봉쇄 토큰의 생성/검증에 사용하는 Alice의 루트 공개키 : $PK_A = K_A^n = h^n(K_A)$
- K_A^i : Alice의 $(n-i)$번째 공개키 : $K_A^0 = K_A$, $K_A^i = h^i(K_A) = h(K_A^{i-1})$
- $h()$: 일방향 해쉬 함수
- $Sigs()$: 서명 서버 G의 디지털 서명
- sk : Alice와 proxy agent 사이에 공유한 비밀키

[프로토콜]

1) Alice는 먼저 Bob에게 보내고자 하는 메시지 m_i를 생성하고 $(ID_A, h(m_i), i, K_A^i)$를 서명서버 G에게 전송한다.



- sk: Alice와 proxy agent사이의 비밀 세션키
- $E_K()$: 키 K를 이용하는 관용 암호방식
- $KH_K()$ keyed hash function

그림 1. Proxy-Signcryption 방식

2) 서명서버 G는 다음 식을 이용하여 Alice의 현재의 공개키 K_A^i를 검증한다.

$$h^{n-i}(K_A^i) = PK_A$$

3) 서명서버 G는 디지털 서명을 생성하여 다음과 같이 후보 NRO 토큰을 생성한다.

$$Sigs(ID_A, h(m_i), i, K_A^i)$$

4) 서명서버 G는 생성한 후보 NRO 토큰을 Alice에게 전송한다.

5) Alice는 서명을 검증하고 i를 $i-1$로 변경한 후 다음과 같이 실제 NRO 토큰을 생성한다.

$$NRO^i = (Sigs(ID_A, h(m_i), i, K_A^i), K_A^{i-1})$$

6) Alice는 Bob에게 전송할 메시지와 NRO 토큰을 Proxy agent와 사전에 공유한 비밀키를 이용 암호화하여 $C = E_{sk}(m_i, NRO^i)$를 Proxy agent에게 전송한다.

7) Proxy agent는 암호문 C를 복호하고 NRO 토큰을 저장한다. 그리고 사전에 위임받은 대리 서명용 키를 이용하여 m_i에 대한 대리인 보호형 Proxy-Signcryption을 생성한다.

① Alice는 $x \in Z_q$를 선택하여 $K \equiv g^x \bmod p$를 계산하고 대리서명용 키 $x_{AP} \equiv (x_A + x \cdot K) \bmod p - 1$를 생성하여 비밀리에 (x_{AP}, K)를 proxy agent에게 전송한다.

② Proxy agent는 $g^{x_{AP}} \equiv (y_A \cdot K^K) \bmod p$를 이용하여 자신이 받은 대리서명용 키가 정당한지 확인한 후, 다음과 같이 alternative proxy x'_{AP}를 생성한다.

$$x'_{AP} \equiv x_{AP} + x_P y_P \bmod q$$

③ Proxy agent는 $x' \in Z_q$를 선택하여 $k \equiv y_B^{x'} \bmod p$ 계산하고, $k = k_1 \| k_2$로 나누어 다음과 같이 메시지 m_i에 대한 Signcryption을 생성한다.

$$r' = KH_{k_2}(m_i)$$

$$s' \equiv (x_{AP}')^{-1} \cdot (x' - r') \bmod q$$

$$c = E_{k_1}(m_i)$$

(c, r', s', K)을 Bob에게 전송한다.

④ Bob은 $y'_{AP} = y_A \cdot y_P^{y_P} \cdot K^K \bmod p$를 계산하고, 비밀키를 이용하여 $k = ((y_{AP}')^{s'} \cdot g^{r'})^{x_B} \bmod p$를 구하고 $k = k_1 \| k_2$로 나눈 후 메시지를 복호한다.

$$m_i = D_{k_1}(c)$$

단, $KH_{k_2}(m_i) = r'$인 경우에만 정당한 Signcryption으로 받아들인다.

8) Proxy agent는 생성한 Proxy-Signcryption (c, r', s', K)를 Bob에게 전송한다.

9) Bob는 Proxy-Signcryption을 검증하여 Alice의 요구에 의해 Proxy agent가 보낸 메시지임을 확인한다.

10) Bob은 9)에 대한 응답을 Proxy agent에게 전송한다.

11) Proxy agent는 메시지가 성공적으로 전달되었음을 Alice에게 알려준다.

그림2에 제시한 대리인 보호형 Proxy Signcryption 방식[7]은 Proxy-Signcryption 방식[6]과 유사하게 서명 생성과 같이 많은 계산량을 요구하는 부분은 서명 서버와 proxy agent에 의해 수행하고, Alice가 proxy agent에게 메시지를 전송하기 전에 서명 서버로부터 해당 메시지에 대한 NRO 토큰을 발급 받으므로 기존의 방식이 제공하지 못한 송신자 부인봉쇄 기능을 제공한다. 또한 송신자의 부인봉쇄 문제를 해결하기 위해 추가된 서명서버의 부정 검출기능도 함께 제공한다. 그러나 대리인 보호형 방식은 아래와 같이 proxy agent와 Bob 사이에 메시지의 안전성 유지가 어렵다는 문제점이 있다[10].

① 가정 : 대리 서명키 x'_{AP}의 노출

② $k = ((y_{AP}')^{s'} \cdot g^{r'})^{x_B} = y_B^{x'_{AP} \cdot s' + r'}$

Bob 이외의 다른 사람이 키 k값을 계산할 수 있고, 이는 대리서명용 키 x'_{AP}에 대한 forward secrecy를 제공하지 못함을 의미하며, x'_{AP}는 특정인의 개인키가 아니므로 대리 서명인의 부주의로 각 개인의 개인키보다 노출 될 확률이 높다.

3. 제안 Proxy-Signcryption 방식

본 장에서는 이동 통신 환경에 응용하기 위하여 수신자 지정 서명 방식과 대리인 보호형 서명 방식을 적용하고, proxy agent에서 forward secrecy를 제공하는 개선된 Proxy-Signcryption 방식을 제안한다.

[시스템 설정] 2장의 시스템 설정에 추가되는 항목

- x_A, x_B, x_P : Alice, Bob, Proxy agent의 비밀키
- y_A : $y_A \equiv g^{x_A} \bmod p$, Alice의 공개키
- y_B : $y_B \equiv g^{x_B} \bmod p$, Bob의 공개키
- y_P : $y_P \equiv g^{x_P} \bmod p$, Proxy agent의 공개키
- S : 위임서명자의 일회용 비밀서명정보
- T_i : time stamp(실시간 값)
- T' : Proxy agent가 암호문을 받는 시간
- ΔT : 채널의 최대 지연시간

3.1 프로토콜

1) 위임정보 생성

이동 통신 단말기를 보유한 Alice는 proxy agent에게 서명생성을 위한 위임정보를 사전 계산(K는 위임정보 생성에 관여하지 않으므로 사전계산 가능)하여 휴대폰 단말기나 스마트카드에 저장한다. 이는 오프라인 상에서 이루어 질 수 있으므로 온라인 접속시에 연산 부하량과 시간을 단축시킬 수 있다.

$$x \in Z_q$$

$$R \equiv g^x \bmod p$$

$$K \equiv y_P^x \bmod p$$

$$S \equiv (x_A + x \cdot R) \bmod p-1$$

Alice는 이동 통신 단말기를 사용하지 않을 때 즉, 무선 네트워크를 사용하지 않거나 음성 통화를 하지 않는 빈 시간에 K, R, S를 계산하고 메시지를 전송하고자 할 때, 사전 저장되어 있는 K, R, S 값을 이용하여 다음과 같이 C를 계산한 후, Proxy agent에게 (R, C)를 전송한다.

$$C \equiv E_K(m \| S \| T_i)$$

Alice는 위의 과정을 반복 수행할 필요 없이 필요시 오프라인 상에서 사전 계산(K, R, S)하여 저장된 값을 이용하여 C를 1번만 수행하면 된다. 따라서 n번 반복 수행시 계산량은 C를 n번 수행한 계산량을 가진다. 또한 K에서 g^x를 계산하기 위해서는 proxy의 비밀 서명정보 x_P를 알아야 하므로 지정된 수신자만이 이를 복호할 수 있으며, S를 암호화한 후 C에 포함하여 송부하므로 공격자는 S를 알 수 없고, R을 이용하여 암호문 C를 복호해야만 S를 알 수 있다. 즉 외부에 공개되는 정보를 최소화 할 수 있다.

2) 위임정보의 확인 및 변환

Proxy agent는 수신된 정보를 기초로 세션키 K를 계산하고, 계산된 K를 이용 암호문을 복호하여 time stamp(T_i)를 다음과 같이 검증한다.

$$K \equiv R^{x_P} \bmod p$$

$$m \| S \| T_i \equiv D_K(C)$$

$$T' - T_i \le \Delta T$$

만약 검증이 만족되지 않으면 요청을 거절하고, 만족하면 위임 서명자의 정당성을 확인하고 다음과 같은 x_{AP}를 생성한다.

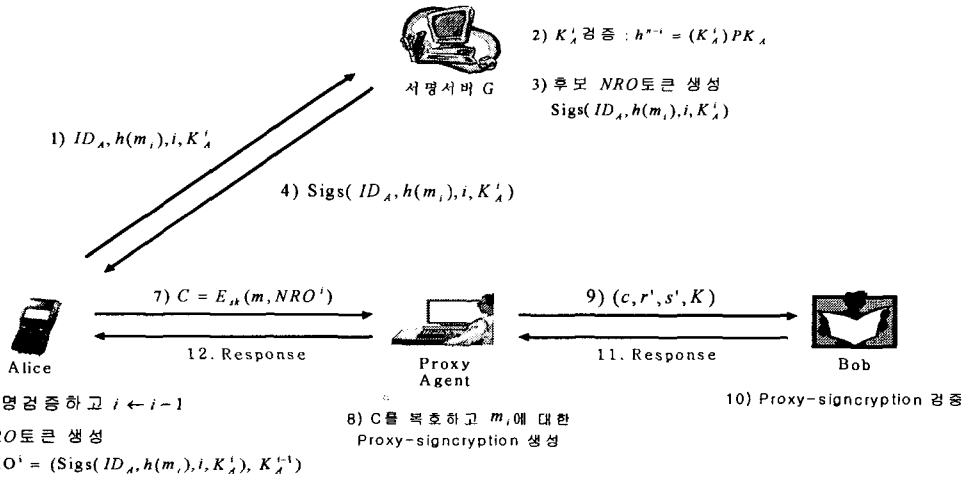


그림 2. 대리인 보호형 Proxy-Signcryption 방식

$$g^S \equiv (y_A \cdot R^R) \bmod p$$

$$x_{AP} \equiv S + x_P y_P \bmod q$$

3) Proxy agent에 의한 Signcryption 생성

$$x' \in Z_q$$

$$k \equiv h(y_B^{x'} \bmod p)$$

$$K' \equiv h(g^{x'} \bmod p)$$

$$r \equiv KH_{K'}(m)$$

$$s \equiv x' - (x_P + x_{AP} \cdot r) \bmod q$$

$$c \equiv E_k(m)$$

Signcryption 메시지 (c, r, s, R)을 Bob에게 전송한다.

4) Proxy-Signcryption 검증

Bob은 $y_{AP} \equiv y_A \cdot y_P^{y_P} \cdot R^R \bmod p$를 계산하고, 다음과 같이 메시지를 복호한다.

$$t_1 \equiv (y_{AP}^r \cdot y_P \cdot g^s) \bmod p$$

$$t_2 \equiv t_1^{x_B} \bmod p$$

$$K' \equiv h(t_1)$$

$$k \equiv h(t_2)$$

$$m \equiv D_k(c)$$

단, $KH_{K'}(m) \equiv r$인 경우에만 정당한 Signcryption으로 받아들인다.

그림3에 보인 제안방식에서 수신자 Bob이 y_{AP}를 계산하는 과정에서 Alice의 공개키 y_A와 proxy agent의 공개키 y_P를 동시에 사용하므로 Alice의 위임에 의해 proxy agent가 생성한 Proxy-Signcryption임을 확인 가능하다. 또한 s를 생성하는데 proxy agent의 비밀키 x_P가 사용되므로 이 값을 모르는 Alice는 정당한 Proxy-Signcryption을 생성할 수 없다.

3.2 제안방식의 고찰

(1) 서명자 기밀성 확보

제안방식은 수신자 지정 대리 서명방식을 적용함으로 수신자를 보호할 수 있다. 즉, 메시지의 진위여부를 판단하기 위해서는 수신자의 도움 없이는 불가능하다. 따라서 서명의 검증기능을 수신자의 통제 하에 두어 수신자만이 이를 복호할 수 있으므로 기밀성을 보장한다고 할 수 있다.

(2) 인증성 제공

이동 통신에서 투명성을 높이기 위해서는 인증성 제공은 필수적이다. 제안방식은 메시지의 송·수신시 출처가 누구이며, 전송 도중 제3자로부터의 위조 및 변경내용 확인이 가능하므로 인증성을 제공한다.

(3) 부인봉쇄 기능

서명 생성시 proxy agent는 자신의 비밀 정보와 서명자의 위임 서명 정보를 함께 포함하여 대리 서명을 수행하게 되므로 Alice의 서명 생성에 대한 부인방지가 가능하다.

(4) 유효성 획득

무선 이동 통신은 메시지 송·수신을 위해 일반 네트워크에 비해 상대적으로 계산능력이 떨어지는 무선 단말기를 사용한다. 따라서 서명 생성시 상대적으로 계산능력이 뛰어난 proxy agent를 이용하여 서명을 수행함으로 유효성을 확보할 수 있다.

(5) 안전성 제공

무선 이동 통신에서 메시지 송·수신에 참여하는 개체에 의한 위조 및 변조가 불가능해야 한다. 따라서

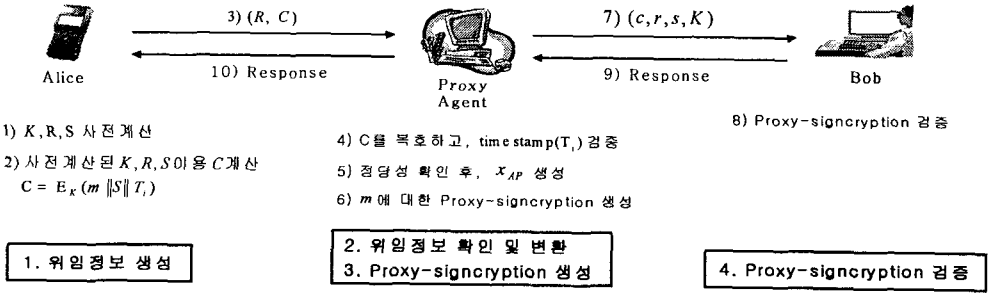


그림 3. 제안하는 효율적인 대리인 보호형 Proxy-Signcryption 방식

제안방식에서는 위임정보 전송시 Alice는 일회용 비밀 서명 정보를 제공하며, K에서 g^x를 계산하기 위해서는 proxy의 비밀 서명정보 x_P를 알아야 하므로 ($K \equiv (g^x)^{x_P} \bmod p$), 지정된 수신자만이 이를 복호할 수 있다. 또한 S를 암호화한 후 C에 포함하여 송부 ($C \equiv E_K(m \| S \| T_i)$)하므로 공격자는 S를 알 수 없고, $R \equiv g^x \bmod p$을 이용하여 암호문 C를 복호해야만 S를 알 수 있으므로 외부에 공개되는 정보를 최소화하고 있다. 서명 생성시 proxy agent는 자신의 비밀 정보를 생성하여 서명을 전송하므로 Alice 및 proxy agent에 의한 불법적인 서명 생성은 불가능하고, proxy agent에서 forward secrecy를 제공하는 개선된 Signcryption을 사용하므로 메시지에 대한 안전성(security)을 제공한다. Unsigncryption 과정에서 $(y_{AP}{}^r\ y_P\ g^s)^{x_B} = y_B{}^{x_{AP}r + x_P + s}$이 성립하나, 대리 서명키 x_{AP}가 드러나는 경우에도 대리 서명자의 개인키 x_P를 알지 못하는 사람은 키를 계산할 수 없고, x_P를 알지 못하는 사람은 대리 서명을 수행할 수 없으므로 대리 서명 위임자의 위조 공격으로부터 대리 서명자를 보호할 수 있으므로 forward secrecy를 제공한다. 즉 x_{AP}와 x_P가 모두 드러나면 키를 계산할 수 있지만, 두 키가 모두 드러날 경우는 x_{AP}만 드러날 경우에 비해 매우 낮은 확률로 발생한다.

기존방식은 Bob의 unsigncryption 과정에서 수신자의 개인키(x_B) 정보가 필요하기 때문에 제3자에게 Proxy-Signcryption의 정당성 여부를 증명하기 위해서는 영지식 증명(zero knowledge proof)과 같은 복잡한 계산과정을 필요로 하거나 서명 서버와 같은 별도의 구성요소를 필요로 한다. 따라서 제안방식은 Bao & Deng[11]이 제안한 공개키에 의한 direct verifiability를 제공한다. 즉, Bob이 제3자에게 (m, r, s)를 보내면 제3자는 proxy agent의 공개키를 이용하여 $K' \equiv h((y_{AP}^r \cdot y_P \cdot g^s) \bmod p)$를 계산하고, $r \equiv KH_{K'}(m)$이 성립하면 proxy agent가 서명을 생성하였음을 확인할 수 있으므로 공개키에 의한 direct verifiability를 제공한다.

(6) Alice의 계산량

제안방식을 이동통신 환경에 적용할 경우 서명 후 암호화하는 방식에 비해 단말기 사용자에게 요구되는 계산량을 감소시킬 수 있다. 또한, 모듈러 멱승과 같은 복잡한 연산을 오프라인에서 사전계산(precomputation)을 통하여 감소시킴으로써 휴대용 단말기와 같은 낮은 연산 처리 능력을 가지는 시스템에 적합하도록 하였다. 즉, 제안방식은 Alice가 1번 수행시 ENC 1번의 계산량을 가지면서 forward secrecy 제공과 노출되는 정보를 최소화하고, time stamp(T_i)를 사용하므로 실시간 값으로 검증이 가능하다. Alice에게 요구되는 계산량을 기존의 방식과 비교하면 표1과 같다.

4. 결 론

네트워크와 휴대용 단말기가 급속도로 발전함에 따라 사용자들이 이동 중에 휴대용 단말기를 이용하여 인터넷 전자 상거래를 이용하는 경우가 많아지고 있다. 이러한 환경에서 이동 통신상의 기밀성, 인증 및 부인봉쇄를 제공하는 효율적인 디지털 서명 방식의 연구는 매우 중요한 주제가 되고 있다.

Proxy-Signcryption 방식의 경우 대리 서명방식과 Signcryption 방식의 적용을 통해 기밀성, 인증성 및 유효성을 보장하고 있으나, 송신자와 대리 서명 에이전트(agent)의 부정을 방지하지 못함으로서 부인 봉쇄

표 1. 각 방식별 특성 비교 분석

구 분	서명자 기밀성	인증성	부인봉쇄	유효성	안전성	forward secrecy	구성요소 개수	Alice의 계산량
Proxy-Signcryption[6]	○	○	×	○	×	×	3	ENC: 1 EXP: 1
대리인 보호형 Proxy-Signcryption[7]	○	○	○	○	×	×	4	ENC: 1 EXP: 1
제안방식	○	○	○	○	○	○	3	ENC: 1 [EXP: 2]

※ EXP: 모듈라 멱승, ENC: 관용암호방식, [•] : 오프라인 연산,
※ 구성요소의 수 : 각 방식에 사용되는 구성요소[Alice, proxy agent, Bob, 서명서버 G]

및 안전성을 만족시키지 못하고 있다. 또한 대리인 보호형 Proxy-Signcryption 방식[7]은 기밀성, 인증성, 유효성 및 부인봉쇄는 제공하고 있으나, proxy agent에서 forward secrecy를 제공하지 못하므로 메시지에 대한 안전성을 제공하지 못하는 문제점이 있다.

따라서 본 논문에서는 수신자 지정 서명 방식과 대리인 보호형 대리 서명 방식 및 proxy agent에서 forward secrecy를 제공하여 원 서명자인 Alice도 proxy agent를 대신하여 정당한 Proxy-Signcryption을 생성할 수 없고, Alice는 자신이 전송한 메시지에 대해 그 사실을 부인할 수 없도록 하였다. 또한 proxy agent는 사용자의 요구가 있는 경우에만 Proxy-Signcryption을 생성할 수 있는 개선된 Proxy-Signcryption 방식을 제안하였다. 이를 통해 제안방식은 기밀성과 효율성을 획득하고 있으며, 동시에 인증성, 부인봉쇄 및 안전성을 만족하고 있기 때문에 계산능력이 상대적으로 낮은 이동 통신환경에 적용할 수 있다.

참 고 문 헌

[1] S.J.Kim, S.J.Park and D.H.Won, "Nominative Signatures." Proc. of ICEIC'95, pp.Ⅱ-68-Ⅱ-71, 1995.

[2] Y.Zheng, "Digital Signctyption or How to Achieve Cost (Signature & Enctyption) << Cost(Signature)+Cost(Enctyption)", Advances in Cryptology-CRYPTO'97, Springer-verlag, LNCS 1294, pp.165-179, 1997

[3] Y.Zheng, "Signcryption and Its Applications in Efficient Public Key Solutions", Proceedings of 1997 Information Security Workshop (ISW'97), LNCS 1397, pp.291-312, Springer-verlag, 1998.

[4] M.Mambo, K. Usuda and E. Okamoto, "Proxy Signature: Delegation of the Power to Sign Message", IEICE Trans. on Fundamentals E79-A(9):1338-1354. 1996.

[5] M.Mambo, K. Usuda and E. Okamoto, "Proxy Signatures for Delegation Signing Operation", Proc. Third ACM Conference on Computer and Communications Security, pp.48-57, 1996.

[6] C.Gamage, J.Leiwo and Y.Zheng, "An Efficient Scheme for Secure Message Transmission Using Procy-Signcryption", Proc. of the 22nd Australasian Computer Science Conference, Jan. 1999.

[7] 오수현, 김현주, 원동호, "이동통신 환경에서의 전자 상거래에 적용할 수 있는 Proxy-Signctyption 방식", 한국정보보호학회 논문지, 제10권 제2호, 2000.6.

[8] N. Asokan, G. Tsudik and M. Waidner, "Server Supported Signatures", Proc. of the Fourth European Symposium on Research in Computer Security(ESORICS), LNCS 1146, pp.131-143, Springer-Verlag, Sept. 1996.

[9] N. Asokan, G. Tsudik and M. Waidner, "Server Supported Signatures", Journal of Computer Security, November 1997.

[10] 정회윤, 이동훈, 임종인, "Forward secrecy를 제공하는 Signcryption" ITRC Forum pp.(D1)11-44, 2001.

[11] F. Bao, R. H. Deng, "A Signcryption Scheme with Signature Directly Verifiable by Public Key", PKC'98, Springer-Verlag, LNCS 1431, pp. 55-59, 1998.

김 동 우

1998년 2월 금오공과대학교 응용수학과 졸업(이학사)
2003년 2월 부경대학교 전산정보학과 졸업(공학석사)
1998년 3월~현재 육군 복무

관심분야 : 정보보호 및 암호학, 무선보안, 디지털 서명

박 지 환

1990년 3월 일본 요코하마국립대 전자정보공학 졸업 (공학박사)
1994년 9월~1995년 3월 동경대 생산기술연구소 방문연구
1998년 1월~1998년 2월 전기통신대학(일본), 방문연구
1999년 7월~1999년 8월 Monash University, Australia, Visiting Research
2001년 2월~2001년 3월 Communication Research Lab(CRL) Japan, STA Fellowship
1996년 4월~현재 동경대학 생산기술연구소 협력연구원
1990년 3월~현재 부경대 컴퓨터멀티미디어공학부 교수
1997년 3월~현재 한국정보보호학회 이사
2002년 3월~현재 한국정보보호학회 영남지부장
1998년 12월~현재 한국멀티미디어학회 운영위원 논문지 편집위원
1999년 3월~현재 한국정보처리학회 논문지 편집위원
2002년 3월~현재 한국정보보호학회 논문지 편집위원
2002년 1월~2월 CRL 방문연구 JSPS Fellowship
관심분야 : 멀티미디어 컨텐츠 보호 및 응용, 암호학

교 신 저 자

박 지 환 608-737 부산시 남구 대연3동 599-1 부경대학교 전자컴퓨터정보통신공학부