이동 통신 환경에 적합한 일회용 대리 서명 방식

김 소 진[†] · 박 지 환[††]

요 약

이동 통신의 발전으로 많은 사람들이 다양한 고품질의 응용 서비스를 손쉽게 제공받고 있다. 그러나 이러한 서비스가 이동 통신상에서 제공되면 유선망에 비해 많은 취약성을 가지게 되고, 단말기 성능의 제약으로 수행될 수 있는 작업에도 한계가 있다. 따라서 본 논문에서는 상대적으로 계산 능력이 뛰어난 대리자(proxy agent)를 통해 사용자의 계산량을 줄이면서 대리자의 부정을 방지할 수 있는 일회용 대리 서명 기법을 제안한다. 제안 방식은 실패-중단 서명기법[1]을 응용한 KBLK 방식[2]을 개선한 것으로 오직 한 개의 메시지에 대해서만 주어진 위임 정보로 대리 서명을 수행하여 대리자의 부정을 방지하도록 구성하였고, 전자 상거래와 같은 환경에서 원 서명자의 신분을 보호하도록 익명성의 기능을 추가하였다.

An One-time Proxy Signature Scheme Suitable for Mobile Communications

So-Jin Kim[†] · Ji-Hwan Park[††]

ABSTRACT

According to the development of mobile communications, many people have been offered high quality of the application services using portable terminals. But those works may have many vulnerabilities and have the limit of excutaions. Because the application services are provided in mobile network and the performanc of portable terminals is lower than that of base stations. To improve these problems, in this paper, we propose one-time proxy signature scheme that can reduce the computational ctsost on a user and prevent a proxy agent's dishonesty. The proposed scheme is based on the KBLK scheme [2] which applied the fail-stop signature scheme [1]. It is constructed that a proxy signer can sign only one message with a proxy key and we add anonimity to it for the user's identity protection in mobile communication like a M-commerce.

키워드 : 일회용 대리 서명(One-time Proxy Signature), 이동 통신(Mobile Communications), 대리자(Proxy Agent), 효율성(Efficiency), 익명성(Anonimity)

1. 서 론

무선 네트워크의 발전으로 언제 어디서나 편리하게 인터넷에 접속하여 정보검색, 동영상 서비스, 전자 상거래, 전자 계약 및 결재 등의 다양한 응용 서비스를 이용할 수 있게 되었다. 그러나 이러한 이동 통신 관련 서비스들은 쉽게 여러 가지 보안상의 문제점들에 노출될 수 있다. 즉, 사용자의 정보는 신뢰되지 못한 제 3자에 의해 악의적으로 이용될 수 있고, 위조나 불법 변경 등과 같은 위협에도 노출될 수 있다. 더우기 사용자 인증 및 부인 봉쇄 등과 같은 문제가 발생할 수 있다. 그리하여 네트워크상에서 발생하는 문제점들을 안전하게 해결하는 효과적인 방법중에 하나가 디지털 서명 기법이다. 그러나 일반 디지털 서명은 누구나 서명 확인이 가능하므로 서명자의 기밀성, 익명성 등을 보장할 수 없으므로 무선 전자 상거래와 같은 응용 서비스의 활성화를 위해 이를 보장하는 특수 디지털 서명 기법이 요구된다.

1.1 관련 연구

디지털 서명은 네트워크 상의 통신 상대방을 인증하고 메시지의 무결성을 보장하여 송·수신자간의 분쟁을 해결할 수 있는 전자 서명 방식이다. 이것은 일반적으로 공개키 암호 시스템을 기반하기 때문에 무선 환경에 그대로 적용하는 것은 사용자 단말기의 제한된 용량(메모리, CPU 파워, 인터페이스 등)으로 효율적이지 못하다는 문제점이 제기되고 있다.

이러한 문제점을 해결하기 위해 1995년 Mambo는 처음으로 사용자의 효율성을 보장하는 대리 서명 방식을 제안

† 준 회 원 : 부경대학교 대학원 정보보호학과
†† 종신회원 : 부경대학교 전자컴퓨터정보통신공학부 교수
논문접수 : 2003년 6월 12일, 심사완료 : 2003년 9월 8일

하였다[3, 4]. 대리 서명은 원 서명자가 지정한 사람(proxy agent)이 원 서명자를 대신해서 서명을 수행하는 방식으로 이동 통신에 적용하면 사용자의 계산량을 줄여주는 장점을 가진다. KPW 방식[5]은 서명 정보와 대리 서명키의 유효 기간을 포함하는 보증서를 통해 대리 서명을 실행시키는 방식으로 Mambo 방식을 확장하였다.

PL 방식[6]은 서명자의 기밀성을 보장하는 수신자 지정 대리 서명을 소개하였다. 이 방식은 이동 통신상에서 계산 능력이 뛰어난 대리자를 이용하여 서명을 수행함으로 원 서명자의 효율성을 확보하지만, 안전한 채널을 가정하지 않은 이동 통신상에서는 원 서명자가 지정한 대리자가 아닌 다른 사람이 대리 서명할 수 있는 문제점이 있다.

Gamage는 Mambo가 제안한 부분 위임 대리 서명 방식과 Zheng의 Signcryption 방식[7]의 장점을 이용하여 proxy-signcryption 방식을 제안하였다[8]. Proxy-signcryption은 사용자가 지정한 대리인이 자신을 대신하여 정당한 Signcryption 메시지를 생성할 수 있도록 하는 방식으로 Signcryption을 생성하는데 요구되는 계산을 상대적으로 계산 능력이 뛰어난 대리자에 의존하는 것이다. 그러나 Gamage의 방식을 실제 응용에 적용할 경우 사용자가 대리자를 대신하여 정당한 대리 서명을 생성할 수 있을 뿐만 아니라, 자신이 전송한 메시지에 대해 부인할 수 있다. 그리하여 OKW 방식[9]에서 대리인 보호형 proxy-signcryption을 제안하였고, 다시 이 방식을 KP 방식에서 개선하였다.

KP 방식[10]은 수신자 지정 대리 서명 방식을 적용하였으므로 메시지의 진위여부를 판단하기 위해서는 수신자의 도움 없이 불가능하여 서명자의 기밀성을 보장하고, 서명 생성시 대리자는 자신의 비밀 정보와 서명자의 위임 정보를 함께 포함므로 원 서명자의 부인 봉쇄도 가능하다. 그러나 원 서명자의 위임 정보가 대리자에 의해 여러 번 반복 사용될 수 있다.

KBLK 방식[2]은 대리자의 부정을 방지할 수 있는 일회용 대리 서명을 소개하였다. KBLK의 일회용 대리 서명은 실패-중단 서명 기법[1]을 사용하여 원 서명자의 허락없이 위임 정보를 재사용할 경우, 대리 서명자의 비밀키가 노출되기 때문에 대리자의 부정을 방지할 수 있다. 그러나 위임 정보의 수가 많고, 대리 서명을 위한 키의 수가 많기 때문에 키 관리와 사용자의 계산량에서 효율적이지 못하다. 또한 이 방식은 수신자를 지정하지 않기 때문에 사용자의 기밀성에 문제가 될 수 있다.

1.2 본 논문의 구성

본 논문에서는 이동 통신 보안 요구사항[6, 11, 12]을 고려하여 KBLK 방식[2]을 개선한 일회용 대리 서명 기법을 제안한다. 제안 방식은 위임 정보의 수를 하나로 줄이고 서명을 위한 키 사용을 줄여 사용자의 계산량을 낮추었고, 전자 상거래와 같은 응용 서비스에 적용 가능하도록 익명성 기능을 추가하였다. 그리하여 원 서명자의 기밀성 및 익명성을 보장하고, 송·수신자의 부인 봉쇄와 대리자의 부정 방지로 안전성을 확보한다.

본 논문의 구성은 다음과 같다. 본 장에서는 기존 대리 서명 기법들에 대해 소개하였고, 2장은 KBLK 방식의 일회용 대리 서명을 분석하며, 3장에서 이동 통신 환경에 적합한 개선된 일회용 대리 서명을 제안한다. 그리고 4장에서는 제안 방식의 안전성을 분석하고, 다른 대리 서명 방식들과 비교한다. 끝으로 마지막 5장에서 결론을 제시한다.

2. KBLK 방식 : 일회용 대리 서명 기법

본 장에서는 대리자의 부정을 방지할 수 있는 KBLK 방식[2]의 일회용 대리 서명 기법을 설명한다. 일회용 대리 서명은 대리 서명자의 부정을 방지하도록 오직 한 개의 메시지에 대해서만 주어진 위임 정보값으로 대리 서명할 수 있는 방식이다. KBLK 방식은 모발 에이전트를 이용한 전자 상거래 환경에서 호스트의 부정에 대한 안전성을 강화하기 위해 제안되었다. <표 1>에 KBLK 방식에서 사용되는 시스템 계수를 나타낸다.

〈표 1〉 매개 변수와 시스템 설정(i)

p	512비트 이상의 큰 소수, 공개
q	$q \mid p-1$인 큰 소수, 공개
Z_p^*	modulo p인 정수의 곱셈군
g, R	위수가 q인 Z_p^*상의 생성자
x_A, y_{A_1}, y_{A_2}	• 원 서명자(소비자)의 비밀키 1개 $x_A \in Z_q^*$ • 원 서명자(소비자)의 공개키 2개 $y_{A_1} \equiv g^{x_A}$, $y_{A_2} \equiv R^{x_A} \pmod p$
x_{B_i}, y_{B_i}, y_{B_k}	• 대리 서명자(호스트)의 비밀키 4개 $x_{B_i} \in Z_q^* \quad i = \{1,2,3,4\}$ • 대리 서명자(호스트)의 공개키 4개 $y_{B_j} \equiv g^{x_{B_j}} \quad j = \{1,3\}$ $y_{B_k} \equiv R^{x_{B_k}} \quad k = \{2,4\}$
ID_A	• 원 서명자의 원 ID
ID_B	• 대리 서명자의 원 ID
req_A	• 사용자의 주문조건(요구사항)
bid_B	• 호스트의 확인/판매 정보
msg	• 서명대상 메시지 $h(ID_A, ID_B, req_A, bid_B)$
$h(\cdot)$	• 안전한 일방향 해쉬함수

2.1 프로토콜

2.1.1 사용자는 로컬 환경에서 다음을 수행한다.

① 비밀키 k_1, k_2, k_3, $k_4 \in Z_q^*$ 선택한다.

② K_1, K_2, K_3, K_4 계산한다.

$$K_i \equiv g^{k_i},\ i \in \{1,3\},\ K_j \equiv R^{k_j} \pmod{p},\ j \in \{2,4\}$$

③ 위임 정보 s_{A_1}, s_{A_2}, s_{A_3}, s_{A_4}를 생성한다.

$$s_{A_i} \equiv x_A \cdot h(req_A \| K_i) + k_i \pmod{p},\ i \in \{1,2,3,4\}$$

모발 에이전트는 사용자의 요구 조건에 유효한 주문 정보를 가진 호스트를 만나면, 사용자의 (ID_A, req_A, K_1, K_2, K_3, K_4, s_{A_1}, s_{A_2}, s_{A_3}, s_{A_4})을 호스트에게 전달한다.

2.1.2 호스트는 주문정보 bid_B를 이용하여 서명할 메시지 $msg = h(ID_A \| ID_B \| req_A \| bid_B)$를 계산한다. 그리고 다음의 값들을 계산한다.

① 에이전트가 전달한 키 값들을 검증한다.

$$g^{s_{A_i}} \equiv y_{B_1}^{h(req_A, K_i)} K_i,\ i \in \{1,3\}$$

$$R^{s_{A_j}} \equiv y_{B_2}^{h(req_A, K_j)} K_j,\ j \in \{2,4\}$$

② 대리 서명을 위한 서명키를 생성한다.

$$s_i \equiv s_{A_i} + x_{B_i} \cdot h(req_A \| K_i),\ i \in \{1,2,3,4\}$$

③ 대리 서명에 대한 공개키 β_1, β_2를 계산한다.

$$\beta_1 \equiv g^{s_1} R^{s_2},\ \beta_2 \equiv g^{s_3} R^{s_4} \pmod{p}$$

④ 메시지 msg에 대한 서명 값 σ_1, σ_2를 생성한다.

$$\sigma_1 \equiv s_1 + msg \cdot s_3 \pmod{q}$$

$$\sigma_2 \equiv s_2 + msg \cdot s_4 \pmod{q}$$

호스트는 모발 에이전트를 통해 (ID_A, ID_B, bid_B, msg, β_1, β_2, σ_1, σ_2)를 사용자에게 전달한다.

2.1.3 사용자는 전달받은 값들을 검증하여 호스트가 생성한 서명에 대한 인증을 수행한다.

① $m = h(ID_A \| ID_B \| req_A \| bid_B)$를 계산하여 $m = msg$인지 검사한다.

② 서명 공개키를 검증하여 호스트가 서명키를 정당하게 생성했는지 검증한다.

$$\beta_1 \equiv (y_{A_1} y_{B_1})^{h(req_A, K_1)} (y_{A_2} y_{B_2})^{h(req_A, K_2)} K_1 K_2 \pmod{p}$$

$$\beta_2 \equiv (y_{A_1} y_{B_3})^{h(req_A, K_3)} (y_{A_2} y_{B_4})^{h(req_A, K_4)} K_3 K_4 \pmod{p}$$

③ 서명을 검증한다.

$$\beta_1 \beta_2^{msg} \equiv g^{\sigma_1} R^{\sigma_2} \pmod{p}$$

2.2 특성 분석

KBLK 방식은 모발 에이전트를 이용한 전자 상거래에서 서명 함수의 수행권한이 호스트에게 전적으로 부여됨으로 이에 대한 안전성을 강화하기 위하여 제안되었다. 이 방식은 실패-중단 서명기법[2]을 적용하여 오직 한 개의 메시지에 대해서만 주어진 위임 정보로 대리 서명을 수행함으로 호스트(대리자)의 부정을 방지할 수 있다. 또한 대리 서명과 모발 에이전트의 적용으로 유·무선 통신에서 요구되는 사용자의 인증성 및 유효성을 제공하며 송·수신자간의 부인방지를 확보하고 있다. 그러나 원 서명자의 위임 정보 생성과 대리 서명시에 많은 값들이 계산되고 사용되어 키 관리의 문제가 있고, 모발 에이전트가 사용자를 대신하여 구매조건에 맞는 상품을 찾아 이동함으로 사용자의 기밀성에 문제가 될 수 있다. 또한 전자 상거래에 적용시 사용자의 익명성을 보호할 수 없어 프라이버시를 보장받지 못하는 문제가 있다. 따라서 본 논문에서는 무선 이동 통신상에 효율적으로 적용 가능한 개선된 일회용 대리 서명 방식을 제안한다.

3. 제안 방식 : 개선된 일회용 대리 서명 기법

〈표 2〉 매개변수와 시스템 설정(ii)

x_R, y_R	• 등록센터의 비밀키, 공개키 $x_R \in Z_q^*$ $y_R \equiv g^{x_R} \pmod{p}$
x_A, y_A	• 원 서명자의 비밀키 $x_A \in Z_q^*$ • 원 서명자의 공개키 $y_A \equiv (g \cdot y_R)^{x_A}$
x_{B_i}, y_{B_i}	• 대리 서명자의 비밀키(2개) $x_{B_i} \in Z_q^*\ i = \{1,2\}$ • 대리 서명자의 공개키(2개) $y_{B_i} \equiv (g \cdot y_R)^{x_{B_i}}$
x_C, y_C	• 원 검증자의 비밀키 $x_C \in Z_q^*$ • 원 검증자의 공개키 $y_C \equiv (g \cdot y_R)^{x_C}$
ID_A'	• 원 서명자의 임시 ID

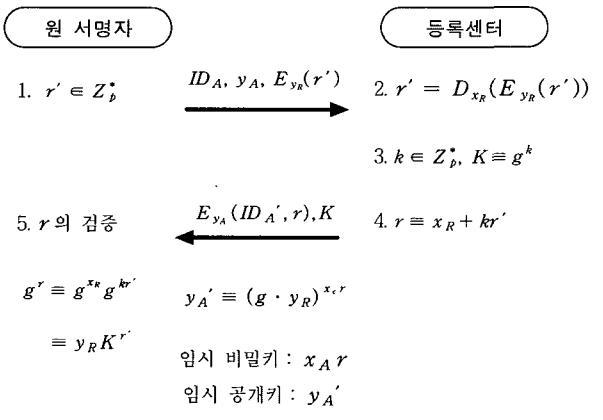
본 장에서는 이동 통신상의 보안 요구 사항[6, 11, 12]을

고려하여 KBLK 방식[2]을 개선한 일회용 대리 서명 기법을 제안한다. KBLK 방식은 수신자를 지정하지 않지만, 제안 방식은 기존 대리 서명 방식들처럼 수신자를 지정한다. 그리고 모든 공개키에 대한 인증과 공개를 위해서 등록 센터를 두었고, 원 서명자의 익명성을 보장하기 위한 임시 비밀키/공개키 쌍은 등록 센터를 통해 생성하고, 등록한다. 제안 방식은 KBLK 방식에 비해 키의 사용을 줄여 계산량을 낮추고, 전자 상거래와 같은 응용 서비스에 적용 가능하도록 원 서명자의 신분을 보호하는 익명성의 기능을 추가하였다. <표 2>에 제안 방식에서 사용되는 시스템 계수를 기술한다.

3.1 제안 프로토콜

3.1.1 등 록

원 서명자는 임시 비밀키/공개키 쌍을 얻기 위해 그림1과 같은 과정을 수행하여 임시 ID인 ID_c'를 얻고, r값을 검사하여 $g^r \equiv y_R K^{r'}$이 검증되면 $x_A r, y_A'$를 생성한다. 이때 r의 유효 기간에 따라 등록 횟수는 달라진다. 만약 r의 유효기간을 설정한다면, r을 생성할 때 유효기간 정보 값도 함께 포함시킨다. 그리고 r의 유효기간을 설정하지 않는다면, 등록은 한번만 하면 된다. 그러면 다음 등록 단계는 생략하고, 대리 서명 위임 단계를 수행하면 된다. 끝으로 등록센터는 자신의 비밀 DB에 원 서명자의 정보인 ID_A, y_A, $E_{y_R}(r)$를 저장하고, 모든 임시 공개키는 공개한다.



(그림 1) 원 서명자의 임시 비밀키/공개키 생성 단계

3.1.2 원 서명자의 위임 정보 생성

전자 상거래와 같은 응용 서비스를 이용할 경우, 원 서명자는 등록 단계에서 생성한 ID_A', $x_A r$, y_A'를 가지고 다음의 연산을 수행한다. 그러나 익명성의 기능이 필요하지 않는 환경이라면 자신의 원 비밀키/공개키 쌍과 원 ID_A를 이용해도 무방하다.

① $k \in Z_{p-1}$, $K \equiv (g \cdot y_R)^k \pmod p$

② ID_c', ID_B, K로 다음을 계산한다.

$$e = h(ID_A' \| ID_B \| m \| K)$$

③ 자신의 임시 비밀키 $x_A r$로 위임 정보를 생성한다.

$$(s \equiv x_A r \cdot e + k \bmod p) \bmod q$$

원 서명자는 대리 서명자에게(ID_A', K, s, m)을 전송하여 위임 서명을 요청한다.

3.1.3 위임 정보 검증 및 대리 서명 생성

대리 서명자는 위임 정보 s를 검증한 후, 수신자 지정 정보를 포함한 대리 서명키를 생성한다. 그리고 서명할 메시지를 계산하여 대리 서명을 수행한다.

① 다음 식이 검증되지 않으면 수행을 중단한다.

$$(g \cdot y_R)^s \equiv y_A'^{\,h(ID_A' \| ID_B \| m \| K)} \cdot K \pmod p$$

y_A'과 ID_A'의 정당성은 등록센터에서 확인 가능하다.

② 수신자 지정 정보를 생성한다.

$$x \in Z_{p-1},\ X \equiv y_C^x \pmod p$$

③ 수신자 지정 정보를 포함한 대리 서명 키 s'를 생성한다.

$$s' \equiv s + x_{B_1} + x_{B_2} + x \cdot X \pmod q$$

④ 대리 서명에 대한 공개키 β를 계산한다.

$$\beta \equiv (g \cdot y_R)^{s'} \pmod p$$

⑤ 서명할 메시지를 다음과 같이 계산한다.

$$msg = h(ID_A' \| ID_B \| ID_C \| m \| K \| x \| X)$$

⑥ 메시지 msg에 대한 서명 값 σ를 생성한다.

$$\sigma \equiv s' \cdot msg + x_{B_1} - x_{B_2} \pmod q$$

대리 서명자는(ID_A', ID_B, msg, σ, K, x, X)를 검증자에게 전달한다.

3.1.4 서명 검증

검증자는 전달받은 값들을 검증하여 대리자가 생성한 서

명에 대한 인증을 수행한다.

① $m = h(ID_A' \| ID_B \| ID_C \| m \| K \| x \| X)$로 $m = msg$인지를 검사한다.

② 서명 공개키를 검증하여 대리 서명자가 서명키를 정당하게 생성하였는지 검증한다.

$$\beta \equiv y_A'^{e} \cdot K \cdot y_{B_1} \cdot y_{B_2} \cdot (g \cdot y_R)^{x \cdot X} \pmod{p}$$

③ 자신의 비밀키 x_C를 가지고 서명을 검증한다.

$$X^X \equiv \{(g \cdot y_R)^{\sigma} \cdot \beta^{-msg} \cdot y_{B_1}^{-1} \cdot y_{B_2}\}^{x_C} \pmod{p}$$

4. 제안 방식의 고찰

제안 방식은 4.1절의 특성들을 통해 무선 이동 통신의 응용 서비스에 대한 요구 사항을 만족하고 있고, 4.2절에서 제안 방식의 안전성을 분석하였다. 그리고 4.3절은 기존에 제시되었던 대리 서명 방식의 분석 및 비교를 통해 이동 통신 환경에서 갖는 제안 방식의 장점을 입증한다.

4.1 제안 방식의 특성

다음과 같이 제안 방식을 무선 이동 통신상에서 확보해야 하는 보안 요구사항[6, 11, 12]에 기준하여 고찰하였다.

4.1.1 서명자의 기밀성 확보

사용자의 기밀성은 의도된 상대만이 통신하고 있는 상대가 누구인지 알 수 있고, 제 3자의 도청으로부터는 자신의 신원을 비밀로 보장하는 것이다. 제안 방식은 대리 서명키 생성시 수신자 지정 정보를 포함하여 계산함으로 서명 검증은 지정된 수신자만이 자신의 비밀키로 검증할 수 있다. 그리하여 제 3자의 도청으로부터 원 서명자의 신원을 보장한다.

4.1.2 인증성 제공

수신된 메시지가 정당한 송신자로부터 전송된 것인지 확인하고, 송·수신자간에 실제 신원을 확인하여 전송 정보의 출처를 보증해야 한다. 제안 방식에서 대리자는 위임 정보를 검증하고, 검증자는 서명 공개키를 검증여 정당성을 확인한다. 그리하여 송·수신자의 인증성을 제공하고, 전송 도중 제 3자로부터의 위조 및 변경이 불가능하다.

4.1.3 유효성 확보

무선 이동 통신은 메시지 송·수신을 위해서 계산 능력이 떨어지는 이동 단말기를 사용하기 때문에 사용자 측면에서 충분히 사용 가능해야 한다. 제안 방식은 원 서명자보다 상대적으로 계산 능력이 뛰어난 대리자가 대신하여 서명을 수행함으로 무선 단말기의 유효성을 확보할 수 있다.

4.1.4 부인봉쇄 기능

송신자가 메시지를 송신한 사실을 부인하거나 수신자가 메시지 수신 사실을 부인할 수 없어야 한다. 제안 서명은 서명 생성시에 대리자가 원 서명자의 위임 서명 정보와 대리자의 비밀 정보를 포함하여 수행하게 되므로 서로의 부인방지가 가능하다.

4.1.5 익명성 제공

신뢰되지 않는 제 3자로부터 자신의 신원을 비밀로 하는 사용자의 기밀성을 유지하더라도 송·수신자간에는 서로의 신분 확인이 가능하다. 그리하여 무선 전자 투표, 전자 입찰 및 전자 상거래 등과 같은 응용 서비스를 이용할 경우, 사용자의 익명성을 보장하지 못한다. 소비자가 프라이버시와 익명성이 보장되지 않는 응용 시스템으로 상거래를 하면, 그 행동자료(언제, 어디서, 무엇을, 얼마만큼 등)들은 수신자의 중앙 데이타베이스에 기록될 수 있다. 이것은 패턴 분석 기술을 이용하여 분석할 수 있고, 그 정보는 기업의 고객 선호도, 생활양식 등을 파악하기 위한 자료(프리이버시 침해)들로 판매될 수 있다. 실제로, 현재 쿠키나 다양한 판매자용 지능 대리 프로그램으로 웹 사용자들의 개인정보가 자신도 모르는 사이에 누출되고 있다. 따라서 일반 디지털 서명은 누구나 서명 확인이 가능하므로 서명자의 익명성을 보장할 수 없으므로 무선 전자 상거래와 같은 응용 서비스의 활성화를 위해 익명성 보장이 필요하다. 제안 방식에서는 임시 비밀키/공개키 쌍을 이용하여 원 서명자의 신분을 보호한다. 이것은 이산대수 문제의 어려움에 기반하며 임시 공개키 $y_A' \equiv (g \cdot y_R)^{x_A r}$에서 $x_A r$은 오직 원 서명자만 알고, 원 공개키 y_A는 등록센터만 알기 때문에 검증자는 임시 공개키 y_A'와 임시 ID_A'만으로 사용자를 인증한다.

4.2 안전성 분석

무선 이동 통신에서 메시지 송·수신에 참여하는 모든 개체와 불법자에 의한 위조 및 변조가 불가능해야 한다. 제안 방식은 전체적으로 이산대수 문제의 어려움에 기반하여 안전성을 확보한다. 위임 정보 생성은 원 서명자만이 할 수 있다. 즉, 위임 정보를 계산하기 위해서는 원 서명자의 비밀키를 알아야하므로 계산적으로 불가능하다 ($s \equiv x_A r e + k$). 게다가 위임 정보는 대리자의 정보를 포함하기 때문에 정당한 대리자만이 이것을 사용할 수 있다. 또한 대리 서명키 생성도 원 대리 서명자만이 수행할 수 있다. 대리자의 비밀키를 모르면 키를 생성할 수 없으며, 서명도 불가능하다

($s' \equiv s + x_{B_1} + x_{B_2}$). 그러므로 원 서명자에 의한 불법적인 서명 생성은 불가능하다. 제안 방식은 대리 서명자의 서명이 일회성임을 보장한다. 즉, 대리자가 원 서명자의 허락없이 서명키를 다른 용도로 사용한다면, 다음과 같이 자신의 비밀키도 노출되기 때문에 대리자의 부정을 방지할 수 있다. 두 메시지 m, m'에 같은 서명키로 서명한 값 $\sigma \equiv s' msg + x_{B_1} - x_{B_2}$와 $\sigma' \equiv s' msg' + x_{B_1} - x_{B_2}$의 차를 구하면, $(\sigma - \sigma') \equiv s'(msg - msg')$값이 되어 서명키 s'가 노출된다. 그리하여 서명값 σ에서 $x_{B_1} - x_{B_2}$의 값도 알 수 있고, $s' \equiv s + x_{B_1} + x_{B_2}$에서 $x_{B_1} + x_{B_2}$도 알 수 있어 대리자의 비밀키 x_{B_1}, x_{B_2}도 노출되게 된다. 서명 단계는 실패-중단 서명기법[1]의 안전성과 동일하다. 불법자가 원 서명(σ)을 위조(τ)하였다면 그는 등록센터의 비밀키 x_R를 알아야 한다. 즉, 불법자는 다음의 계산 가능성을 가지므로 $\log_g y_R$를 계산할 수 있어야 한다는 것이다.

$$\beta^{msg} \equiv g^{\sigma} y_R^{\sigma}\, {y_{B_1}}^{-1}\, y_{B_2} \equiv g^{\tau} y_R^{\tau}\, {y_{B_1}}^{-1}\, y_{B_2}$$

$$\therefore\ g^{(\sigma-\tau)} \equiv g^{x_R(\tau-\sigma)}\ (x_R \equiv (\sigma-\tau)(\tau-\sigma)^{-1})$$

4.3 다른 대리 서명 방식들과의 비교

제안 방식은 무선 환경에서 원 서명자를 대신하여 대리자가 서명을 수행함으로 일반 디지털 서명 방식보다 효율적이다. 또한 익명성을 위한 등록단계는 오프라인에서 사전처리(pre-compu tation)가 가능하여 이동 단말기와 같은 낮은 연산처리 능력을 가진 시스템에도 적용 가능할 것이다. <표 3>은 제안 방식과 KBLK 방식의 일회용 대리서명 방식을 비교한 것으로 사용된 키의 수는 KBLK 방식에 비해 총 7개가 감소한다. 제안 방식은 하나의 서명키로 하나의 서명 값을 생성하므로 각 서명생성 단계의 계산량이 상대적으로 감소하고 통신량도 감소되어 기존 방식보다 효율적이다. 또한 KBLK 방식은 위임 정보 4개, 서명 공개키 2개가 사용되지만, 제안방식은 수신자 지정을 위한 정보값이 증가하더라도 위임 정보 1개, 서명 공개키 1개가 사용됨으로 각 검증 단계가 KBLK 방식보다 간단하다.

〈표 3〉 일회용 대리 서명 비교

	KBLK 방식	제안 방식
일회성	○	○
서명자의 기밀성	×	○
서명자의 익명성	×	○
서명자의 원 비밀키 (원 공개키)	1개 (2개)	1개 (1개)
대리자의 원 비밀키 (원 공개키)	4개 (4개)	2개 (2개)
서명자의 위임 정보	4개	1개
서명자의 임시 비밀키	4개	1개
서명자의 임시 공개키	4개	1개
대리자의 대리 서명키	4개	1개
서명자의 계산량 (modular exponentiations)	4번	1번

<표 4>는 제안된 각 대리 서명 방식들을 이통 통신의 보안 요구사항별로 비교 분석한 것이다. Mambo 방식[3]은 이동 통신상에 적용할 경우 사용자의 계산량을 줄여준다는 장점은 있지만, 대리 서명자가 이전의 위임 정보를 가지고 서명을 생성할 수 있기 때문에 원 서명자가 서명 위임에 대한 부인이 가능하고, 대리자의 부정도 가능하다. 또한 누구나 서명 검증이 가능함으로 무선 환경에서 이를 사용할 경우 원 서명자의 정보 누출이 쉽기 때문에 서명 생성 주체들의 안전성 및 위임 정보의 신뢰성 부분에서 문제점을 가진다. PL 방식[6]은 수신자 지정 서명을 적용하여 오직 지정된 검증자만이 원 서명자의 신원을 확인할 수 있어 사용자의 기밀성과 인증성을 만족한다. 또한 위임 정보는 일회성을 갖는 랜덤 값을 이용함으로 대리자가 임의로 서명을 생성하는 것을 방지한다. 그러나 안전한 채널을 가정하지 않은 이동 통신상에서는 위임 정보 생성시 대리자의 정보를 포함하지 않으므로 원 서명자가 지정한 대리자가 아닌 다른 사람이 쉽게 대리 서명할 수 있다. 그리하여 결국 검증자는 타당하지 않은 대리자가 생성한 서명을 원 서명자의 대리 서명이라고 확신할 수 있게 되어 안전성에 문제가 될 수 있다. OKW 방식[9]은 대리인 보호형 방식으로 서명 생성과 같이 많은 계산량을 요구하는 부분은 서명 서버와 대리자(proxy agent)에 의해 수행하고, 원 서명자가 메시지 전송전에 서명 서버로부터 NRO 토큰을 발급받기 때문에 부인 봉쇄의 기능을 가진다. 그러나 대리자는 사전에 위임받은 대리 서명용 키를 그대로 계속 이용할 수 있기 때문에 이에 대한 대리자의 부정은 방지하지 못한다. KP 방식[10]은 수시자 지정 서명 방식과 대리인 보호형 방식을 결합하여 사용자의 기밀성과 부인 봉쇄를 만족한다. 그리고 서명 생성을 위한 위임 정보를 사전 계산하여 휴대폰이나 스마트 카드에 저장 가능하므로 온라인 접속시에 연산 부하량과 시간을 단축시킬 수 있다. 그러나 대리자의 부정은 고려하지 않았다. 즉, 원 서명자의 일회용 비밀 정보는 대리자에 의해 여러 번 반복 사용할 수 있다. 위임 정보를 사전에 미리 계산하여 필요시 같은 값을 그대로 사용하기 때문에 대리자의 부정이 가능하다. KBLK 방식[2]은 2장에서 설명했듯이 일회용 대리 서명 방식으로 위임 정보 재사용에 대한 대리자의 부정을 방지할 수 있다. 그러나 원 서명자의 위임 정보 생성과 대리 서명시에 많은 값들이 계산되

〈표 4〉 각 대리 서명들의 특성 비교

특 징 / 구 분	서명자 기밀성	인 증 성	부인봉쇄	유 효 성	안 전 성	익 명 성	구성요소 개 수	Alice의 계산량
Mambo 방식[3]	×	○	×	○	×	×	2	EXP : 1
PL 방식[7]	○	○	○	○	×	×	3	EXP : 1
OKW 방식[9]	○	○	○	○	×	×	4	EXP : 1
KP 방식[10]	○	○	○	○	×	×	3	EXP : 1
KBLK 서명[2]	△	○	○	○	○	×	2	EXP : 4
제안 방식	○	○	○	○	○	○	4	EXP : 1

※ EXP : Num. of modular exponentiations.

고 사용됨으로 효율성이 떨어지고, 모발 에이전트가 사용자를 대신하여 구매조건에 맞는 상품을 찾아 이동함으로 사용자의 기밀성에 문제가 될 수 있다. 제안 방식은 KBLK 방식을 개선하여 서명자의 기밀성, 부인 봉쇄를 확보하고, 무선 전자 상거래와 같은 응용 서비스에 적용 가능하도록 익명성 기능을 추가하였다.

5. 결 론

최근 무선 통신의 발전으로 다양한 응용 서비스가 이동 단말기를 통해 제공되고 있다. 그러나 정보의 위조나 불법 변경 등과 같은 위협과 원 서명자의 비밀 정보 유출은 유선망에 비해 더욱 취약하다. 그리하여 이동 통신의 안전한 서비스 사용을 위해서 사용자 기밀성, 인증, 부인봉쇄 등을 확보해야 한다. 이에 따라 디지털 서명 방식이 지속적으로 연구되고 있고, 대리 서명은 사용자의 계산적 부담을 덜어주기 때문에 이동 통신 환경에서 효율적이다. 그러나 기존의 대리 서명 방식들은 이동 통신의 요구사항에 맞추어 적용하기에 몇 가지 문제점이 있었다.

본 논문에서는 이동 통신에 적용 가능한 일회용 대리 서명 기법을 제안하였다. 일회용 서명 기법은 실패-중단 서명을 이용한 KBLK 방식을 개선한 것으로 위임 정보의 재사용에 대한 대리자의 부정을 방지할 수 있었다. 또한 제안 방식은 네트워트상의 요구 사항을 고려하였고, 원 서명자들의 프라이버시를 보호할 수 있도록 익명성 기능도 추가하였다. 향후 다양한 무선 인터넷 서비스 제공을 위해서 디지털 서명기법 뿐만 아니라 더욱 효율적이고 안전한 정보보호 기술 분야의 연구가 필요하겠다.

참 고 문 헌

[1] Heyst, E. van and Pedersen, T. P., "How to make efficient fail-stop signatures," Proceeding of Eurocrypt '92, pp.339-352, 1992.

[2] 김희선, 백준상, 이병천, 김광조, "대리 서명을 이용한 모발일 에이전트의 안전성 강화 방법", 한국정보보호학회, 종합학술발표논문집, Vol.10, No.1, pp.424-437, 2000.

[3] M. Mambo, K. Usuda and E. Okamoto, "Proxy signature," Proceedings of ICEIC '95, pp.II-68-II-71, 1995.

[4] M. Mambo, K. Usuda and E. Okamoto, "Proxy signature : delegation of the power to sign message," IEICE Transaction on Fundamentals, E79-A(9), pp.1338-1354, 1996.

[5] S. J. Kim, S. J. Park and D. H. Won, "Proxy signatures, revisited," Proc. of ICICS '97, LNCS 1334, pp.223-232, 1997.

[6] 박희운, 이임영, "이동 통신에서 적용 가능한 수신자 지정 대리 서명 방식", 한국정보보호학회논문지, 제11권 제2호, pp. 27-36, 2001.

[7] 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.

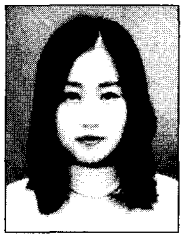
[8] C. Gamage, J. Leiwo and Y. Zheng, "An Efficient Scheme for Secure Message Transmission Using Procy-Signcryption," Proc. of the 22nd Australasian Computer Science Conference, Jan., 1999.

[9] 오수현, 김현주, 원동호, "이동 통신 환경에서의 전자 상거래에 적용할 수 있는 Proxy-Signcryption 방식", 한국정보보호학회논문지, 제10권 제2호, 2000.

[10] 김동우, 박지환, "이동 통신 환경에 적합한 효율적인 Proxy Signcryption", 한국멀티미디어학회논문지, 제6권 제3호, 2003.

[11] H. U. Park and I. Y. Lee, "A 2-pass Key Agreement and Authentication for Mobile Communication," Proceeding of the 2000 International Conference on Electronics, Information and Communications (ICEIC 2000), pp.115-118, 2000.

[12] 조동욱, 최연이, 김희도, 원동호, "이동 통신 환경에 적합한 상호 인증을 제공하는 키분배 프로토콜의 설계", 한국정보보호학회논문지, 제10권 제2호, 2000.



김 소 진

e-mail : sojin@shannon.pknu.ac.kr
2001년 동명정보대학교 정보통신학과 졸업
2003년 부경대학교 전자계산학과 석사
2003년~현재 부경대학교 대학원 정보보호학과
관심분야 : 멀티미디어 보호 및 응용, 암호학

박 지 환

e-mail : jpark@pknu.ac.kr
1984년 경희대학교 전자공학과(공학사)
1987년 일본 국립전기통신대학 정보공학과 (공학석사)
1990년 일본 요코하마국립대학 전자정보 공학과(공학박사)
1990년~현재 부경대학교 전자컴퓨터정보통신공학부 교수
1996년~현재 동경대학 생산기술연구소 협력연구원
1997년~현재 한국정보보호학회 이사
1998년~현재 한국멀티미디어학회 운영위원 및 논문지 편집위원
1999년~현재 한국정보처리학회 논문지 편집위원
2002년~현재 한국정보보호학회 영남지부장 및 논문지 편집위원
관심분야 : 멀티미디어 컨텐츠 보호 및 응용, 암호학