通信情報保護學會論文誌
第 11 券 第 2 號, 2001. 4

이동 통신에서 적용 가능한 수신자 지정 대리 서명 방식

박 희 운*, 이 임 영**

A Digital Nominative Proxy Signature Scheme for Mobile Communication

Hee-Un Park*, Im-Yeong Lee**

요 약

최근 무선 이동 통신의 발전을 기반으로 향후 이동 통신 시스템은 많은 사용자들에게 현재보다 더 나은 고품질의 멀티미디어 서비스를 제공할 것으로 기대된다. 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 무선 이동 통신상에서 상대적으로 계산 능력이 뛰어난 Agent의 도움을 통해 사용자의 전자 서명 및 암호화를 수행할 수 있는 수신자 지정 대리 서명 방식을 제안한다. 제안 방식은 대리 서명을 수행할 경우 발생할 수 있는 사용자 및 대리 서명 Agent의 부정 서명 생성 및 부인 행위를 방지하도록 구성되어 있다. 동시에 정당한 수신자가 서명을 확인하도록 함으로서 이동 통신상에서 기밀성을 획득하는 안전한 방식이라 하겠다.

ABSTRACT

Based on the development of mobile communication, the future mobile communication systems are expected to provide higher quality of multimedia services for users than today's systems. Therefore, many technical factors are needed in this systems. Especially the secrecy and the safety would be obtained through the introduction of the security for mobile communication. In this paper, we presents a digital nominative proxy signature scheme that processes a user's digital signature and encryption using the proxy-agent who has more computational power than origins in mobile communication. The proposed scheme provides non-repudiation and prevents creating illegal signature by the origin and proxy-agent in a phase of proxy signature processing. Also this scheme satisfies the confidentiality and safety in the mobile communication through a confirming signature by the right receiver.

keyword : *Nominative Proxy Signature, Agent, Mobile Communication, Confidentiality, Safety, Non-Repudiation*

1. 서 론

현대 사회는 컴퓨터 및 네트워크의 발전을 통해 정보 통신 분야의 급속한 발전이 이뤄지고 있으며, 이들은 "정보 사회"라는 새로운 문화적 전환기를 창출하고 있다. 정보 사회라는 새로운 패러다임 속에서 우리의 일반적인 생활 양식은 획기적인 변화의 흐름을 일으키고 있다. 즉, 수 없이 많은 정보가 전 세계로 이어진 네트워크를 통해 전송되고 있으며, 컴퓨터 및 응용 분야의 발전은 일반 사용자들로 하여금 더욱 편리하고 빠르게 개인 및 각 공유 정보의 교류를 활성화시키고 있는 것이다. 최근 이러한 조

* 순천향대학교 전산학과 정보보호연구실(heeun@cse.sch.ac.kr)
** 순천향대학교 정보기술공학부 부교수(imylee@sch.ac.kr)

류의 흐름 속에서 네트워크와 컴퓨터를 이용한 다양한 응용 분야들이 연구되고 있다. 전자 상거래, 전자 입찰 및 경매, 전자 복권, 전자 계약 및 결재, 전자 투표 등은 그 좋은 예가 될 것이다. 또한 이동 통신 및 Mobile IP(Internet Protocol) 분야는 IT(Information Technology) 산업계에서 가장 빨리 성장하는 분야 중에 하나로서, 많은 사람들이 이동 통신 서비스를 통해 그 편리성과 유용성을 인지하고 있다. 일 예로, 1995년 유럽에서 이동 통신 사용자 수가 2,200만 명에서 2000년에는 11,000만 명에 이를 전망이다. 기존의 2세대 이동 통신인 GSM과 DECT는 계속적으로 사용될 전망이며, 제3세대 이동 통신인 UMTS는 2002년부터 유럽에서 상용화 될 전망이다. 이와 함께 세계 각국의 이동 통신 서비스의 발전을 바탕으로 그 수요는 계속 늘어날 전망이다. 현재 많은 사용자들이 네트워크에 직접 연결된 컴퓨터를 사용하지 않고도 이동 중에 Hand PC나 PDA와 같은 휴대용 단말기를 이용하여 인터넷에 접속하고 상품 주문 및 계약 등과 같은 다양한 서비스를 지원받고 있다.[1][2][3][4][5]

그러나 이러한 이동 통신 관련 서비스들은 많은 보안상 문제점들에 노출될 수 있다. 즉, 이동 통신에서 신호 교환은 무선 채널을 통해 대기 중에서 수행되므로, 도청자나 그 밖의 신뢰되지 못한 요소들로부터 위조나 불법적 변경 등과 같은 위협들에 대해서는 취약성을 지니고 있다. 뿐만 아니라 사용자 인증 및 부인 봉쇄 등과 같은 문제는 이동 통신상에서 발생할 수 있는 안전성과 관련하여 여러 가지 문제를 발생시킬 수 있다. 따라서 가입자를 제외한 다른 불법적 가입자들로부터 기밀성과 안전성을 확보하고, 사용자의 인증성을 제공하기 위한 방법 중에 하나로서 '수신자 지정 서명' 기법이 제시되었다.[7] 이 기법은 네트워크 상에서 기밀성과 사용자 인증성을 동시에 제공하기 위해서 전자 서명을 수행하고 그 결과에 공개키 암호 방식을 사용하여 전송하게 된다. 그러나 이 방식은 모듈러 멱승과 같은 많은 계산량을 필요하게 되므로 상대적으로 계산 능력이 적은 휴대용 단말기상에서는 사용하기 힘들게 된다. 따라서 본 논문에서는 무선 이동 통신 상에서 인증성과 안전성을 제공하는데 필요한 고려 사항을 살펴보고, 기존의 방식들이 이에 대해 어떻게 대처하는지 살펴볼 것이다.[7][8][9][10] 또한 사용자 이동 단말기에서는 적은 계산량으로 전자 서명을 수행하면서 안전성을 제공하기 위해 대리 서명 Agent를 도입한 수신자 지정 대리 서명 기법을 제안한다. 이를 통해 무선 이동 통신 상에서 발생할 수 있는 사용자의 불법적 행위로부터 대리 서명 Agent를 보호하기 위한 기법을 제공함으로서 안전성을 확보하고 있다.

Ⅱ. 요구 사항 분석

본 장에서는 무선 이동 통신 상에서 수행되는 다양한 응용 분야에서 신뢰성과 효율성을 제공하기 위해 어떠한 요소들이 요구되며, 그 특징은 무엇인지 살펴본다.[11]

2.1 무선 이동 통신 정보 송·수신시 요구 사항

무선 통신상의 정보교환을 위해서 키 분배 및 인증 등이 필요하며 송/수신된 메시지에 대해 부인봉쇄를 수행할 수 있어야 한다. 또한 제 3자의 불법적 도청으로부터 송신자의 신원 노출을 방지하기 위하여 사용자 기밀성을 확보해야 한다. 다음은 이들에 대한 요구 사항을 기술한 것이다.

(1) 사용자 기밀성

무선 이동 통신을 통해 송신자가 메시지를 송신할 경우 제 3자의 도청으로부터 자신의 신원을 보장하기 위하여 안전하고 정확한 방법으로 정당한 수신자에게 전송되어야 한다. 이를 위해서 사용자 기밀성이 요구되며 다양한 기법들을 적용할 수 있다.

(2) 인증성

메시지 송·수신시 출처가 누구이며, 전송 도중 불법적인 제 3자로부터 위조 및 변경되지 않았음을 보증하는 것으로서 전자 서명 기법이 적용된다.

(3) 부인 봉쇄

메시지의 송·수신 여부에 대하여 무선 이동 통신 당사자간에 부인은 방지되어야 하며 이를 위해 전자 서명 기법을 사용한다.

2.2 무선 이동 통신상에서의 구성 요소에 대한 요구 사항

무선 이동 통신상에서 각 통신 주체의 역할 및 환경 구성에 있어 발생할 수 있는 위협에 대해 다음과 같은 보안 요소가 고려되어야 한다.

(4) 유효성

무선 이동 통신은 메시지 송·수신을 위해서 일반 네트워크에 비해 상대적으로 계산 능력이 떨어지는 무선 단말기를 사용한다. 따라서 사용자 측면에서도 충분히 사용 가능해야 한다.

(5) 안전성

무선 이동 통신에서 메시지 송·수신에 참여하는 개체들이라 할지라도 위조 및 변조가 불가능해야한다.

Ⅲ. 연구 배경

유·무선 통신에서 통신 상대방을 인증하고 메시지의 무결성을 보장하는데 있어 가장 각광을 받고 있는 방식 중에 하나가 '전자 서명'이다. 그러나 무선 이동 통신을 위해 사용되는 단말기들은 유선 시스템들에 비해 용량과 계산 능력이 떨어진다. 따라서 공개키 암호화 기법에 기초하는 전자 서명 방식을 무선 통신에 적용하는 것은 상대적으로 많은 시간을 필요로 하게 된다. 이러한 무선 이동 통신 단말기의 특성들은 '유효성'을 보장하는데 장애 요소가 된다.

또한 일반적인 전자 서명은 그 특성상 서명된 메시지의 내용을 누구나 확인할 수 있다는 특징이 있다. 그러나 전자 상거래나 전자 계약 그리고 그 외의 여러 응용 분야들은 메시지 송신자가 자신의 정당함을 입증하면서도, 오직 지정된 수신자만이 이 서명을 확인할 수 있어야만 하는 경우가 발생한다.

본 장에서는 상기 요구 사항 및 문제점을 해결하는데 적용 가능한 특수 서명 기법들을 살펴본다. 이들은 무선 이동 통신 상에서 유효성을 제공할 수 있으며, 여러 특수 목적에 맞게 인증성과 기밀성을 제공하고 있다.

3.1 대리 서명 방식

대리 서명은 본인의 부재 중 자신을 대신하여 다른 사람이 자신의 서명을 수행할 수 있도록 하는 방식이다. 이 방식은 무선 통신 상에서 계산 능력이 부족한 사용자 단말기의 한계를 극복하기 위해 대리 서명 Agent에서 서명을 수행할 수 있도록 확장될 수 있다. 동시에 이 방식에서 검증자는 대리 서명자가 위임 서명자의 위임 사실을 확인할 수 있다는 특징을 가지고 있다. 따라서 대리 서명 방식을 무선 이동 통신에 적용할 경우, 유효성을 높일 수 있다는 장점을 가지고 있다. 그러나 서명 관련 개체들의 부정이 발생할 경우 안전성 및 신뢰성 등에 문제가 발생할 수 있다.[8][9]

3.1.1 시스템 계수

다음은 대리 서명 방식에서 사용되는 시스템 계수를 기술한 것이다.

- p, q : 큰 소수 ($p \geq 512$ 비트, $q \mid p-1$)
- g : 위수가 q인 Z_p상의 원시 원소
- X_A : 위임 서명자의 비밀 서명 정보
- $Y_A \equiv g^{X_A} \bmod p$: 위임 서명자 A의 공개 검증정보
- σ : 대리 서명자의 비밀 서명 정보

3.1.2 프로토콜

대리 서명 방식의 프로토콜을 [그림 1]과 같이 나타내었다.

위임 서명자 A	공개 정보 (g, p, q, Y_A)	대리 서명자 B
· $l \in {}_RZ_p$ · $K \equiv g^l \bmod p$ · $\sigma \equiv (X_A + l \cdot K) \bmod p-1$	$(\sigma \| \| K)$ →	$g^{\sigma} \equiv Y_A K^K \bmod p$

대리 서명자 B	공개정보 (g, p, q, Y_A)	검증자 C
· $r \in {}_RZ_n$ 선택 · $R \equiv g^r \bmod p \bmod q$ · $H = h(M)$ · $S_\sigma(M) \equiv (r - R \cdot \sigma \cdot H) \bmod q$	$(K \| \| S_\sigma(M) \| \| R \| \| M)$ →	
		· $H = h(M)$ · $v \equiv Y_A K^K \bmod p$ · $R \equiv g^{S_\sigma(M)} v^{R \cdot H} \bmod p \bmod q$ 확인

[그림 1] 대리 서명 방식 흐름도

3.1.3 특성 분석

이 방식은 이동 통신상의 전자 상거래 수행시 사용자의 계산량 부담을 줄여주는 장점을 가지고 있지만 대리 서명자가 이전의 서명 정보로부터 서명을 생성할 수 있기 때문에, 위임 서명자가 서명 사실에 대한 부인이 가능하다. 동시에 대리 서명자로부터 수신된 서명 정보에 대해 누구나 확인 가능하므로, 무선 인터넷을 통한 전자 상거래에서 사용할 경우 위임 서명자의 정보 누출이 가능하다는 단점이 발생한

다. 따라서 본 방식은 서명 생성 주체들의 안전성 및 서명 정보 신뢰성 부분에서는 취약점을 나타내고 있다.

3.2 수신자 지정 서명 방식

수신자 지정 서명 방식은 지정된 검증자만이 서명을 확인할 수 있는 방식으로 서명자조차도 서명을 확인할 수 없도록 구성되어 있다. 이 방식의 이러한 특성은 필요시에 제 3자에게 서명이 서명자에 의해 자신에게 발행된 정당한 서명임을 증명할 수 있게 된다. 따라서 이 방식은 전자 상거래 및 기타 응용 분야에서 기밀성과 인증성을 보장하는데 매우 유용하게 사용할 수 있다. 그러나 무선 이동 통신상에서 수신자 지정 서명 방식을 사용할 경우, 서명자의 계산상 부담을 가중시킬 수 있다는 문제점을 안고 있다.[7]

3.2.1 시스템 계수

다음은 수신자 지정 서명 방식에서 사용되는 시스템 계수를 기술한 것이다.

- p : $p \geq 512$ 비트인 큰 소수
- q : $q \mid p-1$인 큰 소수
- g : 위수가 q인 Z_p상의 원시 원소
- X_A : 서명자의 비밀 서명 정보
- $Y_A = g^{X_A} \bmod p$: 서명자 A의 공개 검증정보
- $Y_B \equiv g^{X_B} \bmod p$: 검증자 B의 공개 검증정보

3.2.2 프로토콜

수신자 지정 서명 방식의 프로토콜을 [그림 2]와 같이 나타내었다.

서명자 A	공개정보 (Y_A, Y_B, g, p, q)	검증자 B
· r, $R \in {}_RZ_p$ · $K \equiv g^{R^r} \bmod p$ · $D \equiv Y_B^R \bmod p$ · $e=h(Y_B, K, D, M)$ · $S \equiv (r-X_A \cdot e) \bmod q$	$(M\|\|K\|\|D\|\|S)$ →	
		· $h(Y_B, K, D, M) = e$ · $(g^S Y_A^e K)^{X_B} \equiv D \bmod p$

[그림 2] 수신자 지정 서명 방식 흐름도

3.2.3 특성 분석

이 방식은 오직 검증자만이 서명을 확인할 수 있기 때문에 제 3자의 요청이 없는 경우 오직 검증자만이 서명자의 신원을 증명할 수 있다. 따라서 메시지의 기밀성 유지 및 송신자 인증에는 매우 적합한 방식이다. 그러나 서명에 대한 안전성이 검증자에게 의존하고 있기 때문에, 서명자에 대한 비밀 정보의 안전성이 완벽하게 보장될 수 없다. 또한 서명 생성 및 암호화를 위해 공개키 암호 방식을 사용하게 되므로 무선 이동 통신 단말기에서 많은 계산 능력을 필요로 한다는 문제점을 가지고 있다.

Ⅳ. 기존 방식 분석

본 장에서는 '대리 서명' 방식과 수신자 지정성을 제공하기 위해 제시된 Signcryption 방식을 동시에 적용한 C. Gamage 등의 Proxy-Signcryption 방식에 대해 설명한다.[6][8][10]

Proxy-Signcryption이란 서명자가 선정한 대리인으로 하여금 자신을 대신하여 정당한 '수신자 지정 서명'을 수행할 수 있도록 구성된 방식으로서, 서명 생성시 요구되는 계산을 상대적으로 계산 능력이 뛰어난 대리 서명 Agent(Proxy Agent)에 위탁할 수 있게끔 구성되어 있다.

그러나 이 방식은 서명자가 원할 경우 자신이 대리 서명 Agent를 대신하여 정당한 서명을 생성할 수 있으므로, 대리 서명 Agent를 보호할 수 없다는 문제점을 안고 있다. 또한 대리 서명 Agent 역시 서명자의 요구 없이 임의로 서명을 생성할 수 있다. 그 외에도 서명자가 메시지 서명에 대한 부인이 가능하기 때문에 전자 상거래 등의 여러 응용 분야에 적용하기에는 문제가 있다. 다음에서는 C. Gamage 등이 제안한 Proxy-Signcryption 방식을 기술한다.

4.1 시스템 계수

다음은 Proxy-Signcryption 방식에서 사용되는 시스템 계수를 기술한 것이다.

- p, q : 큰 소수 ($p \geq 512$ 비트, $q \mid p-1$)
- g : 위수가 q인 Z_p상의 원시 원소
- X_A : $X_A \in {}_RZ_q$, 서명자의 비밀 서명 정보
- Y_A : $Y_A \equiv g^{X_A} \bmod p$, 서명자의 공개 검증 정보
- X_B : $X_B \in {}_RZ_q$, 검증자의 비밀 서명 정보

- Y_B : $Y_B \equiv g^{XB} \bmod p$, 검증자의 공개 검증 정보
- $H*(\ )$: 키 *를 이용하는 keyed 해쉬 함수
- $E(\ )/D(\ )$: 관용 암호/복호 알고리즘

4.2 프로토콜

(1) 서명자

- 서명자는 랜덤 수 $l \in {}_RZ_q$를 선택하고 $K \equiv g^l \bmod p$를 계산하여 다음과 같이 대리 서명용 키를 생성한다.

$$\sigma \equiv (X_A + l \cdot K) \bmod q \quad (1)$$

- 서명자는 생성된 대리 서명용 키와 K를 연접해 $(\sigma||K)$를 대리 서명 Agent에게 전송한다.

(2) 대리 서명 Agent

- 대리 서명 Agent는 다음 식을 이용하여 자신이 받은 대리 서명용 키가 정당한지 확인한다.

$$g^{\sigma} \equiv (Y_A \cdot K^K) \bmod p \quad (2)$$

- 검증이 완료되면 비밀 랜덤 수 $R \in_R [1, \ldots, q-1]$를 선택하여 다음을 생성한다.

$$K' \equiv Y_B^R \bmod p \quad (3)$$

- $K' = K_1 \,||\, K_2$로 나누고 다음과 같이 메시지 m에 대한 Signcryption을 생성한다.

$$v = HK_2(m)$$
$$w \equiv R/(v + \sigma) \bmod q$$
$$c = EK_1(m) \quad (4)$$

- 메시지 m에 대한 Signcrypted 메시지$(c||v||w||K)$를 수신자에게 전송한다.

(3) 검증자

- 검증자는 $\sigma' \equiv (Y_A \cdot K^K) \bmod p$를 계산한 후, 자신의 비밀 서명 정보를 이용하여 다음을 생성한다.

$$K' \equiv (\sigma' \cdot g^v)^{w \cdot XB} \bmod p \quad (5)$$

- $K' = K_1 \,||\, K_2$로 나누고 다음과 같이 메시지를 복호한다.

$$m = DK_1(c) \quad (6)$$

- $HK_2(m) = v$라면 정확하게 서명된 것으로 받아들인다.

4.3 특성 분석

C. Gamage 등이 제시한 Proxy-Signcryption 방식은 다음과 같은 특성들을 가지고 있다. 본 방식은 통신 양자간의 안전한 정보 교환을 위하여 대리 서명 방식과 Signcryption 방식을 적용하였다. 이들 방식의 적용을 통해 본 방식은 무선 통신에서 요구되는 기밀성, 인증성 및 유효성을 확보하고 있다. 그러나 이 방식은 서명 메시지 송신시 서명자와 대리 서명 Agent 간의 대리 서명용 키를 이용하게 된다. 따라서 서명자가 원할 경우 자신이 대리 서명 Agent를 대신하여 정당한 서명을 생성할 수 있고, 대리 서명 Agent 역시 서명자의 동의 없이 임의로 서명을 생성할 수 있다. 이러한 특징은 무선 통신상에서 요구되는 안전성에 위배되는 사항이다.

또한 이 방식은 서명자가 메시지 서명에 대한 부인 봉쇄가 불가능하기 때문에 전자 상거래 등의 여러 응용 분야에 적용하기에는 문제가 발생될 수 있다.

V. 수신자 지정 대리 서명 방식 제안

상기 요구 사항을 만족하는 전자 서명을 위하여 다음과 같은 해결책을 제시한다. 본 제안 방식은 무선 이동 통신상에서 유효성을 획득하기 위해 대리 서명 Agent를 도입한다. 또한 상기 2장에서 고려되었던 사항들에 대해 기밀성 및 인증성을 만족할 수 있도록, 대리 서명 메시지는 검증자의 공개키로 암호화되어 전송된다.[7][8][9] 동시에 서명 메시지 생성시 대리 서명 Agent의 비밀 정보와 송신자의 위임 서명 의뢰 정보를 부가함으로서 부인 봉쇄 및 안전성을 확보하고 있다.

5.1 시스템 계수

다음은 제안 방식에서 사용되는 시스템 계수를 기술한 것이다.

- p : $p \geq 512$ 비트인 큰 소수
- q : $q \mid p-1$인 소수

- g : 위수가 q인 Z_p상의 원시 원소
- X_A, X_B, X_G : 위임 서명자(가입자) A, 검증자 B 및 대리 서명 Agent의 비밀 서명 정보
- $Y_A \equiv g^{XA} \bmod p$: 위임 서명자 A의 공개 검증 정보
- $Y_B \equiv g^{XB} \bmod p$: 검증자 B의 공개 검증정보
- $Y_G \equiv g^{XG} \bmod p$: 대리 서명 Agent의 공개 검증 정보
- s_i : 위임 서명자의 일회용 비밀 서명 정보($i \in_R Z$)
- T_i : 타임 스탬프
- $H()$: 안전한 128비트 일방향 해쉬 함수
- M : 메시지

5.2 프로토콜

(1) 위임 정보 생성

- 이동 통신 단말기를 보유한 위임 서명자(가입자) A는 대리 서명 Agent에게 서명 생성을 위한 위임 서명 정보를 다음과 같이 생성한다.

$$a_i \in_R Z_p \ (i \in_R Z)$$
$$d_i \equiv H(M||T_i)$$
$$l \equiv g^{ai} \bmod p$$
$$s_i \equiv (X_A \cdot d_i + a_i \cdot l) \bmod p \qquad (7)$$

위임 서명자 A는 s_i 생성시 일회성을 갖는 랜덤 값 a_i 및 d_i를 이용함으로서 대리 서명 Agent가 임의로 서명을 생성하는 것을 방지하고 있다.

(2) 위임 정보 전송

- 위임 서명자 A는 생성된 위임 서명 정보 s_i, l 및 서명을 수행할 메시지 M과 T_i를 대리 서명 Agent에게 전송한다.

(3) 위임 정보 확인

- 대리 서명 Agent는 다음과 같이 수신된 정보를 기초로 위임 서명자의 정당성을 확인한다.

$$g^{si} \equiv (Y_A^{H(M||Ti)} \cdot l^l) \bmod p \qquad (8)$$

만약 수식이 정확하다면, 전송 정보 및 위임 서명자의 정당성이 인증된다.

(4) 수신자 지정 대리 서명 수행

- 대리 서명 Agent는 랜덤 수 r 및 R을 다음과 같이 선택하고, 위임 서명자의 부정 행위를 방지하기 위한 K를 생성한다.

$$r, R \in_R Z_p$$
$$K \equiv g^{R \cdot r \cdot XG} \bmod p \qquad (9)$$

이를 통해 위임 서명자가 대리 서명 Agent를 가장해 수신자 지정 서명을 생성하는 것을 막을 수 있으며, 차후 분쟁이 발생할 경우 위임 서명자의 부정으로부터 대리 서명 Agent를 보호하게 된다.

- 대리 서명 Agent는 서명 수행을 위해 다음과 같이 D, Z 및 e를 계산한 다음 수신자 지정 서명 $Sa(Z)$를 수행한다.

$$D \equiv Y_B^R \bmod p$$
$$Z = (Y_B||K||D||M)$$
$$e = h(Z)$$
$$Sa(Z) \equiv (X_G \cdot r - R \cdot s_i \cdot e) \bmod q \qquad (10)$$

D 및 e를 생성할 때 검증자 B의 공개키를 사용하는 이유는 제 3자의 도청이 있다 하더라도 검증자만이 서명을 확인할 수 있도록 하기 위함이다. 이를 통해 대리 서명 Agent와 검증자간에 기밀성을 제공하게 된다.

(5) 수신자 지정 대리 서명 정보 전송

- 대리 서명 Agent는 서명 검증을 위해 검증자 B에게 $(M||T_i||l||K||D||R||Sa(Z))$를 전송한다.

(6) 서명 검증

- 검증자 B는 다음과 같이 수신된 정보를 통해 서명 검증을 위한 정보 e와 b를 생성한다.

$$h(Y_B||K||D||M) \equiv e \qquad (11)$$

$$b \equiv (Y_A^{H(M||Ti)} \cdot l^l) \bmod p \qquad (12)$$

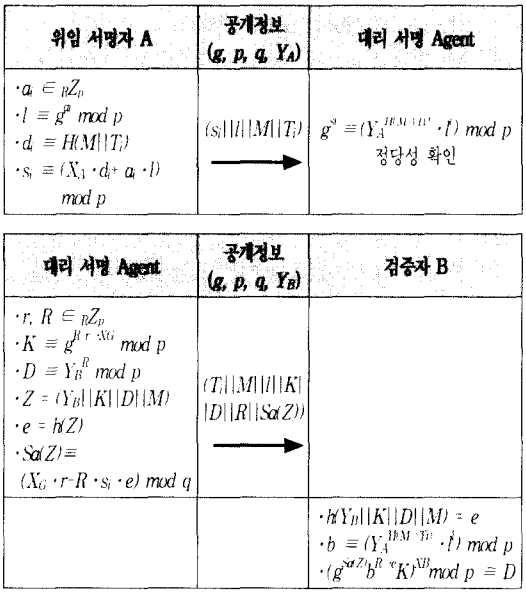
- 생성된 정보를 통해 다음과 같이 수신자 지정 대리 서명을 검증한다.

$$(g^{Sa(Z)} b^{R \cdot e} K)^{XB} \bmod p \equiv D \qquad (13)$$

- 서명 프로토콜 검증은 다음과 같은 과정을 통해 그 유효성을 입증할 수 있다.

$$
\begin{aligned}
&(g^{Sa(Z)}b^{R \cdot e}K)^{XB} \bmod p \\
&\equiv (g^{r \cdot XG \cdot R \cdot si \cdot e}(Y_A^{H(M||Ti)} \cdot t)^{R \cdot e} g^{R \cdot r \cdot XG})^{XB} \bmod p \\
&\equiv (g^{r \cdot XG \cdot R \cdot si \cdot e}(g^{XA \cdot H(M||Ti)} \cdot g^{ai \cdot t})^{R \cdot e} g^{R \cdot r \cdot XG})^{XB} \bmod p \\
&\equiv (g^{r \cdot XG \cdot R \cdot si \cdot e}(g^{ai \cdot t + XA \cdot H(M||Ti)})^{R \cdot e} g^{R \cdot r \cdot XG})^{XB} \bmod p \\
&\equiv (g^{r \cdot XG \cdot R \cdot si \cdot e} g^{si \cdot R \cdot e} g^{R \cdot r \cdot XG})^{XB} \bmod p \\
&\equiv (g^{R})^{XB} \bmod p \\
&\equiv Y_B^{R} \bmod p \\
&\equiv D
\end{aligned}
$$

[그림 3]은 제안된 방식에 대한 개략적인 흐름도를 나타낸 것이다.



[그림 3] 제안 방식

5.3 제안 방식 고찰

기존에 제시되었던 전자 서명 방식들을 고려할 경우, 본 방식은 다음과 같은 특성들을 통해 상기 무선 이동 통신 응용 서비스에 대한 요구 사항을 만족하고 있다.

(1) 서명자 기밀성 확보

본 제안 방식은 수신자 지정 서명 방식을 적용함으로서 오직 검증자만이 서명자의 신원을 확인할 수 있기 때문에, 제 3자에 의한 도청으로부터 서명자 기밀성을 확보하고 있다.

(2) 인증성 제공

이동 통신에서 전자상거래를 수행할 경우 투명성을 높이기 위해 인증성 제공은 필수적이다. 본 방식은 수신자 지정 서명 방식을 이용함으로서 인증성을 제공하고 있다.

(3) 부인 봉쇄 가능

서명 생성시 대리 서명 Agent는 자신의 비밀 정보와 서명자의 위임 서명 정보를 함께 포함하여 대리 서명을 수행하게 된다. 따라서 위임 서명자의 서명 생성 의뢰에 대한 부인을 방지할 수 있다.

(4) 유효성 획득

서명 생성시 위임 서명자는 상대적으로 계산 능력이 뛰어난 대리 서명 Agent를 이용하여 서명을 수행하게 되므로 이동 통신 단말기를 가정하더라도 충분히 유효성을 확보하고 있다.

(5) 안전성 제공

위임 정보 전송시 위임 서명자는 일회용 비밀 서명 정보를 제공하며, 서명 생성시 대리 서명 Agent는 자신의 비밀 정보를 생성하여 서명을 전송하게 된다. 따라서 위임 서명자 및 대리 서명 Agent에 의한 불법적인 서명 생성은 불가능하게 되므로 안전성을 제공하게 된다.

[표 1]은 상기 고려 사항을 살펴 볼 때, 기존의 몇몇 방식과 제안 방식의 기능을 비교 분석한 것이다.

[표 1] 각 방식별 특성 비교 분석

특성 / 방식	서명자 기밀성	인증성	부인 봉쇄	유효성	안전성
수신자 지정 서명	O	O	O	X	X
대리 서명	X	O	X	O	X
C. Gamage 방식	O	O	X	O	X
제안 방식	O	O	O	O	O

Ⅵ. 결 론

컴퓨터 네트워크 및 이동 통신의 발전을 통해 향후 정보화 사회는 전자 상거래 서비스들을 비롯하여 더욱 다양한 응용 서비스들이 제공될 것이다. 이러한 환경하에서 이동 통신상에서 기밀성 및 인증성을 제

공하는 효율적인 전자 서명 방식의 연구는 매우 중요한 주제가 되고 있다.

기존의 수신자 지정 서명 방식의 경우 기밀성 확보를 통해 서명자와 검증자간에 안전한 채널이 형성되어 무선 통신상의 취약성을 극복하고 있다. 그러나 서명 수행시 모듈러 멱승 계산이 서명자의 무선 단말기를 통해 이뤄져야 하므로 효용성이 떨어지게 된다. 대리 서명 방식의 경우 대리 서명자를 도입해 유효성은 확보하고 있으나, 기밀성 및 서명자 부인봉쇄가 불가능한 경우가 발생된다. 그 밖에 C. Gamage 방식의 경우 대리 서명 방식과 Signcryption 방식의 적용을 통해 기밀성, 인증성 및 유효성을 보장하고 있으나, 송신자와 대리 서명 Agent의 부정을 방지 못함으로서 부인 봉쇄 및 안전성을 만족하지 못하고 있다.

이에 본 제안 방식은 기존의 방식들이 안고 있던 문제점을 해결하는 새로운 수신자 지정 대리 서명 방식을 제안하였다. 이를 통해 제안 방식은 기밀성과 효율성을 획득하고 있으며 동시에 인증성, 부인 봉쇄 및 안전성을 동시에 만족하고 있다. 향후 기존에 제안된 많은 서명 방식들을 통하여 더욱 효율적이고 안전한 수신자 지정 대리 서명 방식의 연구가 필요하리라 판단된다.

참 고 문 헌

[1] *ETSI ETS GSM* 02.09, "European Digital Cellular Telecommunications System (Phase 2): Security Aspects," Version 4.2.4, September 1994.

[2] *ETSI ETS* 3000175-7, "DECT Common Interface, Part 7: Security Features," October 1992.

[3] *UMTS Forum*, "A regulatory framework for UMTS," Report no. 1, 1997.

[4] *ETSI ETR* 33.20, "Security Principles for the Universal Mobile Telecommunications System (UMTS)," Draft 1, 1997.

[5] ITU, "Security Principles for Future Public Land Mobile Telecommunication Systems," Rec. *ITU-R* M. 1998.

[6] Y. Zheng, "Signcryption and Its Applications in Efficient Public Key Solutions," *Proc. ISW'97*, LNCS 1397, pp. 291~312, 1998.

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

[8] M. Mambo, K. Usuda and E. Okamoto, "Proxy Signatures," *Proceedings of The 1995 Symposium on Cryptography and Information Security (SCIS 95)*, pp. B1.1.1~17, 4~27 Jan, 1995.

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

[10] C. Gamage, J. Leiwo and Y. Zheng, "An Efficient Scheme for Secure Message Transmission using Proxy-Signcryption," *Proceeding of the Twenty Second Australasian Computer Science Conference*, 18-21 Jan, 1999.

[11] H. U. Park and I. Y. Lee, "A 2-pass key agreement and authentication for mobile communication," *Proceedings of The 2000 International Conference on Electronics, Information and Communications(ICEIC 2000)*, pp. 115~118, 2000.

〈著者紹介〉

박 희 운 (Hee-Un Park) 학생회원
1997년 2월 : 순천향대학교 컴퓨터공학부 졸업
1999년 2월 : 순천향대학교 전산학전공 석사
1999년 3월~현재 : 순천향대학교 전산학전공 박사과정
〈관심분야〉 암호이론, 컴퓨터 보안

이 임 영 (Im-Yeong Lee) 종신회원
1981년 8월 : 홍익대학교 전자공학과 졸업
1986년 3월 : 오사카대학 통신공학전공 석사
1989년 3월 : 오사카대학 통신공학전공 박사
1989년 1월~1994년 2월 : 한국전자통신연구원 선임연구원
1994년 3월~현재 : 순천향대학교 정보기술공학부 부교수
〈관심분야〉 암호이론, 정보이론, 컴퓨터 보안