익명성을 보장하는 Crypto-Cert 서명 메커니즘

박희운, 이임영
순천향대학교 정보기술공학부

A Anonymous Crypto-Cert Signature Mechanism

Hee-Un Park, Im-Yeong Lee
Division of Information Technology, SoonChunHyang University
E-mail : phu24@hotmail.com, imylee@sch.ac.kr

요 약

컴퓨터 및 네트워크의 급속한 성장은 정보 사회로의 발전을 이행해 왔으며, 수많은 정보들이 네트워크를 통해 공유 및 교환되고 있다. 이들은 공개된 네트워크를 전제로 수행되므로, 다양한 형태의 공격으로부터 노출되어 있다. 이를 공격에 대응하고 나아가 사용자 및 메시지 인증을 수행키 위해 각광을 받고 있는 방법 중에 하나로서 디지털 서명을 들 수 있다. 그러나 일반 디지털 서명 방식은 누구나 서명 확인이 가능하므로 서명자의 익명성과 비밀성을 보장해야 하는 전자 투표, 전자 회의 및 전자 입찰 등과 같은 응용 분야에 적용할 경우에는 문제점을 드러내고 있다.

따라서 이들 응용 분야들은 기본적으로 서명자의 신원을 보장하여야 하며, 필요할 경우 이를 확인할 수 있어야 한다. 현재 이와 관련하여 부인 방지 서명 방식과 이를 개선한 수신자 지정 서명 방식이 제안되어 있다. 그러나 이 방식들은 서명자의 익명성이 수신자에게 의존하기 때문에, 수신자에 의해 신원이 노출될 수 있었다. 동시에 이들 방식은 메시지 부가형 서명에 기초하므로 전송되는 서명 정보상의 메시지가 제 3자에게 노출되는 결과를 초래한다.

본고에서는 서명자의 익명성을 보장하면서, 오직 수신자만이 서명자의 신분을 확인할 수 있는 Crypto-Cert 디지털 서명 방식에 대해 고찰한다. 특히 본 방식에서는 필요할 경우 서명자의 신원을 확인할 수 있으며, 전송 메시지에 대해 기밀성을 확보하고 있으므로 다양한 응용 분야에 적용가능하다.

1. 서론

컴퓨터의 보급 확산과 공용 네트워크의 보급 확산은 정보 사회의 발전을 촉진시키고 있으며, 점점 그 사용 범위가 넓어지고 있다. 과거와는 달리 특별한 관련 지식이 없더라도 누구나 쉽게 인터넷과 같은 공용 네트워크를 통해 더욱 편리하고 빠르게 개인 및 각 공유 정보의 교류를 활발하게 진행시키고 있다. 단순하게는 E-mail 사용에서부터 동영상, 전자 상거래 및 여러 네트워크 응용 분야에까지 다양한 발전의 모습들은 그 실 예들이라 할 것이다.

그러나 이러한 응용 서비스들은 공개된 네트워크 상에서 제공되므로 많은 문제점들에 노출될 수 있다. 즉, 정보 교환의 대상이 되는 메시지들이 정보 전송 시 불법적 변조나 위조가 있었는지 확인 가능해야 하며, 송·수신자가 누구인지 정확하게 판단할 수 있어야 한다. 이를 해결하기 위한 기법 중에 하나가 "디지털 서명"이다. 디지털 서명 기법은 네트워크 상에서 인증을 통해 메시지의 무결성을 보장할 수 있으며, 사용자 인증을 통해 송·수신자간의 분쟁을 해결할 수 있는 매우 유용한 도구라 하겠다.

그러나 이러한 일반적인 디지털 서명은 누구나 서명을 확인할 수 있다는 특성을 가지고 있다. 그러므로 서명자의 익명성과 비밀성을 보장해야 하는 응용 분야들 - 전자 투표, 전자 회의 및 전자 입찰 등 - 에서는 몇 가지 문제점에 노출되어 있다. 전자 입찰의 경우, 입찰이 완료되기 전까지는 서명자 신원에 대한 익명성을 보장하여야 하며, 입찰이 완료된 다음에는 이를 확인할 수 있어야 한다. 현재 이와 관련하여 부인 방지 서명 방식과 이를 개선한 수신자 지정 서명 방식이 제안되어 있다. 그러나 이 방식들은 서명자의 신원 확인이 수신자에게 의존하기 때문에, 수신자에 의해 임의적으로 서명자의 신원이 노출될 수 있었다. 동시에 이들 방식은 메시지 부가형 서명에 기초하므로 전송되는 서명 정보상의 메시지가 제 3자에

게 노출되는 결과를 초래한다.

본고에서는 익명성 보장 인증 서비스 응용 분야에서 요구 되는 사항을 고려함과 동시에 서명자의 익명성을 보장하면서, 오직 수신자만이 서명자의 신분을 확인할 수 있는 Crypto-Cert 디지털 서명 방식에 대해 고찰한다. 특히 본 방식에서는 필요할 경우 서명자의 신원을 확인할 수 있으며, 전송 메시지에 대해 기밀성을 확보하고 있으므로 다양한 응용 분야에 적용가능하다.

2. 요구 사항

본 장에서는 익명성 보장 인증 서비스를 수행함에 있어 고려해야할 필수적 요구 사항들을 기술한다.

1) 익명성

: 서명자는 자신이 어떠한 그룹에 속해 있는지를 증명할 수 있다. 단, 수신자는 서명을 통해 서명자의 어떠한 비밀 정보도 알 수 없다.

2) 소속 확인성

: 수신자는 서명자가 누구인지 신원은 알 수 없으나, 어느 그룹에 속해있는지는 증명할 수 있다.

3) 기밀성

: 송·수신되는 서명 메시지를 제 3자로부터 보호하기 위해서는 안전한 통신 채널을 구성해야하며, 기밀성의 확보는 필수적인 요소이다.

4) 수신자 지정성

: 오직 지정된 특정 수신자만이 서명을 확인할 수 있다.

: 서명자는 자신이 발행한 서명의 정당함을 자기 자신에게조차도 증명할 수 없다.

5) 신원 복원성

: 서명자의 부정행위가 발생하거나 프로토콜상의 특성상 서명자의 신원이 밝혀질 필요가 있을 경우, 정당한 절차를 통해 신원 복원이 수행될 수 있어야 한다.

위의 조건들은 익명성 보장 인증 서비스 응용 분야에 따라 약간씩 다르게 적용 된다. 예를 들어, 전자투표의 경우에는 정당한 투표가 이뤄진다면 5)항이 요구되어서는 안되며, 전자 입찰의 경우에는 입찰 과정상에서 2)항이 필요 없지만 입찰 결과 확인을 위해 5)항은 필수적으로 제공되어야 한다.

3. 기반 기술 고찰

익명성 보장 인증 서비스를 구성하는데 다양한 방식들이 적용될 수 있다. 다음은 본 논문에서 적용 가능한 기법들에 대해 고찰한다.

3.1 Crypto-Cert 방식

네트워크 환경은 기존의 물리적인 face-to-face 상의 인증 서비스를 제공하기 위해 디지털 서명 방식 등을 사용하고 있으나, 서명자의 프라이버시와 익명성을 제공함에 있어 문제점을 드러내고 있다. 또한 서명자의 완벽한 익명성이 보장은 서명자의 불법적인 행위를 차단할 수 없다는 단점을 제공한다.

현재 이러한 양립된 입장을 해결하기 위한 방안으로서, 익명성 제어 기법들이 연구되고 있으며, Fair group signature나 Fair blind signature는 대표적인 예가 된다. 이들 방식들은 서명자의 신원을 신뢰된 제 3자의 비밀키로 암호화하여 서명에 부가함으로서, 서명자의 익명성은 보장하되 문제가 발생할 경우 적법한 과정을 통해 서명자의 신원을 확인할 수 있게끔 하는데 이러한 기법을 Crypto-Cert라 한다. 이 방식은 신뢰된 제 3자를 이용하는 익명성 제어 분야에서 상당히 중요한 의미를 갖게된다.

3.2 Signcryption

본 방식은 서명자 메시지의 기밀성과 수신자 지정성을 제공하기 위해 제안된 방식으로서, 익명성 보장 인증 서비스를 수행하는데 있어 계산상 효율성과 신뢰성을 보장할 수 있는 서명 기법이다[11].

3.2.1 시스템 계수

다음은 Signcryption 방식에서 사용되는 시스템 계수를 기술한 것이다.

- p : 512비트 이상의 큰 소수
- q : $q|p-1$인 큰 소수
- g : 위수가 q인 Z_p상의 원시 원소
- X_A : $X_A \in {}_RZ_q$, 송신자의 개인키
- Y_A : $Y_A \equiv g^{XA} \bmod p$, 송신자의 공개키
- X_B : $X_B \in {}_RZ_q$, 수신자의 개인키

- Y_B : $Y_B \equiv g^{XB} \bmod p$, 수신자의 공개키
- K : 대리 서명용 키
- $H*(\ )$: 키 *를 이용하는 keyed 해쉬 함수
- $E(\ )/D(\ )$: 관용 암호/복호 알고리즘

3.2.2 프로토콜

1) 서명자

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

  $k \equiv H(Y_B^x \bmod p)$
- $k = k_1 \| k_2$로 나누고 다음과 같이 메시지 m에 대한 Signcryption을 생성한다.

  $c = Ek_1(m)$

  $r = Hk_2(m)$

  $s \equiv x/(r + X_A) \bmod q$
- 메시지 m에 대한 Signcrypted 메시지(c, r, s)를 수신자에게 전송한다.

2) 수신자

- 수신자는 전송된 정보와, 자신의 비밀키를 이용하여 다음을 생성한다.

  $k \equiv H(Y_A \cdot g^r)^{s \cdot XB} \bmod p$
- $k = k_1 \| k_2$로 나누고 다음과 같이 메시지를 복호한다.

  $m = Dk_1(c)$
- $Hk_2(m) = r$이라면 정확하게 서명된 것으로 받아들인다.

본 방식은 서명 메시지 전송시 대칭키 기법을 이용하므로 기밀성과 계산적 효율성을 제공할 뿐만 아니라, 오직 수신자만이 서명을 검증할 수 있으므로 제 3자에 의한 공격에 대해 안전성을 제공하고 있다. 그러나 서명자가 자신의 비밀키를 분실하거나 제 3자에 의해 노출될 경우, 이전에 서명된 모든 메시지가 노출될 수 있다는 단점이 있다.

4. 기존 방식 분석

디지털 서명 방식은 그 응용 분야에 따라 여러 형태로 적용 가능하다. 이렇게 특수한 환경을 전제로 새롭게 적용된 디지털 서명 방식을 특수 서명 방식이라 한다[4]~[11]. 이들 중 상기 요구 사항과 관련된 몇몇 방식의 특징을 살펴보면 다음과 같다.

1) 부인 방지 서명[4]

이 방식은 서명자의 도움 없이는 서명 검증이 불가능한 서명 방식이다. 이렇게 함으로서 서명자는 자신의 서명임을 검증자에게 확인시키며, 부인 과정을 통해 불법적인 서명에 대해 자신이 서명하지 않았음을 증명하게 한다.

이 방식은 서명의 정당성을 확인하기 위해 대상이 되는 모든 서명자들에게 서명 확인을 수행하게 된다면, 서명자는 서명에 대한 확인이 불가피하게 되고 결국에는 서명자의 신원이 노출됨으로서 거짓말 탐지기와 같은 문제점을 안고 있다.

2) 의뢰 부인 방지 서명[5]

부인 방지 서명이 서명자의 익명성을 보장하지 못하는 점을 부분적으로 개선한 방식이다. 따라서 이 방식은 임의의 검증자가 부인 과정을 수행할 수 없도록 함과 동시에 오직 특정인만이 부인 과정을 수행하도록 함으로서 취약성을 부분적으로 제거한 방식이다.

3) 수신자 지정 서명[6]

수신자 지정 서명 방식은 지정된 수신자만이 서명을 확인할 수 있는 방식으로 서명자조차도 서명을 확인할 수 없도록 구성되어 있다. 이러한 특성을 통해 필요시에 제 3자에게 서명이 서명자에 의해 자신에게 발행된 정당한 서명임을 증명할 수 있게 된다.

그러나 서명에 대한 안전성이 수신자에게 의존하고 있기 때문에, 서명자에 대한 비밀 정보의 안전성이 완벽하게 보장될 수 없다는 문제점을 안고 있다.

4) 그룹 서명[9]

그룹 서명은 자신이 특정 그룹의 서명자임을 제 3자에게 증명할 수 있는 방식이다. 그러나 이 방식은 검증자가 그룹의 서명문을 확인할 수 있으나 서명자를 알 수 없다는 특징을 가지고 있으며, 필요한 경우 누구나 서명자를 확인할 수 있다는 문제점을 가지고 있다.

살펴본바와 같이 본 방식들은 상기 다섯 가지 요구사항을 모두 만족하지 못하고 있음을 알 수 있다. 동시에 계산량에 따른 효율성을 높이기 위해 부가형 디지털 서명 방식을 도입 및 적용하였기 때문에 메시지에 대한 기밀성을 보장하지 못하고 있다. 따라서 익명성 보장 인증 서비스를 제공하기 위한 새로운 방식

의 필요성이 제기된다.

5. Crypto-Cert 서명 메커니즘 제안

본 장에서는 익명성 보장 인증 서비스에 능동적으로 적용 가능한 디지털 서명 방식을 제안한다. 본 방식은 Crypto-Cert 개념과 Signcryption 서명을 결합하여 프로토콜을 구성하였다. 따라서 본 방식은 2장에서 언급된 모든 요구 사항을 만족할 뿐만 아니라 다양한 응용분야에 적용 가능하다.

5.1 시스템 계수

다음은 본 제안 방식에서 사용되는 시스템 계수를 설명한 것이다.

- O, V, TC : 서명자, 검증자 및 신뢰된 센터
- p : 소수 ≥512 bits
- q : 소수 ≥160 bits $(q \mid p-1)$
- g : 생성자
- E_*, D_* : *에 의해 수행되는 대칭키 암호화 및 복호화
- CC : Crypto-Cert
- K_{TC} : TC의 대칭키 암호용 비밀키
- m : 서명 메시지
- H : 160비트 출력을 내는 안전한 일방향 해쉬 함수
- $KH*(\ )$: 키 *를 이용하는 keyed 해쉬 함수
- Sig_* : *의 서명
- r_* : *가 생성한 랜덤 값
- y_*, x_* : *의 공개키 및 개인키
- K_{SG}, K_{PG} : 서명자의 소속 서명 키 리스트 및 서명자의 소속 확인용 공개키 리스트
- T : TC가 생성하는 Time-Stamp

5.2 프로토콜

1) 소속 등록 및 키 분배 단계

소속의 등록은 *TC(Trusted Center)*가 관할하며, 소속에 등록 및 키를 분배받기 위해서는 다음과 같은 일련의 과정을 거친다.

(1) 서명자 O는 자신의 신상 정보 (서명자 이름, ID, 소속, 기타)에 자신의 서명을 붙여 TC에게 제공한다.

$\cdot O : Sig_O(Name||ID_O||\text{소속}) \rightarrow TC$

(2) TC는 서명자의 소속 확인이 끝난 후 비밀키 리스트를 안전한 방식으로 서명자 O에게 전달한다.

$\cdot TC : E_{yO}(K_{SG}=K_{SG1}, \ldots, K_{SGn}) \rightarrow O$

$O : K_{SGk}=K_{SG1}, \ldots, K_{SGk}$ (단, $1 \le k \le n$)
(비밀키 리스트에서 k개의 키를 추출한 것)

서명자의 비밀키는 총 n개의 분할된 키를 갖게 된다. 이 키는 TC에서 만든다고 가정하며, 각 서명자의 공개키로 암호화해 분배되거나, IC카드와 같은 물리적인 형태로 분배된다. 각 서명자는 서명 수행을 위해 분배된 키 리스트 중에서, 날짜 또는 TC의 권고에 따라 k개를 선택해 서명 수행이 가능하다.

따라서 서명 확인을 위한 공개키는 수시로 변화되므로 안전성을 확보할 수 있으며, 별도의 키 생성을 위해 TC가 연산을 수행할 필요가 없기 때문에 효율적이다. 이러한 방식은 새로운 신규 멤버 가입 역시 쉽게 이뤄지는 장점을 가진다.

(3)

TC는 서명자의 소속 확인용 공개키들을 다음과 같이 생성하여 공개키 리스트에 등록한다.

$\cdot TC : K_{PGk} = g^{KSGk} \bmod p$ (단, $1 \le k \le n$)

2) Crypto-Cert 요청 및 수신 단계

(1)

서명 정보 생성을 위해 서명자는 TC에게 자신의 $CC(Crypto\text{-}Cert)$ 정보를 다음과 같이 요청한다.

$\cdot O : Sig_O(CC\_request) \rightarrow TC$

(2)

TC는 CC 정보를 생성하여 자신의 비밀키로 암호화 한 다음, 서명을 붙여 서명자에게 전송한다.

$\cdot TC : CC = Sig_{TC}(E_{KTC}(ID*r_{TC})||T) \rightarrow O$

3) 서명 정보 생성 단계

(1) 서명자는 다음과 같은 정보를 생성한다.

· 큰 소수 p와 q를 생성한 다음 공개한다.

· 생성자 g를 계산한다.
: $h \in \{1,\ldots,p-1\}$를 선택한다.
: $g = h^{(p-1)/q} \bmod p$가 되는 g를 계산해낸 다음, g를 공개한다.

(2) 검증자는 자신의 비밀키와 공개키를 생성한다.

· 자신의 일반 서명용 개인키를 생성한다.
x_V (단, $0 < x_V < q$인 난수)

· 공개키는 다음과 같이 생성한다.

$y_V = g^{x_V} \bmod p$

(3) 서명자는 다음과 같이 서명 정보를 생성하여 검증자 V에게 전송한다.

· 랜덤 수 $x \in R[1, 2, ..., q-1]$를 선택한 후에, 검증자 V의 공개키를 이용하여 다음과 같이 k를 계산한다.

: $k = H(y_V{}^x \bmod p)$

: $k = k_1 || k_2$

· 다음과 같이 서명 정보를 생성한다.

: $c = E_{k1}(m||CC)$

: $r = KH_{k2}(m)$

: $R = g^r \bmod p$

: $s = x / (r + K_{SGk}) \bmod q$

이때 R값을 별도로 생성하는 이유는, 서명자의 실수 또는 제 3자의 공격으로 인해 서명키가 노출되었을 경우 이전 서명 메시지의 안전성을 보장(선방위 공격 방어)하기 위해서이다.

· 계산된 서명 정보를 검증자 V에게 전송한다.

: $(c \;||\; R \;||\; s) \rightarrow V$

4) 서명 검증 단계

(1) 검증자는 다음을 확인함으로서 서명자의 신분을 확인한다.

· 수신된 서명 정보와 자신의 비밀키를 이용해 k를 계산한다.

: $k = H((K_{PGk} * R)^{x_V * s} \bmod p)$

: $k = k_1 || k_2$

· k 값을 이용하여 다음의 수식이 정확한지 확인함으로서 서명을 검증한다.

: $E_{k1}(m||CC) = c$

: $D_{k1}(c) = m||CC$

: $KH_{k2}(m) = r$

: $g^r \bmod p = R$

· TC의 공개키를 이용하여 CC의 서명을 확인한 다음, 의미 있는 time-stamp가 나타나면 CC는 정당한 TC로부터 생성되었다고 판단한다.

5) 신원 복원 단계

만약 서명자의 신원을 검증자가 확인해야 할 경우, 정당성이 인정된 다면 TC의 확인을 통해 서명자의 신원을 복원할 수 있다.

(1) 검증자는 메시지 m에 대해 자신의 서명을 붙여 은닉 인증 정보를 TC에게 전송한다.

· $V : Sig_V(E_{TC}(ID*r_{TC})||T) \rightarrow TC$

(2) TC는 검증자의 서명자 신원 확인 사유가 정당할 경우, 서명을 확인한 다음 신원을 복원한다.

· $TC : D_{TC}(E_{TC}(ID*r_{TC})) = ID*r_{TC}$

$: (ID*r_{TC})/r_{TC} = ID$

다음 그림은 제안 방식의 개략적 흐름도를 나타낸 것이다.

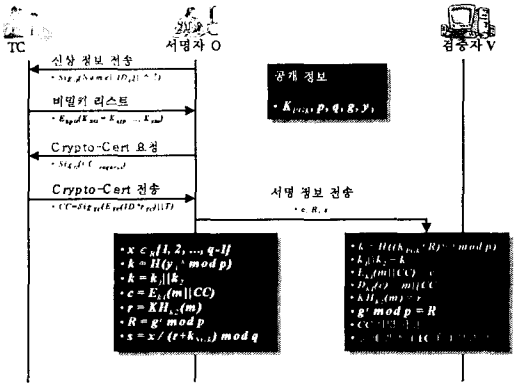

그림 1. 제안 방식 흐름도

5.3 제안 방식 분석

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

1) 익명성 제공

: 서명자는 Crypto-Cert 기법을 통해 제공되는 소속 서명용 키를 통해, 자신이 어떠한 그룹에 속해 있는지를 증명할 수 있다. 이때 검증자는 수신된 서명을 통해 서명자의 어떠한 비밀 정보도 알 수 없으므로 익명성을 제공하고 있다.

2) 소속 확인성 보장

: 검증자는 소속 확인용 공개키들을 통해 서명자가 누구인지 신원은 알 수 없으나, 어느 그룹에 속해있는지는 증명할 수 있다.

3) 기밀성 확보

: 본 방식은 Signcryption 기법을 이용함으로서 송·수신되는 서명 메시지는 세션키 k_1으로 암호화되어 전송된다. 따라서 세션키를 모르는

제 3자로부터 서명 메시지의 기밀성을 확보할 수 있다.

4) 수신자 지정성 보장

: 세션키 k를 서명자가 생성할 때, 검증자의 공개키를 통해 계산되므로, 오직 검증자만이 서명을 확인할 수 있다. 따라서 본 방식은 수신자 지정성을 보장하고 있다.

5) 신원 복원성 제공

: 서명자의 부정행위가 발생하거나 프로토콜상의 특성상 서명자의 신원이 밝혀질 필요가 있을 경우, 정당한 절차를 통해 오직 TC를 통해서 신원 복원이 수행된다.

다음은 상기 요구사항을 고려할 경우, 기존 방식과 제안 방식의 특성을 비교 분석한 결과이다.

표 1. 각 방식별 특성 비교 분석

항목 / 방식	익명성	소속 확인성	기밀성	수신자 지정성	신원 복원성
부인 방지	X	X	X	X	O
의뢰부인 방지	X	X	X	X	O
수신자 지정	X	X	△	O	O
그룹	O	O	X	X	X
제안 방식	O	O	O	O	O

6. 결론

컴퓨터 및 네트워크의 발전을 통해 다양한 응용 분야들이 연구되고 있으며, 정보 전송에 있어 인증성을 확보할 수 있는 디지털 서명 방식의 중요성이 부각되고 있다. 그러나 전자 투표 및 전자 입찰 등과 같은 응용 분야는 필수적으로 서명자의 익명성과 기밀성이 부가적으로 제공되어야 한다.

이에 대해 본 논문에서는 익명성 보장 인증 서비스를 위해 필요한 요구 사항들을 살펴보았으며, 기존의 방식들이 어떻게 대처하는지 그 특징을 고찰하였다.

기존의 특수 디지털 서명 방식들은 필요한 경우 서명 검증을 통해 서명자의 신원이 노출되는 경우가 발생하였다. 만약 서명자의 신원에 대해 익명성을 보장하고, 오직 서명자가 지정한 수신자에게 자신의 소속과 메시지를 디지털 서명을 통해 전송하려 할 경우에 대해서는 현재 고려되어진 특수 디지털 서명 방식이 존재하지 않는다.

이에, 본 제안 방식은 Crypto-Cert 기법과 개선된 Signcryption 방식을 이용하여 기존의 방식들이 안고 있던 서명자의 익명성 부재 문제점을 해결함과 동시에 익명성 제어가 가능하므로 다양한 분야에 적용될 수 있으리라 본다. 또한 현재 제안된 많은 서명 방식들을 응용해 더욱 효율적이고, 안전한 익명성 보장 인증 서비스의 연구가 필요하리라 판단된다.

[참고문헌]

[1] "Specification for a Digital Signature Standard," NIST, FIpS XX. Draft, August 1991[1].

[2] 정보통신단체표준 "부가형 전자서명 방식 표준 - 제 2 부: 확인서 이용 전자서명 알고리즘," www.kisa.or.kr., 1998.

[3] C. Schnorr, "Method for identifying subscribers and for generating and verifying electronic signatures in a data exchange system," US patent #4,995,082, Feb. 1991.

[4] D. Chaum, "Undeniable Signature Systems," U.S. Patent #4,914,689, 3 Apr 1990.

[5] S. J. Park, K. H. Lee and D. H. Won, "An Entrusted Undeniable Signature," Proceedings of the 1995 Japan-Korea Workshop on Information Security and Cryptography, Inuyama, Japan, 24-27 Jan 1995, pp. 120-126.

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

[7] D. Chaum, "Blind Signature Systems," US. Patent #4,759,063, 19 Jul 1988.

[8] M. Mambo, K. Usuda, and E. Okamoto, "Proxy Signatures," Proceedings of the 1995 Symposium on Cryptography and Information Security (SCIS 95), Inuyama, Japan, 24-27 Jan 1995, pp. B1.1.1-17.

[9] D. Chaum, "Group Signature," Advances in Cryptology -EUROCRYPT 91 Proceedings, Springer-Verlag, 1991, pp.257-265.

[10] C. Boyd, "Digital Multisignatures," cryptography and Coding, H.J. Beker and F.C. Piper, eds, Oxford:Clarendon Press, 1989, pp.241-246.

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