通信情報保護學會誌
第6卷 第2號, 1996. 6

특수 디지틀 서명방식에 대한 고찰

A Study on the Special Digital Signature Systems

김 승 주*, 원 동 호**

요 약

계약이나 송금 등을 행하는 서비스에서 서명은 없어서는 안되는 중요한 요소이며, 특히 전자 우편(electronic mail), MHS(Message Handling System)나 EDI(Electronic Data Interchange) 서비스는 기업체는 물론 일반 사용자에게까지 널리 이용될 것으로 사료된다. 이러한 서비스의 특징은 통신망상에서 메시지를 이용하여 다양한 형태의 서비스를 제공하기 때문에 메시지 자체에 대한 인증이나 송신자, 수신자 상호 쌍방간에 인증, 부인 봉쇄 기능을 갖추는 것은 분쟁을 해결하는 필수 불가결한 요소이다. 이를 위한 기술적 대책이 디지틀 서명이다. 디지틀 서명 기술은 기존의 종이 문서에서 사용되는 수서명을 대신할 수 있는 것으로 메시지의 출처와 메시지의 진위 여부를 확인할 수 있는 매우 유용한 서명 방식이다.

그러나, 사실상 디지틀 서명이 많은 응용 업무에서 활용될 것은 자명한 사실이므로 적용 환경 및 적용 업무에 따라서 여러 가지 추가적인 요구조건이 등장할 수 있다. 이러한 특수한 디지틀 서명 프로토콜에 관한 연구는 매우 가치 있는 연구 분야이다.

1. 서 론

통신 기술과 컴퓨터 기술의 발달로 고도 정보화 사회가 급속하게 진행되면서, 이로 인한 고도의 정보 통신망의 실현은 인류에게 유용한 정보를 신속하고 정확하게 처리하여 제공하게 되었다. 그러나 통신망을 통하여 전송되는 정보는 위조, 무단 절취, 파괴의 위험성을 내포하고 있어서, 이러한 위험성을 해결하지 못한다면, 건전한 정보화 사회의 건설은 어렵게 된다. 이러한 정보 보안상의 문제 및 범죄 행위를 사전에 예방하기 위한 방법으로 암호(cryptography)가 이용되고 있다.

암호의 기능은 보호 기능(privacy)과 인증 기능(authentication)으로 나눌 수 있다. 보호 기능이란 데이터가 노출된다 하여도 키를 알지 못하는 한 데이터의 의미를 알 수 없도록 함으로써 정보를 보호하는 것이다. 인증 기능은 "자신이 보낸 정보가 변경되지 않고 상대방에게 정확히 전달되었는가?"를 확인하는 메시지 인증 기능(message authentication)과 정보의 생성·보관·처리 등의 행위에 관여한 사용자의 정당성을 확인하는 사용자 인증 기능(user authentication)으로 구분할 수 있다.

* 성균관대학교 대학원 정보공학과 박사과정
** 성균관대학교 정보공학과 교수

한편, 일상 생활에서 우리가 사용하는 서명이나 인감과 같은 효과를 정보화 사회에서 전자적으로 구현할 때 사용하는 디지틀 서명은 이러한 사용자 인증 기능과 메시지 인증 기능을 모두 만족하여야 한다. 일반적으로 서명이나 인감은 개인의 필요성에 의하여 언제든지 발급될 수 있고, 이 서명 또는 인감을 수신한 사람 역시 수신된 서명이나 인감의 정당성을 쉽게 확인할 수 있으며 서명의 생성자나 인감의 소유자 이외에는 이 서명이나 인감을 발급할 수 없어야 한다. 따라서 디지틀 서명에서도 서명자만이 서명을 생성할 수 있는 유일성, 위조가 불가능한 위조 불가능성, 서명의 진위를 쉽게 확인할 수 있는 진위 확인의 용이성, 자신의 서명을 위조된 것이라고 거부하는 것이 불가능한 거부의 불가능성 등의 요구 사항을 만족하여야 한다. 대부분의 디지틀 서명은 공개키 암호 시스템(public key cryptosystem)[1,2]이나 관용 암호 시스템(conventional cryptosystem)에 의해 구현되는데, 상대적으로 여러 가지 장점을 지닌 공개키 암호 시스템이 많이 사용된다. 일반적인 응용에서는 누구나 이를 확인할 수 있도록 하는 것은 필수적이므로 공개키 암호 시스템을 이용한 일반적인 디지틀 서명이 매우 유용하게 사용될 수 있다.

그러나, 앞에서 언급한 디지틀 서명 프로토콜의 요구조건은 전형적인 디지틀 서명 프로토콜에서의 가장 기본적인 요구조건이다. 사실상 디지틀 서명이 많은 응용 업무에서 활용될 것은 자명한 사실이므로 적용 환경 및 적용 업무에 따라서 여러 가지 추가적인 요구조건이 등장할 것이다.

본고에서는 Blind signature, Group signature, Multisignature, Undeniable signature, Convertible undeniable signature, Entrusted undeniable signature, Nominative signature 등의 특수한 디지틀 서명에 대하여 비교 분석해 본다.

2. 일반적인 디지틀 서명 방식

일반적인 디지틀 서명 모델은 대칭형 암호방식과 중재자를 사용한 모델, 공개키 암호방식을 이용한 모델 및 공개키 암호방식과 일방향 해쉬함수를 사용한 모델이 있는데, 상대적으로 여러 가지 장점을 지닌 공개키 암호방식을 이용한 모델이 많이 사용된다.

공개키 암호방식을 이용한 모델의 서명 방식은 다음과 같다. 서명자는 메시지 m을 자신의 비밀키를 사용하여 서명문 s를 생성하여 검증자에게 전송한다. 검증자는 공개키 디렉토리에 등록된 서명자의 공개키를 사용하여 서명문 s를 검증한다.

공개키 암호방식과 일방향 해쉬함수를 사용한 모델의 서명 방식은 공개키를 이용한 방식과 동일하나 서명 알고리즘의 효율성을 증가시키기 위하여 메시지 m의 서명문을 생성하는 대신에 일방향 해쉬함수(one-way hash function) H를 이용하여 H(m)의 서명문 s를 생성한다.

일반적으로 디지틀 서명 방식이 유용하고 안전하려면 아래의 5가지 조건을 만족하여야 한다.

조건 1) 위조 불가(unforgeable) 조건으로 합법적인 서명자만이 디지틀 서명을 생성할 수 있어야 한다.

조건 2) 서명자 인증(authentic) 조건으로 디지틀 서명의 서명자를 누구든지 검증할 수 있어야 한다.

조건 3) 부인 불가(not repudiated) 조건으로 서명자는 후에 서명한 사실을 부인할 수 없어야 한다.

조건 4) 변경 불가(unalterable) 조건으로 서명한 문서(메시지)의 내용을 변경할 수 없어야 한다.

조건 5) 재사용 불가(not reusable) 조건으로 문서(메시지)의 서명은 다른 문서(메시지)의 서명으로 사용할 수 없어야 한다.

3. 부인 방지 서명방식 (Undeniable signatures)

일반적인 응용에서는 누구나 이를 확인할 수 있도록 하는 것은 필수적이므로 일반적인 디지틀 서명이 매우 유용하게 사용될 수 있다. 그러나 공개키 암호 시스템을 이용한 일반적인 디지틀 서명 방식은 공개키가 모든 사용자에게 공개되기 때문에 통신망에 가입한 사람은 누구든지 메시지의 진위 여부를 확인할 수 있게 되어 필요 이상의 과다한 인증 기회를 제공하게 된다. 이러한 요소는 개인적으로나 상업적으로 민감한 응용 분야에서 임의의 침입자가 디지틀 서명의 사본을 입수한 경우 이를 확인할 수 있게 되어 서명의 사본이 악용될 수 있는 소지를 제공하게 되며 이로 인해 개인의 이익 또는 사생활이 노출될 가능성이 있게 된다. 따라서 서명의 사본만으로는 서명의 정당성을 확인할 수 없고 서명의 인증을 위해서는 반드시 서명자의 도움을 받아야 서명을 확인할 수 있게 하여 서명자나 수신자에 대한 부당 위협 가능성을 줄여 주고 개인의 사생활을 보호할 수 있는 서명 방식이 보다 바람직한 경우가 존재한다.

예를 들어 소프트웨어 공급 회사나 각종 제조업체들이 자사의 제품을 보증하는 디지틀 서명을 발행할 경우 서명자의 도움이 있어야만 발행된 서명을 확인할 수 있게 하여 그 회사의 제품을 직접 구매한 고객만이 해당 업체와의 대화(interactive protocol)를 통해 자신이 구입한 제품이 진본임을 확인할 수 있게 하고, 후에 구입한 제품에 하자가 있을 경우라도 판매회사가 이를 부인할 수 없도록 할 수 있게 하여 서명자의 서명이 남용되는 것을 막을 수 있고 발행된 서명의 안전성에 대한 위협도 방지할 수 있을 것이다.

D. Chaum의 부인 방지 서명방식(undeniable digital signature scheme)은 이러한 목적에 의해 제안되었다.[3,4] 기존에 제안된 디지틀 서명 방식들은 검증 프로토콜에서 단지 서명의 정당성 여부만 확인하는데 비하여 부인 방지 서명은 검증 프로토콜이 확인 프로토콜(confirmation protocol)과 부인 프로토콜(disavowal protocol)로 구성되어 앞에서 언급한 단점을 없앨 수 있어 많은 응용 분야에 적용될 수 있다.

부인 방지 서명방식은 다음의 특징을 가지고 있다.

조건 1) 서명자의 도움 없이는 서명문의 진위를 확인할 수 없어야 하며, 서명자는 필요시에 제3자에게 자신이 발행한 디지틀 서명이 정당함을 보일 수 있다.

조건 2) 서명자는 후에 자신이 발행한 서명문을 부인할 수 없다.

3.1 D. Chaum 등의 부인 방지 서명방식

1) 파라메터

- 시스템 파라메터 : (p, g)
  $p \geq 2^{512}$인 소수 p, 원시 원소 $g \in Z_p$
- 비밀키 : (x)
  $x \in Z_{p-1}$
- 공개키 : (y)
  $y = g^x \pmod p$

2) 서명 생성

메시지 m에 대한 서명 (z)는 서명자에 의하여 다음과 같이 생성된다.

① $z = m^x \pmod p$

3) 확인 프로토콜

① 검증자는 두 개의 난수 a, b $\in_R Z_{p-1}$를 선택하여 $ch = m^a g^b \pmod p$를 만들어 서명자에게 전송한다.

② 서명자는 임의의 난수 q $\in_R Z_{p-1}$를 선택하여 $h_1 = ch \cdot g^q \pmod p$, $h_2 = h_1^x \pmod p$를 계산하여 검증자에게 전송한다.

③ 검증자는 순서 ①에서 선택한 a, b를 서명자에게 전송한다. 서명자는 a, b를 이용하여 ch를 확인하여 정당한 검증자임을 확인하고 q를 검증자에게 전송한다.

④ 검증자는 순서 ②에서 전송 받은 h_1과 h_2가 $h_1 = m^a g^{b+q} \pmod p$, $h_2 = z^a \cdot y^{b+q} \pmod p$인가를 조사하여 정당성을 확인한다.

4) 부인 프로토콜

① 검증자는 임의의 난수 a $\in_R Z_{p-1}$와 검증수 s $\in_R \{0, \cdots, k\}$를 선택해서 $ch_1 = m^s g^a \pmod p$와 $ch_2 = z^s g^{xa} \pmod p$를 계산하여 서명자에게 전송한다.

② 서명자는 ch_1^x / ch_2를 계산하여 그 값이 1이면 본인의 서명이며, 1이 아니면 s값을 구하고 난수 r을 선택하여 blob(r, s)를 검증자에게 전송한다.

③ 검증자는 자신이 선택한 난수 a를 서명자에게 전송한다. 서명자는 ch_1과 ch_2의 정당성을 확인하고 검증자에게 r을 전송한다.

④ 검증자는 서명자가 계산한 s를 확인하여 원래의 서명 z의 정당성을 확인한다.

4. convertible한 부인 방지 서명방식 (Convertible undeniable signatures)

J. Boyar 등은 부인 방지 서명을 비밀키의 일부를 노출시킴으로써 특정한 서명만 선택적으로 혹은 전체 서명을 모두 일반적인 서명으로 변환시킬 수 있는 (selectively) convertible한 부인 방지 서명방식(convertible undeniable signatures)을 제안하였다.[5]

(selectively) convertible한 부인 방지 서명 방식은 다음의 특성을 갖는다.

조건 1) 서명자의 도움 없이는 서명문의 진위를 확인할 수 없어야 하며, 서명자는 필요시에 자신의 비밀키를 노출시키지 않고 임의의 제3자에게 서명의 정당성을 증명할 수 있다.

조건 2) 서명자는 후에 자신이 서명한 사실을 부인할 수 없다.

조건 3) 서명자는 비밀키의 일부를 공개함으로써 대응하는 하나의 부인 방지 서명만 선택적으로 혹은 전체 부인 방지 서명을 모두 보통의 디지틀 서명으로 변환시킬 수 있다.

4.1 J. Boyar 등의 convertible한 부인 방지 서명방식

1) 파라메터

· 시스템 파라메터 : (p, q, α)
  $q|(p-1)$, $p \geq 2^{512}$, $q \geq 2^{140}$인 소수 p, q, 위수가 q인 $\alpha \in Z_p$
· 비밀키 : (x, z)
  $x, z \in Z_q$
· 공개키 : (y, u)
  $y = \alpha^x \pmod p$, $u = \alpha^z \pmod p$

2) 서명 생성

메시지 m에 대한 서명 (T, r, s)는 서명자에 의하여 다음과 같이 생성된다.

① 난수 t, k $\in_R Z_q$를 선택한다.
② $T = \alpha^t \pmod p$
③ $r = \alpha^k \pmod p$
④ $s = k^{-1}((Ttzm) - xr) \pmod q$

3) 확인 프로토콜

① 검증자는 난수 a, b $\in_R Z_q$를 선택하여 ch를 계산하여 서명자에게 전송한다.
$ch = (T^{Tm})^a \cdot \alpha^b \pmod p$
② 서명자는 난수 t $\in_R$ [1, q)를 선택하여 h_1, h_2를 계산하여 검증자에게 전송한다.
$h_1 \equiv ch \cdot \alpha^t \pmod p$
$h_2 \equiv h_1^z \pmod p$
③ 검증자는 단계 ①에서 사용한 난수 a, b를 서명자에게 전송한다.
④ 서명자는 이 a, b가 $ch = (T^{Tm})^a \cdot \alpha^b \pmod p$을 만족하는지 조사하여 이를 만족한다면 단계 ②에서 사용한 난수 t를 전송한다. 이를 만족하지 않는다는 것은 확인자가 프로토콜을 따르지 않는다는 사실을 의미하므로 프로토콜을 중단한다.
⑤ 검증자는 단계 ②에서 받은 h_1, h_2와 단계 ④에서 받은 t를 이용하여 다음을 만족하는지를 검사한다.
$h_1 = (T^{Tm})^a \cdot \alpha^{b+t} \pmod p$?
$h_2 = (y^r r^s)^a \cdot u^{b+t} \pmod p$?

4) 부인 프로토콜

다음의 과정을 k회 반복한다.
① 검증자는 임의의 난수 e $\in_R Z_q$와 $\beta \in_R$ {0, 1}를 선택해서 β가 0이면 $a = \alpha^e \pmod p$, $b = u^e \pmod p$를 계산하고, 1이면 $a = (T^{Tm})^e \pmod p$, $b = (y^r r^s)^e \pmod p$를 계산하여 (a, b)를 서명자에게 전송한다.
② 서명자는 $a^z \pmod p$를 계산하여 그 값이 b이면 $\gamma = 0$, b가 아니면 $\gamma = 1$로 선택하고, 난수 R을 선택하여 bit commitment, $g = BC(\gamma, R)$를 검증자에게 전송한다.
③ 검증자는 자신이 선택한 난수 e를 서명자에게 전송한다. 서명자는 a와 b의 정당성을 확인하고 검증자에게 ans = R을 전송한다.
④ 검증자는 서명자가 계산한 γ를 확인하여 원래의 서명 (T, r, s)의 정당성을 확인한다.

5) 전체 서명을 모두 변환

① 서명자는 비밀키 z를 공개한다.
② 누구라도 $(T^{Tm})^z = y^r r^s \pmod p$를 확인해봄으로써 메시지 m에 대한 서명 (T, r, s)의 진위를 파악할 수 있게 된다.

6) 특정한 서명만 선택적으로 변환

① 서명자는 난수 t를 공개한다.
② 누구라도 $T = \alpha^t \pmod p$, $u^{tTm} = y^r r^s \pmod p$를 확인해봄으로써 서명의 진위를 파악할 수 있게 된다.

5. 의뢰 부인 방지 서명방식 (Entrusted undeniable signatures)

부인 방지 서명방식은 자신의 서명문을 부인하지 못하게 하는 부인 프로토콜로 인하여 일종의 거짓말 탐지기 기능을 제공해주게 된다. 거짓말 탐지기 기능의 예로, 어느 기관에서 근무하는 공직자가 신문사나 방송국 등의 언론기관에 비밀 정보를 제공하려 할 때 신원이 밝혀지는 것을 걱정하여 익명을 요구하며 정보를 제공하려고 하는 경우를 생각해 보자.

언론 기관에서는 허위 정보를 보도할 수 없

으므로 정보 제공자의 신원을 확인할 필요가 있을 것이고 또한, 언론 기관은 정보 제공자의 요구대로 그의 신원을 밝히지 않겠다는 약속을 할 것이다. 이 경우에 일반적인 디지틀 서명은 적합하지 않으며 만일 정보 제공자가 부인 방지 서명을 사용한다고 가정해 보자.

정보가 기사화 되고 그 출처를 알아내기 위해 해당 기관에서 이를 추적하는 과정에서 이 정보와 관련된 정보를 얻었다고 하자. 그러면 그 해당 기관에서는 의심이 갈 만한 모든 내부 직원에게 부인 프로토콜을 수행하게 함으로써 정보의 출처를 알아낼 수 있을 것이다. 즉, 의심을 받은 사람은 부인 프로토콜을 수행하면 쉽게 자신의 누명을 벗을 수 있고 오히려 이를 거부하는 사람은 자신이 그 정보의 출처임을 시인하는 결과가 될 것이므로 이를 거부할 하등의 이유가 없을 것이다.

따라서 결국 정보 제공자는 신원이 밝혀지게 되므로 이와 같은 응용에서는 부인 방지 서명이 적합하지 않음을 알 수 있다.

이와 같은 문제를 해결하기 위하여 T. Okamoto 등이 제안한 것이 non-transitive digital signature이다. 그러나 non-transitive digital signature은 서명이 문제가 되었을 때 분쟁 해결의 기능이 없다는 점에서 디지틀 서명이라고 볼 수 없다.

박성준 등은 영지식 대화형 증명시스템을 이용하여 거짓말 탐지기 기능 문제를 해결하는 의뢰 부인 방지 서명방식(entrusted undeniable signatures)을 제안하였다.[6,13]

부인 방지 서명방식에서 거짓말 탐지기 기능 문제가 발생하는 것은 결국 검증을 원하는 임의의 검증자가 부인 프로토콜을 수행할 수 있다는 데서 기인한다. 따라서 거짓말 탐지기 기능 문제를 해결하기 위해서는 임의의 검증자가 부인 프로토콜을 수행하지 못하고 특정한 자, 예를 들어 분쟁이 일어났을 때 해결해 주는 사람 혹은, 재판관만이 부인 프로토콜을 수행할 수 있도록 만드는 것이다.

의뢰 부인 방지 서명방식의 특성을 가지려면 다음의 요구 조건을 만족해야 한다.

조건 1) 서명자의 도움 없이는 서명문의 진위를 확인할 수 없어야 하며, 서명자는 필요시에 제3자에게 자신이 발행한 디지틀 서명이 정당함을 보일 수 있다.

조건 2) 서명자는 후에 자신이 발행한 서명문을 부인할 수 없다.

조건 3) 임의의 검증자가 부인 프로토콜을 수행할 수 없고 특정한 자만이 부인 프로토콜을 수행할 수 있으며, 디지틀 서명의 특성상 확인 프로토콜은 임의의 검증자가 수행할 수 있다.

5.1 기존의 의뢰 부인 방지 서명방식

1) 파라메터

- 부인 방지 서명 시스템
  - 시스템 파라메터 : (p, g)
    $p \geq 2^{512}$인 소수 p, 원시 원소 $g \in Z_p$
  - 비밀키 : (x)
    $x \in Z_{p-1}$
  - 공개키 : (y)
    $y = g^x \pmod p$

- 재판관
  - 비밀키 : (p, q, d)
    p, q는 큰 소수, $d \in Z_{lcm(p-1, q-1)}$
  - 공개키 : (n, e)
    $n = pq$, $ed = 1 \pmod{lcm(p-1, q-1)}$인 e

2) 서명 생성

메시지 m에 대한 서명 (CS(r), y', z)는 서명자에 의하여 다음과 같이 생성된다.

① 난수 $r \in_R Z_{p-1}$를 선택한다.

② $CS(r) = r^e \pmod n$

③ $y' = (g^x)^r \pmod p$

④ $z = m^{rx} \pmod p$

3) 확인 프로토콜

(1) 〈CS(r), y'〉에 대한 영지식 대화형 증명시스템

다음의 과정을 t회 반복한다.

① 서명자는 난수 $l \in_R Z_{p-1}$를 선택하여 $v_1 = l^e \pmod n$, $v_2 = g^{rlx} \pmod p$를 계산해서 검증자에게 전송한다.

② 검증자는 랜덤 비트 $b \in_R \{0, 1\}$를 서명자에게 전송한다.

③ 서명자는 검증자로부터 전송 받은 b가 0이면 $R = l$을, 1이면 $R = rl$을 검증자에게 전송한다.

④ 검증자는 b = 0을 전송하였을 경우 $v_1 = R^e \pmod n$, $v_2 = (y')^R \pmod p$ 인가를 확인하고 또한, b = 1을 전송하였을 경우 $R^e = v_1 \cdot CS(r) \pmod n$, $v_2 = y^R \pmod p$ 인가를 확인한다.

(2) 〈y', z〉에 대한 확인 프로토콜

비밀키 x를 사용하는 대신에 rx를 사용한다는 것을 제외하고는 D. Chaum의 프로토콜과 같다.

4) 재판관의 부인 프로토콜

(1) CS(r)에서 r을 계산한다.

$r = (CS(r))^d \pmod n$

(2) 〈y', z〉에 대한 부인 프로토콜

① 재판관은 서명문의 부인 여부를 확인하기 위해 임의의 난수 $a \in_R Z_{p-1}$와 검증수 $s \in_R \{0, \cdots, k\}$를 선택하여 $ch_1 = m^s g^a \pmod p$와 $ch_2 = z^{s/r} y^a \pmod p$를 계산하여 서명자에게 전송한다.

② 서명자는 ch_1^x / ch_2를 계산하여 그 값이 1이면 본인의 서명이며, 1이 아니면 s값을 구하고 난수 l을 선택하여 blob(l, s)를 검증자에게 전송한다.

③ 검증자는 자신이 선택한 난수 a를 서명자에게 전송한다. 서명자는 ch_1과 ch_2의 정당성을 확인하고 검증자에게 l을 전송한다.

④ 검증자는 서명자가 계산한 s를 확인하여 원래의 서명 z의 정당성을 확인한다.

6. 수신자 지정 서명방식 (Nominative signatures)

김승주 등에 의하여 연구된 수신자 지정 서명방식은 서명의 인증시에 특정 확인자만이 서명을 확인할 수 있도록 하되, 만일 그 서명이 문제가 되는 경우라도 확인자의 비밀키를 노출시키지 않고 제3자에게 서명의 출처를 증명함으로서 분쟁의 해결 기능을 제공하는 서명방식을 말한다.[7,8,14,15] 즉, 지정된 수신자만이 서명을 확인할 수 있고 필요시 제3자에게 그 서명이 서명자에 의해 자신에게 발행된 서명임을 증명할 수 있게 함으로써 서명의 남용을 서명자가 아닌 검증자(수신자)가 통제할 수 있는 서명방식을 말한다. - 부인 방지 서명은 서명을 검증하기 위하여 서명자의 도움을 필요로 하나 수신자 지정 서명 방식은 수신자의 도움을 필요로 한다. - 이와 같이 특정 수신자만이 서명을 확인할 수 있도록 하는 수신자 지정 서명방식은 부인 방지 서명방식과는 반대로 발행된 서명이 수신자의 개인적인 이해관계나 사생활에 밀접한 관련이 있을 경우 수신자의 동의없이 서명을 확인할 수 없게 되므

로 특정 수신자에 대한 서명의 남용을 방지할 수 있게 된다.

수신자 지정 서명방식의 기능이 요구되는 응용의 예를 들어보자.

갑이 모 회사에 그의 성적증명서를 제출해야 한다고 하자. 이때 성적증명서에는 학교장의 직인이 찍히게 된다. 이와 같은 경우에 서명자(nominator)는 학교의 총장이 되고, 검증자(nominee)는 갑, 제3자는 회사가 된다. 즉, 수신자 지정 서명방식은 서명의 수신자가 서명의 사본들이 불법적으로 사용되는 것을 통제할 수 있으므로 서명의 내용이 검증자의 프라이버시와 밀접한 관계가 있는 경우에 유용하게 사용될 수 있다.

위와 같은 수신자 지정 서명방식의 특성을 가지려면 다음의 2가지 요구 조건을 만족해야 한다.

조건 1) 지정된 수신자(nominee)만이 서명자(nominator)의 서명 S를 확인할 수 있다.
(서명자조차도 서명 S를 확인할 수 없다.)

조건 2) 지정된 수신자만이 필요시에 제3자에게 서명 S가 서명자에 의해 자신에게 발행된 정당한 서명임을 증명할 수 있다.
(서명자조차도 제3자에게 서명 S가 서명자에 의해 수신자에게 발행된 정당한 서명임을 증명할 수 없다.)

6.1 기존의 수신자 지정 서명방식

1) 파라메터

· 시스템 파라메터 : (p, q, α)
$q|(p-1)$, $p \geq 2^{512}$, $q \geq 2^{140}$인 소수 p, q, 위수가 q인 $\alpha \in Z_p$

· 비밀키 : (s)
$s \in Z_q$

· 공개키 : (v)
$v = \alpha^s \pmod p$

2) 서명 생성

서명자 A가 지정 수신자 B만이 확인할 수 있도록 메시지 m을 서명하여 보내고자 하는 경우 메시지 m에 대한 서명 (v_B, x, X, y)은 서명자에 의하여 다음과 같이 생성된다.

① 서명자 A는 난수 r, $R \in_R [1, q)$를 선택하여 $x \equiv \alpha^{R-r} \pmod p$, $X \equiv v_B^R \pmod p$를 계산한다.

② $e = h(v_B, x, X, m)$를 계산하고 $y \equiv r - s_{Ae} \pmod q$를 구하면 ($v_B$, x, X, y)가 메시지 m에 대한 서명이 된다.

3) 서명 검증

① 서명된 메시지 (v_B, x, X, y)를 받은 지정 수신자 B는 $h(v_B, x, X, m) = e$와 $(\alpha^y v_A^e x)^{s_B} \equiv X \pmod p$를 만족하는지 검사함으로써 메시지 m에 대한 서명을 확인할 수 있다.

4) 제3자에 대한 증명 프로토콜

① 제3자(확인자)는 난수 a, $b \in_R [1, q)$를 선택하여 ch를 계산하여 지정 수신자 B(증명자)에게 전송한다.
$ch = (\alpha^y v_A^e x)^a \cdot \alpha^b \pmod p$

② 지정 수신자 B는 난수 $t \in_R [1, q)$를 선택하여 h_1, h_2를 계산하여 제3자에게 전송한다.
$h_1 \equiv ch \cdot \alpha^t \pmod p$
$h_2 \equiv h_1^{s_B} \pmod p$

③ 제3자는 단계 ①에서 사용한 난수 a, b를 지정 수신자 B에게 전송한다.

④ 수신자 B는 이 a, b가 $ch = (\alpha^{y} v_A^{e} x)^{a} \cdot \alpha^{b} \pmod p$을 만족하는지 조사하여 이를 만족한다면 단계 ②에서 사용한 난수 t를 전송한다. 이를 만족하지 않는다는 것은 확인자가 프로토콜을 따르지 않는다는 사실을 의미하므로 프로토콜을 중단한다.

⑤ 제3자는 단계 ②에서 받은 h_1, h_2와 단계 ④에서 받은 t를 이용하여 다음을 만족하는지를 검사한다.

$h_1 = (\alpha^{y} v_A^{e} x)^{a} \cdot \alpha^{b+t} \pmod p$?

$h_2 = X^{a} \cdot v_B^{b+t} \pmod p$?

7. 은닉 서명방식 (Blind signatures)

D. Chaum은 묵지가 내장된 봉투를 사용하는 실제적인 상황을 수식으로 표현한 은닉 서명방식(Blind signatures)을 제안하였다. 이 방식은 메시지를 숨기는 서명 방식으로 제공자(provider : 서명을 받는 사람)의 신원과 메시지를 연결시킬 수 없는 익명성을 유지할 수 있다.[9,10]

은닉 서명의 적용 예로는 다음을 들 수 있다.

은행(서명자)이 만원에 해당하는 서명을 한다고 하자. 고객(provider, 제공자)은 묵지가 내장된 봉투에 서명 받을 용지를 넣어 은행에 보내면, 은행은 그 고객의 계좌에서 만원을 인출하고 고객이 보낸 봉투 위에다 서명을 한다. 이 서명은 내장된 묵지에 의하여 봉투 안에 있는 용지에 서명이 된다. 은행은 서명된 그 봉투를 고객에게 보낸다 고객은 그 봉투를 제거하고 그 안에 있는 용지 위의 서명을 확인하면 된다.

7.1 D. Chaum의 은닉 서명방식

1) 파라메터

- 서명자의 공개 서명함수 : (s)
- 서명자의 비밀 역함수 : (s')
  $s(s'(x)) = x$
- 제공자(provider : 서명을 받는 사람)의 비밀 묵지함수 : (c, c')
  $c'(s'(c(x)) = s'(x)$
- 제공자가 서명자의 도움 없이는 서명을 만드는 것을 불가능하게 하는 지표(predicate) : r

2) 서명 생성

① 제공자는 r(x)인 x를 임의로 택하여 c(x)를 구하고 이것을 서명자에게 보낸다. 이 때 x는 내장된 용지이고 c(x)는 묵지가 있는 봉투에 넣는 것이라고 생각하면 된다.

② 서명자는 s'(c(x))를 구하여 제공자에게 보낸다. 즉 봉투를 뜯지 않고 봉투 위에 서명을 한다.

③ 제공자는 봉투를 뜯어 내장된 용지에 서명을 얻게 된다. 즉, $c'(s'(c(x))) = s'(x)$를 얻게 된다.

3) 서명 검증

① 누구라도 $r(s(s'(x))) = r(x)$를 확인해 봄으로써 서명자에 의한 서명의 진위를 파악할 수 있게 된다.

8. 그룹 서명방식 (Group signatures)

D. Chaum과 E. Heyst는 그룹의 소속원이 자신의 신분을 노출시키지 않고 그룹의 소속원

임을 인증하는 방식을 일반화한 개념인 그룹 서명방식(Group signatures)을 제안하였다.[11]

그룹 서명방식은 다음의 3가지 특성을 갖는다.

조건 1) 그룹의 소속원만이 서명할 수 있다.

조건 2) 검증자는 그룹의 서명문을 확인할 수 있으나 서명자를 알 수 없다.

조건 3) 필요한 경우 서명자를 알 수 있는 방법이 존재한다.

그룹 서명의 적용 예로는 조직 내의 여러 그룹들이 가지고 있는 프린터 사용을 들 수 있다.

그룹 G가 프린터 A를 소유한다고 하자. 그룹 센터 GC는 자신들의 소속원만이 프린터 A를 사용할 수 있게 하고 싶고, 또 그룹의 각 소속원은 자신들의 프라이버시를 위해 프린터 사용을 비밀로 하고 싶을 때 그룹 서명을 사용하면 위의 2 문제를 해결하게 된다.

D. Chaum과 E. Heyst는 4가지 그룹 서명방식을 제안하였다. 그러나 제안한 방식들은 부인 방지 서명방식을 사용하여 많은 전송량과 상호 통신 횟수에 의해 현실적으로 사용하기에는 많은 문제점을 갖고 있다. 더욱이 그들은 효율적인 그룹 서명방식을 설계하는 방법으로, 부인 방지 서명방식을 사용하지 않는 효율적인 그룹 서명방식의 설계를 향후 해결해야 할 문제로 제시하였다.

9. 다중 서명방식 (Multisignatures)

지금까지 개발되어 온 대부분의 디지틀 서명은 문서에 한 사람이 서명하는 단순 서명(single signature) 방식에 중점을 두고 개발되어 왔다. 하지만 이런 단순 서명방식을 실세계에 그대로 적용하기에는 여러 가지 문제점이 있다. 이런 문제 중에 하나가 결재와 서명 운동, 계약의 경우와 같이 여러 사람이 한 문서에 서명하는 경우이다. 단순 서명을 반복해서 적용하여 문제를 해결할 수 있지만, 서명의 길이가 늘어나고, 서명을 검증하려면 서명자의 수만큼 검증과정을 거쳐야 하기 때문에 서명자가 많은 경우 시간이 오래 걸린다는 단점이 있다. 이런 단순 서명방식의 문제를 해결하기 위해 나온 개념이 바로 다중 서명방식(Multisignatures)이다.[12]

대부분의 사무실에서는 계층적 구조를 가지고 있으며, 사무실에서 작성한 문서는 그 문서에 대한 증명과 승인을 위해서 결재가 요구되며 이때 기안자의 서명뿐만 아니라 상급자의 서명이 요구된다. 이와 같이 동일한 디지틀 메시지에 여러 사람이 서명하는 것을 다중 서명이라 한다.

다중 서명방식이라면 갖추어야 할 기본적인 조건들은 다음과 같다.

조건 1) 서명문 길이의 고정 :
다중 서명 생성에 참여한 서명자들이 만들어 내는 서명문의 길이는 서명인의 수에 상관없이 고정되어야 한다.

조건 2) 검증 가능성 :
다중 서명 정보로부터 서명된 문서가 정당한 서명 참여자에 의해서 서명되었다는 것을 서명 참여자들은 물론 제3자도 검증할 수 있어야 한다.

조건 3) 부정 조기 검출성 :
다중 서명을 중간 서명자가 언제든지 검증할 수 있어야 한다.

조건 4) 비밀 유지성 :
다중 서명 정보에서 개인의 비밀정보를 유추해 낼 수 없어야 한다.

조건 5) 공통성 :
다중 서명 생성에 참여하는 각 서명자들이 이용하는 서명 프로토콜이 모두 동일해야 한다.

9.1 Itakura 등의 다중 서명방식

1) 파라메터

- 비밀키 : (p, q, d_i)
  p, q는 큰 소수, $ed_i = 1 \pmod{(p-1)(q-1)(r_i-1)}$인 d_i
- 공개키 : (e, n_0, r_i)
  $\gcd(e, (p-1)(q-1)(r_i-1)) = 1$인 e, $n_0 = pq$, 서명자의 직위에 따른 작은 소수 r_i, $n_i = n_0 r_i \ (= pqr_i)$

2) 서명 생성

메시지 M에 대한 서명 (S)는 서명자에 의하여 다음과 같이 생성된다.

① $S = M^{d_i} \pmod{n_0 r_i}$

3) 서명 검증

① $S^e \pmod{n_0 r_i} = M$

10. 특수 서명의 비교

D. Chaum의 부인 방지 서명방식은 서명자의 도움 없이는 서명문의 진위를 확인할 수 없으며, 서명자는 필요시에 제3자에게 자신이 발행한 디지틀 서명이 정당함을 보일 수 있는 특징을 가지고 있다.

또한 J. Boyar 등은 부인 방지 서명방식을 비밀키의 일부를 노출시킴으로써 특정한 서명만 선택적으로 혹은 전체 서명을 모두 일반적인 서명으로 변환시킬 수 있는 convertible한 부인 방지 서명방식을 제안하였다.

국내에서의 부인 방지 서명방식에 대한 연구는 박성준 등에 의해 연구된 의뢰 부인방지 서명방식과 김승주 등에 의하여 연구된 수신자 지정 서명방식이 있다.

의뢰 부인 방지 서명방식이란 영지식 대화형 증명시스템을 이용하여 거짓말 탐지기 기능 문제를 해결한 서명방식을 말하며, 또한, 수신자 지정 서명방식이란 서명의 인증시에 특정 확인자만이 서명을 확인할 수 있도록 하되, 만일 그 서명이 문제가 되는 경우라도 확인자의 비밀키를 노출시키지 않고 제3자에게 서명의 출처를 증명함으로서 분쟁의 해결 기능을 제공하는 서명방식을 말한다.

D. Chaum의 은닉 서명방식은 메시지를 숨기는 서명 방식으로 제공자의 신원과 메시지를 연결시킬 수 없는 익명성을 유지할 수 있는 특징을 가지고 있다. 또한, D. Chaum과 E. Heyst는 부인 방지 서명방식을 사용하여 자신을 밝히지 않고도 개인식별이 가능한 프로토콜을 일반화한 개념인 그룹 서명방식을 제안하였다.

마지막으로, 결재와 서명 운동, 계약의 경우와 같이 여러 사람이 한 문서에 서명하는 경우에, 단순 서명방식의 문제를 해결하기 위해 나온 개념인 다중 서명방식이 있다.

본 고에서 다룬 특수한 디지틀 서명방식들을 종합적으로 비교 검토하면 다음의 표 1.과 같다.

11. 결 론

컴퓨터의 대량 보급과 통신 기술의 발전으로 현대 사회는 정보화 사회로 발전해 가고 있으며, 종이 문서를 쓰는 대신 컴퓨터와 통신 매체를 이용하여 전자 문서를 작성, 교환하게 되었다. 전자 문서를 이용하면 문서를 작성,

표 1. 특수한 디지틀 서명방식의 비교

방 식	제 안	특 성
Undeniable signatures	Chaum	서명자를 숨기는 서명 방식 ➡ 누구든지 검증 불가능 ➡ 서명자의 도움을 받아야만 검증 가능
Convertible undeniable signatures	Boyar, Chaum, Damgard, Pedersen	부인 방지 서명을 일반적인 서명으로 변환시킬 수 있는 서명 방식
Entrusted undeniable signatures	박성준, 원동호	Undeniable signatures의 거짓말 탐지기 문제를 해결하는 방식
Nominative signatures	김승주, 박성준, 원동호	지정된 수신자 만이 검증할 수 있는 방식 ➡ 누구든지 검증 불가능 ➡ 수신자의 도움을 받아야만 검증 가능
Blind signatures	Chaum	메시지 m을 숨기는 서명 방식
Group signatures	Chaum	신분을 노출시키지 않고 그룹 소속원임을 입증하는 방식 ➡ 자신의 신분을 밝히지 않고 개인 식별하는 방식의 일반화
Multisignatures	Itakura, Nakamura	양자간의 서명을 n명으로 확대

전송, 관리하기가 쉽고, 효율적이라는 장점이 있지만 전자화 되어 있기 때문에 복사와 변조가 쉽다는 단점이 있다. 이런 단점을 보완하기 위해서 종이 문서에 쓰이는 도장이나 서명과 같이 문서의 내용과 서명자를 증명해 줄 수 있는 수단이 요구되었다. 이런 요구를 충족시켜 줄 수 있는 수단이 디지틀 서명이다.

1976년 Diffie, Hellman 등이 공개키 암호화 방식의 개념을 소개한 후 1978년 Rivest, Shamir, Adleman 등이 이 개념을 바탕으로 최초의 디지틀 서명을 개발하였으며, 그 후로 나름대로 진보된 형태의 많은 디지틀 서명들이 개발되어 왔다.

이렇게 많은 디지틀 서명방식들이 개발되었지만 개발과 사용 역사 측면에서 서명이나 도장에 비해 미비하기 때문에 도장이나 서명의 기능을 완전하게 대신하기에는 여러 가지 문제를 가지고 있다. 또한 하나의 디지틀 서명방식이 모든 도장이나 서명의 기능을 대신하기에는 여러 가지 문제점이 있을 수 있다. 이런 디지틀 서명의 취약성을 보완하기 위해 특수 디지틀 서명방식이 개발되었는데 이는 기존의 디지틀 서명방식을 적용 환경에 따라 확장 및 보완한 디지틀 서명방식이다.

사실상 디지틀 서명이 많은 응용 업무에서 활용될 것은 자명한 사실이므로, 적용 환경 및 적용 업무에 따라서 여러 가지 추가적인 요구조건을 만족하는 특수한 디지틀 서명 프로토콜에 대한 연구가 보다 활발히 진행되어야 할 것으로 사료된다.

참 고 문 헌

[1] W. Diffie and M. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory IT-22, pp. 644 - 654, 1976.

[2] R. Rivest, A. Shamir, and L. Adleman, "A method for Obtaining Digital Signature and Public key Cryptosystems", Communication of the ACM, pp. 120 - 128, FEB. 1978.

[3] D. Chaum and H. Antwerpen, "Undeniable signature", Proc. Crypto'89, pp. 212-216.

[4] D. Chaum, "Zero-knowledge undeniable signature", Proc. Eurocrypt'90, pp. 458-464.

[5] J. Boyar, D. Chaum, and I. Damgard, "Convertible undeniable signature", Proc. Crypto'90, pp. 195-208.

[6] S. J. Park, K. H. Lee, and D. H. Won, "An Entrusted Undeniable Signature", Proc. JW-ISC'95, pp. 120-126, 1995.

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

[8] S. J. Kim, S. J. Park, and D. H. Won, "Zero-Knowledge Nominative Signatures", Proc. Pragocrypt'96, 1996.

[9] D. Chaum, "Blind signature for untraceable payments", Crypto'82. pp. 199-203

[10] D. Chaum, "Security without identification : transaction systems to make big brother obsolete", Communications of the ACM, Vol. 28, no. 10, Oct. 1985, pp. 1030-1044.

[11] D. Chaum and E. van Heyst, "Group Signatures", Eurocrypt'91, pp. 257-265, 1991.

[12] Itakura, K. Nakamura, "A public-key cryptosystem suitable for digital multisignatures", NEC J. Res Dev. 71, pp. 1-8, Oct. 1983.

[13] 박성준, 이보영, 원동호, "의뢰 부인 방지 서명방식", 한국통신학회 논문지 제20권 제6호, pp. 1649-1656, 1995. 6.

[14] 김승주, 김경신, 박성준, 원동호, "영지식 수신자 지정 서명방식", 통신정보보호학회 논문지, 1996. 3.

[15] 김승주, 박성준, 원동호, "수신자 지정 서명방식과 부인 방지 서명방식의 통합 시스템", 한국통신학회 논문지, 1996.

□ 著者紹介

김 승 주(金 昇 柱, Seung Joo Kim)

1971년 9월 22일생
1994년 2월 성균관대학교 정보공학과 졸업 (공학사)
1996년 2월 성균관대학교 대학원 정보공학과 졸업 (공학석사)
1996년 3월 ~ 현재 성균관대학교 대학원 정보공학과 박사과정

원 동 호(元 東 豪, Dong Ho Won)

1949년 9월 23일생
1976년 2월 성균관대학교 전자공학과 졸업 (공학사)
1978년 2월 성균관대학교 대학원 전자공학과 졸업 (공학석사)
1988년 2월 성균관대학교 대학원 전자공학과 졸업 (공학박사)
1978년 4월 ~ 1980년 3월 한국전자통신연구소 연구원
1985년 9월 ~ 1986년 8월 일본 동경공대 객원연구원
1982년 3월 ~ 현재 성균관대학교 공과대학 정보공학과 교수
1991년 ~ 현재 한국통신정보보호학회 편집이사
1996년 4월 ~ 현재 정보화추진위원회 자문위원

※ 주관심 분야 : 암호이론, 정보이론