論文 97-22-4-25

지능형 전자 증명 카드에 적합한 통합 서명 시스템에 관한 연구

正會員 김 승 주*, 이 보 영*, 원 동 호*

A Study on the Integrated Digital Signature System for Smart Card

Seungjoo Kim*, Boyoung Lee*, Dongho Won* *Regular Members*

※이 논문은 1996년도 한국학술진흥재단의 공모과제 연구비에 의하여 연구되었음.

요 약

D.Chaum은 단순한 서명의 사본만으로는 서명의 정당성을 확인할 수 없고 서명의 확인을 위해서는 반드시 서명자의 도움을 받아야 하는 undeniable signatures를 제안하였으며, 지금까지 많은 undeniable형 디지틀 서명방식들이 서명의 남용으로부터 서명자나 수신자를 보호하기 위하여 제안되었다.

본 논문에서는 기존의 undeniable형 특수 디지틀 서명방식들과 일반적인 서명방식을 하나로 통합한 일반화된 undeniable형 디지틀 서명을 제안한다. 또한 기존의 undeniable signatures 들이 제3의 도청자로 인하여 응용이 제한적인 경우가 있음을 지적하고, 이를 해결하기 위하여 새로운 개념의 result-indistinguishable undeniable signatures를 제안한다.

ABSTRACT

At Crypto'89 meeting, D. Chaum suggested an undeniable signature scheme. Undeniable signatures are verified via a protocol between the signer and verifier, so the cooperation of the signer is necessary. So far, there have been several variants of undeniable signatures to obtain a signature scheme, which can control the abuse of ordinary digital signatures.

In this paper we integrate these variants into a generalized undeniable-type signature scheme. Also, it will be pointed out, that undeniable signature schemes but its first realization are vulnerable in full view of eavesdropping third party. Moreover, to solve this problem, we propose a new type of digital signature, called "result-indistinguishable undeniable signatures" and construct a practical protocol that implements it.

*성균관대학교 정보공학과
論文番號:97101-0315
接受日字:1997年 3月 15日

Ⅰ. 서 론

정보화 사회로의 진전으로 컴퓨터 네트워크를 통한 다양한 서비스가 요구되고 있다. 특히, 컴퓨터를 이용한 범죄가 늘어나면서 이러한 서비스에 대한 정보 보호의 필요성이 대두되고 있다. 디지틀 서명은 기존의 서류 시스템에서의 인장(도장)이나 서명과 같은 메세지 인증과 사용자 인증의 역할을 정보통신 서비스에서 실현하고자 하는 것이다[1][2][3]. 그러므로 디지틀 서명은 도장이나 서명의 특성을 따르게 된다. 도장의 특성으로는 유일성과 소지성이 있는데 이중에서 유일성은 디지틀 서명방식에서 기본적으로 해결하고 있다. 그 외에도 소지성을 디지틀 서명에 적용시키기 위해 이용자 단말기 기반이 아니라 스마트 카드라는 마이크로프로세서가 내장된 안전한 카드를 사용하여 구현하는 것이 세계적인 추세이다. 즉, 자신의 단말기에서만 디지틀 서명 서비스를 받을 수 있는 것이 아니라, 스마트 카드를 소지한 사람이면 어떤 서비스망 가입 단말기에서도 디지틀 서명 서비스를 받을 수 있다. 이와 같은 소지성과 스마트 카드의 고유 특성인 메모리 영역의 안전성으로 인해 디지틀 서명을 포함한 여러 정보보호 메커니즘의 서비스 적용에 가장 적절한 도구라고 할 수 있다.

누구나 메시지의 출처와 진위여부를 확인할 수 있는 자체인증기능을 갖는 디지틀 서명은 대부분의 응용분야에서는 매우 유용하다. 그러나 개인적으로나 상업적으로 민감한 응용들에서는 이러한 자체인증은 필요 이상의 과다한 인증 기능(서명의 사본으로 누구나 인증 가능)을 제공함으로써 서명의 사본들이 악용될 수 있는 가능성을 높여주게 된다. 따라서 서명의 사본만으로는 서명의 정당성을 확인할 수 없고 서명의 인증을 위해서는 반드시 서명자의 도움을 받아야 하거나 특정 수신자만이 서명을 확인할 수 있게 하는 방법 등에 의해 서명자나 수신자에 대한 부당 위협 가능성을 줄여 주고 개인의 사생활을 보호할 수 있는 서명방식이 보다 바람직한 경우가 존재한다. 이러한 목적에 의해 Crypto'89 회의에서 D.Chaum이 undeniable signature를 제안한 후, (selectively) convertible undeniable signatures, designated confirmer signatures 등의 많은 undeniable형 디지틀 서명방식들이 서명의 남용을 통제하기 위하여 제안되었다. 국내에서의 undeniable signatures에 대한 연구는 박성준 등에 의해 연구된 entrusted undeniable signatures와 임채훈 등의 directed signatures, 김승주 등의 nominative signatures 등이 있다.

본 논문에서는 이러한 여섯 가지 undeniable형 특수 디지틀 서명방식들과 일반적인 디지틀 서명방식을 하나의 서명방식으로 통합한 방식을 제안한다. 스마트 카드의 메모리 비용을 고려할 때 이는 매우 유리할 것이다. 제안된 방식은 P.Horster의 "Meta-ElGamal 서명방식" 개념을 이용하여 "Meta-Undeniable형 서명방식"으로도 확장될 수 있다[4]. 특히 4장에서는 국가 표준화를 목적으로 발표된 디지틀 서명 알고리즘, KCDSA를 이용한 통합 서명 방식도 제안해 본다.

마지막으로 5장에서는 기존의 undeniable형 특수 디지틀 서명방식들이 제3의 도청자로 인하여 응용이 제한적인 경우가 있음을 보이고, 이를 위하여 새로운 개념인 result-indistinguishable undeniable signatures를 제안한다.

Ⅱ. Undeniable형 서명방식

공개키 암호 시스템을 이용한 일반적인 디지틀 서명방식은 공개키가 모든 사용자에게 공개되기 때문에 네트워크에 가입한 사람은 누구든지 메세지의 진위 여부를 확인할 수 있게 되어 필요 이상의 과다한 인증 기회를 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 하거나 특정 수신자만이 서명을 확인할 수 있게 하는 방법 등에 의해 개인의 사생활을 보호할 수 있는 서명방식이 보다 바람직한 경우가 존재한다. D. Chaum의 undeniable signatures는 이러한 목적에 의해 제안되었다.

[정의 1] undeniable signatures … 서명자의 도움 없이는 서명문의 진위를 확인할 수 없으며, 서명자는 필요시에 제3자에게 자신이 발행한 디지틀 서명이 정당함을 보일 수 있다[5][6].

기존에 제안된 일반적인 디지틀 서명방식들은 검

증 프로토콜에서 단지 서명의 정당성 여부만 확인하는데 비하여 D.Chaum에 의해 제안된 부인 방지 서명은 검증 프로토콜이 확인 프로토콜(confirmation protocol)과 부인 프로토콜(disavowal protocol)로 나누어져 있다.

확인 프로토콜은 일반적인 검증 프로토콜과 마찬가지로 서명의 정당성 여부를 판단하는 프로토콜로서 이 프로토콜에 의한 검증이 성공하면 높은 확률로 서명의 정당성을 인증하게 된다. 부인 프로토콜은 확인 프로토콜에서 서명의 정당성 확인이 실패했을 경우, 확인하려고 한 서명이 불법적인 침입자에 의해 만들어진 부당한 서명인지, 아니면 정당한 서명에 대하여 서명자가 부인하려는 의도에서 적절하지 않은 응답을 하였는지를 구분하기 위한 프로토콜이다.

J.Boyar 등은 undeniable signatures를 일반적인 서명으로 변환시킬 수 있는 convertible undeniable signatures를 제안하였다.

[정의 2] **convertible undeniable signatures**… 비밀키의 일부를 노출시킴으로써, 특정한 부인 방지 서명만 선택적으로 혹은 전체 부인 방지 서명을 모두 일반적인 서명으로 변환시킬 수 있는 서명방식이다[7].

그러나, undeniable signatures나 convertible undeniable signatures는 자신의 서명문을 부인하지 못하게 하는 부인 프로토콜의 성질로 인하여 일종의 거짓말 탐지 기능 문제를 갖고 있어 응용이 제한적인 경우가 있다[8].

어느 기관에서 근무하는 공직자가 신문사나 방송국 등의 언론 기관에 비밀 정보를 제공하려 할 때 신원이 밝혀지는 것을 걱정하여 익명을 요구하며 정보를 제공하려고 하는 경우를 생각해 보자. 언론 기관에서는 허위 정보를 보도할 수 없으므로 정보 제공자의 신원을 확인할 필요가 있을 것이고 또한, 언론 기관은 정보 제공자의 요구대로 그의 신원을 밝히지 않겠다는 약속을 할 것이다. 이 경우에도 일반적인 디지틀 서명은 적합하지 않으며 만일 정보 제공자가 undeniable signatures를 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 undeniable signatures가 적합하지 않음을 알 수 있다. 박성준 등은 이를 해결한 entrusted undeniable signatures를 제안하였다.

[정의 3] **entrusted undeniable signatures**… 임의의 검증자가 부인 프로토콜을 수행할 수 없게 하고 특정한 자, 예를 들어 분쟁이 발생하였을 때 중재하는 사람 혹은, 재판관만이 부인 프로토콜을 수행할 수 있도록 하되, 디지틀 서명 특성상 확인 프로토콜은 임의의 검증자가 할 수 있는 서명방식이다[9][10].

또한 undeniable signatures의 경우, 서명자는 자신의 서명에 대한 완전한 통제권을 가지게 됨으로써 서명의 남용으로부터 자신을 보호할 수 있는 장점이 있는 반면, 서명자가 서명 확인/부인 프로토콜을 위한 비밀키를 분실하였다고 주장하거나 서명자의 부재시에는 서명의 진위를 판정할 수 없다는 단점이 있다. D.Chaum의 designated confirmer signatures는 이러한 단점을 해결하기 위하여 제안되었다.

[정의 4] **designated confirmer signatures**… 서명자뿐만 아니라 지명된 제3자(designated third party)도 디지틀 서명의 정당성을 증명할 수 있게 함으로써, undeniable signatures의 "보호 남용(abuse of protection) 문제"를 해결할 수 있는 서명방식이다[11][12].

한편 임채훈 등은 수신자가 서명의 사본들이 불법적으로 사용되는 것을 통제할 수 있도록 하는 directed signatures 개념을 소개하였다.

[정의 5] **directed (or designated verifier) signatures**… 서명자 또는 지명된 수신자(designated verifier)의 도움 없이는 서명문의 진위를 확인할 수 없는

서명방식이다. 이는 "designated third party = receiver"인 designated confirmer signatures의 특별한 경우라고 할 수 있다[13][14][15].

그러나 directed signatures는 수신자뿐만 아니라 서명자 또한 발행된 서명문을 통제할 수 있으므로(즉, 수신자가 자신의 서명에 대한 완전한 통제권을 가지지 못함으로써), 서명자가 지명된 수신자에게 서명한 사실을 부인하기 위해 키를 제3자에게 은밀히 누출시키는 경우 수신자가 자신의 프라이버시에 관련된 서명의 남용을 통제할 수 없다는 약점이 있다[16]. 김승주 등은 undeniable signatures의 쌍대 개념(dual scheme)으로, 발행된 서명이 수신자의 개인적인 이해관계나 사생활에 밀접한 관련이 있을 경우 수신자의 동의없이 서명을 확인할 수 없게 하여 특정 수신자에 대한 서명의 남용을 방지할 수 있는 nominative signatures을 제안하였다.

[정의 6] **nominative signatures**… 지정된 수신자(nominee)만이 서명을 확인할 수 있고 필요시 제3자에게 그 서명이 서명자(nominator)에 의해 자신에게 발행된 정당한 서명임을 증명할 수 있게 함으로써 서명의 남용을 서명자가 아닌 검증자(수신자)가 통제할 수 있는 서명방식이다[17][18][19][23].

Ⅲ. 이산대수 문제에 근거한 일반화된 undeniable형 서명방식

이 장에서는 2장의 여섯 가지 undeniable형 특수 디지틀 서명방식들과 일반적인 디지틀 서명방식을 하나로 통합한 서명방식을 제안한다. 스마트 카드의 한정된 메모리 용량을 고려할 때 이는 매우 바람직할 것이다.

3.1 통합된 서명방식

키 쌍을 생성하기 위하여, 우선 q가 $p-1$의 소인수인 소수 p, q를 선택하고, 다음에는 법 p에 관한 위수가 q인 난수 g를 선택하여 공개한다. 공개키/비밀키 쌍을 생성하기 위하여, q보다 작은 비밀키 x를 선택한 후, $y=g^x \pmod p$를 계산하여 y를 공개키로 발표하고 x를 이에 대응하는 비밀키로 안전하게 보관한다. Schnorr에 의하면 p의 길이를 약 512 bits, q의 길이를 약 140 bits 정도로 선택하는 것이 적당하다고 한다[3].

일반화된 undeniable형 서명의 생성

*Alice*가 *Bob*에게 메세지 m에 대한 서명을 생성하여 보낸다고 가정한다. 또한 *Carol*은 제3자이며 재판관은 모든 서명자에게 공개키 y_{Judge}를 공개한다.

① 서명자 *Alice*는 두 개의 난수 $k_1=f(k, m)$, $k_2 \in Z_q$를 선택하여 $w=g^{k_1-k_2} \pmod p$, $z=A^{k_1} \pmod p$를 계산한다. 여기에서 *Alice*는 다음 표 1의 일곱 가지 유형중 하나를 A로 선정한다(단, $f(k, m)$는 k를 비밀키로 하는 압축 알고리즘).

표 1. A값의 일곱 가지 유형
Table 1. 7 types of A.

유형 (type)	A 값
보통의 디지틀 서명	g
undeniable signatures	y_{Alice}
convertible undeniable signatures	y_{Alice}
entrusted undeniable signatures	$y_{Alice}^{y_{Judge}}$
designated confirmer signatures	$g^{y_{Carol}}$
directed signatures	$g^{y_{Bob}}$
nominative signatures	y_{Bob}

② *Alice*는 $r=h(z, w, m)$을 계산하고 $s=k_2-x_{Alice} \cdot r \pmod q$를 구하면, $(m; w, r, s, (A))$가 메세지 m에 대한 서명이 된다.

서명의 검증

서명문의 진위를 확인하기 위하여 $r \stackrel{?}{=} h((g^s y_{Alice}^r w)^{\log_g A}, w, m)$을 만족하는지를 검사한다. 즉, 이산대수 $\log_g A$를 알고 있는 사용자는 서명의 정당성을 검증할 수 있다.

확인 프로토콜(서명의 정당성을 증명)

① 증명자(prover)는 $z=(g^s y_{Alice}^r w)^{\log_g A}$를 계산하여, 검증자(verifier)에게 전송한다.

② $\log_{g^r y_{Alice}^{k_1-k_2} w} z = \log_g A$를 만족하는 이산대수를 알고 있는지의 여부를 영지식 증명(zero-knowledge) 방법, 예를 들면 Boyar, Chaum, Damgard 등의 BCD 알고리즘[7]으로 증명한다.

BCD 알고리즘

① 확인자(verifier)는 두 난수 $a, b \in Z_q$를 선택하여 $ch = (g^s y_{Alice}^{h(z, m, w)} w)^a g^b \pmod p$를 증명자(prover)에게 전송한다.

② 증명자는 난수 $t \in Z_q$를 선택하여 $h_1 = ch \cdot g^t \pmod p$, $h_2 = h_1^{\log_g A} \pmod p$를 계산, 확인자에게 전송한다.

③ 확인자는 단계 ①의 난수 a, b를 증명자에게 전송한다.

④ 증명자는 확인자로부터 받은 a, b를 이용하여 단계 ①에서 확인자가 적법한 challenge값을 전송했는지를 확인한다. 만일 적법한 값이면 자신의 난수 t를 확인자에게 전송하고 그렇지 않다면 프로토콜을 종료한다.

⑤ 확인자는 증명자로부터 받은 t를 이용하여 $h_1 \stackrel{?}{=} (g^s y_{Alice}^{h(z, m, w)} w)^a g^{b+t} \pmod p$, $h_2 \stackrel{?}{=} z^a A^{b+t} \pmod p$가 성립하는지를 조사한다.

단계 ①~⑤가 정상적으로 수행되면 확인자는 증명자가 $\log_{g^s y_{Alice}^{h(z, m, w)} w} z = \log_g A$를 만족하는 이산대수를 알고 있다는 사실을 확인할 수 있게 된다. 또한 주어진 알고리즘은 영지식 증명 시스템임을 쉽게 증명할 수 있다[7].

[정리 1] 위의 BCD 알고리즘은 대화형 증명 시스템(interactive proof system)이다.

(증명) 만일 비밀키 $\log_g A$를 모르는 제3자가 단계 ⑤의 테스트를 통과할 확률은 기껏해야 $1/q$로 랜덤하게 추측하는 방법뿐이다. 결국 확인자가 부정한 증명자를 검출할 확률은 적어도 $1-1/q$이다.

[정리 2] 위의 BCD 알고리즘은 영지식(zero-knowledge) 증명 시스템이다.

(증명) 위에서 기술한 BCD 알고리즘은 다음과 같이 증명자와의 대화없이 어떤 확인자 V′에 대해서도 통신 내용들을 simulation하는 것이 가능하다.

① V′로부터 challenge값 ch를 얻는다.

② e를 선택하여 $h_1' = g^e \pmod p$, $h_2' = A^e \pmod p$를 계산한다.

③ 확인자로부터 (a, b)를 얻는다. 만일 $ch \neq (g^s y_{Alice}^{h(z, m, w)} w)^a g^b \pmod p$이면 중단하고, 그렇지 않으면 단계 ④로 간다.

④ V′를 challenge 값이 보내진 이후까지 다시 감는다(rewind).
t를 선택하여 $h_1 = (g^s y_{Alice}^{h(z, m, w)} w)^a g^{b+t} \pmod p$, $h_2 = z^a A^{b+t} \pmod p$를 계산한다.

⑤ 확인자로부터 (a', b')를 얻는다.
만일 $ch = (g^s y_{Alice}^{h(z, m, w)} w)^{a'} g^{b'} \pmod p$이면 t를 확인자에게 전송한다. 그렇지 않으면 단계 ④로 간다.

3.2 안전성

방정식 $A = g$를 사용할 경우, 통신망에 가입한 사람은 누구든지 *Alice*의 공개키 y_{Alice}를 이용하여 $r \stackrel{?}{=} h(g^s y_{Alice}^r w, w, m)$을 만족하는지 검사함으로써 메세지 m에 대한 서명 (w, r, s)를 확인할 수 있다(보통의 디지틀 서명방식).

서명자 *Alice*의 공개키 y_{Alice}를 A 값으로 선택하는 경우, 대응되는 비밀키 x_{Alice}를 알고 있는 서명자만이 서명의 진위여부를 판별할 수 있으므로 서명자는 서명의 사본들이 남용되는 것을 막을 수 있다(undeniable signatures). 더욱이 메세지 k_1을 k를 비밀키로 하는 해쉬 알고리즘 $f(k, m)$로 택한 경우에는, k_1을 공개함으로써 이에 대응하는 하나의 메세지 m에 대한 서명만을 보통의 디지틀 서명으로 바꿀 수 있으며, 해쉬 알고리즘 f의 비밀키 k 자체를 공개한다면 임의의 메세지에 대한 서명에 대해서도 누구나 $k_1 = f(k, m)$, $g^{k_1} \stackrel{?}{=} g^s y_{Alice}^{f(y_{Alice}^{k_1}, w, m)} w \pmod p$을 계산할 수 있으므로, 이때까지 발행된 모든 undeniable signatures를 보통의 디지틀 서명으로 변환시킬 수 있다((selectively) convertible undeniable signatures).

한편, $A = y_{Alice}^{y_{Judge}^{x_{Alice}}}$를 사용할 경우, $y_{Judge}^{x_{Alice}}$를 모르는 검증자는 부인 프로토콜을 수행하지 못하나, Diffie-Hellman 공통키, $y_{Judge}^{x_{Alice}} = y_{Alice}^{x_{Judge}} \pmod p$를 알고 있는 제3의 재판관은 다음의 부인 프로토콜을 수행할 수 있게 된다. 이 경우에 확인 프로토콜은 공개키 y_{Alice}를 A로 랜덤화하기 위하여 공통키, $y_{Judge}^{x_{Alice}}$를 사용하였다는 사실을 일반적인 영지식 대화형 증명방식을 이용하여 검증자에게 증명한 후 수행하게 한다(entrusted undeniable signatures).

부인 프로토콜

여기서 안전 파라미터인 k는 공통의 상수로 공개하거나 두 통신 당사자들 사이에 미리 협의되어야 한다. 이때, 증명자가 속일 가능성이 $1/k$이므로 이 가능성을 원하는 레벨 이하로 낮추기 위해서는 부인 프로토콜을 필요한 수만큼 반복 시행해야 할 것이다.

① 재판관은 임의의 난수 $b \in Z_q$와 검증수 $a \in \{0, \cdots, k-1\}$를 선택해서 $ch_1 = (g^s y_{Alice}^r w)^a g^b \pmod p$와 $ch_2 = z^{a/y_{Alice}^{x_{Alice}}} y_{Prover}^b \pmod p$를 계산하여 ($ch_1$, ch_2)를 증명자에게 전송한다.

② 증명자는 $ch_1^{x_{Prover}}/ch_2$를 계산하여 그 값이 1이면 본인의 서명이며, 1이 아니면 다음의 계산을 통하여 a값을 결정한 후, 랜덤수 r을 선택하여 r을 비밀키로 하는 $blob(r, a)$를 재판관에게 전송한다[19].

a를 구하는 계산 :

$ch_1^{x_{Prover}} = ((g^s y_{Alice}^r w)^a g^b)^{x_{Prover}} \pmod p$이므로 $ch_1^{x_{Prover}}/ch_2 = ((g^s y_{Alice}^r w)^{x_{Prover}}/(z^{(y_{Alice}^{x_{Alice}})^{-1}}))^a \pmod p$이다. 그런데, 증명자는 $(g^s y_{Alice}^r w)^{x_{Prover}}$를 알고 있으므로, a값을 구하기 위해 $a = 0, 1, \cdots, k-1$를 식 $((g^s y_{Alice}^r w)^{x_{Prover}}/(z^{(y_{Alice}^{x_{Alice}})^{-1}}))^a = ch_1^{x_{Prover}}/ch_2$가 만족될 때까지 대입한다(trial and error). 이때 위 식을 만족하는 값이 a이다.

여기서 증명자가 a를 결정할 수 있는 것은 $\log_{(g^s y_{Alice}^r w)} (z^{(y_{Alice}^{x_{Alice}})^{-1}}) \neq \log_g y_{Prover}$인 경우이다. 만일 $\log_{(g^s y_{Alice}^r w)} (z^{(y_{Alice}^{x_{Alice}})^{-1}}) = \log_g y_{Prover}$가 성립한다면 결국 $ch_2 = ch_1^{x_{Prover}}$이므로 이 같은 경우는 증명자의 계산능력에 관계없이 정보 이론적으로 ch_1, ch_2는 a에 대한 정보를 전혀 제공하지 않기 때문이다. 이때, 증명자의 계산량이 k에 비례하여 증가하므로 k를 임의로 크게 잡는 것은 불가능하며 실제로 약 1024정도가 적절하다. $k = 1024$로 가정할 경우, 부인 프로토콜을 2회 수행하면 약 100만 분의 1의 확률로 자신의 서명문을 부정할 수 있으며, 부인 프로토콜을 10회 수행하면 자신의 서명문을 부정할 수 있는 확률이 2^{-100}이 된다.

③ 재판관은 자신이 선택한 난수 b를 증명자에게 전송한다.

④ 증명자는 이 b가 $ch_1 = (g^s y_{Alice}^r w)^a g^b$, $ch_2 = z^{a/y_{Alice}^{x_{Alice}}} y_{Prover}^b$를 만족하는지 조사하여 이를 만족하면 단계 ②에서 사용한 난수 r을 전송한다. 이를 만족하지 않는다는 것은 재판관이 프로토콜을 따르지 않는다는 사실을 의미하므로 프로토콜을 중단한다.

⑤ 재판관은 증명자가 계산한 a값과 자신이 선택한 검증수 a를 비교하여 서명의 정당성을 확인한다.

또한, $A = g^{y_{Alice}^{x_{Alice}}}$ 또는 $A = g^{y_{Bob}^{x_{Bob}}}$를 사용하므로 써, Diffie-Hellman 공통키를 알고 있는 서명자와 지명된 제3자(또는 수신자)는 주어진 서명$(m; w, r, s)$의 진위를 확인할 수 있으며, 필요시에 제3자에게 서명의 정당성을 보일 수 있다(designated confirmer signatures (또는 directed signatures)). 마지막으로, 지정된 수신자 *Bob*의 공개키 y_{Bob}을 A 값으로 선택하는 경우, y_{Bob}에 맞는 비밀키 x_{Bob}을 가지고 있는 *Bob*만이 서명을 확인할 수 있고, 서명이 문제가 되는 경우에 제3자에게 그 서명이 *Alice*에 의해 자신에게 발행된 정당한 서명임을 증명할 수 있다(nominative signatures).

Ⅳ. KCDSA를 이용한 일반화된 undeniable형 서명방식

디지틀 서명 알고리즘은 정보보호를 위한 필수적 조건이며 "전산망 보급확장과 이용 촉진에 관한 법률의 개정안"에도 전자 문서의 법적 효력을 인정하고 있고, 디지틀 서명이 들어가야 함을 원칙으로 하고 있다. 따라서 디지틀 서명의 국가 표준화가 시급하다.

이러한 때에 '94년부터 국가 표준화를 목적으로 정보처리 시스템 또는 정보통신망에서 임의의 길이를 갖는 메세지에 대한 생성과 검증을 위한 "부가형 디지틀 서명 방식 표준(안) - 확인서 이용 디지틀 서명 알고리즘(KCDSA, Korean Certificate-based Digital Signature Algorithm)"이 발표되었다[21][22].

본 장에서는 기존의 KCDSA를 개선하여 새로운 일반화된 undeniable형 서명방식을 제안한다.

시스템 초기화

공개키) p: 소수, $|p| = 512 + 128i$, $i = 0, \cdots, 12$.

q: $(p-1)$을 나누는 소수, $|q| = 128 + 32j$, $j = 0, \cdots, 4$.

g: 법 p 상에서 위수가 q인 임의의 수.

y: $y = g^{x^{-1}} \pmod P$.

$h(\ )$: 충돌저항형인(collision-free) 해쉬함수.

$h'(\ )$: 해쉬함수, h와 같을 수도 있으나 충돌 저항형일 필요는 없음.

비밀키) x: q 보다 작은 임의의 수.

서명의 생성

사전계산 (Pre-computation):

① 서명자는 두 개의 난수 k_1, $k_2 \in Z_q$를 선택하여 $w = g^{k_1 - k_2} \pmod q$, $z = A^{k_1} \pmod p$, 그리고 $r = h'(z)$를 계산한다. 여기에서 서명자는 3장에서와 같이 일곱 가지 유형중 하나를 A로 선정한다.

메세지 m의 서명 생성:

② 서명자 *Alice*는 $e = h'(r \| h(w \| m))$를 계산하고 $s = x_{Alice} \cdot (k_2 - e) \pmod q$를 구하면, $(m; w, r, s, (A))$가 메세지 m에 대한 서명이 된다.

서명의 검증

서명문의 진위를 확인하기 위하여 $e = h'(r \| h(w \| m))$를 구한 후, $r \stackrel{?}{=} h'((g^e y_{Alice}^s w)^{\log_g A})$을 만족하는지를 검사한다.

서명의 정당성을 증명

$\log_{g^{A^{h'(z)} h(w \| m)} y_{Alice}^{A^{h'(z)}} w} z = \log_g A$를 만족하는 이산대수를 알고 있는지의 여부를 영지식 증명 방법으로 증명한다.

V. Result-indistinguishable undeniable signatures

5.1 Undeniable signatures의 문제점

일반적으로 undeniable signatures은 다음의 단계로 구성된다.

① *Alice*는 *Bob*에게 서명을 제시한다.

② *Bob*은 랜덤한 challenge 값을 생성하여 *Alice*에게 전송한다.

③ *Alice*는 그녀의 비밀 서명키를 이용하여 challenge에 응답한다(*Alice*는 서명이 정당한 경우에만 challenge에 대응하는 response 값을 생성할 수 있다).

④ Alice의 response에 근거하여, *Bob*은 서명의 진위를 판별한다.

그러나, 문헌 [4]를 제외하고는, 제3자가 *Alice*와 *Bob* 사이의 모든 대화 내용(view)을 도청하는 경우에 도청자 역시도 서명의 정당성을 확인할 수 있게 되며, 이로 인하여 응용이 제한적인 경우가 있다. 더욱이 이러한 문제는 모든 undeniable형 서명방식에서 나타난다.

어느 기관에서 근무하는 공직자 *Alice*가 언론 기관에 익명을 요구하며 비밀 정보를 제공하려고 하는 경우를 생각해 보자. 이 경우에도 일반적인 디지틀 서명은 적합하지 않으며 만일 정보 제공자가 undeniable signatures를 사용한다고 가정해 보자. 언론 기관에서는 허위 정보를 보도할 수 없으므로 확인 프로토콜을 통하여 정보 제공자의 신원을 확인할 필요가 있을 것이고 또한, 언론 기관은 임의로 제3자에게 그의 신원을 밝힐 수 없을 것이다.

그러나, 이때 의심 많은 해당 기관이 *Alice*의 모든 통화 내용을 감시하고 있었다면, 언론 기관뿐만 아니라, *Alice*와 언론 기관 사이의 대화 내용을 가지고 있는 해당 기관도 역시 *Alice*의 서명을 확인할 있을 것이다. 따라서 결국 정보 제공자는 신원이 밝혀지게 되므로 이와 같은 응용에서는 undeniable signatures가 적합하지 않음을 알 수 있다. 본 절에서는 이를 해결할 수 있는 result-indistinguishable undeniable signatures을 제안한다. result-indistinguishable undeniable signatures의 특성을 가지려면 다음의 3가지 요구 조건을 만족해야 한다.

1. (Confirmation) 서명자의 도움 없이는 서명문의 진위를 확인할 수 없다.
2. (Disavowal) 서명자는 정당한 서명에 대하여 허위로 부인할 수 없다.
3. (Result-indistinguishable) 지정된 확인자만이 서명자의 확인 프로토콜을 검증할 수 있다. 즉, 제3의 도청자가 서명자의 모든 대화 내용을 가지고 있더라도 서명을 확인할 수 없다.

Result-indistinguishable undeniable signatures의 구성은 BCD 알고리즘의 response값을 지명된 확인자만이 알 수 있도록 함으로써, 제3자는 확인 프로토콜이 불가능하도록 한다.

5.2 Result-indistinguishable undeniable signatures

제안

시스템 초기화

공개키) p: 소수, $|p|=512$.

g: 법 p 상에서 위수가 $(p-1)$인 임의의 수.

y: $y=g^x \pmod p$.

비밀키) x: $(p-1)$ 보다 작은 임의의 수.

서명의 생성

① 서명자 *Alice*는 $z=m^{x_{Alice}} \pmod p$을 계산하면, $(m;z)$가 메세지 m에 대한 서명이 된다.

확인 프로토콜

① 확인자 *Bob*은 두 난수 $0<a, b<p-1$를 선택하여 $ch=m^a \cdot g^b \pmod p$를 증명자 *Alice*에게 전송한다.

② *Alice*는 난수 $0<r<p-1$을 선택하여 q, s_1, s_2를 계산하여, s_1, s_2를 *Bob*에게 전송한다.

$q=(y_{Bob}{}^r \pmod p) \pmod{p-1}$,

$s_1=ch \cdot g^q \pmod p$,

$s_1=s_1^{x_{Alice}} \pmod p$.

③ *Bob*은 단계 ①의 난수 a, b를 *Alice*에게 전송한다.

④ *Alice*는 *Bob*으로부터 받은 a, b를 이용하여 단계 ①에서 *Bob*이 적법한 challenge값을 전송했는지를 확인한다. 만일 적법한 값이면 $g^r \pmod p$를 *Bob*에게 전송하고 그렇지 않다면 프로토콜을 종료한다.

⑤ *Bob*은 *Alice*로부터 받은 g^r와 자신의 비밀키 x_{Bob}을 이용하여 $q=((g^r)^{x_{Bob}} \pmod p) \pmod{p-1}$을 계산하여 다음이 성립하는지를 조사한다.

$s_1 \stackrel{?}{=} ch \cdot g^q \pmod p$,

$s_2 \stackrel{?}{=} y_{Alice}{}^{b+q} \cdot z^a \pmod p$.

여기서, undeniable signatures과는 달리, q에 대응하는 비밀키 x_{Bob}를 소지한 *Bob*만이 서명을 확인할 수 없다. 또한, 위에서 기술한 확인 프로토콜은 3.1절의 BCD 알고리즘과 마찬가지로 증명자와의 대화 없이도 통신내용들을 simulation하는 것이 가능하며, 또한 비밀키를 모르는 제3자가 테스트를 통과할 확률은 기껏해야 $1/q$로 랜덤하게 추측하는 방법뿐이다.

부인 프로토콜

그릇된 서명 z가 주어졌을 때, 증명자는 $\log_g y_{Prover} \neq \log_m z$ 임을 3.2절의 부인 프로토콜과 유사한 방식으로 증명한다.

5.3 KCDSA를 이용한 result-indistinguishable한 undeniable형 서명방식

시스템 초기화 및 일반화된 undeniable형 서명의 생성은 4장과 같다. 여기서, 지정된 확인자만이 서명자의 확인 프로토콜을 검증할 수 있도록 하기 위하여 BCD 알고리즘을 다음과 같이 변형한다.

확인 프로토콜

① 확인자 *Bob*은 두 난수 $a, b \in Z_q$를 선택하여 $ch=(g^{h'(h'(z)\|h(w\|m))} y_{Alice}{}^s w)^a g^b \pmod p$를 증명자 *Alice*에게 전송한다.

② *Alice*는 난수 $0<r<q$을 선택하여 $t=y_{Bob}{}^r \pmod p) \pmod q$를 구한 후, $h_1=ch \cdot g^t \pmod p$, $h_2=h_1^{\log_g A} \pmod p$를 계산, *Bob*에게 전송한다.

③ *Bob*은 단계 ①의 난수 a, b를 증명자에게 전송한다.

④ *Alice*는 *Bob*으로부터 받은 a, b를 이용하여 단계 ①에서 확인자가 적법한 challenge값을 전송했는지를 확인한다. 만일 적법한 값이면 자신의 난수 $g^r \pmod p$를 확인자에게 전송하고 그렇지 않다면 프로토콜을 종료한다.

⑤ *Bob*은 *Alice*로부터 받은 g^r와 자신의 비밀키 x_{Bob}을 이용하여 $t=((g^r)^{x_{Bob}} \pmod p) \pmod q$를 계산하여 다음이 성립하는지를 조사한다.

$h_1 \stackrel{?}{=} (g^{h'(h'(z)\|h(w\|m))} y_{Alice}{}^s w)^a g^{b+t} \pmod p$,

$h_2 \stackrel{?}{=} z^a A^{b+t} \pmod p$.

Ⅵ. 결 론

본 논문에서는 기존에 제안된 여섯 가지의 undeniable형 디지틀 서명방식들 - 즉, undeniable signatures, convertible undeniable signatures, entrusted undeniable signatures, designated confirmer signatures, directed signatures, nominative signatures - 과 보통의 디지틀 서명방식을 하나의 서명방식으로 통합한 서명방식을 제안하였으며, 국가 표준화를 목적으로 발표된 KCDSA를 이용한 통합 서명 방식도 제안해 보

았다. undeniable형 특수 서명방식들은 사용자가 서명의 남용을 통제할 수 있으므로 개인적으로 민감한 응용들 즉, 주민등록등·초본, 호적등본, 의료보험카드 등에 매우 유용하다. 특히 제안된 통합 서명 방식은 이러한 여러 가지 특수 서명방식들을 하나로 구현할 수 있으므로, 스마트 카드의 메모리 용량을 고려할 때 매우 바람직할 것이다.

또한 기존의 undeniable형 특수 디지틀 서명방식들의 문제점을 지적하고, 이를 위하여 새로운 개념인 result-indistinguishable undeniable signatures을 제안하고 서명 프로토콜을 구성하여 보았다.

참 고 문 헌

1. W.Diffie and M.E.Hellman, "New directions in cryptography," IEEE Transaction on Information Theory, Vol.IT-22 No.6, 1976, pp.644-654.
2. R.Rivest, A.Shamir and L.Adleman, "A method for obtaining digital signature and publickey cryptosystems," Communications of the ACM, Vol.21 No.2, 1978, pp.120-126.
3. C.P.Schnorr, "Efficient signature generation for smart cards," Journal of Cryptology, Vol.4 No.3, 1991, pp.161-174.
4. P.Horster, M.Michels and H.Petersen, "Meta-El-Gamal signature schemes," Proc. 2nd ACM conference on Computer and Communications security, 1994. pp.96-107.
5. D.Chaum and H.Antwerpen, "Undeniable signature," Advances in Cryptology-Crypto'89, Springer-Verlag, 1990, pp.212-216.
6. D.Chaum, "Zero-knowledge undeniable signatures," Advances in Cryptology-Eurocrypt'90, Springer-Verlag, 1991, pp.458-464.
7. J.Boyar, D.Chaum and I.Damgard, "Convertible undeniable signature," Advances in Cryptology-Crypto'90, Springer-Verlag, 1991, pp.189-205.
8. T.Okamoto and K.Ohta, "How to utilize the randomness of zero-knowledge proofs," Advances in Cryptology-Crypto'90, Springer-Verlag, 1991, pp. 437-456.
9. 박성준, 이보영, 원동호, "의뢰 부인방지 서명에 관한 연구," 한국통신학회 논문지 제20권 제6호, 1995, pp.1649-1656.
10. S.J.Park, K.H.Lee and D.H.Won, "An entrusted undeniable signature," Proc. of JW-ISC'95, 1995.
11. D. Chaum, "Designated confirmer signatures," Advances in Cryptology-Eurocrypt'94, Springer-Verlag, 1995, pp.86-91.
12. T.Okamoto, "Designated confirmer signatures and public-key encryption are equivalent," Advances in Cryptology-Crypto'94, Springer-Verlag, 1995, pp.61-74.
13. C.H.Lim and P.J.Lee, "Modified Maurer-Yacobi's scheme and its applications," Advances in Cryptology-Auscrypt'92, Springer-Verlag, 1993, pp. 308-323.
14. 임채훈, 이필중, "상호 신분 인증 및 디지탈 서명 기법에 관한 연구," 통신정보보호학회 논문지 제2권 제1호, 1992, pp.16-35.
15. C.H.Lim and P.J.Lee, "Directed signatures and application to threshold cryptosystems," Proc. of 1996 Cambridge Workshop on Security Protocols, 1996.
16. 김승주, 박성준, 원동호, "수신자 지정 서명방식에 대한 고찰," 한국정보처리응용학회 학술발표회 논문집 제1권 제2호, 1994, pp.530-533.
17. S.J.Kim, S.J.Park and D.H.Won, "Nominative signatures," Proc. of ICEIC'95, International Conference on Electronics, Informations and Communications, 1995, pp.II-68-II-71.
18. 김승주, 김경신, 박성준, 원동호, "영지식 수신자 지정 서명방식," 통신정보보호학회 논문지 제6권 제1호, 1996, pp.15-24.
19. S.J.Kim, S.J.Park and D.H.Won, "Zero-knowledge nominative signatures," Proc. of Pragocrypt-'96 International Conference on the Theory and Applications of Cryptology, 1996. pp.380-392.
20. G. Brassard, D. Chaum and C. Crepeau, "Minimum disclosure proofs of knowledge," Journal of Computer and System Science, Vol.37 No.2, pp. 156-189, 1988.

21. 강신각, 문상재, 박성준, 백재현, 신종태, 원동호, 이경석, 이필중, 임채훈, 장청룡, "부가형 디지틀 서명 표준안에 관한 연구," 한국통신학회 하계종합학술발표회 논문집(I:), 1996, pp.757-760.
22. 한국통신정보보호학회, "정보보호 표준방식 개발," 한국전자통신연구소 최종연구보고서, 1996.
23. 김승주, 박성준, 원동호, "수신자 지정 서명방식과 부인 방지 서명방식의 통합 시스템," 한국통신학회 논문지 제21권 제5호, 1996, pp.1266-1273.

김 승 주(Seungjoo Kim) 정회원
1971년 9월 22일생
1994년 2월 : 성균관대학교 정보공학과 졸업(공학사)
1996년 2월 : 성균관대학교 대학원 정보공학과 졸업(공학석사)
1996년 3월~현재 : 성균관대학교 대학원 정보공학과 박사과정

이 보 영(Boyoung Lee) 정회원
1966년 3월 13일생
1989년 2월 : 성균관대학교 정보공학과 졸업(공학사)
1995년 8월 : 성균관대학교 대학원 정보공학과 졸업(공학석사)
1996년 3월~현재 : 성균관대학교 대학원 정보공학과 박사과정

원 동 호(Dongho Won) 정회원
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
1995년 3월~1997년 2월 : 성균관대학교 교학처장
1991년~현재 : 한국통신정보보호학회 편집이사
1996년 4월~현재 : 정보화추진위원회 자문위원
※주관심분야 : 암호이론, 정보이론