論文 96-21-5-17

수신자 지정 서명방식과 부인 방지 서명방식의 통합 시스템

正會員 김 승 주*, 박 성 준**, 원 동 호*

An Integrated System of Nominative Signatures and Undeniable Signatures

Seung Joo Kim*, Sung Jun Park**, Dong Ho Won* *Regular Members*

요 약

D. Chaum은 단순한 서명의 사본만으로는 서명의 정당성을 확인할 수 없고 서명의 확인을 위해서는 반드시 서명자의 도움을 받아야 하는 부인 방지 서명방식을 제안하였으며, J. Boyar 등은 부인 방지 서명방식을 변형하여 비밀키의 일부를 노출시킴으로써 특정한 서명만 선택적으로 혹은 전체 서명을 모두 일반적인 서명으로 변환시킬 수 있는 (selectively) convertible한 부인 방지 서명방식을 제안하였다.

또한 김승주외 2인은 특정한 수신자만을 상대로 서명을 발행하여 수신자가 자신에게 발행된 서명을 통제할 수 있는-부인 방지 서명방식의 쌍대 개념인-수신자 지정 서명방식을 제안하였다.

본 논문에서는 수신자 지정 서명방식과 부인 방지 서명방식을 하나의 서명방식으로 통합할 수 있는 서명방식을 제안한다. 특히, 통합된 서명방식에서 사용되는 공개키 대신에 랜덤수를 사용함으로써 자연적으로 (selectively) convertible한 부인 방지 서명방식을 구성할 수 있다.

통합 서명방식에서 제안한 서명방식들은 기존에 제안된 Chaum의 부인 방지 서명방식과 Boyar의 (selectively) convertible한 부인 방지 서명방식보다 효율적이다.

ABSTRACT

The nice concept of undeniable signatures was presented by Chaum and van Antwerpen. Briefly, an undeniable signature is a signature which cannot be verified without the help of the signer. They are therefore less personal

*성균관대학교 정보공학과
Department of Information Engineering Sung Kyun Kwan University
**한국정보보호센터
Korea Information Security Agency
論文番號:95413-1202
接受日字:1995年 12月 2日

than ordinary signatures in the sense that a signature cannot be related to the signer without his help. On the other hand, the signer can only repudiate an alleged signature by proving that it is incorrect.

Boyar, Chaum, Damgard and Pedersen introduce convertible undeniable signatures. In this schemes, release of a single bit string by the signer turns all of his signatures, which were originally undeniable signatures, into ordinary digital signatures.

And, S. J. Kim, S. J. Park and D. H. Won propose a new kind of signature scheme, called "nominative signatures", that is the dual scheme of undeniable signatures. nominative signatures achieve these objectives: Only nominee can verify the nominator(signer)'s signature and if necessary, only nominee can prove to the third party that the signature is issued to him(her) and is valid.

In this paper we present an efficient integrated system of nominative signatures and (convertible) undeniable signatures. i.e. we show how nominative signature scheme can be changed into a (convertible) undeniable signatures.

Ⅰ. 서 론

공개키 암호 시스템을 이용한 일반적인 디지틀 서명방식[2][3][4][5][6][7][8][9]은 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 있어 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 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.

D. Chaum의 부인 방지 서명방식(undeniable digital signature scheme)은 이러한 목적에 의해 제안되었다.[10][11] 부인 방지 서명방식은 자신이 발행한 디지틀 서명이 정당함을 보이는 확인 프로토콜(confirmation protocol)과 자신이 발행한 서명을 후에 부인할 수 없도록 하는 부인 프로토콜(disavowal protocol)로 구성되어 앞에서 언급한 단점을 없앨 수 있어 많은 응용 분야에 적용될 수 있다.

또한 J. Boyar 등은 부인 방지 서명방식을 비밀키의 일부를 노출시킴으로써 특정한 서명만 선택적으로 혹은 전체 서명을 모두 일반적인 서명으로 변환시킬 수 있는 (selectively) convertible한 부인 방지 서명방식을 제안하였다.[12]

국내에서의 부인 방지 서명방식에 대한 연구는 박성준 등에 의해 연구된 의뢰 부인방지 디지틀 서명방식(entrusted undeniable signatures)[16][19][20]과 김승주 등에 의하여 연구된 수신자 지정 서명방식(nominative signatures)[17][18][21][22][23][24]이 있다. 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. 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 서명방식은 서명을 검증하기 위하여 서명자의 도움을 필요로 하나 수신자 지정 서명방식은 수신자의 도움을 필요로 한다. 이와 같이 특정 수신자만이 서명을 확인할 수 있도록 하는 수신자 지정 서명방식은 부인 방지 서명방식과는 반대로 발행된 서명이 수신자의 개인적인 이해 관계나 사생활에 밀접한 관련이 있을 경우 수신자의 동의없이 서명을 확인할 수 없게 되므로 특정 수신자에 대한 서명의 남용을 방지

할 수 있게 된다.

본 논문에서는 서로 쌍대 개념(dual scheme)인 수신자 지정 서명방식과 부인 방지 서명방식을 하나의 서명방식으로 통합한 방식을 제안한다. 즉, 통합된 방식은 서명 생성시 사용되는 공개키의 종류에 따라 수신자 지정 서명방식(수신자의 공개키 사용)으로, 또는 부인 방지 서명방식(서명자의 공개키 사용)으로 사용될 수 있다. 특히, 제안하는 통합 서명방식은 사용되는 공개키를 랜덤화 함으로써 (selectively) convertible한 부인 방지 서명방식을 구성할 수 있음을 보인다.

Ⅱ. 수신자 지정 서명방식

수신자 지정 서명방식이란 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, 부인 방지 서명방식의 쌍대 개념인, 서명방식을 말한다. 즉, 부인 방지 서명방식은 서명을 검증하기 위하여 서명자의 도움을 필요로 하나 수신자 지정 서명방식은 수신자의 도움을 필요로 한다.[17][18][21][22][23][24]

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 서명자는 학교의 총장이 되고, 검증자는 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.

이를 위하여 서명자는 서명을 생성할 때 특정 수신자의 공개키를 결부시킴으로써 그 공개키에 대응하는 비밀키의 소유자만이 서명을 인증할 수 있도록 하고 또한 지정 수신자는 자신이 그 서명을 제시해야 할 필요가 있을 때에는 제3자에게 그 정당성을 증명할 수 있도록 한다.

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

조건1) 지정된 수신자만이 서명자의 서명 S를 확인할 수 있다.
(서명자조차도 서명 S를 확인할 수 없다.)

조건2) 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.)

Schnorr의 서명방식을 변형하면 이와 같은 수신자 지정 서명방식을 구성할 수 있다.[4][5] 서명자 A가 지정 수신자 B만이 확인할 수 있도록 메세지 m을 서명하여 보내고자 하는 경우 다음과 같이 서명을 생성할 수 있다.

[초기화]

공개키) p : 소수.
q : 소수. 단, $q \mid p-1$
α : mod p 상에서 위수(order)가 q인 임의의 수.
$v : v = \alpha^s \pmod p$

비밀키) s : q 보다 작은 임의의 수

Schnorr에 의하면 p의 길이를 약 512 bits, q의 길이를 약 140 bits 정도로 선택하는 것이 적당하다고 한다.[4][5]

[수신자 지정 서명 기법]

① 서명자 A는 랜덤수 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 $y \equiv r - s_A e \pmod q$를 구하면 (v_B, x, X, y)가 메세지 m에 대한 서명이 된다.

③ 이를 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 메세지 m에 대한 서명을 확인할 수 있다.

여기서 s_B는 지정 수신자 B만이 알고 있으며 그 외의 어떤 제3자도 (v_B, x, X, y)와 메세지 m으로부터 서명의 진위 여부를 판별할 수는 없으므로, 부인 방지 서명방식과는 상대적으로 서명자가 아닌 수신자 자신

이 서명의 사본들이 남용되는 것을 막을 수 있다.

[제3자에 대한 영지식 대화형 증명 프로토콜]

디지틀 서명의 가장 중요한 기능 중의 하나인 부인 방지 기능을 위해서는 이 서명이 문제가 되었을 때 서명자가 이를 부인할 수 없도록 서명의 수신자가 임의의 제3자에게 그 서명의 정당성을 증명할 수 있는 프로토콜이 필수적이다. 즉 지정 수신자 B는 제3자에게 $(\alpha^y v_A^e x)^{s_B} \equiv X \pmod p$와 $\alpha^{s_B} \equiv v_B \pmod p$를 만족하는 이산대수 s_B를 알고 있다는 사실을 증명할 수 있어야 한다. 이때 제3자는 s_B의 값을 모르지만 지정 수신자 B가 s_B를 소유하고 있음을 확신하게 된다.

이러한 목적으로 사용될 프로토콜로 다음과 같은 프로토콜을 구성할 수 있다.

① 제3자(확인자)는 랜덤수 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 랜덤수 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 랜덤수 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 랜덤수 t를 전송한다. 이를 만족하지 않는다는 것은 확인자가 프로토콜을 따르지 않는다는 사실을 의미하므로 프로토콜을 중단한다.

⑤ 제3자는 단계 ②에서 받은 $h_1 h_2$와 단계 ④에서 받은 t를 이용하여 다음을 만족하는지를 검사한다.
$h_1 = (\alpha^y v_A^e x)^a \cdot \alpha^{b+t} \pmod p$?
$h_2 = X^a \cdot v_B{}^{b+t} \pmod p$?

순서 ①~⑤가 정상적으로 수행되면 제3자는 지정 수신자 B가 $(\alpha^y v_A^e x)^{s_B} \equiv X \pmod p$와 $\alpha^{s_B} \equiv v_B \pmod p$를 만족하는 이산대수 s_B를 알고 있다는 사실을 확인할 수 있게 된다. 또한, 주어진 프로토콜은 영지식 증명 시스템임을 쉽게 증명할 수 있다.[18][24]

Ⅲ. 통합 서명방식

이 장에서는 2장에서 제안된 수신자 지정 서명방식을 이용하여 부인 방지 서명방식과 (selectively) convertible한 부인 방지 서명방식을 하나로 통합한 통합 서명방식을 제안한다.

즉, 통합 서명방식에서 사용되는 공개키의 종류에 따라 수신자의 공개키를 사용하는 수신자 지정 서명방식, 서명자의 공개키를 사용하는 부인 방지 서명방식, 또는 랜덤화된 공개키 사용하는 (selectively) convertible한 부인 방지 서명방식을 구성할 수 있음을 보인다.

제안하는 통합 서명방식은 다음과 같다.

[초기화]

공개키) p : 소수.
q : 소수. 단, $q \mid p-1$
α : mod p 상에서 위수가 q인 임의의 수.
v : $v = \alpha^s \pmod p$

비밀키) s : q 보다 작은 임의의 수

[통합 서명 기법]

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

② e = h(공개키, x, X, m)를 계산하고 $y \equiv r - s_A e \pmod q$를 구하면 (공개키, x, X, y)가 메세지 m에 대한 서명이 된다.

3.1 부인 방지 서명방식

본 절에서는 제안된 통합 서명방식에서 사용되는 공개키를 서명자의 공개키 v_A로 선택함으로써 부인 방지 서명방식을 구성할 수 있음을 보인다.

[서명 생성 과정]

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

② 다음으로 e = h(v_A, x, X, m)를 계산하고 $y \equiv r - s_A e \pmod q$를 구하면 ($v_A$, x, X, y)가 메세지 m에 대한 서명이 된다.

즉, $(\alpha^{y} v_A^{c} x)^{s_A} \equiv X \pmod p$를 만족하는 s_A는 서명자 A만이 알고 있으며 그 외의 어떤 제3자도 (v_A, x, X, y)와 메세지 m으로부터 서명의 진위 여부를 판별할 수는 없으므로, 서명자는 서명의 사본들이 남용되는 것을 막을 수 있다.

이 서명에 대한 확인 프로토콜은 수신자 지정 서명 방식의 "제3자에 대한 영지식 대화형 증명 프로토콜"을 그대로 이용할 수 있으며, 부인 프로토콜은 Chaum의 부인 프로토콜을 사용할 수 있다. 즉, 서명자가 임의의 확인자로부터 (v_A, x, X, y)가 주어진 메세지 m에 대한 유효한 서명인지를 인증해 줄 것을 요청 받았다면 서명자 A는 $(\alpha^{y} v_A^{c} x)^{s_A} \equiv X \pmod p$와 $\alpha^{s_A} \equiv v_A \pmod p$를 만족하는 이산대수 s_A를 알고 있는지의 여부를 확인자와의 대화형 프로토콜인 확인/부인 프로토콜을 통하여 실현할 수 있다. 다음에 확인 프로토콜과 부인 프로토콜을 간략히 기술한다.

[확인 프로토콜]

① 확인자는 랜덤수 $a, b \in_R [1, q)$를 선택하여 ch를 계산하여 증명자 A에게 전송한다.
$ch = (\alpha^{y} v_A^{c} x)^{a} \cdot \alpha^{b} \pmod p$

② 증명자 A는 랜덤수 $t \in_R [1, q)$를 선택하여 h_1, h_2를 계산하여 확인자에게 전송한다.
$h_1 \equiv ch \cdot \alpha^{t} \pmod p$
$h_2 \equiv h_1^{s_A} \pmod p$

③ 확인자 단계 ①에서 사용한 랜덤수 a, b를 증명자 A에게 전송한다.

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

⑤ 확인자는 단계 ②에서 받은 h_1, h_2와 단계 ④에서 받은 t를 이용하여 다음을 만족하는지를 검사한다.
$h_1 = (\alpha^{y} v_A^{c} x)^{a} \cdot \alpha^{b+t} \pmod p$?
$h_2 = X^{a} \cdot v_A^{b+t} \pmod p$?

순서 ①~⑤가 정상적으로 수행되면 확인자는 증명자 A가 $(\alpha^{y} v_A^{c} x)^{s_A} \equiv X \pmod p$와 $\alpha^{s_A} \equiv v_A \pmod p$를 만족하는 이산대수 sA를 알고 있다는 사실을 확인할 수 있게 되며, 서명자 A의 서명 (x, X, y)가 정당한 서명임을 확인할 수 있다. 그러나 확인 프로토콜이 실패한다면 즉, 단계 ⑤의 테스트를 통과하지 못한다면 다음의 두 가지 가능성을 생각할 수 있다. 즉, (x, X, y)가 m에 대한 유효한 서명이 아니거나 유효한 서명인데도 서명자가 이를 부인하려고 하는 경우이다. 이 두 가능성은 후술하는 부인 프로토콜에 의해 구분 가능하다.

위에서 기술한 확인 프로토콜은 수신자 지정 서명 방식의 "제3자에 대한 대화형 증명 프로토콜"과 마찬가지로 증명자와의 대화 없이도 통신내용들을 simulation하는 것이 가능하며 또한 비밀키를 모르는 제3자가 테스트를 통과할 확률은 기껏해야 1/q로 랜덤하게 추측하는 방법뿐이다.

[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 확인자는 임의의 랜덤수 $b \in_R Z_q$와 검증수 $a \in_R \{0, \cdots, k-1\}$를 선택해서 $ch_1 \equiv (\alpha^{y} v_A^{c} x)^{a} \alpha^{b} \pmod p$와 $ch_2 \equiv X^{a} v_A^{b} \bmod p$를 계산하여 ($ch_1$, ch_2)를 증명자 A에게 전송한다.

② 증명자 A는 $ch_1^{s_A}/ch_2$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 확인자에게 전송한다.[15]

[a를 구하는 계산]

$ch_1^{s_A} \equiv ((\alpha^{y} v_A^{c} x)^{a} \alpha^{b})^{s_A} \pmod p$ 이므로 $ch_1^{s_A}/ch_2 = ((\alpha^{y} v_A^{c} x)^{s_A}/X)^{a} \pmod p$ 이다. 그런데, 증명자는 $(\alpha^{y} v_A^{c} x)^{s_A}$를 알고 있으므로, a값을 구하기 위해 $a = 0, 1, \cdots, k-1$를 식 $((\alpha^{y} v_A^{c} x)^{s_A}/X)^{a} = ch_1^{s_A}/ch_2 \pmod p$가 만족될 때까지 대입한다(trial and error). 이때 위 식을 만족하는 값이 a값이다.

③ 확인자는 자신이 선택한 랜덤수 b를 증명자 A에

게 전송한다.

④ 증명자 A는 이 b가 $ch_1 \equiv (\alpha^y v_A^e x)^a \alpha^b \pmod p$, $ch_2 \equiv X^a v_A{}^b \pmod p$를 만족하는지 조사하여 이를 만족한다면 단계 ②에서 사용한 랜덤수 r을 전송한다. 이를 만족하지 않는다는 것은 확인자가 프로토콜을 따르지 않는다는 사실을 의미하므로 프로토콜을 중단한다.

⑤ 확인자는 증명자 A가 계산한 a값과 확인자 B가 선택한 랜덤수 a를 비교하여 서명의 정당성을 확인한다.

위 프로토콜의 단계 ②에서 증명자가 a를 결정할 수 있는 것은 $\log_{(\alpha^y v_A^e x)} X \neq \log_\alpha v_A$인 경우이다. 만일 $\log_{(\alpha^y v_A^e x)} X = \log_\alpha v_A$가 성립한다면 결국 $ch_2 \equiv ch_1^{s_A} \pmod p$ 이므로 이같은 경우는 증명자의 계산능력에 관계없이 정보 이론적으로 ch_1, ch_2는 a에 대한 정보를 전혀 제공하지 않기 때문이다. 따라서 단계 ⑤의 테스트를 통과한다면 그 서명은 증명자의 유효한 서명이 아니라는 사실이 증명되는 것이므로 확인 프로토콜의 실패시의 두 가능성을 구분할 수 있다. 파라미터 k가 커지면 단계 ②에서 증명자의 계산량이 k에 비례하여 증가하므로 k를 임의로 크게 잡는 것은 불가능하며 실제로 약 1024정도가 적절하다. k = 1024로 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.

3.2 (selectively) convertible한 부인 방지 서명방식

J. Boyar 등은 부인 방지 서명방식을 비밀키의 일부를 노출시킴으로써 특정한 서명만 선택적으로 혹은 전체 서명을 모두 일반적인 서명으로 변환시킬 수 있는 (selectively) convertible한 부인 방지 서명방식을 제안하였다.[12]

이 절에서는 통합 서명방식에서 사용되는 공개키를 랜덤화 함으로써 (selectively) convertible한 부인 방지 서명방식을 구성할 수 있음을 보인다. 제안한 서명방식은 두 개의 공개키를 이용하여 ElGamal의 서명으로 구성한 기존의 방식에 비해 단 하나의 공개키만으로 같은 기능의 서명을 구현할 수 있으므로 보다 효율적이라 할 수 있다.

[서명 생성 과정]

① 서명자 A는 메세지 m을 k_{seed}를 비밀키로 하는 해쉬 알고리즘 f로 압축하여 $s_{any} = f_{k_{seed}}(m) \in [1, q)$를 구한 후, 랜덤수 r, $R \in_R [1, q)$를 선택하여 $v_{any} \equiv \alpha^{s_{any}} \pmod p$, $x \equiv \alpha^{R-r} \pmod p$, $X \equiv v_{any}^R \pmod p$를 계산한다.

② 다음으로 $e = h(v_{any}, x, X, m)$를 계산하고 $y \equiv r - s_A e \pmod q$를 구하면 (v_{any}, x, X, y)가 메세지 m에 대한 서명이 된다.

여기서 $(\alpha^y v_A^e x)^{s_{any}} \equiv X \pmod p$를 만족하는 s_{any}는 서명자 A만이 알고 있으며 그 외의 어떤 제3자도 (v_{any}, x, X, y)와 메세지 m으로부터 서명의 진위 여부를 판별할 수는 없으므로, 서명자는 서명의 사본들이 남용되는 것을 막을 수 있다.

[확인/부인 프로토콜]

부인 방지 서명방식에서의 확인/부인 프로토콜과 동일하다. 즉, 서명자 A는 $(\alpha^y v_A^e x)^{s_{any}} \equiv X \pmod p$와 $\alpha^{s_{any}} \equiv v_{any} \pmod p$를 만족하는 이산대수 s_{any}를 알고 있는지의 여부를 확인/부인 프로토콜을 통하여 증명한다.

여기서 만일 s_{any}를 공개한다면 이 s_{any}에 대응하는 하나의 메세지에 대한 서명은 보통의 디지틀 서명으로 바뀌어짐을 쉽게 알 수 있다(selectively convertible).

[Selective conversion]

① 서명자 A는 메세지 m에 대응하는 s_{any}를 공개한다.

② 이를 받은 수신자는 $h(v_{any}, x, X, m) = e$와 $(\alpha^y v_A^e x)^{s_{any}} \equiv X \pmod p$를 만족하는지 검사함으로써 메세지 m에 대한 서명을 확인할 수 있다.

한편 해쉬 알고리즘 f의 비밀키 k_{seed} 자체를 공개한다면 임의의 메세지에 대한 서명에 대해서도 $s_{any} = f_{k_{seed}}(m)$과 같이 누구나 sany를 계산할 수 있으므로 이 때까지 발행된 모든 부인 방지 서명방식을 보통의 디지틀 서명으로 변환시킬 수 있다(convertible). 따라서 두개의 공개키를 이용하여 ElGamal의 서명으로 구성한 J. Boyar 등의 selectively convertible한 부인 방지 서명방식에 비해 단 하나의 공개키만으로 같은 기능의 서명을 구현할 수 있으므로 보다 효율적이라 할

수 있다.

[Conversion of all signatures]

① 서명자 A는 f의 비밀키 k_{seed}를 공개한다.

② 이를 받은 수신자는 $s_{any}=f_{k_{seed}}(m)$와 $e=h(v_{any}, x, X, m)$를 계산한 후, $(\alpha^{y}v_{A}^{e}x)^{s_{any}} \equiv X \pmod p$를 만족하는지 검사함으로써 임의의 메세지 m에 대한 서명을 확인할 수 있다.

Ⅳ. 결 론

D. Chaum은 서명의 사본만으로는 서명의 정당성을 확인할 수 없고 서명의 확인을 위해서는 서명자의 도움을 받아야 하는 부인 방지 서명방식을 제안하였으며, J. Boyar 등은 Chaum의 부인 방지 서명방식을 변형하여 특정한 서명만 선택적으로 혹은 전체 서명을 모두 일반적인 서명으로 변환시킬 수 있는 (selectively) convertible한 부인 방지 서명방식을 제안하였다.

또한 김승주외 2인은 서명의 인증시에 특정 수신자만이 서명을 확인할 수 있도록 하되, 만일 그 서명이 문제가 되는 경우라도 수신자의 비밀키를 노출시키지 않고 제3자에게 서명의 출처를 증명함으로써 수신자가 자신에게 발행된 서명을 통제할 수 있는 수신자 지정 서명방식을 제안하였다.

본 논문에서는 기존에 제안된 수신자를 지정할 수 있는 "수신자 지정 서명방식"과, 서명자의 도움을 받아야만 검증이 가능한 "부인 방지 서명방식", 또한 선택적으로 혹은 전체 서명을 모두 일반적인 서명으로 변환시킬 수 있는 "(selectively) convertible한 부인 방지 서명방식"을 하나로 통합한 통합 서명방식을 제안하였다.

통합 서명방식은 사용되는 공개키로 수신자의 공개키 또는 서명자의 공개키를 선택함으로써 수신자 지정 서명방식 또는 부인 방지 서명방식으로 변환될 수 있다. 또한 통합 서명방식에서 사용되는 공개키를 랜덤화 함으로써 (selectively) convertible한 부인 방지 서명방식도 구성할 수 있다.

부인 방지 서명방식, (selectively) convertible한 부인 방지 서명방식, 수신자 지정 서명 방식을 하나로 통합한 "통합 서명방식"은 시스템 구현 측면과 연산량에서 보다 효율적이다.

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. T. Elgamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Transactions on Information Theory 31, pp. 469-472, 1985.
4. C. P. Schnorr, "Efficient Signature Generation for Smart Cards", Advances in Cryptology-CRYPTO '89 Proceedings, Berlin: Springer-Verlag, pp. 239-252, 1990.
5. C. P. Schnorr, "Efficient Signature Generation for Smart Cards", Journal of Cryptology. v.4, n.3, pp. 161-174, 1991.
6. A. Shamir, "Identity-Based Cryptosystems and Signature Schemes", Crypto'84, pp. 47-53, 1985.
7. A. Fiat and A. Shamir, "How to Prove Yourself: Practical Solution to Identification and Signature Problem", Crypto'86, pp. 186-194, 1987.
8. L. C. Guillou, J. J. Quisquater, "A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing both Transmission and Memory", EUROCRYPT'88, pp. 123-128, 1998.
9. L. C. Guillou, J. J. Quisquater, "A Paradoxical Identity-Based Signature Scheme Resulting from Zero-Knowledge" CRYPTO'88, pp. 216-231. 1988.
10. D. Chaum and H. Antwerpen, "Undeniable signature", Proc. Crypto'89, pp. 212-216.
11. D. Chaum, "Zero-knowledge undeniable signature", Proc. Eurocrypt'90, pp. 458-464.
12. J. Boyar, D. Chaum, and I. Damgard, "Convertible undeniable signature", Proc. Crypto'90, pp. 195-208.
13. D. Chaum, "Designated Confirmer Signatures", Proc. of Eurocrypt '94, LNCS, Springer-Verlag,

pp. 95-101.
14. T. Okamato and K. Ohta, "How to utilize the randomness of zero-knowledge proofs", Proc. Crypto'90, pp. 437-456.
15. G. Brassard, D. Chaum and C. Crepeau, "Minimum Disclosure Proofs of Knowledge", in Journal of Computer and System Science, Vol. 37 No. 2, October 1988, pp. 156-189.
16. S. J. Park, K. H. Lee and D. H. Won, "An Entrusted Undeniable Signature", Proc. JW-ISC'95, 1995. 1.
17. S. J. Kim, S. J. Park and D. H. Won, "Nominative Signatures", Proc. ICEIC'95, pp. II-68~II-71, 1995.
18. S. J. Kim, S. J. Park and D. H. Won, "Zero-Knowledge Nominative Signatures", Proc. Pragocrypt'96. 1996.
19. 박성준, 이보영, 원동호, "의뢰 Undeniable Signature", 한국통신학회 학술 발표회 논문집, pp. 47-49, 1994. 7.
20. 박성준, 이보영, 원동호, "의뢰 부인방지 서명에 관한 연구", 한국통신학회 논문지 제20권 제6호, pp. 1649-1656, 1995.
21. 김승주, 박성준, 원동호, "수신자 지정 서명방식에 대한 고찰", 한국정보처리응용학회 학술발표논문집 제1권 제2호, pp. 530-533, 1994.
22. 김승주, 박성준, 원동호, "수신자 지정 서명방식", 통신정보보호학회 학술발표논문집 Vol. 4 No. 1 pp. 24-28, 1994.
23. 김승주, 박성준, 원동호, "효율적인 수신자 지정 서명방식", 대한전자공학회 학술발표논문집 Vol. 18 No. 1 pp. 222-224, 1995.
24. 김승주, 김경신, 박성준, 원동호, "영지식 수신자 지정 서명방식", 통신정보보호학회 논문지 제6권 제1호, pp. 15-24, 1996. 3.

김 승 주(Seung Joo 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

박 성 준(Sung Jun Park) 정회원
1960년 10월 29일생
1983년 2월 : 한양대학교 수학과 졸업(이학사)
1985년 2월 : 한양대학교 대학원 수학과 졸업(이학석사)
1985년 1월~1994년 3월 : 한국전자통신연구소 부호기술부 선임연구원
1992년 3월~1996년 2월 : 성균관대학교 대학원 정보공학과 졸업(공학박사)
1996년 4월~현재 : 한국정보보호센터 연구개발부 책임연구원
※주관심분야 : 암호이론, 계산이론, 정보이론

원 동 호(Dong Ho 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
1991년~현재 : 한국통신정보보호학회 편집이사
1996년 4월~현재 : 정보화추진위원회 자문위원
※주관심분야 : 암호이론, 정보이론