通信情報保護學會論文誌
第 8 卷 第 4 號, 1998. 12

효율적인 검증가능 위탁 서명과 그 응용

박 상 준*, 박 성 모*, 원 동 호**, 김 대 호*

An Efficient Verifiable Escrowed Signature and Its Applications

Sang joon Park*, sung mo Park*, Dong Ho Won**, Dea Ho Kim*

요 약

최근의 공정한 정보 교환 프로토콜 연구에서는 중재자를 이용하지만 통신 쌍방 사이에 분쟁이 발생하는 경우에만 중재자가 개입하는 방법으로 중재자의 역할을 최소화시키고 있다. Mao는 공정한 정보 교환 프로토콜에 응용 가능한 검증가능 위탁 서명이라는 새로운 서명 개념을 제안하였다. 그러나, Mao의 방식은 Stadler의 이산로그에 대한 검증가능 암호 기법을 이용하기 때문에 통신량과 계산복잡도가 매우 높다. 본 논문에서는 제곱근에 대한 검증가능 암호와 검증가능 암호를 이용한 검증가능 위탁 서명 방식을 제안하였다. 제안된 검증가능 위탁 서명 방식은 통신량이 적고 계산 효율성이 높은 장점이 있으나 위탁 기관을 단 하나밖에 허락하지 않는 단점이 있다. 또한, 본 논문에서는 제안된 검증가능 위탁 서명 방식의 응용으로 공정한 전자 계약 프로토콜과 공정한 전자 등기 우편 프로토콜을 함께 제안하였다.

Abstract

Mao proposed the new concept of verifiable escrowed signature that can be applied to fair exchange protocols. But, since Mao's scheme uses the verifiable encryption of discrete logarihtm which was proposed by Stadler, the complexites of communications and computations are very high. In this paper, we propose a verifiable encryption of square root and an efficient verifiable escrowed signature. The proposed verifiable escrowed signature is more efficient than Mao's one. As applications of a verifiable encryption and a verifiable escrowed signature, we propose fair contract signing protocol and fair certified mail protocol.

* 한국전자통신연구원
** 성균관대학교 정보공학과

1. 서 론

통신 단말기 보급과 전산망의 발전으로 기존의 종이로 작성된 각종 서류들이 전자 문서 형태로 보관되고 유통된다. 인터넷의 발전은 전자 정보의 단순 유통 뿐 아니라 구매자와 생산자를 연결시켜 전산망을 통한 상거래도 가능하게 하였다. 그러나, 전산망을 이용한 계약, 구매 입찰, 상품 구매, 전자 등기 우편등의 업무에서 쌍방간에 안전하고 신뢰성 있는 거래가 이루어지기 위해서는 정보를 동시에 교환하는 동시성이 보장되어야 한다.

공정한 정보의 교환을 성립시키기 위해서 가장 쉽게 접근할 수 있는 방법은 중간에 신뢰할 수 있는 중재자를 놓고, 중재자를 통하여 정보를 교환하는 방법이 있다[1]. 그러나, 이러한 방법은 통신 쌍방이 모든 정보를 중재자를 통해서 교환하여야 하기 때문에 시스템 사용자가 증가할 경우 중재자의 부담이 클 뿐 아니라, 프로토콜의 안전성이 중재자의 신뢰성에 전적으로 의존하는 단점이 있다.

중재자를 이용하는 방식에서 중재자에게 걸리는 과부하 문제를 해결하고, 전자 계약 프로토콜에서의 동시성 문제를 해결하기 위하여 여러 종류의 암호 프로토콜이 제안되었다[2][3][4][5][6]. 그러나 이러한 방식은 쌍방간에 너무 많은 송·수신 트랜잭션이 일어날 뿐 아니라 각 트랜잭션에서 많은 계산량을 요구하기 때문에 현재의 인터넷 환경에서 사용하기에는 부적절하다.

중재자를 이용하는 방식과 암호 프로토콜을 이용하는 방식의 단점을 보완하기 위하여 최근에는 중재자를 이용하기는 하지만 중재자의 역할을 최소화하는 방법에 대하여 연구되고 있다[7][9][8].

통신 쌍방은 중재자를 통하지 않고 정보를 교환하지만, 양쪽중 어느 한쪽이 비정상적으로 프로토콜을 진행하는 경우에만 중재 기관이 개입하여 분쟁을 해결한다. 이러한 방식에서도 신뢰성 있는 중재 기관이 필요하지만 중재 기관은 분쟁이 발생하는 경우에만 개입하기 때문에 역할을 최소화할 수 있다.

Mao[10]는 공정한 정보 교환 프로토콜에서 효과적으로 사용될 수 있는 검증가능 위탁 서명이라는 개념을 제안하였다. 검증가능 위탁 서명이란 서명의 송신자가 자신의 서명을 직접 서명 수신자에게 주지않고, 중재자의 공개키로 암호화시켜 수신자에게 제공한다. 이때 서명자는 수신자에게 암호문이 자신이 만든 서명의 암호문이 됨을 증명한다. 따라서 분쟁이 발생하는 경우 수신자는 중재자에게 암호문을 복호시켜줄 것을 요구하여 서명을 얻을 수 있다. Mao는 Stadler[11]의 이산 로그를 이용하는 검증가능 암호(Verifiable Encryption)를 사용하여 검증가능 위탁 서명(Verifiable Escrowed Signature)을 실현하였다. 그러나 이산 로그를 이용하는 검증가능 암호는 계산 복잡도와 통신해야 하는 정보의 양이 너무 많기 때문에 현실적이지 못하다.

본 논문에서는 제곱근에 대한 검증가능 암호를 제안하고, 제안된 검증가능 암호를 사용하여 검증가능 위탁 서명을 제안하고자 한다.

제안 방식에서는 Rabin 암호 시스템[12]의 합성수 n의 소인수를 알고 있는 중재 기관(위탁 기관)만이 검증가능 암호문으로 부터 서명(또는 평문)을 구할 수 있다. 제안 방식은 Mao의 방식 보다 통신량과 계산량이 적으나 Rabin 암호 시스템 합성수 n의 소인수를 알고 있는 하나의 위탁 기관만을 허락한다. 또한, 본 논문에서는 검증가능 암호와 검증가능 위탁 서명 방식의 응용으로 공정한 전자 계약 프로토콜과 공정한 전자등기우편 프로토콜을 함께 제안함으로서 공정한 전자 교환 서비스에서 검증가능 암호와 검증가능 위탁 서명 방식이 응용될 수 있음을 보이고자 한다.

본 논문은 모두 5개 절로 구성된다. 2절에서는 제곱근에 대한 새로운 검증가능 암호 방식을 제안하고, 제안된 검증가능 암호 방식을 이용하여 검증가능 위탁 서명 방식을 제안하였다. 3절과 4절에서는 제안된 방식의 응용으로서 공정한 전자 계약 프로토콜과 공정한 전자등기우편 프로토콜을 제안한다. 5절은 결론부이다.

2. 검증가능 암호와 검증가능 위탁 서명

Mao의 방식은 Stadler의 검증가능 암호중에서 이산 로그에 대한 검증가능 암호를 사용한다. 그러나, 이산 로그에 대한 검증가능 암호는 전송해야할 정보량이 매우 많을 뿐 아니라 서명자와 수신자가 서명의 정당성을 증명하는 과정과 서명을 검증하는 과정에서 너무 많은 계산량을 요구하기 때문에 현실적으로 실현하기 어려운 면이 있다.

본 절에서는 제곱근에 대한 검증가능 암호와 검증가능 위탁 서명을 제안하고자 한다. 제안된 검증가능 암호는 Stadler의 이산 로그에 대한 검증가능 암호와 비교하였을 때 계산량과 통신량이 매우 적어 구현이 용이하다.

검증가능 암호는 Rabin 암호와 ElGamal 암호[13]의 결합으로 구성되며, 검증가능 위탁 서명에서는 Schnorr 서명[14]을 제안된 검증가능 암호 방식으로 암호화한다. 이때, Rabin 암호 시스템 합성수 n의 소인수를 알고 있는 신뢰성 있는 위탁 기관(또는 중재 기관)은 암호문으로 부터 서명을 구할 수 있다. 따라서, 위탁 기관이 합성수 n의 소인수를 알고 있는 하나의 기관으로 제한되는 단점이 있다.

2.1 효율적인 검증가능 암호

위탁 기관은 Rabin 암호 시스템을 위한 합성수 $n = p \cdot q$(p, q는 소수)와 소수 $Q = 2 \cdot n + 1$을 생성한다. 또한, 위수 n을 갖는 $GF(Q)$의 생성원 g를 생성한다($g^n = 1 \pmod{Q}$). 이때, g의 Jacobi 심볼은 1이된다($J(g/Q) = 1$). n, Q, g를 시스템의 공개된 공통 인수로 공개하고, p, q는 위탁 기관의 비밀 정보로 보관한다. 임의의 메시지 $0 < m < n$에 대한 검증가능 암호문을 만드는 과정은 다음과 같다.

(1) $V = g^m \pmod{Q}$

(2) 메시지 m에 대한 Rabin 암호 : $c = m^2 \pmod{n}$

(3) $r_1 = g^k \pmod{Q}$, $r_2 = (g^m)^k \pmod{Q}$ ($k \in Z_n$은 난수)

(4) $c' = m \cdot h(r_1, r_2, V, c) + k \pmod{n}$

(5) (r_1, r_2, V, c, c')을 m의 검증가능 암호문으로 수신자에게 보낸다.

c는 메시지 m에 대한 Rabin 암호시스템의 암호문이다. 수신자는 위탁 기관의 비밀키 p, q를 알 지 못하기 때문에 암호문 c로부터 m를 구할 수 없다. 그러나, c가 메시지 m의 제곱이라는 사실을 다음과 같은 방법으로 검증할 수 있다.

(1) V, r_1, r_2의 Jacobi 심볼이 1이 되는지 체크한다.

$$J(r_1/Q) = J(r_2/Q) = J(V/Q) = 1$$

(2) 다음 관계식을 확인하여 만족하면 (r_1, r_2, V, c, c')를 m에 대한 검증가능 암호문으로 받아들인다.

$$g^{c'} \stackrel{?}{=} V^{h(r_1, r_2, V, c)} \cdot r_1 \pmod{Q},$$
$$V^{c'} \stackrel{?}{=} (g^c)^{h(r_1, r_2, V, c)} \cdot r_2 \pmod{Q}$$

위탁 기관은 소수 p, q를 알고 있기 때문에 암호문 c로부터 4개의 제곱근을 구할 수 있다. $V = g^m \pmod{Q}$이므로 4개의 제곱근을 $\alpha_0, \alpha_1, \alpha_2, \alpha_3$라 하면 $V = g^\alpha \pmod{Q}$를 만족하는 하나의 α가 존재한다. 따라서, 위탁 기관은 평문 $m (=\alpha)$을 결정할 수 있다.

2.2 효율적인 검증가능 위탁 서명

p, q, Q, n, g는 검증가능 암호와 같다. 서명자는 비밀키 $0 < x < n$와 공개키 $y = g^x \pmod{Q}$를 갖는다. 서명자가 메시지 m에 대한 검증가능 위탁 서명을 만드는 과정은 다음과 같다.

(1)메시지 m에 대한 Schnorr 서명

$$r = g^k \pmod{Q}, s = x \cdot e + k \pmod{n}$$
$$(k \in Z_n \text{는 난수}, e = h(m, r))$$

(2) 서명 s에 대한 Rabin 암호 : $c = s^2 \pmod n$

(3) $r_1 = g^{k'} \pmod Q$, $r_2 = (g^s)^{k'} \pmod Q$ ($k' \in Z_n$은 난수)

(4) $c' = s \cdot h(r_1, r_2, c, e) + k' \pmod n$

(5) 검증가능 위탁 서명 (r, r_1, r_2, c, c')을 수신자에게 보낸다.

(r, r_1, r_2, c, c')는 Schnorr 서명 s의 검증가능 암호이고 c는 s에 대한 Rabin 암호문이다. 따라서, 서명 수신자는 위탁 기관의 비밀키 p, q를 모르기 때문에 암호문 c로부터 서명 s를 구할 수 없다. 그러나, 서명 수신자는 c가 서명 s의 제곱이라는 사실을 다음과 같은 방법으로 검증할 수 있다.

(1) r, r_1, r_2의 Jacobi 심볼이 1이 되는지 체크한다.

$$J(r/Q) = J(r_1/Q) = J(r_2/Q) = 1$$

(2) $e = h(m, r)$, $V = y^e \cdot r \pmod Q$ 계산

(3) 다음 관계식을 확인하여 만족하면 (r, r_1, r_2, c, c')을 검증가능 위탁 서명으로 받아들인다.

$$g^{c'} \stackrel{?}{=} V^{h(r_1, r_2, c, e)} \cdot r_1 \pmod Q,$$
$$V^{c'} \stackrel{?}{=} (g^{c'})^{h(r_1, r_2, c, e)} \cdot r_2 \pmod Q$$

위탁 기관은 소수 p, q를 알고 있기 때문에 암호문 c로부터 4개 제곱근을 구할 수 있다. 4개의 제곱근 중에서 $g^s = y^e \cdot r \pmod Q$을 만족하는 서명 s를 결정할 수 있다.

제안된 방식은 검증가능 위탁 서명 방식을 처음 제안한 Mao의 방식에 비하여 계산량이 매우 적다. 각 과정에서 요구되는 계산량은 다음과 같다.

- 서명 과정 : 지수승 3번, 곱셈 2번, 덧셈 2번
- 검증 과정 : Jacobi 심볼 계산 3번, 지수승 5번, 곱셈 3번
- 전송 데이터의 양 : $5|n| + 3$ 비트

2.3 안전성

g, Q, n의 정의에 의하여, $\{a | J(a/Q) = 1\} = \{g^i \pmod Q | 0 \le i < n\}$이고 집합 $\{a | J(a/Q) = 1\}$의 원소 개수는 n이 된다. $y = g^x \bmod Q$라 하면 $J(y/Q) = 1$이 된다.

정리 1 $V = y^{h(m, r)} \cdot r \pmod Q$이고 $J(r/Q) = 1$라 하면, $V = g^s \pmod Q$인 *Schnorr* 서명 s가 유일하게 존재한다.

(증명) $J(r/Q) = J(y/Q) = 1$이므로, $J(V/Q) = 1$. 그러므로, $y = g^x \pmod Q$, $r = g^k \pmod Q$이고 $V = g^s \pmod Q$인 유일한 x, k, s가 존재하므로, $s = x \cdot h(m, r) + k \pmod n$이 된다.

정리 2 $V = g^s \pmod Q$이고 $J(r_1/Q) = J(r_2/Q) = 1$라 하자. 만일 $g^{c'} = V^{h(r_1, r_2, c, e)} \cdot r_1 \pmod Q$이고 $V^{c'} = (g^{c'})^{h(r_1, r_2, c, e)} \cdot r_2 \pmod Q$이면, $c = s^2 \pmod n$이다.

(증명) $J(r_1/Q) = J(r_2/Q) = 1$이므로 $r_1 = g^{k_1} \pmod Q$이고 $r_2 = g^{k_2} \pmod Q$을 만족하는 k_1, k_2가 존재한다. 그러므로, $c' = s \cdot h(r_1, r_2, c, e) + k_1 \pmod n$이고 $s \cdot c' = c \cdot h(r_1, r_2, c, e) + k_2 \pmod n$이다. 그러면, $h(r_1, r_2, c, e)(c - s^2) + k_2 - sk_1 = 0 \pmod n$이다. 왜냐하면 $h(\cdot)$은 랜덤하므로, $h(r_1, r_2, c, e)$ 값에 관계없이 앞의 등식이 성립한다. 따라서, $c = s_2 \pmod n$이고 $k_2 = s \cdot k_1 \pmod n$이다.

유사하게, 검증가능 암호에서도 다음 정리가 성립한다.

정리 3 $J(r_1/Q) = J(r_2/Q) = J(V/Q) = 1$라 하자. 만일 $g^{c'} = V^{h(r_1, r_2, c, e)} \cdot r_1 \pmod Q$이고 $V^{c'} = (g^{c'})^{h(r_1, r_2, c, e)} \cdot r_2 \pmod Q$이면, $V = g^m \pmod Q$인 $0 < m < n$이 존재하고 $c = m^2 \pmod n$이다.

정리 1, 2는 $V = y^{h(m, r)} \cdot r \pmod Q$의 이산 로그가 m의 서명이면서 동시에 c의 제곱근이됨을 보여준다. 수신자가 서명 s를 계산하는 것은 n에 대

한 인수분해와 V의 이산 로그를 계산하는 문제에 달려있기 때문에 계산상 불가능하다. 또한, 위탁 기관을 포함하여 어느 누구도 위탁 서명을 계산하지 못한다. 정리에 의하여 검증 과정을 만족시키는 값 V는 유일하게 결정되며 V의 이산 로그는 c의 제곱근이 된다. 그러므로, 만일 위탁 기관이 위탁 서명을 계산할 수 있다면 서명자의 비밀키 x를 모르고서도 c로 부터 Schnorr 서명 s를 얻을 수 있게된다. 그러나 이것은 현재까지 Schnorr 서명 방식이 안전하다고 알려진 사실과 모순된다.

3. 공정한 전자 계약 프로토콜

본 절에서는 제안된 검증가능 위탁 서명 방식을 사용한 전자 계약 프로토콜을 제안하고자 한다. 전자 계약 프로토콜은 분쟁 발생시 분쟁을 조정하는 중재자(또는 위탁 기관, 신뢰 기관), 계약을 체결하는 계약자 A, 계약자 B로 구성된다. 중재자는 계약자 A와 B가 신뢰하는 신뢰 기관으로서, 제안된 검증가능 위탁 서명 방식에서 필요한 시스템 변수 p, q, n, Q, g를 생성한다.

3.1 계약 프로토콜

VES_A, VES_B는 각각 A, B의 검증가능 위탁 서명으로서, 서명의 형태는 2절에서 제안된 검증가능 위탁 서명과 같다.

- Org : 프로토콜에서 메시지 m에 대한 서명 정보를 먼저 보내는 계약자 A

  (비밀키 : $0 < x_A < n$, 공개키 : $y_A = g^{x_A} \bmod Q$)
- Rec : Org의 서명을 받는 계약자 B

  (비밀키 : $0 < x_B < n$, 공개키 : $y_B = g^{x_B} \bmod Q$)
- $VES_A = (r_A, r_{A1}, r_{A2}, c_A, c'_A)$: 메시지 m에 대한 검증가능 위탁 서명으로 c_A, c_A'은 다음과 같다.

  $r_A = g^{k_A} \bmod Q$, $e = h(A, Org, r_A, m)$

  $s_A = x_A \cdot e + k_A \bmod n$

  $r_{A1} = g^{k'} \bmod Q$, $r_{A2} = (g^{x_A})^{k'} \bmod Q$

  $c_A = s^{x_A} \bmod n$, $c'_A = s_A \cdot h(r_{A1}, r_{A2}, c_A, e) + k'_A \bmod n$

  (r_A, s_A) : (A, Org, m)에 대한 A의 Schnorr 서명
- $VES_B = (r_B, r_{B1}, r_{B2}, c_B, c'_B)$: m과 VES_A에 대한 검증가능 위탁 서명으로 c_B, c'_B은 다음과 같다.

  $r_B = g^{k_B} \bmod Q$, $e = h(B, Rec, r_B, m, VES_A)$

  $s_B = x_B \cdot e + k_B \bmod n$

  $r_{B1} = g^{k_B} \bmod Q$, $r_{B2} = (g^{x_B})^{k'} \bmod Q$

  $c_B = s^{x_B} \bmod n$, $c'_B = s_B \cdot h(r_{B1}, r_{B2}, c_B, e) + k'_B \bmod n$

  (r_B, s_B) : (B, Rec, m, VES_B)에 대한 B의 Schnorr 서명

계약자 A, B가 계약 내용 m에 서로 합의하였다고 하자. 이제 A와 B는 메시지 m에 대한 서로의 서명을 공정하게 교환하기 위하여 다음과 같이 계약 프로토콜을 구성한다.

- 단계 1 : 계약자(Originator) A
  (1) 메시지 m에 대한 검증가능 위탁 서명 VES_A를 생성한다.
  (2) (A, Org, m, VES_A)을 수신자 B에게 전송한다.
- 단계 2: 계약자(Recipient) B
  (1) VES_A가 메시지 m의 검증가능 위탁 서명임을 확인하여 A의 검증가능 위탁 서명이 아니면 프로토콜은 분쟁없이 중단된다.
  (2) 메시지 m과 VES_A에 대한 B의 검증가능 위탁 서명 VES_B를 계산한다.
  (3) (B, Rec, VES_B)를 A에게 전송한다.
- 단계 3 :계약자 A
  (1) VES_B가 m과 VES_A에 대한 검증가능 위탁 서명임을 확인하여 B의 검증가능 위탁 서명이 아니면 프로토콜은 분쟁없이 중단된다. 이 경우, A는 B의 검증가능 위탁 서명 VES_B를 얻을 수 없으나, B는 A의 검증가능 위탁 서명 VES_A를 갖게된다. 그러나,

VES_A 만으로는 계약의 실효성을 얻지 못한다.

(2) 검증이 성공하면, 메시지 m에 대한 일반 서명 s_A를 B에게 전송한다.

• 단계 4 : 계약자 B

(1) 메시지 m에 대한 일반 서명 s_A를 검증한다 ($g^{s_A} = y_A^{r_A} \cdot k_A \bmod Q$). 서명 검증에 실패하면 서명의 재전송을 요구한다. 만일, A가 서명 s_A를 보내주지 않으면 B는 중재자에게 (A, Org, m, VES_A)와 (B, Rec, m, VES_B)를 전송하고 중재를 요청한다.

(2) 서명 s_A에 대한 검증이 성공하면 메시지 m에 대한 자신의 서명 s_B를 A에게 전송한다.

• 단계 5: 계약자 A

(1) 메시지 m에 대한 일반 서명 s_B를 검증한다 ($g^{s_B} = y_B^{r_B} \cdot k_B \bmod Q$). 서명 검증에 실패하면 서명의 재전송을 요구한다. 만일, B가 서명 s_B를 보내주지 않으면 A는 중재자에게 (A, Org, m, VES_A)와 (B, Rec, m, VES_B)를 전송하고 중재를 요청한다.

(2) S_B의 검증에 성공하면 A와 B의 m에 대한 계약이 성사된다.

제안된 프로토콜에서 A와 B가 계약 내용을 제3자에게 증명하기 위해서는 메시지 m에 대한 일반 서명 s_A, s_B를 가지고 있어야 한다. 따라서, 단계 1과 2에서 A와 B가 가지고 있는 검증가능 위탁 서명 VES_A와 VES_B는 분쟁이 발생하는 경우에 중재자가 이용하는 서명 정보이지 계약의 실효성을 제 3자에게 증명할 수 있는 서명 정보가 아니다.

3.2 중재 프로토콜

다음은 제안된 계약 프로토콜이 비정상적으로 중단되어 중재자에게 중재를 요청하였을 경우 중재자가 수행하는 중재 프로토콜이다.

• B에 의한 중재 요청

- 프로토콜

(1) B는 중재 요청시 (A, Org, B, Rec, m, VES_A, VES_B)를 중재자에게 전송한다.

(2) 중재자는 위탁서명 VES_A, VES_B를 검증한다.

(3) 중재자는 A가 VES_A, VES_B를 정당한 검증가능 위탁 서명으로 받아들이고 계약 체결을 원할 경우, VES_A, VES_B으로 부터 일반 서명 s_A, s_B를 계산하고, A에게는 s_B, B에게는 s_A를 전송한다. 반대로 A가 위탁 서명 VES_A, VES_B를 받아들이지 않으면 계약은 파기되고 중재자는 계약 무효 메시지 m_R를 A와 B에게 전송한다.

- 프로토콜에서 계약의 성사 여부는 A의 결정에 전적으로 의존하지만, 중재 요청 결과는 공정하게 처리된다.

- 단계 2에서 B가 중재 요청을 하는 경우 비록 A는 B로 부터 검증가능 위탁 서명 VES_B를 받지 못하였다 하여도 중재자를 통하여 VES_B를 받을 수 있으므로 A와 B는 동등한 위치에 놓이게 된다.

- 단계 4에서 B가 중재 요청하는 경우에는 B가 A로 부터 일반 서명 s_A를 받지 못하였기 때문에 중재자를 통하여 A가 계약을 성립시킬 의지가 있는지 확인할 수 있음을 의미한다.

• A에 의한 중재 요청

- 프로토콜

(1) A는 (A, Org, B, Rec, m, VES_A, VES_B)를 중재자에게 전송한다.

(2) 중재자는 위탁서명 VES_A, VES_B를 검증한다.

(3) 중재자는 A와 B중 어느 한쪽이 계약 성사를 원할 경우에 계약을 성사시킨다. 이때, 계약 성립의 증거로서 위탁 서명 VES_A, VES_B로 부터 일반 서명 s_A, s_B를 계산하고, A에게는 s_B, B에게는 s_A를 전송한다. 역으로, A와 B 모두 계약 철회를 요구할 경우에는 계약 무효 메시지 m_R를 A와 B에게 전송하여 계약이 파기되었음을 알린다.

- A가 중재를 요청하는 시기는 단계 3 또는 단

계 5에서 발생할 수 있다. 이 단계는 A와 B가 최소한 상대방의 검증가능 위탁 서명을 가지고 있는 상태이다. A와 B 중 어느 한쪽이 계약을 원할 경우 계약을 성사시키는 것이 공정하다.

- 단계 3에서 요청하는 경우는 A가 s_A를 B에게 주어 프로토콜을 정상적으로 진행시켜 B로 부터 s_B를 얻으려 하지 않고, 중재자에게 직접 s_B을 얻으려 하는 경우이다.
- 단계 5의 경우에는 B가 자신의 서명 S_B를 A에게 제공하지 않기 때문에 발생한다. 만일 B가 A의 일반 서명S_A를 갖고 있는 상태에서 중재자가 B의 계약 철회 요구를 받아들인다면 프로토콜은 공정하지 못하게 된다. 그러나, 제안된 프로토콜에서 A가 계약을 원할 경우 중재자로 부터 B의 일반 서명 s_B를 얻을 수 있으므로 프로토콜은 공정하다.
- 단계 5에서 A와 B가 모두 계약 파기를 원할 경우 B는 A의 서명 s_A를 가지나 A는 B의 서명 s_B를 얻지 못하는 경우가 발생할 수 있다. 그러나, A는 중재자로 부터 계약이 파기 되었다는 증거 m_R을 가지게 되므로 프로토콜의 공정성은 유지된다.

4. 공정한 전자 등기 우편

전자 등기 우편은 송신자가 메시지 m을 보내는 것과 함께 수신자가 메시지 m을 받았다는 영수증을 받아야 한다. 그러나 순차적으로 진행되는 통신 프로토콜에서 이러한 두가지 사건이 동시에 일어나는 것은 불가능하다. 메시지 수신자는 메시지 m을 받았음에도 불구하고 메시지를 받았다는 영수증을 송신자에게 주지 않을 수 있다. 이 경우 송신자는 메시지 m을 수신자에게 전달하였음에도 불구하고 제3자에게 이러한 사실을 증명하지 못한다.

따라서, 전자 등기 우편 프로토콜에서도 전자 계약 프로토콜에서와 같이 정보의 동시 교환에 관련된 문제가 발생하며, 이러한 문제를 해결하기 위하여 검증가능 암호와 검증가능 위탁 서명을 사용하고자 한다. 송신자는 평문 메시지 m을 보내는 대신 검증가능 암호문를 보냄으로서 수신자를 프로토콜에 계속 끌어들일 수 있으며, 수신자는 문제가 발생할 경우 검증가능 암호문을 중재자에게 제공함으로 평문을 얻을 수 있다.

4.1 전자 등기 우편 프로토콜

전자 등기 우편은 전자 계약 프로토콜과 유사하게 분쟁 발생시 분쟁을 조정하는 중재자, 메시지 송신자(Originator), 메시지 수신자(Recipient)로 구성된다. 메시지 송신자는 메시지 m을 DES와 같은 비밀키 암호 알고리즘(Secret Key Algorithm)을 사용하여 암호화한다. K를 비밀키 암호 알고리즘의 키라 하면, 송신자는 m 대신 K를 검증가능 암호화시킴으로서 계산 효율성을 증대시킬 수 있다.

다음은 전자 등기 우편 프로토콜에서 사용하는 주요 표기이다. A는 메시지 송신자(Org)이고, B는 메시지 수신자(Rec)이다. A, B가 사용하는 공개키와 비밀키는 검증가능 위탁 서명과 같다.

- $cp = E(K, m)$: 비밀키 암호 알고리즘에서 메시지 m을 키 K로 암호화하는 과정을 나타냄
- $m = D(K, cp)$: 비밀키 암호 알고리즘에서 암호문 cp를 키 K로 복호화하는 과정을 나타냄
- $VE_A = (r_{A1}, r_{A2}, V, c_A, c'_A)$: 키 K에 대한 검증가능 암호문이다.

  $V = g^K \bmod Q,\ c_A = K^e \bmod n$

  $r_{A1} = g^{k'_A} \bmod Q,\ r_{A2} = V^{k'_A} \bmod Q$

  $e = h(A, Org, r_{A1}, r_{A2}, V, c_A, cp),\ c'_A = K \cdot e + k_A \bmod n$
- (r'_A, s_A) : (A, Org, cp, VE_A)에 대한 A의 Schnorr 서명

  $r'_A = g^{k'_A} \bmod Q,\ e = h(A, Org, cp, VE_A, r'_A)$

  $s_A = x_A \cdot e + k'_A \bmod n$
- $VES_B = (r_B, r_{B1}, r_{B2}, c_B, c'_B)$: 메시지 m의 암호문 cp와 검증가능 암호문 VE_A를 받았음을 확인

하여 주는 영수증(검증가능 위탁서명)이다.

$$r_B = g^{KB} \bmod Q,\ e = h(B, Rec, r_B, cp, VE_A)$$
$$s_B = x_B \cdot e + k_B \bmod n$$
$$r_{B1} = g^{K'B} \bmod Q,\ r_{B2} = (g^{e})^{K'B} \bmod Q$$
$$c_B = s^{2}{}_B \bmod n,\ c'_B = s_B \cdot h(r_{B1}, r_{B2}, c_B, e) + K' \bmod n$$

- (r_B, s_B) : (B, Rec, cp, VEA)에 대한 B의 Schnorr 서명

다음은 메시지 송신자 A와 수신자 B가 진행하는 공정한 전자 등기 우편 프로토콜이다.

- 단계 1 : 송신자(Originator) A
  (1) 메시지 m을 비밀키 암호 알고리즘의 키 K로 암호화한다($cp = E(K, m)$).
  (2) 키 K와 암호문 cp에 대한 검증가능 암호 VE_A를 생성한다.
  (3) (A, Org, cp, VE_A)에 대한 A의 Schnorr 서명 (r_A', s_A)을 생성한다.
  (4) $(A, Org, cp, VE_A, r'_A, s_A)$을 수신자 B에게 전송한다.
- 단계 2: 수신자(Recipient) B
  (1) (A, Org, cp, VE_A)에 대한 A의 서명 (r'_A, s_A)를 검증한다.
  (2) VE_A가 V의 이산대수 K에 대한 검증가능 암호임을 확인하고 아니면 프로토콜은 분쟁 없이 중단된다.
  (3) 암호문 cp를 받았음을 확인할 수 있도록 cp와 VE_A에 대한 검증가능 위탁서명 VES_B를 계산한다.
  (4) (B, Rec, VES_B)를 A에게 전송한다.
- 단계 3 :송신자 A
  (1) VES_B가 cp, VE_A에 대한 검증가능 위탁서명이 아니면 프로토콜은 분쟁 없이 중단된다. 이 경우, A는 B의 검증가능 위탁서명 VES_B를 얻을 수 없으나, B는 A의 검증가능 암호문 VE_A를 갖게된다. VE_A만으로는 암호문 cp에 대응되는 키 K를 구할 수 없으므로 B는 메시지 m을 얻을 수 없다.
  (2) 검증에 성공하면, 암호키 K를 포함한 메시지 (A, Org, K)를 B에게 전송한다.
- 단계 4 : 수신자 B
  (1) $V \stackrel{?}{=} g^K \bmod Q,\ c_A \stackrel{?}{=} K^2 \bmod n$임을 확인하고, 만족하지 않으면 프로토콜을 중단하고 중재자에게 $(A, Org, cp, VE_A, r'_A, s_A)$와 (B, Rec, VES_B)를 보내어 중재를 요청한다.
  (2) (1)의 관계식이 만족되면, 암호문 cp을 복호하여 메시지 m을 얻는다($m = D(K, cp)$).
  (3) 암호문 cp, VE_A에 대한 Schnorr 서명 s_B를 A에게 보낸다.
- 단계 5: 송신자 A
  (1) cp, VE_A에 대한 Schnorr 서명 s_B를 검증한다 검증에 실패하면 A는 중재자에게 (A, Org, m, cp, VE_A)와 (B, Rec, VES_B)를 보내고 중재를 요청한다.
  (2) s_B의 검증에 성공하면 전자 등기 우편 프로토콜은 성공적으로 끝난다.

제안된 프로토콜을 성공적으로 마칠 경우 B는 메시지 m을 얻는다. 반면, A는 메시지 m의 암호문 cp, VE_A를 B가 받았다는 증거로서 서명 s_B를 얻을 수 있다. A는 서명 s_B가 메시지 m에 대한 서명이라는 사실을 K를 공개함으로서 증명할 수있다. 임의의 사용자는 서명 s_B가 평문 메시지 m의 암호문 cp에 대한 서명이라는 사실을 다음과 같이 검증할 수 있다.

$$e = h(B, Rec, r_B, cp, VE_A),\ g^{e} = y^{e}{}_B \cdot r_B \bmod Q$$
$$V = g^K,\ c_A = K^2 \bmod n,\ m = D(K, cp)$$

4.2 중재 프로토콜

제안된 전자 등기 우편 프로토콜이 비정상적으로 중단되어 중재자에게 중재를 요청하였을 경우 중재자가 분쟁을 해결한다. 중재 프로토콜은 다음과 같다.

(1) B는 $(A, Org, cp, VE_A, r'_A, s_A)$ (B, Rec, VES_B)

를 중재자에게 보낸다.

(2) 중재자는 VE_A, (r'_A, s_A), VES_B를 검증한다. A에게 $(A, Org, cp, VE_A, r'_A, s_A)$와 (B, Rec, m, VES_B)를 보낸다.

(3) A는 VE_A, (r'_A, s_A), VES_B를 검증한 후 평문 m을 B에게 전달하여 줄 것을 요청하든가, 아니면 프로토콜 중단을 요청한다.

(4) 중재자는 A가 메시지 m의 전달을 원할 경우 VE_A로 부터 암호키 K를 추출하고, VES_B로 부터 일반 서명 s_B를 계산하여 K는 B에게 s_B는 A에게 제공한다. 반대로 A가 프로토콜 중단을 요청할 경우에는 A와 B에게 전자 우편 프로토콜이 중단되었음을 알려준다.

중재 과정은 계약 프로토콜의 경우와는 달리 A가 중재 요청을 하는 경우와 B가 중재 요청을 하는 경우가 동일하게 처리된다. A에 의한 중재 요청은 VES_B를 B로 부터 받은 이후에나 가능하다. 따라서, B는 암호문 cp에 대응되는 평문 메시지를 받을 의사가 있음을 A에게 확인하여 주었다고 볼 수 있다.

5. 결 론

검증가능 암호에 대한 개념은 Stadler가 제안하였으며, 검증가능 위탁 서명의 개념은 Mao가 제안하였다. 그러나, Stadler와 Mao의 방식은 통신량과 계산복잡도가 매우 높기 때문에 실현이 어려운 문제가 있다.

본 논문에서는 제곱근에 대한 검증가능 암호를 바탕으로 새로운 검증가능 위탁 서명 기법을 제안하였다. 제안된 검증가능 위탁 서명 방식은 통신량이 적고 계산 효율성이 높은 장점이 있으나 중재 기관을 단 하나밖에 허락하지 않는 단점이 있다. 또한, 본 논문에서는 제안된 검증가능 암호와 검증가능 위탁 서명 방식을 사용하여 공정한 전자 계약 프로토콜과 공정한 전자 등기 우편 프로토콜을 제안하였다. 검증가능 암호와 검증가능 위탁 서명 방식은 최근 인터넷의 발전으로 각광을 받고 있는 전자 상거래에서 요구되는 공정한 정보 교환 프로토콜등에 사용될 수 있을 것으로 생각된다.

본 논문에서 제안된 검증가능 위탁 서명 방식은 하나의 중재 기관만을 허용하기 때문에 전체 시스템의 안전성이 하나의 중재 기관에 집중된다. 따라서, 여러개의 중재 기관을 허용하면서 통신량과 계산 복잡도가 적은 검증가능 위탁 서명 방식을 개발하는 것이 앞으로 해결하여야 할 과제이다.

참고서적

[1] ISO/IEC JTC1, Information Technology - Open Systems Interconnection - Security Frameworks in Open Systems, Part 4: Non-repudiation, ISO/IEC DIS 10181-4, April 1995.

[2] M. Ben-Or, O. Goldreich, S. Micali, and R. Rivest, A Fair Protocol for Signing Contracts, IEEE Transactions on Information Theory, 36(1):40-46, January 1990.

[3] E. F. Brickell, D. Chaum, I. B. Damgard, and J. van de Graaf, Gradual and Verifiable Release of a Secret, In Advances in Cryptology : Proceedings of Crypto'87, LNCS 293, pp. 156-166, Springer-Verlag, 1988.

[4] R. Cleve, lqlq Controlled Gradual Disclosure Schemes for Random Bits and Their Applicationsrqrq, In Advances in Cryptology:Proceedings of Crypto'89, LNCS 435, pp. 573-588, Springer-Verlag, 1990.

[5] I. B. Damgard, Practical and Provably Secure Release of a Secret and Exchange of Signatures, In Advances in Cryptology: Proceedings of Eurocrypt' 93, LNCS 765, pp. 200-217, Springer-Verlag, 1994.

[6] S. Even, O. Goldreich, and A. Lempel, A Randomized Protocol for Signing Contracts, Communications of the ACM, Vol. 28, No. 6, pp. 637-647, June 1985.

[7] N. Asokan, M. Schunter and M. Waidner, Optimistic Protocols for Fair Exchange, Proceedings of 4th ACM CCS, p.7-17, 1997.

[8] M. K. Franklin anf M. K. Reiter, Fair Exchange with a Semi-Trusted Third Party, Proceedings of 4th ACM CCS, p.1-6, 1997.

[9] J. Zhou and D. Gollman, A Fair Non-repudiation Protocol, In Proceedings of 1996 IEEE Symposium on Security and Privacy, pp.55-61, May 6--8, 1996.

[10] W. Mao, lqlq Verifiable escrowed signaturerqrq, em Proc. of ACISP' 97, LNCS 1270, Springer, 1997, pp.240-248.

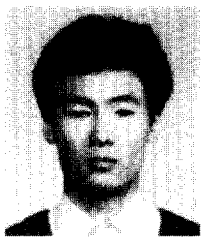
[11] M. Stadler, Publicly verifiable secret sharing, Advances in Cryptology - EUROCRYPT' 96, LNCS 1070, Springer, 1996, pp.190-199.

[12] M. O. Rabin, Digitalized signatures and public key fuctions as intractable as factorization, MIT/LCS/TR-212, MIT Laboratory for Computer Science, 1979.

[13] T. ElGamal, A Public Key Cryptosystem and A Signature Scheme Based On Discrete Logarithms, Advances in Cryptology - CRYPTO' 84, LNCS 196, Springer, 1996, pp.10-18.

[14] C. P. Schnorr, Efficient signature generation for smart cards', Journal of Cryptology, 4(3), pp.161-174, 1991.

□ 著者紹介



박 상 준

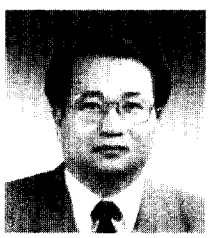
1984년 2월 한양대학교 수학과 졸업(이학사)
1986년 2월 한양대학교 대학원 수학과(이학석사)
1986년 1월 ~ 현재 한국전자통신연구원 선임연구원
1995년 3월 ~ 현재 성균관대학교 대학원 정보공학과 박사과정

※ 주관심 분야 : 암호이론, 암호 분석, 인증 및 서명

박 성 모

1992년 서울대학교 수학과 졸업(이학학사)
1994년 포항공과대학교 대학원 수학과 졸업(이학석사)
1994년 7월 - 현재 한국 전자통신연구원 재직(연구원)

※ 주관심 분야 : 암호이론, 정보이론



원 동 호

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

□ 著者紹介

김 대 호

1977년 2월 한양대학교 전자공학과(공학사)
1984년 2월 한양대학교 산업대학원 전자공학과(공학석사)
1993년 2월 Visiting Scholar(University of Maryland at College Park Dept. of Computer Science)
1977년 ~ 현재 한국전자통신연구원 책임연구원

※ 주관심 분야 : 전송분야, 통신 및 컴퓨터 보안