情報保護學會論文誌
第13券 第2號, 2003. 4

공동으로만 Unsigncrypt할 수 있는 Signcryption 기법

구 재 형*, 이 동 훈**

Jointly Unsigncryptable Signcryption Schemes

Jae Hyung Koo*, Dong Hoon Lee**

요 약

Signcryption은 메시지의 인증과 은닉성을 동시에 효율적으로 제공하기 위하여 제안되었다. 현재까지 제안된 기법들에서는 signcrypt된 메시지를 받은 지정된 어떠한 수신자도 혼자 unsigncrypt한 뒤 메시지를 확인할 수 있다. 본 논문에서는 t명 이상이 unsigncrypt 과정에 참여해야만 unsigncrypt가 가능한 $(t, n)-threshold$ 기법을 제안한다.

ABSTRACT

Signcryption has been proposed to provide authentication and confidentiality of a message efficiently. In the existing schemes, any recipient can unsigncrypt the signcrypted message alone. In this paper, we propose a $(t, n)-threshold$ signcryption scheme in which at least t recipients must participate in an unsigncryption process.

Keyword : *은닉성, 무결성, Signcryption 기법, Secret-Sharing 기법*

Ⅰ. 서 론

Zheng[1]은 서명과 암호화를 동시에 할 수 있는 signcryption 기법을 제안하였다. 또한, [1]에서는 메시지를 안전하고 인증이 가능한 방법으로 전송해야 할 경우 signcryption 기법을 사용하는 것이 서명 후 암호화하여 보내는 방법보다 훨씬 효율적이라는 것을 명백하게 입증하였다.

Signcryption 기법에서는 지정된 수신자만이 unsigncryption할 수 있게 된다. 변형된 형태의 signcryption 기법인 여러 명의 지정된 수신자에 의해 unsigncryption 될 수 있는 기법이 [2]에서 제안되었고, [5]에서 Mu와 Varaharajan은 그룹 내의 어떤 멤버도 그룹을 대표하여 signcryption을 할 수 있는 그룹 기반의 signcryption 기법을 제안하였다. 이러한 기법들에서는 어떠한 수신자도 홀로 unsigncryption을 할 수 있다.

그러나 많은 경우에 있어서 한 명의 수신자에 의해 메시지가 복구되고 서명이 검증되는 것을 막아야 할 필요가 있다. 예를 들어, 일정한 기간을 두고 입찰자들이 비공개로 경매 서비스 제공자를 통해 입찰한 뒤 경매 기간이 끝난 후, 최고 입찰자에게 경매품목이 배당되는 경우를 생각해 보자. 경매자가 경매했다는 사실을 보장하기 위해서 서명이 필요하고, 비공개 경매이기 때문에 경매자의 경매 내용을 숨기기 위해 암호화가 필요하게 된다. 따라서, 서명과 암호화를 효율적으로 제공하기 위해 signcryption 기법을 사용할 수 있다. 그러나 기존의 기법처럼 수신자가 바로 확인할 수 있는 경우엔 입찰자와 경매 서비스

* 본 연구는 2002년도 고려대학교 특별연구비에 의하여 수행되었음
* 고려대학교 정보보호연구센터(CIST) (ideao@cist.korea.ac.kr)
** 고려대학교 정보보호연구센터(CIST) (donghlee@korea.ac.kr)

제공자 간의 공모가 가능하게 된다. 즉, 특정 입찰자는 경매 서비스 제공자가 제시한 정보를 통해 항상 원하는 경매품목을 얻을 수 있게 된다. 이러한 문제점을 해결하기 위해서는 경매 서비스 제공자를 여럿을 두고, 정해진 숫자 이상의 경매 서비스 제공자들이 합의한 경우에만 입찰자의 입찰 정보를 알 수 있게 하는 방법이 필요하다. 입찰자의 signcryption된 입찰 정보를 여러 개의 조각으로 나눈 뒤 하나의 경매 서비스 제공자에게 하나의 조각만을 갖게 하여 정해진 숫자 이하의 서비스 제공자의 공모로는 입찰자에 대한 어떠한 정보도 얻을 수 없게 해야한다. signcryption + secret-sharing 기법은 이러한 특성을 제공할 수 있다. 여기서, secret-sharing 기법[7]은 Shamir가 제안한 방법으로, 어떠한 비밀 정보를 여러 개의 조각으로 나눈 뒤, 각 조각을 정해진 사용자에게 전송하여, 프로토콜 초기에 정의한 숫자 이상의 사용자들이 모였을 경우에만 비밀 정보를 복구할 수 있는 기법이다.

본 논문에서는 서명 후 암호화된 메시지를 여러 개의 조각들로 나눈 뒤 각각의 조각들을 수신자들에게 전송하게 되고, 나중에 t명 이상의 수신자가 동의할 경우에만 복호화한 뒤 서명을 검증할 수 있는 공동으로만 unsigncryption 할 수 있는 signcryption 기법들을 제안한다.

제안하는 기법의 계산 비용과 통신 비용은 전형적인 서명 후 암호화하는 기법에 secret-sharing 기법을 사용하는 것보다 훨씬 경제적이다.

II. Zheng의 Signcryption 기법

본 절에서는 Zheng이 제안한 signcryption 기법에 대해 간단히 살펴보도록 하겠다.

본 논문 전체에서 공개되는 매개 변수들은 큰 소수인 p, q 그리고 집합 $[1, \ldots, p-1]$에 있는 위수가 q인 정수 값 g이다. 송신자 A의 개인키는 x_a, 공개키는 $y_a (= g^{x_a} \bmod p)$이고, 마찬가지로 수신자 B의 개인키는 x_b, 공개키는 y_b가 된다.

먼저 송신자 A는 $[1, \ldots, q]$에서 임의의 값 x를 선택한 후 $K = y_b{}^x \bmod p$를 계산한 다음, K를 (K_1, K_2)로 나눈다. A는 다음과 같이 (c, r, s)를 계산한 후 수신자 B에게 전송한다.

$$r = KH_{K_2}(m)$$

$$s = x/(r + x_a) \bmod q$$

$$c = E_{K_1}(m)$$

여기서 $KH_{K_2}(m)$는 메시지 m을 키 K_2를 사용하여 해쉬시키는 함수이고, (r, s)가 메시지 m에 대한 A의 서명이 된다. $E_{K_1}(m)$은 키 K_1을 사용하여 메시지 m을 암호화하는 대칭키 암호 알고리즘이고, c는 알고리즘을 통해 얻게되는 암호문이다.

B는 공개된 매개변수 g, p와 A의 공개키 y_a, signcryption (c, r, s)와 자신의 개인키 x_b를 사용하여 K를 복구한 후 (K_1, K_2)로 나눈다.

$$K = (y_a \cdot g^r)^{s \cdot x_b} \bmod p$$

그런 후, 다음과 같은 과정을 통해 메시지를 복구한 후 서명을 검증한다.

$$m = D_{K_1}(c)$$

$$r \stackrel{?}{=} KH_{K_2}(m)$$

이 기법의 안전성은 이산로그 문제에 기반한다. 오직 지정된 수신자만이 송신자로부터 전송된 메시지를 복구할 수 있다. 즉, x_b를 아는 사람만이 K를 복구할 수 있고, K를 복구한 후에야 메시지를 복호화하여 서명을 검증할 수 있다.

$$\begin{aligned} K &= (y_a \cdot g^r)^{s \cdot x_b} \bmod p \\ &= (g^{x_a + r})^{(x/(r+x_a)) \cdot x_b} \bmod p \\ &= g^{x \cdot x_b} \bmod p \end{aligned}$$

III. Shamir의 Secret-Sharing 기법

앞 절에서 signcryption 기법에 대해서 살펴보았다. 여기에서는 제안하는 기법에서 사용하는 또 다른 기법인 secret-sharing 기법[7]에 대해 간략히 소개하도록 하겠다.

Secret-sharing 기법에서는 송신자가 비밀 정보를 n개의 서로 다른 조각들로 나눈 뒤 이것을 n명의 수신자들에게 각각 하나씩 나눠준다. 조각낸 비밀 정보는 최소한 t명 이상의 수신자들이 합의할 경우에만 복구할 수 있다. 즉, 어떠한 $t-1$명의 집합도 비밀 정보를 구할 수 없다.

Secret-sharing 기법을 사용하기 위해서 송신자는

먼저 다항식 $f(x)$를 정해야 한다.

$$f(x) = \sum_{i=1}^{t-1} a_i x^i + k \bmod p$$

여기서 a_i는 송신자가 비밀리에 보관하는 값이고, k는 수신자들에게 보낸 송신자의 비밀 정보이다. 송신자가 비밀 정보 k를 조각내어 수신자들에게 보내기 위해서 각각의 수신자들에 대한 난수를 선택해야 한다. 예를 들어, j번째 수신자에 대해 난수 w_j를 선택한 뒤 $f(w_j)$를 계산한다. 송신자는 수신자 j에게 공개 채널을 통해 $f(w_j)$를 보내고, w_j는 비밀 채널을 통해 전송한다.

비밀 정보 k를 복구하려면 t명 이상의 수신자들이 모여서 자신들이 가지고 있는 $(w_j, f(w_j))$를 내놓은 뒤 이 값들을 통해 a_i를 구할 수 있고, 그로부터 쉽게 비밀 값 k를 복구할 수 있다. 즉, t명 이상의 수신자들의 $(w_j, f(w_j))$가 모이면 t개의 미지수가 있는 다항식에 대한 t개 이상의 식을 얻을 수 있기 때문에 쉽게 미지수 a_i 값들과 k를 구할 수 있다.

Ⅳ. 공동으로만 unsigncryption 할 수 있는 sign- cryption 기법

앞의 두 절에서는 제안하는 기법에서 사용되는 signcryption 기법과 secret-sharing 기법에 대해 알아보았다. 본 절에서는 이러한 기법들을 바탕으로 하여 비공개 경매나 무기명 투표 등에서 사용될 수 있는 효율적인 기법을 제안한다.

제안하는 기법은 두 가지 형태로 나눌 수 있다. 모든 수신자들이 unsigncryption 과정에 참여할 경우에만 signcryption을 unsigncryption할 수 있는 (n, n)-threshold signcryption 기법과 최소한 t명 이상의 수신자들이 동의하면 unsigncryption할 수 있는 (t, n)-threshold signcryption 기법의 두 가지 형태로 나눌 수 있다.

메시지를 signcryption하여 전송하는 전송자 A의 개인키는 x_a, 공개키는 $y_a(=g^{x_a} \bmod p)$이다. j번째 수신자는 U_j로 표기되고, U_j의 개인키는 x_j, 공개키는 $y_j(=g^{x_j} \bmod p)$가 된다.

3.1 (n, n)-threshold signcryption 기법

(n, n)-threshold signcryption 기법은 모든 멤버들의 공개키의 곱의 형태로 되어 있는 그룹 키 $y_G(=\prod y_i)$를 사용하여 signcryption 과정을 수행한다. 본래의 signcryption 기법에서는 송신자가 임의의 난수 x와 수신자 B의 공개키 y_b를 사용하 K를 만들었기 때문에 $K=g^{x_b \cdot x} \bmod p$의 형태가 되지만 (n, n)-threshold signcryption 에서는 $K=g^{(\sum_1^n x_j) \cdot x} \bmod p$의 형태가 된다.

다음은 A가 수행하는 signcryption 과정이다.

(1) 전송자인 A는 메시지를 signcryption하여 보내줄 멤버들의 공개키를 사용하여 그룹키를 만든다.

$$(y_G = \prod y_j \bmod p \text{ for } 1 \le j \le n).$$

(2) A는 $[1, \ldots, q]$에서 임의의 수 x를 선택하여 $K = y_G{}^x \bmod p$를 계산한 후, K를 사용하여 다음과 같이 signcryption (c, r, s)를 만든다.

$$K \rightarrow K_1 \| K_2$$
$$r = KH_{K_2}(m)$$
$$s = x/(r + x_1) \bmod q$$
$$c = E_{K_1}(m)$$

(3) 마지막으로 A는 (c, r, s)를 수신자들에게 전송한다.

수신자 U_j가 Ⅱ.에서와 같은 방법으로 (c, r, s)를 unsigncryption하게 되면 실제의 키인 K 대신 $K_j(=(y_a)^{ax_j} \bmod p)$를 얻게 된다.

나중에 모든 수신자들이 unsigncryption에 동의했을 경우에만 다음의 과정을 통해 (c, r, s)을 unsigncryption을 할 수 있게 된다.

(1) 모든 수신자들이 가지고 있는 조각(K_j)를 공개하면, 조각들을 이용하여 K를 복구할 수 있다.

$$\left(\prod_{j=1}^{n} K_j\right) \cdot (y_G) \bmod p = (y_a{}^{ax_G}) \cdot (g^r) \bmod p$$
$$= K$$

(2) K를 복구한 뒤에, 본래의 signcryption 기법과

같은 방법으로, 수신자들은 다음과 같이 (c, r, s)를 unsigncryption 할 수 있게 된다.

$$K \rightarrow K_1 \| K_2$$
$$m = D_{k_1}(c)$$
$$r \stackrel{?}{=} KH_{k_2}(m)$$

즉, K를 구하게 되면, K를 (K_1, K_2)로 나눈 후 메시지를 복호화한 뒤 서명을 검증할 수 있다.

3.2 (t, n)-threshold signcryption 기법

(t, n) - threshold signcryption 기법과 (n, n)-threshold signcryption 기법의 가장 큰 차이는 (t, n)-threshold signcryption 기법에서는 최소한 t명 이상의 수신자가 unsigncryption에 동의하게 되면 signcryption을 unsigncryption할 수 있게 된다는 점이다. 다음 과정은 전송자 A에 의해 수행되는 signcryption 과정이다.

(1) A는 먼저 $[1, \ldots, q]$에서 임의의 두 수 x와 z를 선택 한 뒤, 다음과 같이 키 K를 계산한다.
$K = g^{zx} \bmod p$
(2) A는 다항식 $f(\alpha) = \sum_{i=1}^{t-1} a_i \alpha^i + z \bmod p$ 를 만든다.
(3) A는 각각의 수신자 U_j가 얻게 될 값인 $K_j (= (y_j)^{ax_a} \bmod p)$를 계산한 뒤에 U_j에게 보내줄 조각인 $f(K_j)$를 만든다.
(4) (n, n)기법에서와 같은 방법으로 A는 메시지를 signcryption하게 된다.
(5) 마지막으로 A는 각각의 $(c, r, s, f(K_j))$를 해당 U_j에게 보낸다.

최소한 t명 이상의 수신자들이 unsigncryption 과정에 참여하게 되면, 수신자들은 다음과 같이 unsigncryption을 할 수 있게 된다.

(1) 최소한 t명 이상의 수신자들은 z를 쉽게 복구할 수 있다. 즉, 각각의 사용자들이 자신이 가지고 있는 조각쌍 $(K_j, f(K_j))$를 내놓으면, t개의 미지수를 가진 식에 대해 t개 이상의 방정식을 만들 수 있기 때문에 쉽게 미지수들을 구하여 쉽게 z를 복구할 수 있다.
(2) 수신자들은 z를 사용하여 다음과 같이 K를 계산한다.
(3) K를 복구한 후에 수신자들은 (n, n)기법과 같은 방법을 통해서 (c, r, s)를 unsigncryption 할 수 있게 된다.

3.3 안전성과 효율성 분석

제안하는 기법들은 [1]에서와 같이 위조방지, 부인봉쇄, 그리고 은닉성의 세 가지 안전성을 보장하고 추가로 [1]에서 가능했던 공모공격[2]에 대해서도 안전하다.

- 위조방지 : 위조방지는 (c, r, s)에만 해당되고 안전성은 [1]에서와 같이 Pointcheval과 Stern기술 [6]을 사용하여 증명할 수 있다.
  간단히 설명하자면, 정당한 키를 모른다면, 암호문 (c)에 포함되어 있는 m을 사용하여 r을 만들 수 없으며, 전송자의 개인키 x_a와 임의의 난수 x를 모르면 정당한 s를 만들어 낼 수 없다. 즉, K와 x_a를 아는 사람만이 c와 관련된 r과 s를 만들 수 있다.
- 부인봉쇄 : 만일 A가 signcryption을 만든 사실을 부인하게 되면 *trustee*가 이를 쉽게 중재할 수 있다. trustee는 먼저 각각의 수신자들과 영지식 상호증명 과정을 통해서 각각의 수신자들이 임의로 조각을 만들어낼 수 없다는 점과 각 조각들이 A가 만든 정당한 조각인지를 증명하게 된다. 만약 모든 조각들이 정당하다면 trustee는 K를 복구한 뒤에 unsigncryption 과정이 제대로 수행되는 지를 검사하여 A가 signcryption을 했는지 여부를 알 수 있게 된다.
  즉, x_a를 모르는 상태에서 각각의 수신자들 이 올바르게 unsigncryption 과정을 통과할 수 있는 K_i를 임의로 만들 수 없기 때문에, trustee는 각 수신자들의 조각들을 모두 공개하게 한 후 unsigncryption 과정을 수행하여 올바른 signcryption인가를 검사한다.
- 은닉성 : (c, r, s)에 대한 은닉성은 [1]과 같다. 즉, 암호문인 c는 사용되는 대칭키 암호 알고리즘이 안전하다고 가정하면 안전하게 만들어질 수 있고, r 역시 안전한 해쉬함수를 사용하여 안전하게 제공할 수 있다. 공격자가 $K(\rightarrow K_1 \| K_2)$를 알지 못한 상황 속에서는 c 와 r을 만들기 위해 사용된 메시지 m을 알아내는 것을 계산상 불가능하다.

각각의 조각들에 대해서는 secret-sharing의 특성에 따라 t명 이하의 공모로는 어떠한 정보를 얻을 수가 없다. 다시 말해서, 미지수가 t개인 식에 대해 t보다 적은 수의 방정식을 구성하면 미지수를 구할 수 없다. 예를 들어, 2차 방정식의 경우(t=3인 경우) 세 개의 미지수 a, b, c에 대해 다음과 같은 방정식을 만들수 있다.

$$f(x) = ax^2 + bx + c$$

여기서 미지수들의 값을 구하기 위해서는 세개의 방정식이 필요하다. 즉, 세 쌍의 값 $(x_1, f(x_1))$, $(x_2, f(x_2))$, $(x_3, f(x_3))$이 있으면 연립 방정식을 통해 세 미지수의 값을 구할 수 있다. 그러나 한 명이나 두 명이 모여서는 두 개의 방정식만을 얻을 수 있기 때문에 세미지수의 값을 구할 수 없다.

위와 같이, 제안하는 기법은 signcryption과 secret-sharing을 안전성을 모두 수용한다.

또한 signcryption의 특성에 의해 제안하는 기법은 일반적인 서명 후 암호화하는 방법보다 더 효율적이다. 계산 비용에 대해서는 전형적인 서명 후 암호화하는 방법을 사용하였을 때보다 세 번의 지수승 계산을 줄일 수 있고 통신비용에 대해서는 p 크기의 두 배 정도의 오버헤드를 줄일 수 있다. 효율성에 대한 비교는 [표 1], [표 2]와 같다.

표에서 사용되는 기호는 다음과 같다.
- EXP : 모듈로 지수계산 수
- MUL : 모듈로 곱셈계산 수
- DIV : 모듈로 나눗셈계산 또는 역 수
- ADD : 모듈로 덧셈 또는 뺄셈 계산 수
- HASH : 일방향 또는 키를 사용한 해쉬 함수의 계산 수
- ENC : 비밀키 암호화를 사용하는 암호화 수
- DEC : 비밀키 암호화를 사용하는 복호화 수
- FUNC : 조각을 나누기 위해 secret-sharing을 사용한 수
- for a recipient : 한 명의 수신자가 해야하는 계산량(조각을 받을 때)

Ⅳ. 결 론

본 논문에서는 signcryption 기법과 secret-sharing 기법을 특성을 효율적으로 사용하여 공동으로만 unsigncryption할 수 있는 signcryption 기법을 제안하였다. 제안하는 기법은 signcryption 기법의 효율성과 secret-sharing 기법의 안전성을 모두 제공하며 비공개 경매나 전자투표 등 여러 응용에서 사용될 수 있으리라 기대된다.

〔표 1〕 (n, n)-threshold 기법에 대한 비교

Schemes	Computational cost	Communication overhead
(n,n)-threshold signature-then-encryption based on Schnorr signature and ElGamal encryption	EXP=3, MUL=n+2, DIV=0 ADD=1, HASH=1, ENC=1 for a recipient : EXP=1	|KH(·)| + |q| + 2|p|
[Decryption-then-Verification]	[EXP=2, MUL=n+2, DIV=0 ADD=0, HASH=1, DEC=1]	
(n,n)-threshold signcryption	EXP=1, MUL=n, DIV=1 ADD=1, HASH=1, ENC=1 for a recipient : EXP=1, MUL=1	|KH(·)| + |q|
[Unsigncryption]	[EXP=1, MUL=n+2, DIV=0 ADD=0, HASH=1, DEC=1]	

〔표 2〕 (t, n)-threshold 기법에 대한 비교

Schemes	Computational cost	Communication overhead
(t,n)-threshold signature-then-encryption based on Schnorr signature and ElGamal encryption	EXP= n+3, MUL=2, DIV=0 ADD=1, HASH=1, ENC=1, FUNC=n for a recipient : EXP=1	|KH(·)| + |q| + (n+2)|p|
[Decryption-then-Verification]	[EXP=3, MUL=2, DIV=0 ADD=0, HASH=1, DEC=1 FUNC=t]	
(t,n)-threshold signcryption	EXP= n+1, MUL=1, DIV=1 ADD=1, HASH=1, ENC=1, FUNC=n for a recipient : EXP=1, MUL=1	|KH(·)| + |q| + n·|p|
[Unsigncryption]	[EXP=2, MUL=2, DIV=0 ADD=0, HASH=1, DEC=1 FUNC=t]	

참 고 문 헌

[1] Y. Zheng, "Digital signcryption or how to achieve cost(signature & encryption) <<cost(signature)+cost (encryption," Proc. CRPTO'97, pp. 165~179, 1997.

[2] Y. Zheng, "Signcryption and its applications in efficient public key solutions," Proc ISW'97, Berlin, New York, Tokyo, 1997.

[3] F. Bao, "A signcryption scheme with signature directly verifiable by public key", Proc. PKC'98, volume 1431 of LNCS, pp. 55~59, 1998.

[4] C. Gamage, J. Leiwo, and Y. Zheng, "An efficient scheme for secure message transmission using

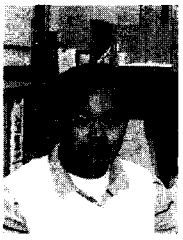
proxy-signcryption", Technical Report 98~01, Peninsula School of Computing & Information Technollogy, Monash University, July, 1998.

[5] Y.Mu, and V. Varadharajan "Distributed signcryption", Proc. INDOCRYPT'2000, pp. 155~164, 2000.

[6] D. Pointcheval, and J. Stern, "Security proofs for signature schemes", Proc. EUROCRYPT'96, pp. 19 0~1999, 1996.

[7] A. Shamir. How to share a secret. In *Comm. Assoc. Comput. Mach.*, vol.22.,no.11, pages. 612~613.

〈著者紹介〉



구 재 형 (Jae Hyung Koo) 학생회원

1997년11월~1999년1월 : 삼성 소프트웨어 멤버쉽 활동
2000년 2월~고려대학교 전산학과 졸업(이학사)
2002년 2월~고려대학교 전산학과 석사
2002년 3월~현재 : 고려대학교 정보보호 대학원 박사과정
<관심분야> 암호이론, 암호 프로토콜, 키교환 기법, 무선통신 보안

이 동 훈 (Dong Hoon Lee) 정회원

1984년 : 고려대학교 경제학과 졸업(이학사)
1987년~Oklahoma Univ. 전산학과 석사
1992년~Oklahoma Univ. 전산학과 박사
1993년~2001 : 고려대학교 전산학과 교수
2001년~현재 : 고려대학교 정보보호 대학원 교수
<관심분야> 암호이론, 암호 프로토콜, 키교환 기법, 무선통신 보안