# 공동으로만 Unsigncrypt할 수 있는 Signcryption 기법

구재형*, 이동훈*, 임종인*

*고려대학교, 정보보호센터

# Jointly Unsigncryptable Signcryption Schemes

Jae-Hyung Koo*, Dong Hoon Lee, and Jong Im Lim

*Center for Information Security Technologies, Korea Univ.

## 요 약

Signcryption은 메시지의 인증성과 은닉성을 동시에 효율적으로 제공하기 위해 제안된 기법이다. 현재까지 제안되어 온 모든 signcryption 기법들에서는 signcryption을 받은 수신자가 signcryption을 받자마자 혼자서도 unsigncryption을 할 수 있다. 하지만 때로는 개인이 임의로 unsigncryption하는 것을 방지하고 정해진 수 이상의 멤버들이 모였을 때에만 unsigncryption되어야 하는 특성이 요구될 수 있다. 본 논문에서는 최소한 $t$명 이상의 수신자들이 unsigncryption 과정에 참가할 경우에만 unsigncryption할 수 있는 $(t, n)$-threshold signcryption 기법을 제안한다.

## I. 서론

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

Signcryption 기법에서는 지정된 수신자만이 unsigncryption할 수 있게 된다. 변형된 형태의 sigcnryption 기법인 여러 명의 지정된 수신자에 의해 unsigncryption될 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. Signcryption + Secret-sharing 기법은 이러한 특성을 제공할 수 있다.

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

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

## II. 공동으로만 unsigncryption 할 수 있는 signcryption 기법

제안하는 기법은 두가지 형태로 나눌 수 있다.

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

본 논문 전체에서 공개되는 매개 변수들은 큰 소수인 $p, q$ 그리고 위수가 $q$인 집합

$[1,\ldots,p-1]$에 있는 정수 값 $g$이다. $j$번째 수신자는 $U_j$로 표기되고, $U_j$의 개인키는 $x_j$, 공개키는 $y_j(=g^{x_j} \bmod p)$가 된다.

## 1. $(n,n)$-threshold signcryption 기법

$(n,n)$-threshold signcryption 기법은 모든 멤버들의 공개키의 곱의 형태로 되어 있는 그룹 키 $y_G$를 사용하여 서명, 암호화, 그리고 서명 후 암호화된 값을 조각으로 나눈 뒤 각각의 수신자에게 나눠주는 작업을 동시에 수행한다.

다음은 전송자 $U_1$이 수행하는 signcryption 과정이다.

(1) 전송자인 $U_1$은 큰 소수 $p$를 선택한 후 $g(\in[1,\ldots,p-1])$를 선택한다. 그런 다음 멤버들의 공개키를 사용하여 그룹 키를 만든다. ($y_G=\prod y_j \bmod p$ for $1\le j\le n$).

(2) $U_1$은 $[1,\ldots,q]$에서 임의의 수 $x$를 선택한 후 $K=y_G{}^x \bmod p$를 계산한다. $U_1$은 $K$를 사용하여 다음과 같이 signcryption $(c,r,s)$를 만들게 된다.

$$K \rightarrow K_1 \| K_2$$

$$r = KH_{k_2}(m)$$

$$s = x/(r+x_1) \bmod q$$

$$c = E_{k_1}(m)$$

(3) 마지막으로 $U_1$은 $(c,r,s)$를 수신자들에게 전송한다.

수신자 $U_j$가 [1]과 같은 방법으로 $(c,r,s)$를 unsigncryption하게 되면 실제의 키인 $K$ 대신 $K_j(=(y_a)^{\alpha_j} \bmod p)$를 얻게 된다.

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

(1) 모든 수신자들은 가지고 있는 조각($K_j$)를 공개하고 조각들을 이용하여 $K$를 복구해 내게 된다.

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

(2) $K$를 복구한 뒤에, 수신자들은 다음과 같이 $(c,r,s)$를 unsigncryption 할 수 있게 된다.

$$K \rightarrow K_1 \| K_2$$

$$m = D_{k_1}(c)$$

$$r \stackrel{?}{=} KH_{k_2}(m)$$

## 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 $t$ 명 이상의 수신자가 unsigncryption에 동의하게 되면 signcryption을 unsigncryption할 수 있게 된다는 점이다. 다음 과정은 $U_1$에 의해 수행되어지는 signcryption 과정이다.

(1) $U_1$은 먼저 $[1,\ldots,q]$에서 임의로 두 수 $x$와 $z$를 선택 한 뒤 키로 사용될 $K$를 계산한다. ($K=g^{zx} \bmod p$)

(2) $U_1$은 다항식 $f(\alpha)=\sum_{i=1}^{t-1} a_i\alpha^i + z \bmod p$를 만든다.

(3) $U_1$은 각각의 수신자 $U_j$가 얻게 될 값인 $K_j(=(y_j)^{\alpha_0} \bmod p)$를 계산한 뒤에 $U_j$에게 보내줄 조각인 $f(K_j)$를 만들게 된다.

(4) $(n,n)$기법에서와 같은 방법을 통하여 $U_1$는 메시지를 signcryption하게 된다.

(5) 마지막으로 $U_1$는 $(c,r,s,f(K_j))$를 $U_j$에게 보낸다.

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

(1) 최소한 $t$명 이상의 수신자들은 $z$를 쉽게 복구할 수 있다.

(2) 수신자들은 $z$를 사용하여 $K$를 계산한다.

(3) $K$를 복구한 후에 수신자들은 $(n, n)$ 기법과 같은 방법을 통해서 $(c, r, s)$를 unsigncryption 할 수 있게 된다.

## 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 Stern 기술 [6]을 사용하여 증명할 수 있다.

- 부인봉쇄 : 만일 $U_1$이 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 $U_1$이 만든 정당한 조각인지를 증명하게 된다. 만약 모든 조각들이 정당하다면 trustee는 $K$를 복구한 뒤에 unsigncryption 과정이 제대로 수행되는 지를 검사하여 $U_1$이 signcryption을 했는지 여부를 알 수 있게 된다.

- 은닉성 : $(c, r, s)$에 대한 은닉성은 [1]과 같다. 각각의 조각들에 대해서는 secret-sharing의 특성에 따라 $t$명 이하의 공모로는 어떠한 정보를 얻을 수가 없다.

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

또한 signcryption의 특성에 의해 제안하는 기법은 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 2와 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 해쉬계산 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)

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<br>ADD=1, HASH=1, ENC=1<br>for a recipient : EXP=1 | \|KH(·)\| + \|q\| + 2\|p\| |
| [Decryption-then-Verification] | [EXP=2, MUL=n+2, DIV=0<br>ADD=0, HASH=1, DEC=1] | |
| (n,n)-threshold signcryption | EXP=1, MUL=n, DIV=1<br>ADD=1, HASH=1, ENC=1<br>for a recipient : EXP=1, MUL=1 | \|KH(·)\| + \|q\| |
| [Unsigncryption] | [EXP=1, MUL=n+2, DIV=0<br>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<br>ADD=1, HASH=1, ENC=1, FUNC=n<br>for a recipient : EXP=1 | \|KH(·)\| + \|q\| + (n+2)\|p\| |
| [Decryption-then-Verification] | [EXP=3, MUL=2, DIV=0<br>ADD=0, HASH=1, DEC=1 FUNC=t] | |
| (t,n)-threshold signcryption | EXP= n+1, MUL=1, DIV=1<br>ADD=1, HASH=1, ENC=1, FUNC=n<br>for a recipient : EXP=1, MUL=1 | \|KH(·)\| + \|q\| + n\|p\| |
| [Unsigncryption] | [EXP=2, MUL=2, DIV=0<br>ADD=0, HASH=1, DEC=1 FUNC=t] | |

## 4. 결 론

본 논문에서 signcryption의 새로운 기법인 공동으로만 unsigncryption할 수 있는 signcryption 기법을 제안하였다. 논문에서 보였듯이 제안하는 기법은 전형적인 서명 후 암호화한 뒤 조각으로 나누는 기법보다 훨씬 효율적인 기법이다.

## 참고문헌

[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. 190-1999, 1996.