# 부인봉쇄 과정에서 기밀성 문제를 해결한 개선된 Signcryption

김동우, 박지환
부경대학교 전산정보학과

# An Improved Signcryption with Confidentiality in Non-repudiation

Dong-Woo Kim, Ji-Hwan Park
Dept. of Computer and Information, PuKyong National University

요 약

Y.Zheng은 디지털 서명과 암호화를 동시에 수행할 수 있는 Signcryption 방식을 제안하였다. 본 논문에서는 기존에 제안된 Signcryption 방식들이 부인봉쇄 과정에서 기밀성을 유지하고 있지 못하는 문제점을 해결하고, Y.Zheng의 Signcryption과 계산량 및 통신량이 비슷하면서 기존 Signcryption 방식에 비해 개선된 방식을 제안한다.

## 1. 서론

송수신자가 공개통신망에서 비밀리에 메시지를 교환하고자 할 때, 메시지에 대한 전자서명은 별개의 과정에 따라 암호화되어 상대방에게 전해지는 것이 일반적이며, 이런 방법을 signature-then-encryption 이라고 한다.

Y.Zheng은 이런 두 개의 과정을 하나로 통합한 Signcryption 이라는 새로운 개념을 제안하였다[1]. Signcryption 방식은 전자서명의 고유기능인 부인봉쇄는 물론 암호화의 기밀성도 제공한다. H.Petersen 등은 Y.Zheng의 Signcryption 방식을 이용할 때, 수신자가 제3자(중재자 혹은 공공기관등)에게 송신자의 전자서명을 증명하기 위하여 관련정보를 공개하는 경우, 제3자는 이를 이용하여 송수신자간의 암호화된 메시지를 풀수 있는 키를 만들 수 있음을 지적하고, 이를 개선한 새로운 Signcryption 방식을 제안하였다[2,3]. 그러나 Y.Zheng이 제안한 방식과 유사한 문제점이 있음을 김성덕[6]이 지적하였다.

본 논문에서는 기존 Signcryption의 기밀성 문제점을 해결하고, Y.Zheng의 Signcryption과 계산량 및 통신량이 비슷한 개선된 Signcryption방식을 제안한다. 2장에서는 기존의 Signcryption 방식의 문제점을 분석하고, 3장에서 기존 Signcryption 문제점을 해결한 개선된 Signcryption 방식을 제안한 후, 4장에서 결론을 맺는다.

## 2. 기존 Signcryption의 문제점

본 장에서는 Y.Zheng과 M.Michel의 Signcryption 방식의 문제점과 김성덕의 Signcryption을 살펴본다.

### 2.1 기호 및 표기

$p$ : 큰 소수
$q$ : $p-1$을 나누는 큰 소인수
$g$ : 유한체 상의 위수 q인 $Z_p^*$에 속하는 정수
$h$ : 일방향 해쉬 함수
$KH$ : Keyed 일방향 해쉬 함수
$E$, $D$ : 비밀키를 사용하는 암호화/복호화 알고리즘
$x_a$, $x_b$ : Alice와 Bob의 비밀키
$y_a$, $y_b$ : Alice와 Bob의 공개키( $y_i = g^{x_i} \bmod p$)

### 2.2 Y. Zheng의 Signcryption방식과 문제점

1997년 Y.Zheng은 SDSS1과 SDSS2로 명명된 두 가지의 Signcryption 방식을 제안하였으며, 각각의 Signcryption

생성과 검증 과정은 [그림 1]과 같다.

| | |
|---|---|
| 생성 | $x \in Z_q^*$<br>$k = h(y_b^x \bmod p)$<br>$k = k_1 \| k_2$<br>$r = KH_{k_2}(m)$<br>[SDSS 1] $s = x(r+x_a)^{-1} \bmod q$<br>[SDSS 2] $s = x(1+x_a r)^{-1} \bmod q$<br>$c = E_{k_1}(m)$ |
| 통신 | $c$, $r$, $s$ |
| 검증 및 복호 | [SDSS 1] $k = h((y_a g^r)^{s \cdot x_b} \bmod p)$<br>[SDSS 2] $k = h((y_a^r g)^{s \cdot x_b} \bmod p)$<br>$k = k_1 \| k_2$<br>$m = D_{k_1}(c)$<br>check if $r = KH_{k_2}(m)$ |

[그림 1] Y.Zheng의 Signcryption 방식

Y.Zheng은 제안한 방식이 공개통신로상에서 전자문서의 기밀성을 보장할 뿐만 아니라 전자 서명을 통해 부인봉쇄도 동시에 제공한다고 하였다. 하지만 제안된 Signcryption 방식은 Bob이 Carol에게 Alice의 Signcryption을 증명하는 과정에서 중간정보가 공개되는 경우에 Carol은 이 정보를 이용하여 $y_{ab}$를 계산할수 있게 되고, Carol은 이 $y_{ab}$를 이용하여 Alice와 Bob사이에서 이루어지는 Signcryption 에 의한 암호통신문을 언제든지 복호 할 수 있는 키를 생성할 수 있음을 H.Petersen 등이 지적하였으며, 그 과정은 다음과 같다[2].

1. Carol에게 공개되는 정보 : $k$, $r$, $s$, $y_b$
2. [SDSS 1] $y_{ab} = k^{s^{-1}} y_b^{-r} \bmod p = (y_b^x)^{s^{-1}} y_b^{-r}$
   $= (y_b^x)^{r+x_a / x} y_b^{-r} = y_b^{r-r+x_a}$
   $= y_b^{x_a} \bmod p$
3. 통신로 상의 정보 : $s'$, $r'$, $c'$
4. [SDSS 1] $k' = y_{ab}^{s'} y_b^{r's'} \bmod p$
   $= y_b^{s'x_a} y_b^{r's'} = y_b^{s'(x_a + r')}$
   $= y_b^{(x_a + r')x' / (x_a + r')}$
   $= y_b^{x'} \bmod p$
5. $k' = k_1' \| k_2'$
6. $m' = D_{k_1'}(c')$

[SDSS 2]도 유사하게 계산할 수 있다.

즉, Y.Zheng의 Signcryption 방식은 기밀성을 유지하지 못한다.

### 2.3 M. Michel의 Signcryption 방식과 문제점

H. Petersen 등은 Signcryption 방식의 단점을 지적하고 이를 보완한 새로운 Signcryption을 제안하였지만 이방식은 Signcryption의 생성과정에서 변수 사이의 연관성 결여로 수신자가 송신자의 Signcryption을 생성할 수 있기 때문에 부인봉쇄 기능을 보장할 수 없다는 단점이 있다[2].

H. Petersen의 공동 집필자인 M. Michel은 이런 사실을 인지하고 기존의 방식을 수정한 [그림 2]와 같은 Signcryption 방식을 제안 하였다[3].

| | |
|---|---|
| 생성 | $x_1, x_2 \in Z_q^*$<br>$C = E_{x_1}(M \| H(M))$<br>$k = H(y_b^{x_2} \bmod p, C)$<br>$r = x_1 k \bmod q$<br>$s = x_2(r+x_a)^{-1} \bmod q$ |
| 통신 | $s$, $r$, $C$ |
| 검증 및 복호 | $K = y_b^{rs} y_a^{sx_b} \bmod p$<br>$k = H(K, C)$<br>$x_1 = rk^{-1} \bmod q$<br>$M \| H(M) = D_{x_1}(C)$ |

[그림 2] M. Michel의 Signcryption 방식

하지만 M. Michel의 Signcryption 방식 역시 Y.Zheng의 Signcryption 방식과 유사한 문제점을 가지고 있음을 김성덕이 지적하였으며, 그 과정은 다음과 같다[6].

1. 공개정보 : $y_b$, $K$, $s$, $r$
2. $y_{ab} = K^{s^{-1}} y_b^{-r} \bmod p = (y_b^{rs} y_a^{sx_b})^{s^{-1}} y_b^{-r}$
   $= g^{rx_b + x_a x_b - rx_b} = g^{x_a x_b} \bmod p$
3. Signcryption : $s'$, $r'$, $C'$
4. $y_{ab}^{s'} y_b^{r's'} = y_b^{r's' + s'x_a} = y_b^{s'(x_a + r')}$
   $= y_b^{(x_a + r')x'_2 / r' + x_a} = y_b^{x'_2} \bmod p$
   $k' = H(y_b^{x'_2} \bmod p, C)$
5. $x_1' = r'k'^{-1}$, $M' = D_{x_1'}(C')$

즉, M. Michel의 Signcryption 방식도 기밀성을 유지할 수 없다.

### 2.4 김성덕의 Signcryption 방식과 특징

김성덕은 M. Michel이 제안한 Signcryption 역시 Y.Zheng의 Signcryption 방식과 유사한 문제점이 있음을 지적하고, 이를 보완한 [그림 3]과 같은 새로운 Signcryption을 제안하였다.

| | |
|---|---|
| 생성 | $x \in Z_q^*$<br>$K = g^x \bmod p$<br>$r = y_b^x \bmod p$<br>$k = H(K, M) \bmod q$<br>$T = x - x_a k \bmod q$<br>$C = E_K(M \| T)$ |
| 통신 | $r$, $C$ |
| 검증 및 복호 | $K' = r^{x_b^{-1}} \bmod p$<br>$M' \| T' = D_{K'}(C)$<br>$k' = H(K', M') \bmod q$<br>check if $K' = y_a^{k'} g^{T} \bmod p$ |

[그림 3] 김성덕의 Signcryption 방식

김성덕 등이 제안한 Signcryption 방식의 특징을 살펴보면 $y_b^x$를 전자서명 값으로 직접 이용하여 제 3자가 $y_{ab}$를 계산하더라도 전자서명의 안전성을 유지할 수 있도록 하였고, $r$에서 $g^x$을 계산하기 위해서는 Bob의 $x_b$를 알아야 하므로 수신자 만이 이를 복호할 수 있다. 또한 s를 암호화하여 C에 포함하여 송부하므로 공격자는 s를 알 수 없다. 즉 $r$을 이용하여 암호문 C를 복호해야만 s를 알 수 있는 특징을 가지고 있다.

## 3. 제안하는 Signcryption 방식

Y.Zheng과 M. Michel이 제안한 방식은 Signcryption을 Carol에게 증명하게 되면, Carol이 Alice와 Bob의 암호화된 송수신 메시지를 복호해 볼 수 있어 기밀성을 유지하지 못함을 살펴 보았다. 본장에서는 기존의 Signcryption 방식들이 가지고 있던 문제점을 해결한 [그림 4]과 같은 Signcryption방식을 제안한다.

제안한 Signcryption 방식의 특징은 다음과 같다.

제안하는 방식은 T. ElGamal의 encryption[5]과 C.P. Schnorr의 signature기법[4]을 이용하였으며, Signcryption을 Carol에게 증명하는 과정에서 중간 정보들이 공개되어도 Carol은 Alice와 Bob사이의 암호문을 풀어볼 수 없는 특징이 있다.

| | |
|---|---|
| 생성 | $x \in Z_q^*$<br>$k = h(y_b^x \bmod p)$<br>$r = KH_k(m)$<br>$c = E_k(m)$<br>$s = x - x_a r \bmod q$ |
| 통신 | $s$, $r$, $c$ |
| 검증 및 복호 | $k = h((g^s \cdot y_a^r)^{x_b} \bmod p)$<br>$m = D_k(c)$<br>check if $r = KH_k(m)$ |

[그림 4] 제안하는 Signcryption 방식

### 3.1 기밀성(Confidentiality)

기존에 제안된 방식들은 별도의 정보를 이용하여 $y_b^x$를 복원하기 때문에 제 3자에게 정보가 공개 되는 경우 제 3자는 공개된 정보를 이용하여 $y_{ab}$를 계산할 수있고 이를 기반으로 암호문의 복호에 필요한 키를 만들 수 있다는 공통점이 있다. 제안하는 방식에서는 ($s$, $c$, $r$)을 동일하게 생성하고 제 3자에게 송신자의 전자서명을 증명하기 위해 관련정보를 공개하여 제 3자가 $y_{ab}$를 계산한다 하더라도 전자서명의 안전성을 유지하도록 하였다.

### 3.2 계산량과 통신량

암호시스템과 전자서명 시스템의 효율성은 주로 계산량과 통신량을 기준으로 한다. [표 1]은 Y.Zheng의 P1363 제출자료[1]를 기반으로 계산량과 통신량을 비교하였다. 통신량의 비교에서 암호문의 길이는 동일하므로 표에서는 생략한다.

제안한 Signcryption 방식은 서명후 암호화 하는 방식에 비해 모듈러 멱승이 2번 적고, 통신에 따른 오버헤드가 적음을 알수 있다. 또한 기존의 Y.Zheng의 Signcryption 방식과 계산량 및 통신량에서 큰 차이 없이 Signcryption을 생성할 수 있다.

[표 1] Signcryption 방식 비교

| 구 분 | SDSS 1 | | SDSS 2 | | Michel | | 김성덕 | | 제안방식 | | Sign(Schnorr) Encryption | | Sign(DSS) Encryption | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Sign | Verify | Sign | Verify | Sign | Verify | Sign | Verify | Sign | Verify | Sign | Verify | Sign | Verify |
| EXP | 1 | 1.17 | 1 | 1.17 | 1 | 1.17 | 2 | 2.17 | 1 | 2.17 | 3 | 2.17 | 3 | 2.17 |
| MUL | 0 | 2 | 1 | 2 | 2 | 4 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| DIV | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 2 |
| ADD | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| HASH | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 1 | 2 | 2 | 1 | 1 | 1 | 1 |
| Com Overhead | \|H()\|+\|q\| | | \|H()\|+\|q\| | | \|H()\|+2\|q\| | | \|p\|+\|q\| | | \|H()\|+\|q\| | | \|H()\|+\|q\|+\|p\| | | 2\|q\|+\|p\| | |

## 4. 결 론

본 논문에서는 기존의 Signcryption 방식들의 문제점을 살펴보고 이를 해결한 개선된 Signcryption 방식을 제안하였다. 제안한 방식은 일반적인 서명 후 암호화하는 방식보다 효율적이며, 기존의 Signcryption 방식과 계산량과 통신량에서 크게 차이 없이 Signcryption을 생성하고, 기존의 방식에서 발생할 수 있는 문제점을 해결한 방식이다.

그러므로 제안한 방식은 정보의 기밀성을 유지하면서 동시에 송신자의 전자서명이 필요한 분야에 유용하게 사용될 수 있을 것이라고 생각한다.

## 참 고 문 헌


[1] Y.Zheng, "Digital Signcryption or How to Achieve Cost(Signature & Enctyption) << Cost(Signature) + Cost(Enctyption)", Advances in Cryptology - CRYPTO'97, Springer-verlag, LNCS 1294, pp. 165-179, 1997

[2] H.Petersen and M.Michel. "Cryptanalysis and Improvement of Signcryption Schemes" IEE Computer and Digital Techniques 1998.

[3] H.Petersen and M.Michel. "Cryptanalysis and Improvement of Signcryption Schemes" IEE Computer and Digital Techniques 1998. (Revised Version)

[4] C.P.Schnorr "Efficient Signature Generation for Smart Cards", Advance in Cryptology-CRYPTO '89 Proceeding.

[5] T. ElGamal, "A public key ctyptosystem and a Signature Scheme based on Discrete Logarithms", IEEE Transactions on Information Theory, IT-31(4) : 469~472, 1985

[6] 김성덕, "다자전송 효율성을 가진 Signcryption 방식" 통신정보보호학회 논문지, 제 10권 제 3호, 2000.9

[7] F.Bao, R.H.Deng, "A Signcryption Scheme with Signature Directly Verigiable by Public Key", PKC'98, Spring-Verlag, LNCS 1431, 55~59, 1998