通信情報保護學會論文誌
第 10 券 第 3 號, 2000. 9

다자전송 효율성을 가진 Signcryption 방식

김 성 덕*, 정 재 동*, 양 형 규**

An Efficient Signcryption Scheme for Multi-Sending

Sung-duk Kim*, Jae-dong Jung*, Hyung-kyu Yang**

요 약

Y. Zheng은 디지털 서명과 암호화를 동시에 수행할 수 있는 Signcryption 방식을 제안하였다. Signcryption 방식은 first-sign-then-encrypt 혹은 first-encrypt-then-sign과 같은 일반적인 방식보다 계산량과 통신량 측면에서 효율적인 방식이다. 본 논문에서는 기존에 제안된 Signcryption 방식들을 분석한 결과, M. Michels의 Signcryption방식에 문제점이 있음 밝히고 송신자가 동일한 문서에 Signcryption하여 여러 명에게 송신할 때, 기존 Signcryption 방식에 비해 효율적인 Signcryption 방식을 제안한다.

ABSTRACT

Y. Zheng suggested a new concept called signcryption that provides confidentiality with digital signature properties. The signcryption scheme is more efficient than general method what we call first-sign-then-encrypt or first-encrypt-then-sign in computational and communicational cost. But, H. Petersen et al pointed out weakness to Y. Zheng' scheme and suggested new one. In this paper we survey three signcryption schemes suggested by Y. Zheng and H. Petersen et al respectively and cryptanalysis M. Michels's revised scheme. And we suggest a new signcryption is more efficient when originator makes several signcryption on the same document.

keyword : *Signcryption, Authenticated Encryption*

Ⅰ. 서 론

송수신자가 공개통신망에서 비밀리에 메시지를 교환하고자 할 때, 공개키 암호방식은 비밀키 암호방식과 비교하여 같은 길이의 메시지를 암호화하는데 많은 시간과 자원이 소요되기 때문에 키의 분배단계에서는 공개키 암호방식을 사용하고 실질적인 메시지 교환단계에서는 비밀키 암호방식을 이용하는 하이브리드 방식을 많이 사용하고 있다. 이런 방식의 대표적인 예로 임의의 난수로 키를 만들어 메시지를 암호화하고 RSA 암호시스템을 이용하여 수신자의 공개키로 암호키를 암호화한 후 상대방에게 보내는 방법이 있다.

이렇게 메시지를 교환함에 있어 메시지에 대한 전자서명은 별개의 과정에 따라 암호화되어 상대방에게 전해지는 것이 일반적이며, 이런 방법을 first-sign-then-encrypt이라고 한다.[4]

Y. Zheng은 이런 두 개의 과정을 하나로 통합한 Signcryption이라는 새로운 개념을 제안하였고, 두 가지 Signcryption 방식을 개발하여, 현재 IEEE P1363a에 등록했으며, 현재 심사 중이다.[5]

Signcryption 방식은 전자서명의 고유기능인 부

* 한국증권전산(주) SignKorea (sdkim@koscom.co.kr, jjd@koscom.co.kr)
** 강남대학교 전산학과 (hkyang@kns.kangnam.ac.kr)

인봉쇄는 물론, 암호화의 고유기능인 기밀성도 제공한다. Signcryption 방식과 유사한 방법으로 H. Petersen 등이 제안한 Authenticated Encryption이 있으나,[8] 이 방식은 수신자가 송신자를 모방할 수 있기 때문에 부인봉쇄 기능을 제공하지 못한다.

H. Petersen 등은 Y. Zheng의 Signcryption 방식을 이용할 때, 수신자가 제3자(판사 혹은 공공기관 등)에게 송신자의 전자서명을 증명하기 위하여 관련정보를 제3자에게 공개하는 경우, 제3자가 공개정보를 바탕으로 해당 송수신자간의 암호화된 메시지를 풀어볼 수 있는 키를 만들 수 있음을 지적하고 이를 개선한 새로운 Signcryption방식을 제안했다.[2]

Y. Zheng이 제안한 방식의 문제는 영지식 증명을 통하여 해결할 수 있지만, 단일 프로토콜 내부에서 발생하는 문제를 별도의 프로토콜을 이용하여 해결해야한다는 점과 영지식 증명방식의 경제적인 문제점이 있다고 할 수 있다.

본 논문에서는 H. Petersen의 Signcryption 방식이 변수 연관성 결여로 부인봉쇄기능을 제공하지 못하여 이를 M. Michels가 보완했지만[3], 보완한 방식이 Y. Zheng이 제안한 방법과 유사한 문제점이 있음을 밝히고 이를 해결한 새로운 Signcryption방식을 제안한다.

2장에서는 Y. Zheng의 Signcryption방식의 문제점을 기술하고, 3장에서는 H. Petersen 등의 Signcryption 방식의 문제점을 분석하며, 4장에서는 기존의 문제점을 해결한 Signcryption방식을 제안한 후, 5장에서 결론을 맺는다.

본 논문에서 가정하는 환경은 다음과 같다.[1,7]

Alice와 Bob은 Signcryption을 주고받으며 Carol은 제3자가 된다. 인증기관은 충분히 큰 소수 p와 q를 선택한다. 이때 p와 q 사이에는 $q|(p-1)$의 관계가 성립하여야 하며, 아울러 위수가 q인 원시원소 g를 선택한다. Alice와 Bob은 전자서명생성키 S_A S_B를 각각 선택한 후 전자서명검증키인 Y_A, Y_B를 다음과 같이 계산하여 인증기관에 등록한다.

$$Y_A = g^{S_A} \bmod P,\ Y_B = g^{S_B} \bmod P$$

M과 C는 각각 평문과 암호문을 의미하며, 암복호화함수 E와 D는 키 v를 이용하여 각각 암/복호화되고 다음의 특성을 갖는다.

$$C = E_v(M),\ M = D_v(C)$$

이외에 본 논문에서 사용하는 기호는 다음과 같다.

- r : 임의로 선택한 q 보다 적은 임의의 난수
- e, K_1, K_2, K : Signcryption계산용 변수
- T, k, C : Signcryption
- $||$: 구분자를 이용한 연접(Concatenation)

II. Y. Zheng의 Signcryption 방식과 문제점

1997년 Y. Zheng은 SDSS1과 SDSS2으로 명명된 두 가지의 Signcryption 방식을 제안하였으며, 각각의 Signcryption 생성과 검증과정은 그림 1과 같다.[4,5]

Y. Zheng은 제안한 방식이 공개통신로 상에서 전자문서의 기밀성을 보장할 뿐만 아니라 전자서명을 통해 부인봉쇄도 동시에 제공한다고 주장하였다.

하지만, 제안된 Signcryption방식은 Bob이 Carol에게 Alice의 Signcryption을 증명하는 과정에서 중간정보가 공개되는 경우에 Carol은 이 정보를 이용하여 Y_{AB}를 계산할 수 있게 되고, Carol은 이 Y_{AB}를 이용하여 Alice와 Bob사이에서 이루어지는 Signcryption에 의한 암호통신문을 언제든지 복호할 수 있는 키를 생성할 수 있음을 H. Petersen 등이 지적하였으며 그 과정은 다음과 같다.[2]

Bob이 Carol에게 Alice의 Signcryption을 증명하는 과정에서 1)과 같이 (e, k, T, Y_B)를 공개한다면 Carol은 [SDSS1]과 [SDSS2] 각각에 대해 2)의 과정을 수행하면 Y_{AB}를 구할 수 있다. Y_{AB}를 알고 있는 Carol이 Alice와 Bob의 비밀통신을 복호화하여 보고 싶다면 3)과 같이 공개된 통신로상의 Signcryption 정보를 가져온 후, Y_{AB}를 이용하여 4)의 수식에 따라 e'를 구할 수 있다. Alice는 평문 M'를 e'의

생성	$r_A \in_R Z_q^*$ $e = Y_B^{r_A} \bmod p$ $K_1 \| K_2 = H(e)$ $k = H(K_2, M)$ [SDSS1] $T = r_A(k + S_A)^{-1} \bmod q$ [SDSS2] $T = r_A(1 + S_A k)^{-1} \bmod q$ $C = E_{K_1}(M)$
통신	T, k, C
검증 및 복호	[SDSS1] $e = (Y_A g^k)^{TS_B} \bmod p$ [SDSS2] $e = (Y_A^k g)^{TS_B} \bmod p$ $K_1 \| K_2 = H(e)$ $M = D_{K_1}(C)$ Check if $k = H(K_2, M)$

[그림 1] Y. Zheng의 Signcryption 방식

해쉬값을 이용하여 암호화하였으므로 Carol은 5)의 과정을 통해 복호키를 만들고 6)에 따라 암호문을 복호화하면 Alice의 평문 M'를 구할 수 있게 된다.

1) *Carol*에게 공개되는 정보 : (e, k, T, Y_B)
2) [*SDSS1*] $Y_{AB} = e^{T^{-1}} Y_B^{k} \ mod\ p = g^{S_A S_B} mod\ p$
   [*SDSS2*] $Y_{AB} = e^{(T^{-1}-1)k^{-1}} \ mod\ p = g^{S_A S_B} mod\ p$
3) 통신로상의 정보 : (T', k', C')
4) [*SDSS1*] $e' = Y_{AB}^{T} Y_B^{k T} \ mod\ p$
   [*SDSS2*] $e' = Y_{AB}^{kT} Y_B^{T} \ mod\ p$
5) $K_1' \| K_2' = H(e')$
6) $M' = D_{K_2'}(C')$

즉 Y. Zheng의 Signcryption 방식은 기밀성을 유지하지 못한다.

Ⅲ. H. Petersen 등의 Signcryption방식과 문제점

H. Petersen 등은 Y. Zheng의 Signcryption 방식이 가지고 있는 단점을 지적하고 이를 보완하여 그림 2와 같은 새로운 Signcryption 방식을 제안하였다.[2]

하지만, 이 Signcryption방식은 Signcryption의 생성과정에서 e와 r_2사이에 아무런 연관관계가 없는 관계로 Bob은 Alice의 전자서명을 모방할 수 있기 때문에 부인봉쇄 기능을 보장할 수 없다는 단점이 있다.

Bob의 모방과정은 다음과 같다.

Bob은 Alice의 Signcryption을 수신한 후, 1)과 같이 q보다 작은 임의의 난수 r_3를 선택한 후, 2)의 과정에 따라 $Y_B^{r_1}$을 생성한 뒤, 3)의 절차를 따르면 e'를 구할 수 있다. Bob은 4)절차에 따라 기존의 Alice가 송신한 Signcryption 중에서 k를 고정한 후 적당한 r_2'를 계산할 수 있다. 그리고 5)와 같이 r_3를 기존의 T에 곱하여 T'를 생성하고, r_2로 새로운 메시지 M'를 암호화하여 C'를 생성하면, 새로운 Signcryption (T', k, C')을 구할 수 있다.

1) $r_3 \in_R Z_q^*$
2) $(Y_A g^{k})^{TS_B} \ mod\ p = Y_B^{r_1} \ mod\ p$
3) $e' = H(Y_B^{r_1 r_2} \ mod\ p)$
4) $k = r_2' e' \ mod\ q$ (k는 고정)
5) $T' = r_3 T = r_3 r_1 (k + S_A)^{-1} \ mod\ q$
6) $C' = E_{r_2'}(M')$

즉, 이 방식은 기밀성은 유지할 수 있지만 수신자가 송신자의 Signcryption을 생성할 수 있기 때문에 부인봉쇄를 할 수 없다는 문제점이 있다.

H. Petersen과 공동집필자인 M. Michels은 이런 사실을 인지하고 기존의 방식을 수정한 그림 3과 같은 Signcryption 방식을 제안하였다.[3]

하지만, 저자가 M. Michels의 Signcryption 방식을 분석한 결과, Y. Zheng등의 Signcryption 방식과 유사한 문제점을 가지고 있다는 것을 발견하였다. 다음의 과정을 따르면 Carol은 Alice와 Bob의 암호통신문을 복호할 수 있다.

Bob이 Alice의 Signcryption을 받아 Carol에게 이를 증명하게 된다면, Carol은 1)과 같은 정보를 획득할 수 있다. 이 정보를 기반으로 2)의 절차에 따르면 Carol은 Y_{AB}를 구할 수 있다. Carol은 Alice와 Bob이 주고받는 정보가 궁금한 경우에 3)과 같은 Signcryption을 가져와 4)의 절차를 따르면 e'를 구할 수 있으며, 5)의 절차에 따라 키를 만들어 암호통신문을 복호하여 M'를 볼 수 있다.

생성	$r_1, r_2 \in_R Z_q^*$ $e = H(Y_B^{r_1} \ mod\ p)$ $k = r_2 e \bmod q$ $T = r_1 (k + S_A)^{-1} \bmod q$ $C = E_{r_2}(M)$
통신	T, k, C
검증 및 복호	$e = H(Y_B^{kT} Y_A^{TS_B} mod\ p)$ $r_2 = k e^{-1} \bmod q$ $M = D_{r_2}(C)$

〔그림 2〕 H. Petersen의 Signcryption 방식

생성	$r_1, r_2 \in_R Z_q^*$ $C = E_{r_1}(M \| H(M))$ $e = H(Y_B^{r_2} \ mod\ p, C)$ $k = r_1 e \bmod q$ $T = r_2 (k + S_A)^{-1} \bmod q$
통신	T, k, C
검증 및 복호	$K = Y_B^{kT} Y_A^{TS_B} \ mod\ p$ $e = H(K, C)$ $r_1 = k e^{-1} \bmod q$ $M \| H(M) = D_{r_1}(C)$

〔그림 3〕 M. Michels의 Signcryption 방식

1) 공개정보 : (Y_B, K, T, k)

2) $Y_{AB} = K^{T^{-1}} Y_B^{k} \bmod p$

$= g^{S_B r_2 r_2^{-1}(k+S_A) - S_B k} \bmod p$

$= g^{S_A S_B} \bmod p$

3) $Signcryption : (T', k', C')$

4) $Y_{AB}^{T} Y_B^{k T} = g^{S_A S_B T' + S_B k' T'}$

$= g^{S_B T'(S_A + k')}$

$= g^{S_B r_2} \bmod p$

$e' = H(g^{S_B r_2} \bmod p, C')$

5) $r_1' = k' e'^{-1}$, $M' = D_{r_1'}(C')$

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

Ⅳ. 제안하는 Signcryption 방식

Y. Zheng등과 H. Petersen등이 제안한 방식은 Signcryption을 Carol에게 증명하게 되면, Carol이 Alice와 Bob의 암호화된 송수신 메시지를 복호해 볼 수 있게 되거나 Bob에 의해 부인봉쇄기능을 상실하는 문제점을 가지고 있음을 살펴보았다. 4장에서는 그림 4와 같은 Signcryption 방식을 제안한다.

제안하는 방식은 기밀성과 부인봉쇄를 동시에 제공하며, Signcryption을 Carol에게 증명하는 과정에서 중간정보들이 공개되어도 Carol은 Alice와 Bob간의 암호문을 풀어볼 수 없다.

제안한 Signcryption 방식의 특징은 다음과 같다.

4.1 기밀성(Confidentiality)

기존에 제안된 방식들은 Y_B^r를 외부에 노출하지 않는 대신 별도의 정보를 이용하여 Y_B^r를 복원하기 때문에 제3자에게 정보가 공개되는 경우에 제3자는 공개된 정보를 이용하여 Y_{AB}를 계산할 수 있고, 이를 기반으로 암호문의 복호에 필요한 키를 만들 수 있다는 공통점이 있다. 제안하는 방식에서는 Y_B^r를 전자서명 값으로 직접 이용하여 제 3자가 Y_{AB}를 계산하더라도 전자서명의 안전성을 유지할 수 있도록 하였다. 또한 k에서 g^r을 계산하기 위해서는 Bob의 전자서명생성키(S_B)를 알아야 하므로 수신자만이 이를 복호할 수 있다. 그러므로 기밀성을 보장한다고 할 수 있다.

생성	$r \in_R Z_q^*$ $K = g^r \pmod p$ $k = Y_B^r \pmod p$ $e = H(K, M) \pmod q$ $T = r - S_A e \pmod q$ $C = E_K(M \| T)$
통신	k, C
검증 및 복호	$K' = k^{S_B^{-1}} \pmod p$ $M' \| T' = D_K(C)$ $e' = H(K', M') \pmod q$ $Check\ if\ K' = Y_A^{e'} g^{T'} \pmod p$

[그림 4] 제안하는 Signcryption 방식

또한 기존 Signcryption 방식은 T, k, C을 공개적으로 Bob에게 송부하지만, 제안하는 방식은 T를 암호화한 후 C에 포함하여 송부하므로 공격자는 T를 알 수 없다.

k를 이용하여 암호문 C를 복호해야만 T를 알 수 있다. 그러므로 기존의 방식에 비해 외부에 공개되는 정보를 최소화할 수 있다.

4.2 부인봉쇄(Non-Repudiation)

제안하는 Signcryption 방식의 부인봉쇄 기능은 Schnorr의 전자서명방식을 기반으로 한다.[7] 단, Schnorr의 전자서명방식에서는 전자서명이 e, T이지만, 제안하는 방식에서는 e대신 암호문 C를 복호할 수 있는 k를 Bob에게 주고 Bob이 암호문을 복호하여 e를 생성하도록 하였다.

Schnorr의 전자서명방식이 안전하므로 제안하는 Signcryption 방식에서 제공하는 부인봉쇄기능도 안전하다고 할 수 있다.

4.3 다자전송 효율성

기존에 제안된 Signcryption방식은 수신자의 공개키가 전자서명 생성에 직접 관련되기 때문에 수신자 지정형 서명방식의 특성을 갖게 되어 각 수신자별로 Signcryption을 생성해야 한다. 하지만 제안하는 방식은 수신자의 공개키가 전자서명 생성에 영향을 주지 않기 때문에 수신자와 직접적으로 관련된 정보인 Y_B^r만 Y_C^r로 변경하면 C의 변화 없이 Carol을 위한 Signcryption을 만들 수 있다.

이런 특성은 동일한 문서에 Signcryption을 생성하여 다수의 사람에게 송부할 때 효율적일 수 있는데 메일 프로그램에서 cc를 이용하여 참조하는 사람에게 동일한 메일을 보내는 경우가 한 예라 할 수 있다.

〔표 1〕 Signcryption 방식 비교

구분	SDSS1		SDSS2		Petersen2		[illegible]		Sign(Schnorr) Encryption		Sign(DSS) Encryption	
	Sign	Verify	Sign	Verify	Sign	Verify	[illegible]		Sign	Verify	Sign	Verify
EXP	1	1.17	1	1.17	1	1.17	[illegible]		3	2.17	3	2.17
MUL	0	2	1	2	2	4	[illegible]		1	1	1	1
DIV	1	0	1	0	1	1	[illegible]		0	0	1	2
ADD	1	0	1	0	1	0	[illegible]		1	0	1	0
HASH	2	2	2	2	2	2	[illegible]		1	1	1	1
Com Overhead	|H()|+|q|		|H()|+|q|		|H()|+2|q|		[illegible]		|H()|+|q|+|p|		2|q|+|p|	

4.4 계산량 및 통신량

암호시스템 및 전자서명시스템의 효율성은 주로 계산량과 통신량을 기준으로 한다. 표 1은 Y. Zheng의 P1363 제출 자료를 기반으로 H. Petersen의 방식과 제안한 방식을 추가하여 계산량과 통신량을 비교하였다. 통신량의 비교에서 암호문의 길이는 동일하므로 표에서는 생략하였다.[5]

제안한 Signcryption 방식은 서명 후 암호화 방식에 비해서 모듈러 멱승의 수가 적고 통신에 따른 오버헤드가 적음을 알 수 있다. 또한 Signcryption의 생성과정에서 K는 Signcryption의 수신인, 대상문서 등과 관련이 없기 때문에 사전에 계산하여 안전하게 저장한 후 이를 사용할 수 있으므로 이를 적용하는 경우에 기존에 발표된 Signcryption방식과 큰 차이 없이 Signcryption을 생성할 수 있다. (※ 표 1에서 연산부분의 "( )"는 사전계산이 가능함을 의미한다.)

또한 통신량은 기존의 Signcryption 방식에 비해서는 많지만 서명 후 암호화방법에 비해서는 적은 량을 수신자에게 보낸다.

V. 결 론

본 논문에서는 기존의 Signcryption 방식의 문제점을 살펴보고 문제점을 찾아 이를 수정한 새로운 Signcryption을 제안하였다. 제안한 방식은 일반적인 서명 후 암호화 방식보다 계산량과 통신량에서 효율적이며, 기존의 Signcryption방식에서 발생할 수 있는 문제점을 해결한 방식이다.

현재 3개의 공인인증기관이 설립되었으며, 공인인증서비스가 확산되고 있다. 인증서비스를 이용하는 고객은 전자서명 서비스와 동시에 정보의 기밀성 유지를 요구하고 있다.

그러므로 제안한 방식은 메시지 내용을 비공개하면서 동시에 송신자의 전자서명이 필요한 분야에 유용하게 사용될 수 있을 것으로 사료된다.

참 고 문 헌

〔1〕 T. ElGamal, "A Public key cryptosystem and a signature scheme based on discrete logarithms", *IEEE Transactions on Information Theory*, IT-31 (4) : pp. 469~472, 1985.

〔2〕 H.Petersen and M. Michels, "Cryptanalysis and improvement of signcryption schemes", *IEE Computer and Digital Techniques* 1998. (http://www.geocities.com/CapeCanaveral/Lab/8967/publications.html)

〔3〕 H.Petersen and M. Michels, "Cryptanalysis and improvement of signcryption schemes", *IEE Computer and Digital Techniques* 1998.(Revised Version). (http://www.geocities.com/CapeCanaveral/Lab/8983/pu.html)

〔4〕 Y.Zheng, "Digital signcryption or how to achieve cost(signature and encryption cost(signature)+cost(encryption)", In *Advances in Cryptology CRYPTO-97*, LNCS 1294, Springer-Verlag, pp. 165~179, 1997

〔5〕 Y. Zheng, "Shortened Digital Signature, Signcryption and Compact and Unforgeable Key Agreement Schemes" P1363 Sub-

missions to the Study Group for Future Public-Key Cryptography Standards. (http://grouper.ieee.org/groups/1363-/StudyGroup/submissions.html#Hybrid)

[6] W. Diffie, M. Hellman, M "New directions in cryptography", *IEEE Transactions on Information Theory* IT-22(1976) pp. 472~492.

[7] C.P. Schnorr "Efficient Signature Generation for Smart Cards", *Advances in Cryptology-CRYPTO '89* Proceedings, Springer-Verlag, 1990, pp. 239~252.

[8] P. Horster, M. Michels, H. Petersen "Authenticated encryption with low communication costs", *Electronic Letters*, Vol. 30, No. 15, July 1994, pp. 1230~1231.

〈著者紹介〉

김 성 덕 (Sung-duk Kim)
1994년 2월 : 성균관대학교 정보공학과 졸업
1996년 2월 : 성균관대학교 정보공학과 석사
1996년 3월 ~ 1999년 6월 : 한국전산원 주임연구원
1999년 6월 ~ 현재 : 한국증권전산(주) 전자인증사업부 연구원
〈관심분야〉 암호이론, 인증서비스, 통신보안

정 재 동 (Jae-dong Jung)
1983년 2월 : 연세대학교 수학과 졸업
1994년 8월 : 연세대학교 전산학과 석사
1998년 7월 ~ 현재 : 숭실대학교 컴퓨터공학과 박사과정
1982년 11월 ~ 현재 : 한국증권전산(주) 전자인증사업부장
〈관심분야〉 인증서비스, 멀티미디어 보안, 정보보호관리

양 형 규 (Hyung-Kyu Yang) 정회원
1983년 2월 : 성균관대학교 전자공학과 학사
1995년 2월 : 성균관대학교 전자공학과 석사
1994년 8월 : 성균관대학교 정보공학과 박사
1982년 12월~1990년 2월 : 삼성전자 컴퓨터 부문 선임연구원
1995년 3월~ 현재 : 강남대학교 이공대학 산전전공학부 전자계산전공 조교수
〈주관심분야〉 암호 이론 및 응용, 네트워크 보안, 전자화폐, 정보 은닉 등