韓國 컴퓨터情報學會 論文誌
第11卷 第2號, 2006. 5.

2006-11-2-2-5

안전성을 보완한 ID기반 signcryption 기법

곽 병 옥*, 정 윤 수**, 이 상 호***

ID-based signcryption with improved security

Byeong-Ok Kwak *, Yoon-Su Jeong **, Sang-Ho Lee ***

요 약

Zheng이 제안한 Signcryption 기법은 전자 서명과 대칭키 암호화를 논리적으로 한 단계에 수행함으로써 기존의 서명 후 암호화 기법들에서 요구되는 계산비용보다 적은 비용을 가지는 새로운 암호학적인 기법이다. 현재까지 제안되어 온 Signcryption 기법들에서는 송신 부인이 발생하여 제3자가 이를 검증해야 할 경우 수신측의 비밀키 노출이 불가피하였다. 이 문제를 해결하기 위해 이 논문에서는 익명성과 Unlinkability를 지원하는 다목적의 ID기반 Signcryption기법을 제안한다. 제안된 기법은 Weil-pairing을 암호화에 이용하면서 random oracle 모델의 안전성을 유지하고, 결정적 쌍선형 Diffie-Hellman 의미론적 보안의 형식적 증명을 따르기 때문에 기존 Signcryption 기법들보다 안전하면서 효율적이다.

Abstract

Zheng's signcryption scheme is a new encryptical scheme of which can save more expense than those of the current signature encryption by using digital signature and symmetric key encryption logically. The current signcryption schemes have a problem that is to be exposed the secret key of the receiver in the case of checking repudiation of origin by the third party. To solve this problem, a solution suggested in this paper is to use multi-purpose ID-based signcryption scheme with anonymity and unlinkability. This solution is safe and more efficient than current signcryption schemes because the suggested scheme keeps the security of the random oracle model as using Weil-pairing in encryption, and follows a formal proof of semantic security of the decisional Diffie-Hellman problem.

▸ Keyword : Signcryption, Diffie-Hellman, random oracle

• 제1저자 : 곽병옥
• 접수일 : 2006.03.14, 심사완료일 : 2006. 5.24
* 한국전자통신연구원 선임연구원, ** 충북대학교 대학원 전자계산학과 박사수료
*** 충북대학교 전기전자 컴퓨터공학부 교수

Ⅰ. 서 론

Zheng에 의해 최초로 제안된 Signcryption 기법은 새로운 암호의 기본 요소로써 서명과 암호 기능을 논리적인 한 스텝으로 동시에 처리할 수 있으며 계산 비용 측면에 있어서도 전통적인 서명 후 암호 패러다임에 의해 요구되는 계산량보다 현저히 낮은 암호학적인 기법이다[1, 2]. Zheng의 Signcryption 기법은 보안 파라메터(security parameter)들의 크기에 비례해서 비용 효율이 증가하기 때문에 높은 레벨의 보안을 요구하는 어플리케이션에 대해 더욱 큰 비용 효율을 기대할 수 있지만 서명이 제 삼자에 의해 검증되어져야 하는 경우에는 이용될 수 없는 단점을 가지고 있다. 이러한 문제를 해결하기 위하여 Bao와 Deng (이하 "BD기법"이라 함)이 Zheng의 Signcryption 기법을 수정하여 서명 검증에 수신자의 개인키를 요구하지 않는 기법을 제시하였으나 계산량 측면에서 Zheng의 기법만큼 효율적이지 못하였다[25].

BD기법의 문제점인 메시지의 기밀성을 해결하면서 방화벽 시스템을 이용하기 위한 방법으로 Gamage, Leiwo, Zheng (이하 "GLZ기법"이라 함)은 BD기법을 수정한 새로운 Signcryption 기법을 제시하였다[26]. 또한 기존 Signcryption 기법이 forward secrecy를 제공하지 못하는 단점을 보완하여 2001년 Zheng과 Jung이 새로운 Signcryption 기법을 제안하였지만 한 번의 추가적인 멱승 연산을 필요로 하는 계산량 때문에 비효율적이다[3, 20, 23]. 그리고 2002년에는 Malone-Lee가 Hess의 ID기반 signature를 이용하여 IBE(ID-based Encryption) 암호시스템을 단순화시킨 Signcryption 기법을 제안하였지만 계산적 쌍선형 문제의 어려움보다 강한 가정으로 동일한 권한에 의존하지 않는 송신자로부터 signcrypt된 메시지를 수신받기 위해 시스템의 사용자는 계층적인 ID기반 Signcryption을 요구하는 문제점을 가지고 있다[18].

따라서, 이 논문에서는 기존 Signcryption에서 제공되지 못했던 보안속성 중 메시지의 익명성과 Unlinkability를 제공하기 위해 Weil-pairing 기법을 이용하여 random oracle 모델의 안전성과 결정적 쌍선형 Diffie-Hellman의 의미론적 보안을 만족하는 다목적 ID기반 Signcryption 기법을 제안한다. 제안된 기법은 암호화된 메시지를 그룹정보와 개인정보의 조합으로 구성된 짧은 암호문를 이용하기 때문에 동일한 그룹 세션 정보를 가지는 수신자들의 서명을 검증할 수 있다. 특히 집단 서명의 기능을 만족하기 때문에 계산 비용과 통신 비용은 전형적인 서명 후 암호화하는 기법보다 훨씬 경제적이다.

이 논문의 구성은 다음과 같다. 2장에서는 Signcryption의 일반적인 구조 및 요구사항, 안전성 기반문제와 서명 검증에 사용되는 Gap Diffie-Hellman Group과 Weil-pairing, 기존 Signcryption 기법들을 기술한다. 3장에서는 보안속성을 만족하는 Weil-pairing 기반의 새로운 Signcryption 기법을 설명한다. 4장에서는 제안기법의 보안성과 효율성을 분석한다. 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 관련 연구

이 장에서는 Signcryption의 일반적인 구조와 요구사항을 2.1절에서 간단하게 살펴보고, 안전성 기반문제와 서명 검증을 위해 2.2절에서 Gap Diffie-Hellman 문제와 Weil-pairing에 대해서 설명한다. 그리고 Signcryption 관련 기법들을 2.3절에서 소개한다.

2.1 Signcyprtion 구조 및 요구사항

전통적인 IBE 시스템처럼 Signcryption 기법은 Setup, Keygen, Signcrypt, Unsigncrypt의 4가지 알고리즘으로 구성된다[21].

Setup

안전한 매개변수 K가 주어지면 PKG는 시스템의 공개 파라미터 $params$를 생성한다.

Keygen

개인식별정보 ID가 주어지면 PKG는 ID와 일치하는 개인키 d_{ID}를 계산하고 안전한 방법으로 그것을 Alice에게 전송한다.

Signcrypt

Bob에게 메시지 m을 보내기 위해서 Alice는 암호문 σ를 얻기 위해서 $Signcrypt(\sigma, d_{ID_b}, ID_a)$을 계산한다.

Unsigncrypt

Bob이 σ를 수신했을때 $Unsigncrypt(\sigma, d_{ID_b}, ID_a)$를 계산하고 σ가 ID_a와 ID_b사이의 명확한 암호문이라면 텍스트 m이나 심볼 ⊥을 얻는다.

안전한 그룹 signature는 다음의 속성을 만족해야 한다[28].

- Correctness

sign을 사용하여 그룹 멤버에 의해 처리되는 signature는 Verify에 의해 받아들여진다.

- Unfrogeability

그룹 멤버들만이 그룹에 속한 메시지를 sign할 수 있다.

- Anonymity

주어진 signature, identifying의 실제 signer는 그룹 멤버 이외에는 계산상으로 어렵다.

- Unlinkability

두개의 서로 다른 signature가 동일한 그룹 멤버에 의해 계산되었던 결정은 계산상으로 어렵다.

- Traceability

그룹 관리자는 항상 명백한 signature를 가지고 있는 멤버의 identity를 만들 수 있다.

- Exculpability

그룹 멤버나 그룹 멤버의 일부가 공모할지라도 그룹 멤버에 포함되지 않은 멤버들에 의해서 sign되지는 않는다.

- Coalition-resistance

공모한 그룹 멤버들의 subset은 추적할 수 없는 명백한 그룹 signature를 생성할 수 없다.

- Efficiency

그룹 signature의 효율성은 파라미터에 기반한다. (그룹 공개키의 크기, 그룹 signature의 길이, 알고리즘의 효율성, 그룹 signature의 프로토콜)

2.2 Gap Diffie-Hellman Group과 Weil-pairing

이 장에서는 안전성 기반문제와 서명 검증을 위해 2.2.1절에서는 제안한 방식에 사용된 안전성 기반 문제 즉, 계산적인 Diffie-Hellman 문제와 결정적인 Diffie-Hellman 문제와의 관계에서 나온 Gap Diffie-Hellman 문제를 다루고 2.2.2절에서는 서명 후의 검증과정에 사용되는 bilinear 함수와 Weil-pairing에 대해서 설명한다.

2.2.1 Gap Diffie-Hellman 군

이산대수 문제를 이용한 암호 및 서명 방식의 안전성은 Diffie-Hellman 시스템의 어려움에 기반하고 있다. Diffie-Hellman 문제는 계산적 Diffie-Hellman 문제, 결정적 Diffie-Hellman 문제, Gap Diffie-Hellman 문제로 분류되며 이 논문에서 사용되는 Diffie-Hellman 문제를 정리하면 다음과 같다.

- 계산적 Diffie-Hellman 문제
  (CDHP:Computational Diffie-Hellman Problem)

  g, $g^x \pmod p$와 $g^y \pmod p$를 계산하는 문제

- 결정적 Diffie-Hellman 문제
  (DDHP : Decisional Diffie-Hellman Problem)

  g, $g^x \pmod p$, $g^y \pmod p$와 w로부터 $w = g^{xy} \pmod p$인지를 결정하는 문제

위 문제들 사이의 관계를 살펴보면 CDHP가 해결되면 DDHP가 해결됨을 알 수 있다. 이들의 동치관계에 대하여 수많은 노력이 있었지만 그 역의 성립에 대하여는 알려진 사실이 없다. 이에 대하여 2001년 T. Okamoto와 D. Pointcheval은 CDHP와 DDHP해결의 어려움에 차이가 있을 경우, 이 차이에 기반한 서명 방식의 존재 가능성을 제시하였다[10, 24]. 그들은 CDHP의 해결은 어려우면서, DDHP의 해결은 쉬운 군(Group)을 Gap Diffie-Hellman(GDH)군이라고 정의하고 이러한 문제를 GDH문제라고 정의하였다. 즉,

- Gap Diffie-Hellman
  (GDHP : Gap Diffie-Hellman Problem)

  g, $g^x \pmod p$, $g^y \pmod p$로부터 DDH Oracle을 이용하여 $g^{xy} \pmod p$를 계산하는 문제

이 후 2001년 D. Bonech, B. Lynn와 H. Shacham은 타원곡선 상에서의 이산대수문제(DLP : Discrete Logarithm Problem)의 공격에 이용되었던 Weil-pairing을 암호화에 응용하여, GDH군에서 실제로 구현 가능한 새로운 서명 방식을 제안하였다[8]. 그들은 서명을 수신한 사람은 누구든지 수신된 서명의 정당성을 쉽게 확인할 수 있어야 하지만, 서명의 생성자 이외에는 누구도 서명을 생성

할 수 없어야 한다는 사실에 착안하여 GDHP특성을 만족하는 예를 찾았다. 그리고 같은 년도에 D. Bonech와 D. Franklin은 Weil-pairing을 이용한 ID기반의 암호방식도 제안하였다[9]. 또 다른 GDH군을 찾기 위해 많은 학자들의 연구가 이루어지고 있지만, Weil-pairing과 같은 bilinear함수를 적용한 초특이 타원곡선을 제외하고는 현재까지 알려진 GDH군은 존재하지 않는다.

2.2.2 Gap Diffie-Hellman 군

Weil-pairing은 타원곡선 이산대수 문제의 공격에 사용되어 왔으나, 2001년에 몇 편의 논문을 통하여 암호 응용 프로토콜에도 사용이 될 수 있다는 사실이 알려지기 시작했다. 이러한 이유는 Weil-pairing을 이용하면 삼자 키 공유 시스템의 구성도 가능하며, Diffie-Hellman 계산 문제는 여전히 어려우면서도 Diffie-Hellman 판별 문제도 쉽게 해결이 될 수 있기 때문이다[12, 13, 14].

Weil-pairing은 초특이 타원곡선 상에서 정의되는 쌍선형사상(bilinear map)으로 E가 초특이 타원곡선 위의 점으로 이루어지는 군이고, F_{p^2}의 크기가 p^2인 유한체라고 할 때, 쌍선형사상 e는 다음과 같이 정의된다[11].

$$e : E \times E \rightarrow F_{p^2}$$

이 때, 쌍선형사상은 다음과 같은 성질을 만족한다.

$$e(aP, bQ) = e(P, Q)^{ab}$$

Weil-pairing에 대한 엄밀한 정의 및 수학적인 결과는 [16]을 통하여 살펴볼 수 있다.

타원곡선 위의 점들(P, aP, bP, cP)이 주어졌을 때, Diffie-Hellman 판별 문제는 Weil-pairing을 사용하여 다음의 식이 만족하는지만 계산하면 쉽게 해결할 수 있다.

$$e(aP, bP) = e(P, cP)$$

위의 계산은 쉽게 할 수 있다. 따라서 Okamoto와 Point-cheval이 소개한 Gap problem 특성을 만족하는 예가 될 수 있으며, Weil-pairing을 이용하면 실제 구현 가능한 서명 방식의 구성이 가능하다[8]. 실제 [8]에서는 어떠한 방법을 통하여 서명 방식의 구성이 가능하며, 이 때 사용되는 파라미터 등을 어떻게 선택하는지에 관하여 다루고 있으며, 짧은 길이의 서명문을 만드는 시스템에 관하여 소개하고 있다.

2.3 Signcryption 기법

2.3.1 Zheng의 Signcryption 기법

기존 Signcryption과 Unsigncryption 알고리즘, 그리고 사용되는 공개키와 비밀키 파라메터들을 다음의 [표1]와 같이 요약할 수 있다

표 1 Zheng의 Signcryption 기법
Table 1 Zheng's Signcryption Scheme

A(Signcryption)	⇒	B(Unsigncryption)
$x \in_R [1,2,\ldots,q-1]$ $k = \text{hash}(y_b^x \bmod p)$ $k_1 \mid\mid k_2 = k$ $c = E_{k_1}(m)$ $r = KH_{k_2}(m)$ $s = x/(r + x_a) \bmod q$	(c, r, s)	$K = \text{hash}((y_a g^r)^{s \cdot x_b} \bmod p)$ $k_1 \mid\mid k_2 = k$ $m = D_{k_1}(c)$ $KH_{k_2}(m)$ = r 인지 검증

여기서, p는 512bit 이상의 큰 소수이고 q는 q|(p)를 만족하는 큰 소수, g는 법 p상에서 위수 q인 정수이며 hash는 일 방향 해쉬 함수, E()와 D()는 대칭키 암호화 및 복호화 함수이며, $k_1 \parallel k_2$ 는 k_1 와 k_2 의 연접(concatenation)을 의미하고, KH()는 keyed-해쉬 함수이다.

사용자 A는 랜덤 비밀 값 x와 사용자 B의 공개키 $y_b = g^{x_b}$ 를 이용하여 세션키 k를 생성한다. 그 후 그 세션키 k를 k_1 와 k_2 로 분리한 후 각각 암호화 키와 keyed-해쉬 함수의 키로 사용한다. 또한 사용자 A는 랜덤 비밀 값 x, keyed-해쉬 값 r, 그리고 자신의 비밀키 x_a 를 이용하여 법 q상에서 서명 값 s를 생성하여, (c, r, s)를 사용자 B에게 전송한다. 이를 수신 받은 사용자 B는 사용자 A의 공개키 $y_a = g^{x_a}$ 와 자신의 비밀키 x_b 를 이용하여 세션키 k를 계산하여 암호화된 메시지 c를 복호화하고, 메시지에 대한 서명 검증을 실시한다. 만일 사용자 A의 비밀키 x_a 가 노출되었을 경우, 그 키를 알고 있는 사람은 다음의 식에 의해 세션키 k를 계산할 수 있게 된다.

$$(y_a g^r)^{s \bullet x_b} = (y_b^{x_a + r})^s$$

따라서, 기존 기법은 forward secrecy를 제공하지 못한다.

2.3.2 F. Bao의 변형 Signcryption 기법

이 기법은 F. Bao 등에 의해 제안되었으며, signcrypt된 메시지에 대해 수신자의 비밀키 없이 누구나 검증 가능하도록 변형된 기법이다[25]. 이 기법은 [표 2]와 같이 요약될 수 있으며, 사용되는 파라메터들에 대한 정의는 다음과 같다.

p는 큰 소수이고 q는 q|ϕ(p)를 만족하는 큰 소수, g는 법 p상에서 위수 q인 정수이며 hash는 일방향 해쉬 함수, E(·)와 D(·)는 대칭키 암호화 및 복호화 함수이며, $k_1 \parallel k_2$는 k_1과 k_2의 연접(concatenation)을 의미하고, KH(·)는 keyed-해쉬 함수이다.

이 기법에서 A가 송신부인을 하였을 경우, B는 Signcrypt된 메시지가 A에 의해 서명되었다는 것을 증명하기 위해 (c, r, s)를 제 삼자에게 전송하게 되고, 제 삼자는 다음의 절차를 수행하여 검증을 할 수 있게 된다:

$k_2 = hash((y_a \bullet g^r)^s mod p)$

$r = KH_{k_2}(m)$ 인지 검증

하지만, 이 기법에서는 반드시 제 삼자에게 평문이 노출되어야만 하는 단점이 존재하게 된다.

표 2 F. Bao의 변형 Signcryption 기법
Table 2 F. Bao's Transformation Signcryption Scheme

A(Signcryption)	⇒	B(Unsigncryption)
$x \in_R [1,2,\ldots,q-1]$ k_1 = hash(y_b^x mod p) k_2 = hash(g^x mod p) c = $E_{k_1}(m)$ r = $KH_{k_2}(m)$ s = x/(r+ x_a) mod q	(c, r, s)	$t_1 = (y_a g^r)^s$ mod p $t_2 = t_1^{x_b}$ mod p $k_1 = hash(t_2)$ $k_2 = hash(t_1)$ $m = D_{k_1}(c)$ $KH_{k_2}(m)$ = r 인지 검증

2.3.3. Malone-Lee의 Signcryption 기법

2002년 Malone-Lee는 ID기반의 Signcryption기법을 제안했다[18]. 이 기법은 Hess의 ID기반 signature와는 다르게 signature를 Boneh-Franklin암호 기법에 단순히 조합하였다[9, 19]. Malone-Lee 기법에 의해 생성된 암호문은 signaeture와 암호문이 연이어 일어나는데 흔히 이것을 encrypt-and-sign이라고 불리운다. [표 3]은 Malone-Lee의 Signcryption 기법을 나타내고 있다.

이 기법에서는 사용자에 의존하지 않으면서 미리 계산된 $e(P, P_{pub})$을 사용하여 효율적이지만 $e(P, P_{pub})$에 사용된 P, P_{pub}을 이용한 Known Key 공격이나 key control에 취약성을 가지고 있다[13]. 또한 동일한 권한에 의존하지 않는 송신자로부터 signcrypt된 메시지를 수신받기 위해 시스템의 사용자는 계층적인 ID기반 Signcryption을 찾아야 하는 연구가 필요하다.

표 3 Malone-Lee의 Signcryption 기법
Table 3 Malone-Lee's Signcryption Scheme

Setup	Keygen
보안 파라미터 k를 보내면, PKG는 소수 q의 그룹 G_1 과 G_2 를 선택한다. G_1의 생성자 P, 쌍선형사상 $e : G_1 \times G_1 \rightarrow G_2$ 와 해쉬 함수 $H_1 : \{0,1\}^* \rightarrow G_1$, $H_2 : \{0,1\}^* \rightarrow F_q^*$, $H_3 : G_2 \rightarrow \{0,1\}^n$. 마스터 키 s$\in F_q^*$ 을 선택하고 $P_{pub} = sP$을 계산한다. 시스템의 공개 파라미터는 P = (G_1, G_2, n, e, P, P_{pub}, H_1, H_2, H_3) 와 같으며 암호문의 크기는 n으로 지정한다.	개인 인식 정보 ID가 주어지면 PKG는 $Q_{ID}=H_1(ID)$와 개인키 $d_{ID}=sQ_{ID}$을 계산한다.
Signcrypt	**Unsigncrypt**
Bob에게 메시지 m을 보내기 위해서 Alice는 다음의 단계를 수행한다. 1. $Q_{ID_B}=H_1(ID_B)\in G_1$을 계산한다. 2. $x \leftarrow_R F_q^*$를 선택하고 $k_1 = e(P, P_{pub})^x$와 $k_2 = H_2(e(P_{pub}, Q_{ID_B})^x)$을 계산한다. 3. c=$E_{k_2}(m)$, r=$H_3(c, k_1)$을 계산한다. $S = xP_{pub} - rd_{ID_A} \in G_1$ 암호문은 σ =(c,r,S)이다.	σ =(c,r,S)을 수신하였을때 Bob은 다음을 수행한다. 1. $Q_{ID_A}=H_1(ID_A)\in G_1$을 계산한다. 2. $k_1=e(P,S)e(P_{pub}, Q_{ID_A})^r$을 계산한다. 3. $\tau=e(S, Q_{ID_B})e(Q_{ID_A}, d_{ID_B})^r$와 $k_2=H_2(\tau)$을 계산한다. 4. $m=D_{k_2}(c)$을 복구하고 $r=H_3(c, k_1)$을 만족하면 σ을 받아들인다.

III. Weil-pairing 기반의 다목적 ID기반 Signcryption

Zheng은 효율적인 Signcryption 기법을 만들기 위해 SDSS1과 SDSS2 시그너처(signatures) 구조를 사용하였고 안전성을 제공하기 위해 shortened ElGamal 기반 시그너처 기법이나 Schnorr 시그너처 기법을 사용하고 있다[15, 17]. 하지만 여기서 제안하는 기법은 Hess의 ID기반 구조를 기반으로 안전하면서도 효율적인 Signcryption을 얻기 위해 random 오라클 모델의 안전성과 결정적 쌍선형 Diffie-Hellman 의미론적 보안의 형식적 증명을 만족하는 블록을 만들어 사용한다.

3.1 시스템 계수

- p : 큰 소수
- q : q|ϕ(p)를 만족하는 큰 소수
- g : 법 p상에서 위수 q인 정수
- H() : 일방향 해쉬함수
- KH() : keyed 해쉬함수
- E(·)/D(·) : 대칭키 암호화 및 복호화 함수

3.2 Weil-pairing 기반의 다목적 ID기반 Signcryption 기법

제안 기법은 전통적인 IBE 시스템처럼 Setup, Keygen, Signcrypt, Unsigncrypt의 4가지 알고리즘으로 구성된다.

위 구조의 일관성은 타원곡선상에 정의되는 쌍선형사상(bilinear map)으로 쉽게 검증할 수 있다.

표 4 Weil-pairing 기반의 다목적 ID기반 Signcryption 기법
Table 4 Weil-pairing based multi-purpose ID based Signcryption Scheme

Setup	Keygen
보안 파라미터 k와 n을 준다. PKG는 안전한 대칭 암호문 (E,D)를 선택하는 것을 제외하면 Malone-Lee 기법과 같은 시스템 파리미터를 선택한다. 그리고, 해쉬 함수는 다음과 같다. $H_1 : \{0,1\}^* \rightarrow G_1$, $H_2 : G_2 \rightarrow \{0,1\}^n$, and $H_3 : \{0,1\}^* \times G_2 \rightarrow F_q$	인식 ID를 주면 PKG는 ID_G를 생성하고 ID를 사용하여 공개키 $Q_{ID}=H_1(ID)$ 를 계산한다. 그리고, 개인키 $d_{ID} = sQ_{ID}$를 계산한다.
Signcrypt	**Unsigncrypt**
1. $Q_{ID_B} = H_1(ID_B) \in G_1$을 계산한다. 2. B의 ID_B와 PKG의 ID_G 정보를 이용하여 그룹 정보를 만든다. $ID_P = ID_G \oplus ID_B$, 와 $Q_{ID_G} = H_1(ID_P) \in G_1$ 을 계산한다. 3. x $\leftarrow {}_R F_q^*$ 을 선택하고 난 후 $k_1 = e(sP, Q_{ID_G})^x$와 $k_2 = H_2(e(Q_{ID_G}, sQ_{ID_B})^x)$을 계산한다. 4. c= $E_{k_2}(m)$와 r= $H_3(c, k_1)$와 V = $sQ_{ID_G} - xrd_{ID_A}$를 계산한다. 암호문 σ=(c, r, V)이 만들어진다.	1. $Q_{ID_A} = H_1(ID_A) \in G_1$을 계산한다. 2. A의 ID_A와 PKG의 ID_G 정보를 이용하여 그룹 정보를 만든다. $ID_P = ID_G \oplus ID_A$, $Q_{ID_G} = H_1(ID_P) \in G_1$ 3. $k_1=(P, V)(sP, Q_{ID_A})^r$을 계산한다. 4. r=$e(V, Q_{ID_B})(Q_{ID_A}, d_{ID_B})^r$와 $k_2=H_2(r)$을 계산한다. 5. m= $D_{k_2}(c)$ 을 복구하고 r= $H_3(c, k_1)$이 맞다면 σ를 받아들인다.

$$e(P, V)e(sP, Q_{ID_A})^r = e(P, sQ_{ID_G})e(P, -xrd_{ID_A})e(sP, Q_{ID_A})^r = e(P, sQ_{ID_G})^x(P, -rd_{ID_A})(P, rd_{ID_A})^r = e(sP, Q_{ID_G})^x$$

그리고

$$e(V, Q_{ID_B})e(Q_{ID_A}, d_{ID_B})^r = e(sQ_{ID}, Q_{ID_B})e(-xrd_{ID_A}, Q_{ID_B})e(Q_{ID_A}, d_{ID_B})^r = e(sQ_{ID_G}, Q_{ID_B})e(-rd_{ID_A}, Q_{ID_B})^x e(rd_{ID_A}, Q_{ID_B}) = e(Q_{ID_G}, sQ_{ID_B})^x$$

제 삼자는 위의 step 1에서 k_1을 복구하기 위해 메시지의 origin을 확인하고 $r=H(c, k_1)$의 상태를 체크한다. 이때 사용되는 평문 m의 정보는 메시지 origin의 공개적인 검증에는 사용하지 않고 Alice가 일부 평문 m의 송신자라고 누군가 확신하기 위해서 수신자는 제 3자에게 임시적인 복호화 키 k_2를 포워드(forward)한다.

$r=H_3(m, k_1)$에서 $r=H_3(c, k_1)$의 변환은 BD기법의 초기 구조를 수정하였을때 시스템의 위조방지에 영향을 받지 않으면서 Malone-Lee 기법의 의미적 보안과 같은 동일한 효과를 나타내고 있다. 이것은 의미적 레벨에 있어서 초기 BD기법 보안을 향상시킨 것이다. 또한 P와 그룹 정보를 이용하여 메시지 signcrypt에 사용하였기 때문에 시스템 사용자의 계층적 정보를 이용하여 송신자의 동일한 권한에 의존하지 않기 때문에 기존 기법보다 효율적이면서 비용 또한 기존 Malone-lee기법과 유사하다.

제안기법의 signcrypton 동작은 G_2의 2 멱승과 $aP+bQ \in G1$의 계산이 1번 사용되고, Unsigncrypt 동작에서는 2 pairing 계산과 2 멱승만이 사용된다. 더욱이 위의 구조는 의미적 보안을 수행하기 위한 강력한 Fujisaki-Okamoto 전송 가정을 필요로 하지 않는다[27].

IV. Weil-pairing 기반의 다목적 ID기반 Signcryption 성능분석

4.1 보안 속성

제안기법은 [21]처럼 기밀성, 부인봉쇄, 그리고 암호문 인증의 세 가지 안전성을 보장하고 추가로 비연결성(Unlinkability), 익명성(Anonymity)의 집단서명 기능을 함께 제공하기 때문에 기존 기법보다 더 효율적이다.

정리 1. 랜덤 오라클 모델에서, t의 수행시간과 q_{H_1} 신원 해싱 중 q_R H_3, q_R Signcrypt, q_U Unsigncrypt 등의 요구를 요청할 때 이익 ε 을 가지는 게임에서 암호문을 구별할 수 있는 적 A는 IND-IDSC-CCA을 가진다고 가정한다.

그때, $Adv(\beta)^{DBDH(G_1,P)} > 2(\varepsilon - q_U/2^{k-1})/q_{H_1}^4$ 이점을 가지면서 $O(t+(8q_R^2+4q_U)T_\varepsilon)$ 시간에 결정적 쌍선형 Diffie-Hellman 문제를 풀 수 있는 구별자 β 가 존재한다. 여기서 T_ε 은 쌍선형의 계산시간을 나타낸다.

증명. [21] 참조.

정리 1은 Fujisaki-Okamoto기법을 변형하기 위해 GDHP 기반의 약한 쌍선형 Diffie-Hellman 가정으로 의미적(semantical) 보안을 증명하고 있다. 정리 1의 증명을 통해 adaptive chosen message 공격에 대한 위조방지는 Hess의 ID기반 signature 기법의 보안으로부터 유추된다. [26]과 유사한 가정아래 signcrypt된 메시지를 위조할 수 있는 공격은 Hess의 signature을 변형한 기법에 의해서 signature을 위조할 수 있다.

제안기법은 Signcryption의 집단서명 기능들을 함께 지원하고 있고 아래와 같은 기능들을 만족하기 위한 증명은 [4, 5, 6, 7, 21]을 근거로 하였다.

4.1.1 정확성

정확성은 특정집단의 구성원이 생성한 Signcryption 메시지가 수신집단의 구성원에 의해서 정확히 Unsigncryption이 되어야 한다는 성질로서, 이 논문에서는 정확성을 [표 5]의 Signcryption에 의해 생성된 암호문 σ=(c, r, V)을 수신자가 Unsigncryption을 통해 정확히 m= $D_{k_2}(c)$ 을 복구하여 r= $H_3(c, k_1)$이 맞는지 검증하는 과정에서 정확성을 알 수 있으며 동작과정은 3.2절에서 확인할 수 있다.

4.1.2 위조방지

제안기법에서는 위조방지를 위해 평문 m이 가지고 있는 정보를 메시지 검증에 이용하고 있지 않다. 단지 Alice가 일부 평문 m의 송신자라고 누군가 확신하기 위해서 수신자는 제 3자에게 임시적인 복호화 키 k_2를 포워드하고 있다. 그리고, ${}_RF_q^*$에서 선택된 X는 난수발생기의 역할을 하고 있기 때문에 각 집단 구성원들의 k_1과 k_2는 자신을 제외한 누구에게도 노출되지 않는다. 안전성은 [1]에서와 같이 Pointcheval과 Stern기술을 사용하여 증명하고 있다[22].

4.1.3 익명성

익명성은 수신자가 송신한 Signcryption을 자신의 비밀정보로 복호한 후에도 송신집단의 어떤 구성원으로부터 받은 지를 확인하는 것은 계산상 불가능하다. 제안기법에서는 기존 Signcryption에서 제공하지 않은 익명성을 지원하기 위해 송신자의 정보를 $H_3(c, k_1)$와 $sQ_{ID_G} - xrd_{ID_A}$ 형태로 숨기도록 하였고, 이 정보가 이산대수 문제의 어려움과 세션마다 변하는 난수를 알지 못한다는 것에 기인하여 제안기법의 수신자는 송신자의 정보가 누구인지를 알아내기가 계산상 불가능하다.

4.1.4 기밀성

제안기법에서는 기밀성을 제공하기 위해서 Alice가 Bob에게 보내는 전체 메시지 σ=(c, r, V)가 전부 대칭키나 공개키 암호방식으로 이루어져 있고, 전체 메시지 σ는 각각 메시지 c=$E_{k_2}(m)$, 서명값 r= $H_3(c, k_1)$, 그리고 세션키 V = $sQ_{ID_G} - xrd_{ID_A}$로 암호화되어 있다. 그리고 제안기법에 사용된 전체 메시지 σ의 부가적인 연산으로 인해 Zheng의 Signcryption보다 강한 기밀성을 제안기법에서 제공하고 있다.

4.1.5 Unlikability

두개의 서로 다른 signature가 동일한 그룹 멤버에의해 계산된 결정은 계산상 어렵다는 Unlinkability 성질을 만족하기 위해 제안기법에서는 유효한 두개의 복호된 메시지 $D_{k_2}(c)$와 $D_{k_2}^{'}(c)$로부터 송신자가 동일한지 아닌지 알아낼 수가 없도록 하였다. 이 기능은 익명성의 경우와 유사하게 어느 누구도 송신자의 정보를 지닌 $H_3(c, k_1)$와 $sQ_{ID_G} - xrd_{ID_A}$에서 매번 변하는 난수 s와 r을 알지 못하므로, 두 메시지간의 연계성을 알 수 없다.

표 5 제안기법의 보안속성 비교분석
Figure 5 Proposed Scheme Security Property Analysis

○ : 지원 △ : $\frac{1}{2}$지원 × : 미지원

보안속성 / 기 법	위조방지	익명성	Unlinkability	기밀성	부인방지	Exculpability	Coalition-resistance
Zheng의 Signcryption[1]	×	△	×	△	×	○	×
D. Bonech의 Signcryption.[9]	○	×	○	○	×	○	○
Hess의 Signcryption[19]	○	×	×	△	○	○	×
Malone-Lee의 Signcryption[18]	○	×	×	○	○	○	○
제안기법	○	○	○	○	○	○	○

4.1.6 Exculpability

안전한 그룹 signature속성 중 어떤 집단 구성원 및 관리자도 다른 집단의 구성원을 대신해서 위조를 하지 못해야 한다는 Exculpability 성질을 만족하기 위해서 제안기법에서는 이산대수 문제에 근거하여 어떤 구성원 및 관리자도 σ 로부터 각 구성원의 비밀키 s를 알아낼 수 없어 위조가 불가능함을 〔표 5〕에서 보이고 있고 그 집단의 관리자 역시, 자신의 집단구성원을 대신해서 서명 및 암호를 할 수가 없다.

4.1.7 부인봉쇄(Traceability)

부인봉쇄를 지원하기 위해 제안기법에서는 분쟁 발생시 메시지를 받은 ID_G 구성원인 ID_a의 관리자에게 $H_3(c, k_1)$과 복호한 메시지 $D_{k_2}(c)$를 전송한다. 관리자는 자신이 알고 있는 $\{Q_{ID}, ID_p, Q_{ID_G}\}$정보를 바탕으로 $e(P, V)e(sP, Q_{ID_A})^r = e(sP, Q_{ID_G})^x$ 와 $e(V, Q_{ID_B})e(Q_{ID_A}, d_{ID_B})^r = e(Q_{ID_G}, sQ_{ID_B})^x$ 인지를 확인하여 누가 Signcryption 하였는지를 알아내어 분쟁을 해결한다.

4.1.8 Coalition-resistance

안전한 그룹 signature 속성 중 집단의 구성원 여러 명이 담합하여도 위조를 할 수 없어야 된다는 성질이 Coalition-resistance이다. 이 속성을 만족하기 위해서 제안기법에서는 관리자가 구성원으로부터 ID를 받아 Q_{ID}, ID_P, Q_{ID_G}, d_{ID}를 그 구성원에게 전달한다. 전달된 Q_{ID}, ID_P, Q_{ID_G}, d_{ID}는 어떤 경우의 담합에도 관리자나 유효한 구성원의 도움 없이는 유효한 $H_3(c, k_1)$, V를 생성할 수가 없다.

4.2 성능평가

기존에 제안되었던 여러 Signcryption 구조를 모듈라 연산의 관점에서 제안 기법을 보안속성과 연산량 측면에서 비교하면 〔표 5〕, 〔표 6〕와 같다. 특히 안전한 그룹 signature 속성을 만족하는 제안기법은 ID기반 signed encryption이 가지고 있는 문제를 해결하고 더불어 기밀성/부인방지 뿐만 아니라 암호문의 인증보장, 무결성, unlinkability 등의 보안특징의 조합(unmatched combination)을 제공한다.

아래 〔표 5〕는 기존기법과 제안기법을 기밀성, 부인방지, 인증, Unlinkability, 익명성등으로 비교평가한 것이다. 〔표 5〕에서 비교평가되고 있는 〔18, 19〕의 Signcryption 기법들은 암호문 인증과 익명성 사이에서 암호문의 크기가 큰 경우 비용이 많이 들면서 암호문의 익명성을 제공하고 있지 않다. 그리고 〔1, 18, 19〕은 두 개의 서로 다른 signature을 동일한 그룹 멤버에 의해 계산하기 어렵다는 이유로 Unlinkability속성이 지원하고 있지 않다. 또한 〔1, 9〕은 부인방지가 제공되지 않는다. 그러나 제안기법은 기존 Signcryption에서 제공하고 있지 않은 보안 속성중에서 암호문 인증, 무결성, Unlinkability등을 모두 제공하고 있다. 제공되는 보안속성의 증명은 4.1절에서 기술한다.

제안 모델과 기존 Signcryption기법들의 효율성을 비교분석하기 위해 〔표 6〕은 암호문의 크기, G_1과 $G_2 + F_p$ 요소의 수, 시간 등을 이용하고 있다. 〔표 6〕의 Time은

〔표 6〕 제안기법의 효율성 비교분석
Table 6 Proposed Scheme Performance Analysis

연산량 / 기법	Size:#el. Cipher pairs (#p,#q)	G_1, $G_2 + F_p$ Plain	Time: (#b, #m, #e)			
			Sign	Encrypt	Decrypt	Verify
Zheng의 Signcryption〔1〕	3,1	3,0	1,1,0	2,1,0	1,0,0	2,1,0
D. Bonech의 Signcryption.〔9〕	0,2	-	-	1,0,0	1,0,0	-
[2)-a]Hess의 Signcryption〔19〕	2,0	2,0	… 1,3,0 …		… 4,0,1 …	
Malone-Lee의 Signcryption〔18〕	1,1	1,1	… 2,2,2 …		… 4,0,2 …	
제안기법	1,1	1,1	… 2,2,2 …		… 4,0,2 …	

triples 〈#b, #m, #e〉로 표현되고 #b는 이중선형의 수, #m은 G_1 지수의 수, #e는 G_2나 F_P의 지수의 수로 나타낸다. G_1의 단순한 그룹 동작과 F_p나 G_2의 곱과 역은 이 논문에서 사용하지 않았다. 〔표 6〕의 Sizes Pairs (#p,#q)의 #p는 G_1 요소의 수이고 #q는 F_P요소의 수이다. 〔표 6〕에서 사용한 암호문(cipher)과 plain의 의미를 세부적으로 살펴보면 다음과 같다. 암호문(cipher)의 크기는 암호(encryption)을 지원하기 위해 사용된 ||c||-||m|| 의 암호문 오버헤드이고. plain의 크기는 복호화나 ||(m,s)||-||m||후의 signature 오버헤드이다.

효율성을 비교평가하고 있는 〔표 6〕은 〔1, 9, 18, 19〕에서 증명된 것을 기반으로 하고 있다. 〔표 6〕에서 보여준 제안기법은 블록 암호방식을 사용하면서 그룹속성을 만족하고 있기 때문에 그룹속성을 만족하고 있지 않은 Malone-lee의 Signcyption보다 효율적이고, 기존 기법들이 제공하지 않았던 익명성과 Unlinkability를 제공하기 때문에 기존 기법보다 안전하다고 볼 수 있다. 또한 DBDH(Decisional Bilinear Diffie-Hellman) 문제와 상호작용하는 기법의 보안성을 정리 1과 유사한 방법으로 기술하면 정리 2와 같다.

정리 2. 랜덤 오라클 모델에서, t의 수행시간과 q_{H_1} 신원 해싱 중 q_R H_3 쿼리, q_R Signcrypt 쿼리, q_U Unsigncrypt 쿼리등의 요구를 요청할 때 이익 ε 을 가지는 정의 1의 게임 동안 암호문을 구별할 수 있는 적 A는 IND-IDSC-CCA을 가진다고 가정한다.

그때, $Adv(\beta)^{DBDH(G_1,P)} > 2(\varepsilon - q_U/2^{k-1})/q_{H_1}^4$ 이점을 가지면서 $O(t+(8q_R^2+4q_U)T_\varepsilon)$ 시간에 결정적 쌍선형 Diffie-Hellman 문제을 풀 수 있는 구별자 β가 존재한다. 여기서 T_ε 은 쌍선형의 계산시간을 나타낸다.

증명. 〔21〕 참조.

정리 2는 정리 1처럼 동일한 성공 확률을 가질 수 있을 뿐만 아니라 축소도 별로 차이가 나지 않는다.

V. 결론

Zheng에 의해 최초로 제안된 Signcryption 기법은 새로운 암호의 기본 요소로써 서명과 암호 기능을 논리적인 한 스텝으로 동시에 처리할 수 있으며 계산 비용 측면에 있어서도 전통적인 서명 후 암호 패러다임에 의해 요구되는 계산량보다 현저히 낮은 암호학적인 기법이지만 서명이 제삼자에 의해 검증되어져야 하는 경우에는 이용될 수 없는 단점을 가지고 있다. 이러한 기존 Signcryption 기법이 제공하지 못하는 단점을 보완한 기법으로 〔3, 23〕이 제안되었으나, 이는 한 번의 추가적인 멱승 연산을 필요로 함으로써 계산량 측면에서 비효율적이었다. 그리고 2002년 BD기법을 수정한 Hess의 signature는 Malone-Lee 기법보다 더욱 안전성을 제공하는 효율적인 ID기반 Signcryption 기법을 사용하였다.

그러나 기존 Signcryption 기법에서는 송신 부인이 발생하여 제3자가 이를 검증해야 할 경우 수신측의 비밀키 노출이 불가피하여 보안속성 중 익명성과 Unlinkability를 지원하지 못하였다. 익명성과 Unlinkability를 제공하기 위해 이 논문에서는 random oracle 모델의 안전성과 결정적 쌍선형 Diffie-Hellman의 의미론적 보안을 만족하는 짧은 암호문를 이용한 다목적 ID기반의 Signcryption 암호시스템 모델을 제안했다.

비록 이것이 계산적 쌍선형 문제의 어려움보다 강한 가정이지만 암호시스템의 보안을 위한 합당한 기반이 될 것으로 보이고 다른 애플리케이션이나 효율적인 기법을 만드는데 이용될 것이다. 또한 시스템 사용자의 그룹정보을 이용하기 때문에 송신자의 메시지는 동일한 권한에 의존하지 않아 기존 기법들보다 효율적이다. 앞으로는 제안기법보다 더욱 효율적이면서 안전한 암호기법을 연구해야 할 것이다.

2) [a]〔19〕의 Signcryption 기법은 〔18〕에서처럼 CCA-secure에 부적합하다.

참고문헌

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

[2] Y.Zheng, "Signcryption and its applications in efficient public key solutions," In Proceedings of 1997 Information Security Workshop(ISW'97), LNCS, 1997

[3] Y. Zheng, "Identification, Signature and Signcryption using High Order Residues Modulo an RSA Composite," Proc. of PKC'01, LNCS 1992, Springer, pp. 48-63, 2001

[4] J. Camenisch and M. Stadler, "Efficient group signature schemes for large groups," In Advances in Cryptology-CRYPTO'97, LNCS 1294, pp. 410~424, 1997

[5] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik "A practical and provably secure coalition-resistant group signature scheme," In Advances in Cryptology-CRYPTO. 2000, LNCS 1880, pp.255~270, 2000

[6] E. Bresson and J. Stern, "Efficient revocation in group signcryption," In Proceeding of PKC'2001, LNCS 1992, pp. 190~206, 2001

[7] Y. Lyuu and M. Wu, "Convertible group undeniable signatures," In proceeding of ICISC' 2002, LNCS, Vol 2587, pp. 46~61, 2002

[8] D. Bonech, B. Lynn and H. Shacham, "Short signatures from the Weil pairing," Advances in Cryptology-Proceeding of Asiacrypt 2001, Springer-Verlag, preprint, 2001

[9] D. Bonech, M. Franklin, "Identity Based Encryption From the Weil Pairing," Advances in Cryptology - Crypto'01, LNCS 2139, Springer, 2001

[10] T. Okamoto and D. Pointcheval, "The Gap-problem : A new class of problems for the security of cryptographic schemes," 4th International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2001, Springer Verlag, preprint, pp. 104-118., 2001

[11] N.P. Smart. "An Identity based authenticated Key Agreement protocol based on the Weil Pairing," Cryptology ePrint Archive, Report 2001/111, http://eprint.iacr.org/, 2001

[12] H.Sakazaki, E.Okamoto, M.Mambo, "Constructing identiy-based key distribution systems over elliptic curves," IEICE TRANS. Fundamentals, Vol. E81-A,pp 2138-2143, 1998

[13] D. Nalla, K. C. Reddy, "ID-based tripartite Authenticated Key Agreement Protocols from pairings," Cryptology ePrint Archive, Report 2003. 04

[14] K. G. Paterson, "ID-based signatures from pairings on elliptic curves," Cryptology ePrint Archive, Report 2002. 04

[15] T. El-Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Trans. Inform. Theory,vol IT-31, pp.469-472,1985

[16] J. H. Silverman, "The Arithematic of elliptic curves," volume 106 of Graduate Texts in Mathematics," Springer-Verlag, 1986

[17] E. Okamoto, K. Tanaka, "Identity-based Information Security Management System for Personal Computer Networks," IEEE J. Select. Areas Commun., vol. SAC-7, pp. 290-294, 1989

[18] J. Malone-Lee, "Identity based Signcryption," available at http://eprint.iacr.org/2002/098

[19] F. Hess, "Efficient identity based signature schemes based on pairings," to appear in proceedings of SAC 2002, Springer Verlag, Lecture Notes in Computer Science series

[20] J-B. Shin, K. Lee, K.Shim, "New DSA-verifiable signcryption schemes," to appear in proceedings of ICISC 2002.

Springer Verlag, Lecture Notes in Computer Science series.

[21] Benoit Libert, Jean-Jacques Quisquater, "New identity based signcryption schemes from pairings." IEEE Information Theory Workshop Available 2003, March 30 April, Paris, France. Extended version available as IACR eprint archive

[22] D. Pointcheval, and J. Stern, "Security proofs for signature schemes," Proc. EUROCRYPT'96, pp. 190-1999, 1996

[23] H. Y. Jung, D. H. Lee, J. I. Lim and K. S. Chang, "Signcryption Schemes with Forward Secrecy," Procedding of Workshop on Information Security Applications(WISA'2001), Vol.2, pp .463-475, 2001

[24] E. Okamoto, and K. Tanaka, "Identity-based information security management system for personal computer networks," IEEE Journal on selected areas in communications, Vol. 7, No. 2, pp. 290-294, 1989

[25] F. Bao and R. H. Deng, "A Signcryption Scheme with Signature Directly Verifiable by Public Key," Proc. of PKC'98, LNCS, Vol. 1431, Springer-Verlag, pp. 55-59, 1998

[26] C. Gamage, J. Leiwo, and Y. Zheng, "Encrypted Message Authentication by Firewalls," Proc. of PKC'99, LNCS, Vol. 1560, Springer-Verlag, pp. 69-81, 1999

[27] E. Fujisaki, T. Okamoto, "Secure integration of asymmetric and symmetric encryption schemes," Advances in Cryptology - Crypto'99, LNCS 1666, Springer, pp. 537-554, 1999

[28] Xiaofeng Chen, Fangguo Zhang and Kwangjo Kim, "A New ID-Based Group Signature Scheme from Bilinear Pairings", In Proc. of WISA2003, pp.585-592, Aug. 25-27, 2003, Jeju Island, Korea.

저 자 소 개

곽 병 옥

1998년 8월: 충북대학교 전자계산학과 박사수료

2000~ 현재 : 한국전자통신연구원 선임연구원

정 윤 수

2000년 2월: 충북대학교 전자계산학과 이학석사

2003~ 현재 : 충북대학교 컴퓨터전공 박사수료

이 상 호

1989년 2월 : 숭실대학교 컴퓨터네트워크학과 공학박사

1981년~ 현재 : 충북대학교 전기전자컴퓨터공학부 교수