아이디 기반 대리 Signcryption 기법들에 대한 연구

윤여정, 박찬일, 윤현수

한국과학기술원

yjyoon@nslab.kaist.ac.kr, chanil@nslab.kaist.ac.kr, hyoon@nslab.kaist.ac.kr

A Study on ID-Based Proxy Signcryption Schemes

Yeojeong Yoon, Chanil Park, Hyunsoo Yoon

Korea Advanced Institute of Science and Technology

요 약

아이디 기반 암호 체계는 공개키를 생성하기 위하여 별도의 정보 교환을 하지 않고, 사용자의 신원을 확인할 수 있는 고유 정보를 이용하여 공개키를 생성함으로써 효율적인 공개키 생성 및 관리가 가능하다. 또한 대리 서명 기법은 원 서명자가 부득이하게 서명을 할 수 없을 경우 자신이 선택한 대리 서명자에게 서명 권한을 위임함으로써 대리 서명자가 원 서명자 대신 서명을 할 수 있는 기능을 제공하는 기법이다. Signcryption 기법은 하나의 기법으로 서명과 암호화 모두를 수행 할 수 있다. 위 기법들의 장점을 한번에 취할 수 있는 기법이 아이디 기반 대리 Signcryption 기법이다. 본 논문에서는 아이디 기반 대리 Signcryption 기법을 이해하기 위해 필요한 기반 지식과 아이디 기반 대리 Signcryption 기법에 대하여 기술하고자 한다.

1. 서 론

기밀성(confidentiality), 무결성(integrity), 부인봉쇄(non-repudiation) 및 인증(authentication)은 암호체계 및 보안 어플리케이션에서 중요한 요구사항이다.[1] 보안 시스템에서는 이러한 요구사항을 만족시키기 위해서 독립적인 서명 프로토콜과 암호 프로토콜을 사용한다. 하지만 두 개의 독립적인 프로토콜을 사용하는 것은 계산량과 통신량이 늘어나는 단점이 있다. 1997년 Zheng[2]은 이러한 단점을 해결하기 위하여 서명과 암호화를 논리적으로 한 번에 수행하는 Signcryption 기법을 처음 제안하였다. Signcryption 기법을 사용함으로써 암호 체계가 갖추어야 할 요구 조건을 모두 만족시키면서도 독립적인 서명 및 암호 프로토콜을 사용하는 것에 비하여 계산 부하 및 통신 오버헤드를 줄일 수 있다.

기업 환경의 실 생활에서 기업의 대표가 불가피한 사정으로 자리를 비울 경우에 대표가 자리에 없음에도 불구하고 반드시 서명을 해야 하는 계약서나 사내 문서가 생길 수 있다. 이런 경우 믿을 만한 하급 직원에게 일부 문서에 대해 서명할 수 있는 권한을 위임하고 하급직원이 대표를 대신하여 서명하도록 할 수 있다. 이러한 대리 서명 상황에 적용할 수 있는 특수 전자 서명 기법을 대리(proxy) 서명 기법이라고 한다. 대리 서명 기법은 M. Mambo등[3]에 의해서 1996년에 처음 제시되었으며, A.Boldyreva등[4]이 대리 서명 기법의 정형적인 안전성 모델을 처음 정립하였다.

1999년 C. Gamage등[5]은 대리 서명 기법과 Signcryption 기법을 통합하여 대리(proxy) Signcryption 기법을 처음 제안하였다. 그리고 2004년 Xiangxue Li등[10]은 기존의 대리 Signcryption기법에 아이디 기반의 암호 체계를 적용시킨 아이디 기반 대리 Signcryption 기법을 처음 제안하였다. 대리 Signcryption 기법은 개인 휴대 정보 단말기, 휴대용 컴퓨터, 핸드폰 등 하드웨어 자원이 넉넉하게 지원 되지 않는 기기들에서의 대리 서명과 메시지 보안이 가능한 보안 체계를 구축하기 위해서 유용하게 사용되고 있다. 이 기법에서 원(original) signcrypter는 자신의 signcryption 권한을 대리인에게 위임할 수 있고, 그 대리인을 대리(proxy) signcrypter라 부른다. 대리 signcrypter는 원 signcrypter처럼 signcryption을 수행할 수 있다. 따라서 아이디 기반 대리 Signcryption 기법은 대리 서명의 기능을 수행함과 동시에, 아이디 기반 암호 체계가 가지고 있는 키 관리에 대한 효율성과 하나의 기법으로 서명과 암호화가 가능한 Signcryption 기법의 이점을 모두 취할 수 있다. 본 논문에서는 아이디 기반 대리 Signcryption 기법에 대하여 정리하고자 한다.

2장과 3장에서는 아이디 기반 대리 Signcryption 기법을 이해하는 데에 필요한 배경 지식과 기본 기법들에 대해서 서술 한다. 4장에서는 여러 가지 아이디 기반 대리 Signcryption 기법에 대하여 비교

분석하고, 5장에서는 결론을 기술 한다.

2. 배경 지식

보통의 아이디 기반 대리 Signcryption 기법은 Bilinear Pairing을 사용하기 때문에 이와 관련된 개념[11]을 살펴보고자 한다.

2.1 Bilinear 함수

G_1과 G_2를 위수가 소수 q인 순환군이며 G_1은 덧셈군, G_2는 곱셈군이라 하자. 함수 $\hat{e} : G_1 \times G_1 \rightarrow G_2$ 가 임의의 $P, Q, R \in G_1$ 에 대하여 다음 조건을 만족하면 Bilinear 함수라 한다.

(1) [Bilinearity] $a, b \in F_q$에 대하여

$\hat{e}(P+Q, R) = \hat{e}(P, R)\hat{e}(Q, R)$

$\hat{e}(P, Q+R) = \hat{e}(P, Q)\hat{e}(P, R)$

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

를 만족한다

(2) [Non-degenerate]

$\hat{e}(P, Q) \neq I_{G_2}$ 를 만족한다. (I_{G_2}는 G_2의 identity)

(3) [Computability]

$\hat{e}(P, Q)$의 계산이 효율적인 알고리즘이 존재한다.

3. 관련 연구

아이디 기반 대리 Signcryption 기법은 아이디 기반 Signcryption 기법과 대리 서명 기법을 조합한 것으로, 각 기법의 기능과 장점을 하나의 기법으로 취할 수 있다. 따라서 본 장에서는 아이디 기반 대리 Signcryption 기법의 근간이 되는 두 가지 연구에 대하여 간략하게 살펴보고자 한다.

3.1 아이디 기반 Signcryption 기법

Signcryption은 서명 기법과 암호화 기법을 통합하여 계산량이나 통신 횟수 면에서 상당히 효율적이면서도 메시지의 기밀성과 인증을 모두 취할 수 있는 기법으로써, 1997년 Zheng에 의하여 처음 소개 된 후 효율성 면에서 많은 연구자들의 큰 주목을 받아 왔다. 그 후 수학적인 보안 모델[9]이 제시되었으며, 아이디를 기반으로 하는 Signcryption 기법들[7,8]도 제안되었다. 아이디 기반 대리 Signcryption 기법을 이해하기 위해서는 아이디 기반 Signcryption의 전반적인 흐름을 알아야 하기 때문에 아이디 기반 Signcryption 기법의 대략적인 구성을 기술하고자 한다. 아이디 기반 Signcryption 기법들은 다음과 같은 네 개의 알고리즘으로 구성되어 있다.

(1) 셋업(Setup)

보안 매개 변수(security parameter) k가 존재하고, 개인 키 생성자(private key generator, PKG)가 시스템 공개 매개 변수들(public parameters)을 생성한다.

(2) 키 생성(Key generation)

신원을 알 수 있는 아이디가 존재하고, PKG가 아이디에 대응되는 개인키 d_{ID}를 생성한다. 그리고 생성된 개인키를 해당 아이디를 가진 사용자에게 안전한 방법으로 전송한다.

(3) Signcrypt

사용자 A가 사용자 B에게 메시지 m을 전달하고자 한다고 가정 할 경우, 사용자 A는 $Signcrypt(m, d_{ID_A}, ID_B)$를 계산하고, 계산 결과 평문 m에 대응하는 암호문 σ를 얻게 된다.

(4) Unsigncrypt

사용자 B가 암호문 σ를 받은 후 사용자 B는 $UnSigncrypt(\sigma, d_{ID_B}, ID_A)$를 계산하고, 계산 결과로 평문 m을 얻는다. 만약 암호문 σ가 옳지 않은 암호문일 경우, 거짓(false)를 반환한다.

아이디 기반 Signcryption 기법은 아래와 같은 조건을 항상 만족해야만 한다.

$m = UnSigncrypt(Signcrypt(m, d_{ID_A}, ID_B), d_{ID_B}, ID_A)$

3.2 대리 서명 기법

대리서명 기법은 원 서명자가 자신의 서명에 대한 권한을 대리 서명자에게 위임함으로써 대리 서명자가 원 서명자 대신 서명을 할 수 있도록 하는 기법이다. 아이디 기반 대리 Signcryption 기법을 이해하기 위해서는 그 근간이 되는 대리 서명 기법을 알아야 하기 때문에, 대리 서명 기법의 종류와 특성[19]에 대해서 간략히 기술하고자 한다.

대리서명 기법은 위임 권한 조건에 따라서 완전 위임(Full Delegation), 부분 위임(Partial Delegation), 보증 위임(Delegation by warrant)으로 구분된다.

(1) 완전 위임

완전 위임에서는 대리 서명자가 원 서명자의 서명키와 동일한 서명키를 갖게 되고, 따라서 두 서명자가 같은 서명을 생성하게 된다. 따라서 서명의 검증자 입장에서는 원 서명자의 서명인지 대리 서명자의 서명인지 구분할 수 없게 된다.

(2) 부분 위임

부분 위임에서는 원 서명자가 자신의 서명키를 이용하여 대리 서명키를 생성하고, 그것을 대리 서명자에게 다른 사용자가 사용할 수 없게끔 안전하게 전송한다. 또는 자신의 서명키를 이용하여 부분적인 대리 서명키를 생성하여 대리 서명자에게 안전하게 전송하고, 대리 서명자는 그것을 이용하여 특정 계산 알고리즘을 통해 자신의 대리 서명키를 생성하기도 한다. 두 방법 모두 대리 서명키를 통하여 원 서명자의

서명키를 계산할 수 없어야 한다. 대리 서명자는 대리 서명키를 이용하여 서명하게 되고, 검증자 입장에서는 서명을 보고 그것이 원 서명자의 서명인지, 대리 서명자의 서명인지를 분간할 수 있다.

(3) 보증 위임

보증 위임은 원 서명자가 자신이 대리 서명자에게 자신의 서명 권한을 위임한다는 보증서를 발행함으로써 실행된다. 보통 보증서에는 원 서명자의 신원과 대리 서명자의 신원, 대리 서명자의 공개키, 대리 서명의 유효기간 등이 포함된다.

대리 서명기법은 구별 가능성, 검증 가능성, 위조불가, 확인 가능성, 부인 방지, 오남용 불가 등의 보안 요구사항을 만족시켜야만 한다. 이는 대리 Signcryption 기법 또한 만족시켜야 할 요구사항이다. 각각에 대한 설명은 아래와 같다.

(1) 구별 가능성

대리 서명자가 생성한 대리 서명과 원 서명자가 생성한 서명을 제3자가 구분할 수 있어야 한다.

(2) 검증 가능성

검증자가 대리 서명으로부터 서명된 메시지에 대해 원 서명자가 동의했는지를 확신할 수 있어야 한다.

(3) 위조 불가

대리 서명자는 원 서명자를 대신해서 서명을 생성할 수 있지만, 원 서명자나 권한을 위임 받지 않은 제3자가 대리 서명자로써 유효한 대리 서명을 생성할 수 없어야 한다. (완전 위임에서는 본 성질이 제외된다.)

(4) 확인 가능성

누구든지 대리 서명을 생성한 대리 서명자의 신원을 확인할 수 있어야 한다.

(5) 부인 불가

대리 서명자가 원 서명자의 유효한 대리 서명을 생성하면, 생성된 대리 서명에 대해서 대리 서명자가 부인할 수 없어야 한다.

(6) 오남용 불가

대리 서명자는 유효한 대리 서명을 생성하는 것 이외의 목적으로 대리 서명을 할 수 없어야 한다.

4. 아이디 기반 대리 Signcryption 기법

아이디 기반 대리 Signcryption 기법은 대리 서명 기법과 아이디 기반 Signcryption 기법을 통합한 기법으로써, 하나의 기법으로 두 기법의 장점을 모두 취할 수 있다는 강점을 지니고 있다. 이는 특히 계층 구조적인 통신에서 반드시 필요한 대리 서명기법의 기능을 수행하면서도 Signcryption의 이점을 통하여 메시지의 기밀성과 인증을 한 번에 취할 수 있다. 아이디 기반 대리 Signcryption 기법의 기본적인 아이디어는 다음과 같다. 원 signcrypter A가 대리 signcrypter B에게 자신의 서명과 함께 B에게 자신의 signcryption 권한을 위임한다는 내용이 담긴 위임장을 전달한다. 대리 signcrypter B는 이것을 이용하여 자신만이 이용할 수 있는 대리 signcryption키를 생성한다. 이 때에 보통 대리 signcryption키에는 A의 공개 키와 B의 공개 키에 대한 정보가 담겨 있어야 한다. 대리 signcrypter B는 대리 signcryption키와 signcryption 알고리즘을 이용하여 메시지를 signcryption한다. 위임장과 signcryption 된 메시지를 받은 검증자는 원 signcrypter A의 공개키와 대리 signcrypter B의 공개키를 이용하여 unsigncryption 할 수 있는 key를 생성하게 되고, unsigncryption 알고리즘에 따라 인증과 복호화를 수행하게 된다.

4.1 일반적인 대리 Signcryption 기법

일반적인 대리 Signcryption 기법은 다음과 같은 여섯 개의 알고리즘으로 구성된다.

(1) Parameter Generation: $PG(1^k)$

*PG*는 공개/비밀 매개 변수를 생성하는 알고리즘으로 *k*는 보안 매개 변수이다. 이 알고리즘을 실행하면 시스템 매개 변수(*Public parameters, Secret parameters*)가 생성된다.

(2) Key Extraction: *KE*(*Public parameters, Secret parameters*)

*KE*는 시스템 매개 변수를 사용하여 사용자의 공개키/개인키 쌍(PK_{ID}, SK_{ID})을 생성하는 알고리즘이다.

(3) Proxy Delegation Protocol: $DP(PK_A, SK_A, PK_B, SK_B)$

*DP*는 원 signcrypter A와 대리인 B에 의하여 수행되며, 각자의 공개키와 개인키를 이용하여 대리 signcryption키 SK_P를 생성하는 프로토콜이다.

(4) Proxy Signcryption: $PS(SK_P, M)$

*PS*는 메시지 *M*에 대하여 대리인이 signcryption을 수행하여 암호문 $p\sigma$ 을 생성하는 알고리즘이다.

(5) Proxy Verify: $PV(PK_A, PK_B, p\sigma)$

*PV*는 검증자가 대리인이 생성한 암호문의 유효성을 검증하기 위한 알고리즘이다. 암호문이 유효할 경우 복호화 과정을 통하여 원문 M을 얻게 되고, 유효하지 않을 경우 거짓을 반환한다.

(6) Proxy Identification: $PID(p\sigma)$

*PID*는 검증자가 대리인 B를 검증하는 알고리즘이다.

4.2 여러 가지 아이디 기반 대리 Signcryption 기법들

본 장에서는 현재까지 제시된 다양한 아이디 기반 대리 Signcryption 기법들을 소개하고, 각각의 특성을 비교하고자 한다.

4.2.1 기본적인 아이디 기반 대리 Signcryption 기법

2004년 Xiangxue Li등[10]은 Bilinear Pairing을 이용한 아이디 기반 대리 Signcryption 기법을 처음 제안하였다. 처음으로 기존의 대리 Signcryption 기법에 아이디 기반의 암호 체계를 적용시킴으로써 공개키 생성과 관리를 더욱 효율적으로 수행할 수 있게 했다는 점에서 큰 의의를 갖는 기법이라 할 수 있다. 허나 Xiangxue Li 등이 제안한 아이디기반 대리 Signcryption 기법은 원 Signcrypter가 대리인에게 위임장을 전달할 때 공격의

[표1] Xiangxue Li와 Kefei Chen의 아이디 기반 대리 Signcryption 기법[10]과 Qin Wang과 Zhenfu Cao의 아이디 기반 대리 Signcryption 기법[12]의 계산량 비교

알고리즘	[10]	[12]
대리 signcryption키 생성	1A + 3M + 1E + 3P	4A + 5M + 2P
대리 Signcryption	2A + 2M + 2E+ 2P	3M + 1P
UnSigncryption / 검증	4E + 8P	1A + 1M + 3P
대리인 검증	2E + 4P	1A + 1M + 2P

가능성이 전혀 없는 안전한 채널로 전달해야만 한다는 제약 조건을 가지고 있다. 이러한 취약점을 해결하기 위하여, 2005년 Qin Wang등[12]은 보다 효율적인 아이디 기반 대리 Signcryption 기법을 제안하였다. 이 기법은 원 signcrypter가 대리인에게 위임장을 보낼 때에 공개 채널을 이용하여 전달해도 대리 signcryption키가 노출되는 등의 위험이 발생하지 않는다. 또한 이전 기법[10]보다 계산량과 암호문의 길이를 감소시켰다는 면에서 큰 발전이 있다. [표1]은 Xiangxue Li등의 기법과 Qin Wang등의 기법의 계산량을 비교한 것이다. A는 덧셈, M은 곱셈, P는 Pairing 연산, E는 지수 연산을 나타낸다. 덧셈과 곱셈 연산에 비하여 지수 연산과 Pairing 연산에 상대적으로 더 많은 시간이 소요되는 것을 감안하면 Qin Wang등의 기법은 이전 기법에 비하여 계산량을 상당히 줄인 것으로 볼 수 있다.

이 밖에도 2005년 Qin Wang등[17]은 인증서 기반 대리 Signcryption 기법과 함께 아이디 기반 대리 Signcryption 기법을 제안하였으며, 2008년 Hassan Elkamchouchi등[15]은 부분 위임 대리 서명의 기능을 지닌 아이디 기반 대리 Signcryption 기법을 제안하였다.

4.2.2 아이디 기반 Threshold 대리 Signcryption 기법

Threshold 대리 서명 기법이란 서명 권한을 위임 받은 n명의 대리인들이 존재하고, 대리인 t명 이상이 서명을 했을 경우에만 효력이 있는 대리 서명이 생성되는 기법[13]을 말한다. 이러한 Threshold 대리 서명 기법과 아이디 기반 Signcryption 기법을 조합한 것이 아이디 기반 Threshold 대리 Signcryption 기법이다. 이 기법은 2007년 Fagen Li등[16]에 의해서 제안 되었으며 Threshold 대리 서명 기법과 마찬가지로 n명의 대리 signcrypter들이 존재하고, t명 이상의 대리인들이 협력하여 signcryption을 수행함으로써 암호문을 생성할 수 있으며 t-1명 이하의 대리인들이 signcryption을 수행할 경우에는 그 결과가 인정되지 않는다. 이러한 기법은 signcryption 권한을 여러 사람에게 위임하고, 일정 수 이상의 동의가 있을 때 서명 생성 및 암호화가 가능하게 하기 때문에, 실 생활에 적용하였을 때 오로지 한 명의 대리인에게 권한을 위임함으로써 발생할 수 있는 권한 남용 등의 문제점을 해결 할 수 있다.

4.2.3 아이디 기반 다중-대리 다중-Signcryption(Multi Proxy Multi-Signcryption) 기법

다중-대리 다중-서명(Multi-Proxy Multi-Signature)기법이란 다수의 원 서명자 그룹과 다수의 대리 서명자의 그룹이 존재하고, 원 서명자 모두가 대리 서명 키 생성에 참여하고 그것을 전달 받은 대리 서명자들이 모두 대리 서명 생성에 참여해야만 유효한 대리 서명이 만들어 지는 기법으로, 2004년 Hwang등[14]이 처음 제안하였다. 이러한 다중 대리 다중 서명기법과 아이디 기반 Signcryption기법을 조합한 것이 아이디 기반 다중-대리 다중-Signcryption 기법으로, 2007년 Sunder Lal등[6]이 처음 제안하였다. 이후 2009년 Zhou Xiaoyan등[18]이 Sunder Lal등의 기법이 잘못된 형식의 Pairing을 사용하여 계산이 불가능하다는 것을 지적하면서 정확한 계산이 가능한 아이디 기반 다중-대리 다중-Signryption 기법을 제안하였다. 기업 환경의 경우에 하나의 문서에 대하여 여러 부서의 대표자들에게 서명을 받아야 하고, 그 대표자들의 부재로 인하여 각 대표자의 대리 서명자에게 서명을 받고, 암호화를 해야 하는 경우가 발생하기 때문에 이 기법은 실 생활에 적용할 경우 상당히 유용하다.

5. 결론

최근까지도 활발하게 연구되고 있는 아이디 기반 암호 체계는 공개키를 생성하기 위하여 별도의 정보 교환을 하지 않고, 사용자의 신원을 확인할 수 있는 고유 정보(아이디 등)를 이용하여 공개키를 생성함으로써 효율적인 공개키 생성 및 관리가 가능하다. 또한 대리 서명 기법은 원 서명자가 부득이하게 서명을 할 수 없을 경우 자신이 선택한 대리 서명자에게 서명 권한을 위임함으로써 대리 서명자가 원 서명자 대신 서명을 할 수 있는 기능을 제공하는 기법이다. 서명과 암호화 기법을 통합한 Signcryption 기법은 하나의 기법으로 메시지의 기밀성과 인증을 모두 취할 수 있다. 따라서 위 기법들의 장점을 한번에 얻을 수 있는 기법이 아이디 기반 대리 Signcryption 기법이라 할 수 있다. 본

논문에서는 아이디 기반 대리 Signcryption 기법에 관한 최근의 연구 동향을 조사하였다. 먼저, 아이디 기반 대리 Signcryption 기법을 이해함에 있어 기본이 되는 아이디 기반 Signcryption 기법과 대리 서명 기법에 대하여 기술하였으며, 다양한 아이디기반 대리 Signcryption 기법의 특징 및 성능을 기술하였다.

여러 형태의 대리 서명 기법들이 존재하는 만큼 그것들을 활용한 아이디 기반 대리 Signcryption 기법들이 제안되었으나, 다른 아이디 기반 기법들에 비하여 다양성이 부족하고 발전 속도가 더딘 편이다. 하나의 기법으로 많은 기능을 수행할 수 있는 만큼 다른 기법들에 비하여 계산량이 많기 때문에 계산량과 통신 횟수를 최소화 하는 노력이 필요할 것으로 보인다. 또한 현재 일대다 통신이 확산되는 만큼, 브로드캐스트 환경에 적합한 아이디 기반 대리 Signcryption 기법이 제안될 경우 실 생활에 상당히 유용하게 적용 가능할 것이다.

참 고 문 헌

[1] Shamir. A, "Identity-based cryptosystems and signature schemes", In : Blakely, G. R., Chaum, D. (eds.) Advances in Cryptology-CRYPTO'84, Springer, Heidelberg, LNCS, vol. 196, pp. 47-53. 1984.

[2] Zheng, Y, "Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost(encryption)", In: Kaliski Jr., B.S. (ed.) Advances in Cryptology - CRYPTO '97, Springer, Heidelberg, LNCS, vol. 1294, pp. 165-179, 1997.

[3] M. Mambo, K. Usuda, E. Okamoto, "Proxy signatures for delegating signing operation", 3rd ACM conference on Computer and Communications Security(CCS'96), pp. 48-57, 1996.

[4] A. Boldyreva, A. Palacio, B. Warinschi, "Secure Proxy Signature Scheme for Delegation of Signing Rights", IACR ePrint Archive, available at http://eprint.iacr.org/2003/096/, 2003.

[5] Gamage, C., Leiwo, J., Zheng, Y, "An efficient scheme for secure message transmission using proxy-signcryption", In: 22nd Australasian Computer Science Conference, Auckland, New Zealand, pp. 420-431, 1999.

[6] Sunder Lal and Tej Singh, "New ID-Based Multi-Proxy Multi-Signcryption Scheme from Pairings", available at arxiv.org/pdf/cs/0701044.₩, 2007.

[7] B. Libert and J. Quisquater, "New Identity Based Signcryption from Pairings", In Proceedings of IEEE Information Theory Workshop 2003, 2003.

[8] J. Malone-Lee, "Identity Based Signcryption", available at http://eprint.iacr.org/2002/072/, 2002.

[9] J. Baek, R. Steinfeld and Y. Zheng, "Formal Proofs for the Security of Signcryption", In Proceedings of PKC'02, 2002, Springer LNCS 2274. 2002.

[10] Xiangxue Li and Kefei Chen, "Identity Based Proxy-Signcryption Scheme from Pairings", In IEEE SCC, pages 494-497, 2004.

[11] D. Boneh, M. Franklin, "Identity-based encryption from the Weil pairing", Advances in Bryptology - Crypto'2001, LNCS 2139, pp. 213-229, 2001.

[12] Wang Q, Cao Z, "Efficient ID-based proxy signature and proxy signcryption form bilinear pairings", In: Computational Intelligence and Security-CIS 2005, LNAI 3802, Springer-Verlag, pp 167-172, 2005.

[13] Jing Xu, Zhenfeng Zhang, and Dengguo Feng, "Identity Based Threshold Proxy Signature", ACR ePrint Archive,available at http://eprint.iacr.org/2004/250.pdf, 2004.

[14] S. Hwang, C. Chen, "New multi-proxy multi-signature schemes", Appl. Math. Comput. 147, pp. 57-67, 2004.

[15] Hassan Elkamchouchi and Yasmine Abouelseoud, "A New Proxy Identity-Based Signcryption Scheme for Partial Delegation of Signing Rights", ACR ePrint Archive,available at http://eprint.iacr.org/2008/041.pdf, 2008.

[16] Fagen Li, Yupu Hu, and Shuanggen Liu, "ID-Based (t, n) Threshold Proxy Signcryption for Multi-agent Systems", Computational Intelligence and Security, pages 406-416, 2007

[17] Wang Q and Cao Z F, "Two proxy signcryption schemes from bilinear pairings", Proc of CANS 2005, Berlin: Springer-Verlag, LNCS 3810: 161-171, 2005.

[18] Zhou Xiaoyan and Wu Yan, "An Improved ID-Based Multi-Proxy Multi-Signcryption Scheme", 2009 Second International Symposium on Electronic Commerce and Security, pp.466-469, 2009.

[19] Haeryong Park, "An Efficient ID-based Proxy Signature Scheme", 한국인터넷정보학회 학술발표대회 논문집, Vol.9, No.2, pp. 101-106, 2008.