情報保護學會論文誌
第20卷 第5號, 2010. 10

ID기반 온라인/오프라인 사인크립션(Signcryption) 기법*

박 승 환,† 김 기 탁, 구 우 권, 이 동 훈‡
고려대학교 정보경영공학전문대학원

Identity-Based Online/Offline Signcryption Without Rnadom Oracles*

Seunghwan Park,† Kitak Kim, Woo Kwon Koo, Dong Hoon Lee‡
Graduate School of information Management and Security, Korea University

요 약

ID기반 사인크립션(Signcryption) 기법은 메시지의 기밀성과 메시지 인증을 동시에 제공한다. 하지만 높은 연산 비용이 요구되기 때문에 스마트카드나 PDA와 같은 저전력 디바이스 환경에서는 사용되기 어렵다. 이러한 문제점을 해결하기 위한 새로운 개념의 기법이 온라인/오프라인 기법이다. 온라인/오프라인 기법은 서명이나 암호화의 연산 단계를 두 단계로 나누어서 한다. 첫 번째 단계는 오프라인 단계로서 서명 또는 암호화될 메시지를 알기 전에 수행할 수 있는 연산을 미리 하는 단계이다. 두 번째 단계는 온라인 단계로서 보낼 메시지와 수신자의 공개키를 알고 나서 서명 또는 암호화 연산을 수행하는 단계이다. 온라인 단계에서는 가능한 한 페어링이나 지수승 같은 연산 비용이 높은 연산을 하지 않게 설계되어 진다. 이러한 온라인 단계의 효율성 때문에 온라인/오프라인 기법은 스마트카드와 같은 연산 비용의 한계가 있는 디바이스에서 유용하게 사용될 수 있다. 본 논문에서는 기밀성과 메시지 인증을 제공하는 ID기반 사인크립션을 제안하고, 저전력 디바이스에서 사용될 수 있는 ID기반 온라인/오프라인 사인크립션 기법을 제안한다. 이 기법은 랜덤오라클 모델에 안전성을 두지 않는 최초의 ID기반 온라인/오프라인 사인크립션 기법이다.

ABSTRACT

Signcryption is a cryptographic primitive which offers authentication and confidentiality simultaneously with a cost lower than signing and encrypting the message independently. We propose a new cryptographic notion called Identity-based online/offline signcryption. The notion of online/offline scheme can be divided into two phases, the first phase is performed offline prior to the arrival of a message to be signed or encrypted and the second phase is performed online phase after knowing the message and the public key of recipient. The Online phase does not require any heavy computations such as pairings or exponents. It is particularly suitable for power-constrained devices such as smart cards. In this paper, we propose ID-based signcryption scheme and ID-based online/offline signcryption scheme where the confidentiality and authenticity are simultaneously required to enable a secure and trustable communication environment. To our best knowledge, this is the first ID-based online/offline signcryption scheme that can be proven secure in the standard model.

Keywords: Signcryption, Online/Offline, ID Based Cryptosystem

접수일: 2010년 4월 6일; 채택일: 2010년 8월 28일
* 본 연구는 지식경제부 및 한국산업기술평가관리원의 산업원천기술개발사업(정보통신)의 일환으로 수행하였음. [KI002113, car-헬스케어 보안 기술개발]

† 주저자, sgusa@lycos.co.kr
‡ 교신저자, donghlee@korea.ac.kr

I. 서 론

1.1. 개요

Shamir에 의해 1984년에 최초로 제안된 ID기반 암호 시스템[13]은 기존의 공개키 암호 시스템에서 인증서 관리에 대한 문제를 해결하였다. 공개키 기반 암호 시스템 구조에서는 사용자가 생성한 임의의 공개키에 대하여 신뢰할 수 있는 인증기관이 발급해주는 공개키 인증서가 필요하다. 하지만 ID기반 암호시스템은 사용자의 이름, 전화번호, 이메일 등과 같은 신원정보를 공개키로 사용하므로 이러한 사용자 공개키에 대응하는 비밀키를 안전하게 발급해 주는 신뢰할 수 있는 제 3의 기관인 키 발급 기관(KGC : Key Generation Center)이 필요하다. 이러한 ID기반 암호 시스템은 송신자와 수신자의 송수신 과정에서 인증서 교환이나 확인 같은 작업이 필요하지 않기 때문에 기존의 공개키 기반 암호 시스템보다 편리하고 효율적이라고 볼 수 있다. 이와 같은 이유로 ID기반 암호 시스템은 암호와 전자서명 분야 등에서 많이 연구가 되어오고 있으며, 다양한 분야에서 파생되어 적용되고 있다[3,5,14,7,8,15]. 특히 ID기반 사인크립션(Signcryption) 기법은 2002년에 Malone-Lee[11]에 의하여 처음으로 제안되었다. 사인크립션은 암호와 서명의 기능을 동시에 지원하는 기법으로 단순히 현존하는 암호 기법과 서명 기법을 각각 적용하는 하이브리드(hybrid) 기법보다 연산 및 통신비용 측면에서 효율적이다. 이러한 장점에도 불구하고 저장공간과 계산량의 한계가 있는 스마트카드와 같은 저전력 디바이스 환경에서는 ID기반 암호[2]나 사인크립션 같은 기법을 적용시키기 어렵다. 이와 같은 문제를 해결하기 위해서는 새로운 개념의 기법이 필요한데, 그 중 하나가 온라인/오프라인 기법이다. 온라인/오프라인 디지털 서명의 개념은 1990년에 Even 등[6]에 의해서 처음 소개되었다. 이 개념은 서명의 연산 단계를 메시지와 공개키를 알기 이전에 계산할 수 있는 연산들을 미리 수행하는 오프라인 단계와 메시지와 공개키를 알고 나서 연산을 수행하는 온라인 단계로 나뉜다. 온라인 단계에서는 보낼 메시지와 메시지를 받을 수신자가 결정된 이후에 가능하면 최소한의 연산만을 수행하도록 설계된다. 많은 연산 비용이 요구되는 페어링(pairing) 연산이나 지수승 연산은 대부분 오프라인 단계에서 연산하도록 설계하기 때문에 온라인/오프라인 기법은 매우 효율적이다. 그렇기 때문에 오프라인 단계에서 최대한의 연산을 어떻게 수행할 것이며, 온라인 단계에서는 메시지와 키를 이용한 연산을 얼마나 줄일 수 있느냐가 온라인/오프라인 기법 설계의 핵심이라고 볼 수 있다.

1.2. 관련 연구

기법의 안전성을 증명할 때 가정하는 모델은 크게 세 가지로 구분된다. 랜덤 오라클 모델은 증명 과정에서 랜덤 오라클의 존재를 가정하여 증명한다. 완전한 모델(Full Model)에서는 랜덤 오라클을 사용하지 않는다. 랜덤 오라클을 사용하지 않는 점에서는 완전한 모델과 동일하지만, 공격자가 공격 대상을 정하고 난 뒤 공격이 시작되는 모델을 선택적인 ID모델 & 랜덤 오라클을 사용하지 않는 모델(Selective ID Model & Without Random Oracle Model)이라고 한다. 약한 가정을 하고 안전성 증명이 가능한 기법을 개발하는 것 역시 활발히 연구되고 있는 분야이다.

최근에는 위에서 언급한 증명 모델 하에 온라인/오프라인 개념을 적용하여 ID기반 암호와 ID기반 서명 기법에 관한 연구가 이루어지고 있다. 2008년에는 F. Guo 등[8]이 Boneh 등[1]이 2004년에 제안한 ID기반 암호기법을 확장하여 ID기반의 온라인/오프라인 암호기법 GMC08-1을 제안하였고 Gentry[7]가 2005년에 제안한 ID기반 암호기법을 확장하여 GMC08-2 기법을 제안하였다. J.K Liu[10] 등은 랜덤오라클 모델 하에 효율성 있는 ID기반 온라인/오프라인 기법을 제안하였다. 이처럼 1990년대에 서명 기법에 관하여 활발히 연구되던 온라인/오프라인 기법은 최근에 들어서야 ID기반 암호기법에 관한 연구가 이루어졌으며, 아직까지는 온라인/오프라인 사인크립션 기법에 관해서는 연구가 이루어지지 않았다. 사인크립션 기법은 메시지의 기밀성(Confidentiality), 무결성(Integrity)과 송신자의 부인방지(Non-repudiation) 등의 암호학적 특성을 제공한다. 이와 같은 사인크립션 기법을 ID기반에서 설계하게 되면 암호화 과정이나 서명 과정에서 페어링 연산이나 지수승 연산이 늘어나서 전체 기법의 효율성이 떨어지게 된다. ID기반 사인크립션 기법에 온라인/오프라인 기법을 적용하면 스마트카드와 같은 환경에서 이용할 수가 있다. 하지만 모든 기법에 효율성을 떨어트리지 않는 온라인/오프라인 기법을 적용하기는 힘들다. Y. Yu 등[15]은 Waters[14]가 2005년에 제안한 ID

〔표 1〕 관련 연구 동향 (IBSC: Identity Based Signcryption, IBOOE: Identity Based Online/Offline Encryption, IBOOSC: Identity Based Online/Offline Signcryption)

	Random Oracles	Without Random Oracles	
		Full Model	Selective ID
IBSC	Malone02[11], Boyen03[3] 등	YYSZ09[15]	제안 IBSC 기법
IBOOE	LZ09[10]	GMC08-2[8]	GMC08-1[8]
IBOOSC	DYW08[16]	없음	제안 IBOOSC 기법

기반 암호기법의 구조를 이용하여 처음으로 풀 모델(Full Model)에서 증명되는 사인크립션 기법을 제안하였다. 이 기법은 Waters의 ID기반 암호 기법의 구조를 따르기 때문에 기법의 구조상 메시지와 수신자의 공개키가 정해진 이후의 연산 단계인 온라인 단계에서의 연산 비용을 효율성 있게 줄이기가 힘들다. 이 기법은 선택 평문 공격에 의한 평문 구분불가능성(IND-CPA)에 안전하지 않다. 이에 관한 내용은 IV장에서 간단히 언급한다.

1.3. 기여도

우리는 Boneh[1] 등이 2004년에 제안한 ID기반 암호기법의 구조를 이용하여 안전성 증명에 랜덤오라클 모델을 사용하지 않은 사인크립션 기법을 제안하고, 스마트카드와 같은 저전력 환경에서 이용할 수 있는 온라인/오프라인 사인크립션 기법을 제안한다. 제안 사인크립션 기법은 완전한 모델에서 증명되는 것은 아니지만, 온라인/오프라인 기법을 설계하기 위한 기반이 되는 기법이다. 제안 사인크립션 기법을 기반하여 설계된 온라인/오프라인 사인크립션 기법은 ID 기반에서 최초의 온라인/오프라인 사인크립션 기법이며 랜덤 오라클을 가정하지 않은 모델에서 안전성 증명이 가능하다. 관련 연구의 내용과 제안 기법들을 종합하여 〔표 1〕에 정리하였다.

이 후 논문의 구성은 다음과 같다. II장에서는 제안한 기법을 위한 정의를 설명한다. III장에서는 ID기반 온라인/오프라인 사인크립션 기법의 형식적 모델과 안전성 모델을 기술한다. IV장에서는 ID기반 사인크립션 기법과 ID기반 온라인/오프라인 사인크립션 기법을 제안한다. V장에서는 제안한 기법들의 안전성을 기술한 안전성 모델 하에서 증명한다. VI장에서는 결론을 내린다.

II. 정의(Definitions)

본 장에서는 제안 기법의 설계 및 안전성 증명에 필요한 겹선형 함수(bilinear map) 및 이와 관련된 복잡도 (complextity assumption) 가정들을 살펴본다.

겹선형 함수(Bilinear Maps). G_1과 G_T가 위수를 소수 p로 갖는 순환 군(group)이라고 하자. 군 G_1과 G_2에서 모두 이산대수문제(Discrete Logarithm Problem)가 어렵다고 가정하자. 겹선형 함수는 다음과 같은 성질을 갖는 $G_1 \times G_1$에서 군 G_T 위로 맵핑되는 함수 $e: G_1 \times G_1 \rightarrow G_T$이다:

(1) **겹선형성** (Bilinearlity): 임의의 군 원소 $g \in G_1$와 $a, b \in Z_p^*$에 대하여 $e(g^a, g^b) = e(g,g)^{ab}$을 만족한다.

(2) **비소실성** (Non-degeneracy): $e(g,g) \neq 1$을 만족시키는 $g \in G_1$가 존재한다.

(3) **계산 가능성** (Computability): 임의의 $g_1, g_2 \in G_1$에 대해서 $e(g_1, g_2)$를 계산하는 효율적인 알고리즘이 존재한다.

계산적 Diffie-Hellman 문제 및 가정 (Computational Diffie-Hellman Assumption, CDH). 주어진 G_1의 생성원 g에 대해 g^a, g^b가 주어졌을 때 CDH 가정이란 g^{ab}을 의미 있는 확률로 효율적으로 계산할 수 있는 알고리즘 A이 존재하지 않음을 말한다. 알고리즘 A의 이점(advantage)는 다음과 같은 확률 값으로 정의된다.

$$\Pr\left[g^{ab} \leftarrow A(G_1, g, g^a, g^b)\right] \geq \epsilon$$

겹선형 Diffie-Hellman 문제 및 가정 (Bilinear Diffie-Hellman Assumption, BDH). 주어진 G_1의 생성원 g에 대해 g^a, g^b, g^c가 주어졌을 때 BDH 가정이란 $e(g,g)^{abc}$을 의미 있는 확률로 효율적으로 계산할 수 있는 알고리즘 A이 존재하지 않음을 말한다. 알고리즘 A의 이점(advantage)는 다음과 같은 확률 값으로 정의된다.

$$\Pr\left[e(g,g)^{abc} \leftarrow A(G_1, g, g^a, g^b, g^c)\right] \geq \epsilon$$

결정적 겹선형 Diffie-Hellman 문제 및 가정 (Decision Bilinear Diffie-Hellman Assumption, DBDH). 주어진 G_1의 생성원 g에 대해 g^a, g^b, g^c, T가 주어졌을 때 DBDH 가정이란 $T = e(g,g)^{abc}$인지 T가 임의의 난수인지를 의미 있는 확률로 판단할 수 있는 알고리즘 A이 존재하지 않음을 말한다. 알고리즘 A의 이점(advantage)는 다음과 같은 확률 값으로 정의된다.

$$\Pr[A(g, g^a, g^b, g^c) = e(g, g^{abc})] \geq \epsilon$$

III. 형식적 모델(Model)

본 장에서는 ID기반 온라인/오프라인 사인크립션 기법의 형식적 정의와 안전성 모델[11]에 대해 설명한다.

3.1. ID기반 온라인/오프라인 사인크립션 기법의 정의

ID기반 사인크립션 기법(Identity-Based Signcryption Scheme, IBSC)[11]은 다음과 같은 5개의 다항식 시간(polynomial-time) 알고리즘들로 구성된다:

- $Setup(1^k)$: 셋업(Setup) 알고리즘은 보안 상수 k를 입력으로 받고, 마스터 비밀키 msk와 공개 상수 $param$를 출력한다.
- $Extract(param, msk, ID)$: 공개 상수 $param$, 마스터 비밀키 msk와 ID를 입력으로 받고, 비밀키 D_{ID}를 출력한다.
- $Signcrypt(param, m, D_{ID_s}, ID_r)$: 공개 상수 $param$, 메시지 m, 송신자의 비밀키 D_{ID_s}와 수신자의 아이디 ID_r를 입력으로 받고, 암호문 ϕ을 출력한다.
- $Unsigncrypt(param, \phi, D_{ID_r})$: 공개 상수 $param$, 암호문 ϕ과 수신자의 비밀키 D_{ID_r}을 입력으로 받고, 메시지 m과 서명 σ을 출력한다.
- $Verify(param, m, \sigma, ID_s)$: 공개 상수 $param$, 메시지 m, 서명 σ과 송신자의 아이디 ID_s를 입력으로 받고, 유효한 서명이면 $Valid$를 출력하고, 유효하지 않으면 서명이면 $\perp$을 출력한다.

ID기반 온라인/오프라인 사인크립션 기법(Identity-Based Online/Offline Signcryption Scheme, IBOOSC)은 ID기반 사인크립션 기법과 비교하여 *Signcrypt* 알고리즘이 온라인 단계와 오프라인 단계로 나누어지고, 그밖에 알고리즘들은 같다. 다음과 같은 6개의 다항식 시간 알고리즘들로 구성된다:

- $Setup(1^k)$: 셋업(Setup) 알고리즘은 보안 상수 k를 입력으로 받고, 마스터 비밀키 msk와 공개 상수 $param$를 출력한다.
- $Extract(param, msk, ID)$: 공개 상수 $param$, 마스터 비밀키 msk와 ID를 입력으로 받고, 비밀키 D_{ID}를 출력한다.
- $Offline-Signcrypt(param, D_{ID_s})$: 공개 상수 $param$와 송신자의 비밀키 D_{ID_s}를 입력으로 받고, 오프라인 암호문 ϕ_{of}을 출력한다.
- $Online-Signcrypt(param, m, \phi_{of}, ID_r)$: 공개 상수 $param$, 메시지 m, 오프라인 암호문 ϕ_{of}과 $ID_r \neq ID_s$를 만족하는 수신자의 아이디 ID_r를 입력으로 받고, 암호문 ϕ을 출력한다.
- $Unsigncrypt(param, \phi, D_{ID_r})$: 공개 상수 $param$, 암호문 ϕ과 수신자의 비밀키 D_{ID_r}을 입력으로 받고, 메시지 m과 서명 σ을 출력한다.
- $Verify(param, m, \sigma, ID_s)$: 공개 상수 $param$, 메시지 m, 서명 σ과 송신자의 아이디 ID_s를 입력으로 받고, 유효한 서명이면 $Valid$를 출력하고, 그렇지 않으면 $\perp$을 출력한다.

3.2. ID기반 온라인/오프라인 사인크립션 기법의 안전성 모델

ID기반 사인크립션 기법과 ID기반 온라인/오프라인 사인크립션 기법의 안전성은 다음과 같은 암호 기법과 서명 기법에서 고려해야 하는 기본적인 성질을 모두 만족시켜야 한다.

정의.1 기밀성(Confidentiality): 어떠한 다항 함수 시간에 동작되는 공격자(adversary) F에 대하여도 F가 다음과 같이 정의된 게임에서 이길 성공 확률이 무시(negligible)할 수 있는 값이면 주어진 ID기반 온라인/오프라인 사인크립션 기법은 IND-sID-CPA 관점에서 안전하다고 정의한다.

- 초기설정($Initialization$): 공격자는 챌린지(Challenge) 할 아이디 ID_r*를 선택한다.

- 셋업($Setup(1^{\lambda})$) : 챌린저(challenger) C는 마스터 비밀키 msk와 공개 상수 $param$을 얻기 위해 $Setup$ 알고리즘을 실행한다. 챌린저 C는 공개 상수 $param$을 공격자 F에게 준다.
- 질의 1단계 : 공격자 F는 챌린저 C에게 다음과 같은 질의를 선택적으로 한다.
  - $Extract(ID)$: 공격자가 ID에 대한 비밀키를 요청할 때, C는 비밀키 D_{ID}을 생성하여 준다.
  - $Signcryption(D_{ID_s}, ID_r, m)$: 공격자가 송신자의 비밀키 D_{ID_s}, 수신자의 아이디 ID_r와 메시지 m에 대한 암호문을 요청할 때, 챌린저 C는 암호문 ϕ를 생성하여 준다.
- 챌린지($Challenge$) : 공격자는 챌린저 C에게 챌린지 메시지 (ID_s^*, m_0, m_1)를 준다. 챌린저 C는 ID_s^*에 대응하는 비밀키 $D_{ID_s}^*$를 생성하고, $b \in \{0,1\}$을 선택한다. $\phi_{ch} = Signcrypt(ID_r^*, D_{ID_s}^*, m_b)$를 생성하여 공격자에게 준다.
- 질의 2단계 : 공격자 F는 질의 1단계에서와 같은 질의를 다음의 경우를 제외하고 계속하여 요청할 수 있다. ID_r^*을 $Extract$ 질의를 할 수 없다.
- 추측($Guess$) : 공격자 F는 $b' \in \{0,1\}$를 출력하고 $b' = b$인 경우 F가 위의 게임에서 이긴다.

정의.2 위조 불가능(Unforgeability): 어떠한 다항 함수 시간에 동작되는 공격자(adversary) F에 대하여도 F가 다음과 같이 정의된 게임에서 이길 성공 확률이 무시할(negligible)할 수 있는 값이면 주어진 ID기반 온라인/오프라인 사인크립션 기법은 sUF-sID-CMA 관점에서 안전하다고 정의한다.

- 초기설정($Initialization$): 공격자는 챌린지(Challenge) 할 아이디 ID_s^*, m^*를 선택한다.
- 셋업($Setup(1^{\lambda})$) : 챌린저(challenger) C는 마스터 비밀키 msk와 공개 상수 $param$을 얻기 위해 $Setup$ 알고리즘을 실행한다. 챌린저 C는 공개 상수 $param$을 공격자 F에게 준다.
- 질의 단계 : 공격자 F는 챌린저 C에게 다음과 같은 질의를 선택적으로 한다.
  - $Extract(ID)$: 공격자가 ID에 대한 비밀키를 요청할 때, C는 비밀키 D_{ID}을 생성하여 준다.
  - $Signcryption(D_{ID_s}, ID_r, m)$: 공격자가 송신자의 비밀키 D_{ID_s}, 수신자의 아이디 ID_r와 메시지 m에 대한 암호문을 요청할 때, 챌린저 C는 암호문 ϕ를 생성하여 준다.
  - $Unsigncryption(\phi, ID_r)$: 공격자가 암호문 ϕ에 대한 평문을 요청할 때, 챌린저 C는 암호문을 $Unsigncryption$한다. 만약 $Unsigncryption$의 결과로 나온 메시지와 서명이 송신자의 아이디로 유효하게 검증이 되면 챌린저 C는 복호화한 평문 m을 F에게 주고, 그렇지 않다면 거절한다.
- 위조($Forge$) : 공격자는 아이디 ID_r^*와 암호문 ϕ^*을 생성한다. 공격자는 생성한 아이디와 암호문이 다음을 만족할 경우 게임에서 이긴다.

$Unsigncryption(\phi^*, ID_r^*)$을 하여 나온 메시지와 서명 쌍$(m^*, \sigma^*)$이 $valid \leftarrow Verify(m^*, \sigma^*, ID_s^*)$를 만족한다.

IND-sID-CPA 모델(Selective-ID Model). 위에서 기밀성에 대하여 정의한 안전성은 선택적인 ID 모델이다. 공격자가 공개 상수나 키를 설정하는 셋업 단계 이전에 초기설정에서 미리 공격할 ID_r^*를 정하는 선택적인 ID 모델은 미리 선택한 ID_r^*로 챌린지 암호문이 생성이 된다. 이 모델에 의한 증명은 2004년에 Boneh 등[1]의 암호기법에서 처음 쓰였으며, 암호 기법[1,5]에서 증명 방법으로 많이 쓰이고 있다.

선택 암호문 공격에 대한 안정성(Chosen Ciphertext Security). 2004년에 Canetti[4] 등이 제안한 논문에서 선택 평문 공격에 안전한 $(\ell+1)$-HIBE이 있으면, 선택 암호문 공격에 안전한 ℓ-HIBE를 효율적으로 설계할 수 있다는 결과가 나왔다. 본 논문에서는 선택 평문 공격에 안전한 1-HIBE를 제안하였고, Boneh 등이 제안한 IBE의 방법으로 2-HIBE를 설계할 수 있으며, 결과적으로 안전성 증명에 랜덤 오라클 모델을 사용하지 않은 선택 암호문 공격에 안전한 ID기반 온라인/오프라인 사인크립션 기법을 설계할 수 있다.

sUF-sID-CMA 모델(Selective Forgery & Selective-ID Model). 위에서 위조불가능에 대하여 정의한 안전성은 선택한 메시지에 대한 위조와 선택적인 ID 모델이다. 공격자가 공개 상수나 키를 설정하는 셋업 단계 이전에 초기설정에서 미리 공격할 m^*와 ID_s^*를 정하는 sUF-sID-CMA 모델은 미리 선택한 m^*와 ID_s^*로 공격자는 서명 위조를 하게 된다. EUF-sID-CMA 모델에 의한 증명은 서명 기법

[5,9]에서 증명 방법으로 많이 쓰이고 있으며, sUF-sID-CMA 모델 역시 서명 기법[12]에서 증명 방법 모델로 쓰이고 있으며, Shahandashti 등[12]이 발표한 논문에서 선택한 메시지에 대한 위조에 대한 안전성을 존재적 위조(Existential Forgery)에 대한 안전성으로 변환하는 방법에 대한 결과가 나와 있다.

IV. 제안하는 ID기반 Online/Offline 사인크립션 기법

본 장에서는 Boneh 등의 ID기반 암호 기법의 구조를 이용하여 안전성 증명 시에 랜덤 오라클이 필요하지 않고 IND-sID-CPA 모델과 sUF-sID-CMA 모델에 안전한 ID기반 사인크립션 기법을 제안하고, 제안한 ID기반 사인크립션 기법을 바탕으로 ID기반 온라인/오프라인 사인크립션 기법을 제안한다.

4.1. ID기반 사인크립션 기법

본 절에서는 Boneh 등이 제안한 ID기반 암호 기법의 구조를 이용하여 ID기반 사인크립션 기법을 제안한다. IND-CPA에 안전한 암호 기법과 EUF-CMA에 안전한 서명 기법을 가지고 사인크립션을 구성하더라도 서명을 복호화 된 메시지와 송신자의 공개키만을 가지고 검증을 하게 되면 사인크립션 기법은 IND-CPA에 안전하지 않게 된다. IND-CPA 게임에서 챌린지 메시지 중에 하나를 선택해서 검증을 해보임으로서 챌린지 암호문이 어느 메시지로 암호화 되었는지 확인해 볼 수 있기 때문이다. Y. Yu 등이 Waters[14]의 ID기반 암호 기법을 기반으로 제안한 사인크립션 기법은 검증과정에서 복호화 된 메시지와 송신자의 공개키만을 가지고 검증을 하기 때문에 IND-CPA에 안전하지 않다. 기본적으로 사인크립션을 구성할 때에는 메시지 이외에 정당한 수신자만이 구할 수 있는 값을 검증과정에 넣어야 한다. 본 절에서는 Boneh 등의 IND-sID-CPA에 안전한 ID기반 암호 기법과 같은 구조를 갖는 sUF-sID-CMA에 안전한 서명 기법[12]을 이용하여 IND-sID-CPA와 sUF-sID-CMA에 안전한 사인크립션을 제안한다. ID기반 사인크립션 기법은 다음과 같이 셋업, 비밀키 생성, Signcrypt, Unsigncrypt, 검증의 5개의 알고리즘들로 구성된다.

- *Setup*(1^k): 겹선형 함수와 관련된 순환군(cyclic group)들 (G_1, G_T, e)을 생성한다. 이 때 G_1와 G_T는 소수 p를 위수로 갖으며, g는 G_1의 생성원이다. $e: G_1 \times G_1 \rightarrow G_T$는 어드미서블 겹선형함수(admissible bilinear map)이다. G_1의 임의의 생성원 g를 선택한다. 임의의 난수 $a \in Z_p^*$를 선택하여 $g_1 = g^a$을 만족하는 g_1을 생성하고, G_1에서 임의의 난수 $g_2, g_3, h_1, h_2, h_3, h_4 \in G_1$와 암호학적인 해쉬 함수 $H_1 : G_T \rightarrow Z_p^*$와 $H_2 : G_T \times G_1 \rightarrow Z_p^*$를 선택한다. 공개 상수 $param$와 마스터 비밀키 msk는 다음과 같이 설정한다.

$$param = (g, g_1, g_2, g_3, h_1, h_2, h_3, h_4, H_1, H_2), \quad msk = g_2^a$$

- *Extract*$(param, msk, ID)$: 비밀키 생성 알고리즘은 공개 상수 $param$, 마스터 비밀키 msk와 ID를 입력으로 받는다. 임의의 난수 $r_1, r_2 \in Z_p^*$를 선택하여 생성하는 송신자의 서명 비밀키와 수신자의 복호화 비밀키는 다음과 같다.

$$D_{ID_s} = (ssk_1, ssk_2) = (g_2^a (h_2 g_1^{ID_s})^{r_2}, g^{r_2}),$$

$$D_{ID_r} = (d_1, d_2) = (g_2^a (h_1 g_1^{ID_r})^{r_1}, g^{r_1})$$

- *Signcrypt*$(param, m, D_{ID_s}, ID_r)$: *Signcrypt* 알고리즘은 공개 상수 $param$, 메시지 $m \in Z_p^*$, 송신자의 비밀키 D_{ID_s}와 수신자의 아이디 ID_r를 입력으로 받는다. 임의의 난수 $s_1, s_2 \in Z_p^*$를 선택한 후 메시지 m에 대한 사인크립션을 다음과 같이 계산한다.

$$e(g_1, g_2)^{s_1} = T_1, \quad H_1(T_1) = T_2, \quad H_2(T_1, g^{s_2}) = T_3$$

$$\phi = ((h_1 g_1^{ID_r})^{s_1}, T_2 \cdot m, g^{s_1}, ssk_1 (h_4 g_3^{T_3})^{s_1} (h_3 g_1^m)^{s_2},$$

$$ssk_2, g^{s_2} = (\phi_1, \phi_2, \phi_3, \phi_4, \phi_5, \phi_6)$$

- *Unsigncrypt*$(param, \phi, D_{ID_r})$: *Unsigncryption* 알고리즘은 공개 상수 $param$, 암호문 ϕ과 수신자의 비밀키 D_{ID_r}을 입력으로 받는다. 다음과 같이 메시지를 복호화 한다.

$$\phi_2 / H_1\left(\frac{e(d_1, \phi_3)}{e(\phi_1, d_2)}\right) = m$$

- *Verify*$(param, m, \sigma, ID_s)$: 검증 알고리즘은 공개 상수 $param$, 메시지 m, 서명 σ과 송신자의 아이디 ID_s를 입력으로 받는다. 메시지와 서명은 다

음과 같이 검증한다.

$$\frac{e(d_1,\phi_3)}{e(\phi_1,d_2)}=T_1,\quad H_2(T_1,g^{s_2})=T_3,$$

$$\frac{e(\phi_4,g)}{e(h_2g_1^{ID_s},\phi_5)e(h_4g_3^{T_3},\phi_3)e(h_3g_1^{m},\phi_6)}={}^{?}e(g_1,g_2)$$

정확성(Correctness). 위에서 제안한 기법은 정확성을 가짐을 다음과 같이 쉽게 보일 수 있다.

- 복호화 과정. 주어진 사인크립션 $\phi=((h_1g_1^{ID_r})^{s_1},\ T_2\cdot m,g^{s_1},g_2^{a}(h_2g_1^{ID_s})^{r_2}(h_4g_3^{T_3})^{s_1}(h_3g_1^{m})^{s_2},g^{r_2},g^{s_2})$ $=(\phi_1,\phi_2,\phi_3,\phi_4,\phi_5,\phi_6)$과 수신자의 비밀키 $D_{ID_r}=(d_1,d_2)=(g_2^{a}(h_1g_2^{ID_r})^{r_1},g^{r_1})$에 대하여 메시지 m을 다음과 같은 과정을 통하여 생성할 수 있다.

$$\phi_2/H_1\left(\frac{e(d_1,\phi_3)}{e(\phi_1,d_2)}\right)$$

$$=T_2\cdot m/H_1\left(\frac{e(g_2^{a}(h_1g_1^{ID_r})^{r_1},g^{s_1})}{e((h_1g_1^{ID_r})^{s_1},g^{r_1})}\right)$$

$$=H_1(e(g_1,g_2)^{s_1})\cdot m/H_1\left(\frac{e(g_2^{a}(h_1g_1^{ID_r})^{r_1},g^{s_1})}{e((h_1g_1^{ID_r})^{s_1},g^{r_1})}\right)=m$$

- 검증 과정. 주어진 사인크립션 $\phi=((h_1g_1^{ID_r})^{s_1},\ T_2\cdot m,g^{s_1},g_2^{a}(h_2g_1^{ID_s})^{r_2}(h_4g_3^{T_3})^{s_1}(h_3g_1^{m})^{s_2},g^{r_2},g^{s_2})=(\phi_1,\phi_2,\phi_3,\phi_4,\phi_5,\phi_6)$, 메시지 m과 송신자의 아이디 ID_s에 대하여 서명은 다음과 같은 과정을 통하여 검증할 수 있다.

$$\frac{e(d_1,\phi_3)}{e(\phi_1,d_2)}=\frac{e(g_2^{a}(h_1g_1^{ID_r})^{r_1},g^{s_1})}{e((h_1g_1^{ID_r})^{s_1},g^{r_1})}$$

$$=\frac{e(g_2^{a},g^{s_1})e((h_1g_1^{ID_r})^{r_1},g^{s_1})}{e((h_1g_1^{ID_r})^{s_1},g^{r_1})}=e(g_1,g_2)^{s_1}=T_1,$$

$$H_2(T_1,g^{s_2})=T_3$$

$$\frac{e(\phi_4,g)}{e(h_2g_1^{ID_s},\phi_5)e(h_4g_3^{T_3},\phi_3)e(h_3g_1^{m},\phi_6)}$$

$$=\frac{e(g_2^{a}(h_2g_1^{ID_s})^{r_2}(h_4g_3^{T_3})^{s_1}(h_3g_1^{m})^{s_2},g)}{e(h_2g_1^{ID_s},g^{r_2})e(h_4g_3^{T_3}),g^{s_1})e(h_3g_1^{m},g^{s_2})}$$

$$=\frac{e(g_2^{a},g)e((h_2g_1^{ID_s})^{r_2},g)e((h_4g_3^{T_3})^{s_1},g)e((h_3g_1^{m})^{s_2},g)}{e(h_2g_1^{ID_s},g^{r_2})e(h_4g_3^{T_3},g^{s_1})e(h_3g_1^{m},g^{s_2})}$$

$$=e(g_2^{a},g)$$

4.2. ID기반 온라인/오프라인 사인크립션 기법

본 절에서는 앞의 절에서 제안한 ID기반 사인크립션 기법(IBSC)에 F. Guo 등이 제안한 ID기반 온라인/오프라인 암호 기법의 구조를 적용하여 ID기반 온라인/오프라인 사인크립션 기법(IBOOSC) 제안한다. IBOOSC 기법은 셋업, 비밀키 생성, Online-Signcrypt, Offline-Signcrypt, Unsigncrypt, 검증의 6개의 알고리즘들로 구성된다.

- *Setup*(1^k): 공개 상수 *param*와 마스터 비밀키 *msk*는 앞의 절에서 제안한 IBSC 기법에서의 *Setup* 알고리즘과 같다.
- *Extract*$(param, msk, ID)$: 비밀키 생성과정은 앞의 절에서 제안한 IBSC 기법에서의 *Extract* 알고리즘과 같다.
- *Offline*$-$*Signcrypt*$(param, D_{ID_s})$:

  Offline$-$*Signcrypt* 알고리즘은 공개 상수 *param*와 송신자의 비밀키 D_{ID_s}를 입력으로 받는다. 임의의 난수 $s_1,s_2,\delta_1,\delta_2,\beta_1,\beta_2\in Z_p^*$를 선택한 후 메시지 $m\in Z_p^*$에 대한 *Offline*$-$*Signcrypt*을 다음과 같이 계산한다.

$$e(g_1,g_2)^{s_1}=T_1,\ H_1(T_1)=T_2,\ H_2(T_1,g^{s_2})=T_3$$

$$\phi_{of}=((h_1g_1^{\delta_1})^{s_1},g_1^{s_1\beta_1},H_1(e(g_1,g_2)^{s_1}),g^{s_1},$$

$$ssk_1(h_4g_3^{T_3})^{s_1}(h_3g_1^{\delta_2})^{s_2},g_1^{s_2\beta_2},ssk_2,g^{s_2})$$

$$=(\phi_1,\phi_2,T_2,\phi_5,\phi_6,\phi_7,\phi_9,\phi_{10})$$

위에서 생성된 암호문과 난수 $\delta_1,\delta_2,\beta_1^{-1},\beta_2^{-1}\in Z_p^*$는 안전한 저장소에 저장되고, *Online*$-$*Signcrypt* 알고리즘을 수행할 때, 쓰이게 된다.

- *Online*$-$*Signcrypt*$(param, m, \phi_{of}, ID_r)$:

  Online$-$*Signcrypt* 알고리즘은 공개 상수 *param*, 메시지 m, 오프라인 암호문 ϕ_{of}와 수신자의 아이디 ID_r를 입력으로 받는다. 메시지 m에 대한 *Online*$-$*Signcrypt*을 다음과 같이 계산한다.

$$\phi_{on}=((\beta_1^{-1}(ID_r-\delta_1),\ T_2\cdot m,(\beta_2^{-1}(m-\delta_2))$$

$$=(\phi_3,\phi_4,\phi_8)$$

온라인 단계에서의 연산은 위와 같으며, 최종적으로 생성되는 암호문은 다음과 같다.

$$\phi=(\phi_1,\phi_2,\phi_3,\phi_4,\phi_5,\phi_6,\phi_7,\phi_8,\phi_9,\phi_{10})$$

$$\phi=((h_1g_1^{\delta_1})^{s_1},g_1^{s_1\beta_1},\beta_1^{-1}(ID_r-\delta_1),\ T_2\cdot m,g^{s_1},$$

$$ssk_1(h_4g_3^{T_3})^{s_1}(h_3g_1^{\delta_2})^{s_2},g_1^{s_2\beta_2},\ \beta_2^{-1}(m-\delta_2),ssk_2,g^{s_2})$$

- *Unsigncrypt*$(param, \phi, D_{ID_r})$: *Unsigncryption* 알고리즘은 공개 상수 *param*, 암호문 ϕ과 수신자의 비밀키 D_{ID_r}을 입력으로 받는다. 다음과 같이 메시지를 복호화 한다.

$$\phi' = (\phi_1\phi_2^{\phi_3}, \phi_4, \phi_5, \phi_6\phi_7^{\phi_8}, \phi_9, \phi_{10})$$

$$= (\phi_1', \phi_2', \phi_3', \phi_4', \phi_5', \phi_6')$$

$$\phi_2' / H_1\left(\frac{e(d_1, \phi_3')}{e(\phi_1', d_2)}\right) = m$$

- *Verify*$(param, m, \phi', ID_s)$: 검증 알고리즘은 공개 상수 *param*, 메시지 m, 서명 σ과 송신자의 아이디 ID_s를 입력으로 받는다. 메시지와 서명은 다음과 같이 검증한다.

$$\frac{e(d_1, \phi_3')}{e(\phi_1', d_2)} = T_1, \quad H_2(T_1, g^{s_2}) = T_3,$$

$$\frac{e(\phi_4', g)}{e(h_2 g_1^{ID_s}, \phi_5')e(h_4 g_3^{T_3}, \phi_3')e(h_3 g_1^{m}, \phi_6')} \stackrel{?}{=} e(g_1, g_2)$$

V. 안전성 증명(Security)

5.1. ID기반 사인크립션 기법의 안전성

정리.1 기밀성(Confidentiality) 제안한 ID기반 사인크립션 기법 IBSC는 랜덤 오라클 모델을 사용하지 않고 DBDH 가정하에서 IND-sID-CPA 관점에서 안전하다.

증명. 제안 기법 IBSC의 IND-sID-CPA 안전성을 의미 있는(non-negligible) 확률로 깰 수 있는 알고리즘 F가 존재한다고 가정하다. 그러면 F를 이용하여 *DBDH* 문제를 효율적으로 해결할 수 있는 알고리즘 B가 존재함을 보일 것이다. B는 임의로 선택된 $a, b, c \in Z_p^*$와 $g \in G_1$에 대한 *DBDH* 문제 인스턴스(instance) $(G_1, g, g^a, g^b, g^c, T)$를 입력 받는다. B의 목적은 $T = e(g, g)^{abc}$임을 판단하는 것이다.

- 초기설정(*Initialization*): F는 챌린지(Challenge) 할 아이디 ID_r^*를 선택한다.
- 셋업(*Setup*) : 공개 상수를 생성하기 위해 B는 $g_1 = g^a$, $g_2 = g^b$, $msk = g_2^a = g^{ab}$로 설정하고, 임의의 난수 $d, e, f, w, \alpha \in Z_p^*$를 선택해서 $g_3 = g^d$, $h_1 = g^{\alpha} g_1^{-ID_r^*}$, $h_2 = g^e$, $h_3 = g^f$, $h_4 = g^w$로 설정한다. 해쉬 함수 $H_1 : G^T \rightarrow Z_p^*$과 $H_2 : G_T \times G_1 \rightarrow Z_p^*$를 선택하고, B는 IBSC의 공개 상수 $(g, g_1, g_2, g_3, h_1, h_2, h_3, h_4, H_1, H_2)$를 F에게 준다.
- 질의 1단계 : B는 F의 오라클 질의들의 응답을 다음과 같이 시뮬레이션 한다.

- *Extract*(ID_{si}): F가 ID_{si}에 대한 서명 비밀키를 요청할 때 B는 임의의 난수 $r_{2i} \in Z_p^*$를 선택하고, 마스터 비밀키 msk와 공개 상수 *param*를 가지고 서명 비밀키 $D_{ID_{si}}$를 다음과 같이 생성하여 F에게 반환한다.

$$D_{ID_{si}} = (g^{ab}(h_2 g_1^{ID_{si}})^{r_{2i}}, g^{r_{2i}})$$

B는 임의의 난수 $\widetilde{r_{2i}} \in Z_p^*$를 선택하여 다음과 같은 방법으로 마스터 비밀키 msk의 계산 없이 정당한 서명 비밀키를 생성한다.

$$r_{2i} = -b/ID_{si} + \widetilde{r_{2i}}$$

$$g^{ab}(h_2 g_1^{ID_{si}})^{r_{2i}} = g^{ab}(g^e g^{aID_{si}})^{-b/ID_{si} + \widetilde{r_{2i}}}$$

$$= (g^b)^{-e/ID_{si}} (g^e)^{\widetilde{r_{2i}}} (g^a)^{ID_{si}\widetilde{r_{2i}}}$$

- *Extract*(ID_{ri}): F가 ID_{ri}에 대한 복호화 비밀키를 요청할 때 B는 임의의 난수 $r_{1i} \in Z_p^*$를 선택하고, 마스터 비밀키 msk와 공개 상수 *param*를 가지고 복호화 비밀키 $D_{ID_{ri}}$를 다음과 같이 생성하여 F에게 반환한다.

$$D_{ID_{ri}} = (g^{ab}(h_1 g_1^{ID_{ri}})^{r_{1i}}, g^{r_{1i}})$$

B는 임의의 난수 $\widetilde{r_{1i}} \in Z_p^*$를 선택하여 다음과 같은 방법으로 마스터 비밀키 msk의 계산 없이 정당한 복호화 비밀키를 생성한다.

$$r_{1i} = -b/(ID_{ri} - ID_r^*) + \widetilde{r_{1i}}$$

$$g^{ab}(h_1 g_1^{ID_{ri}})^{r_{1i}} = g^{ab}(g^{\alpha} g^{a(ID_{ri} - ID_r^*)})^{-b/(ID_{ri} - ID_r^*) + \widetilde{r_{1i}}}$$

$$= (g^b)^{-\alpha/(ID_{ri} - ID_r^*)} g^{\alpha \widetilde{r_{1i}}} (g^a)^{(ID_{ri} - ID_r^*)\widetilde{r_{1i}}}$$

- *Signcryption*(ID_{si}, ID_{ri}, m_i): F가 ID_{si}, ID_{ri}와 m_i에 대한 암호문을 요청할 때 B는 임의의 난수 $s_{1i}, s_{2i} \in Z_p^*$를 선택하고, 마스터 비밀키 msk와 공개 상수 *param*를 가지고 암호문 ϕ_i를 다음과 같이 생성하여 F에게 반환한다.

$$\phi_i = ((h_1 g_1^{ID_{ri}})^{s_{1i}}, H_1(e(g_1, g_2)^{s_{1i}}) \cdot m_i, g^{s_{1i}},$$

$g^{ab}(h_2 g_1^{ID_{si}})^{r_{2i}}(h_4 g_3^{H_2(e(g_1,g_2)^{r_{1i}},g^{s_{2i}})})^{s_{1i}}(h_3 g_1^{m})^{s_{2i}}, g^{r_{2i}}, g^{s_{2i}})$

- 챌린지($Challenge(ID_s^*, m_0, m_1)$) : F는 선택한 아이디와 챌린지 메시지들의 쌍 (ID_s^*, m_0, m_1)를 B에게 준다. B는 ID_s^*에 대응하는 서명 비밀키 $D_{ID_s}^*$를 생성하고, $b \in \{0,1\}$을 선택한다. 임의의 난수 $r', s_2 \in Z_p^*$를 선택하고, 마스터 비밀키 msk와 공개 상수 $param$를 가지고 챌린지 암호문 $\phi_{ch} = Signcrypt(ID_r^*, D_{ID_s}^*, m_b)$를 생성하여 F에게 반환한다.

$s_1 = c, g^{s_1} = g^c, H_2(T, g^{s_2}) = T_3$

$\phi_{ch} = ((g^c)^{\alpha}, H_1(T) \cdot m_b, g^c, ssk_1 (g^c)^w$

$\phi_{ch} = ((g^c)^{\alpha}, H_1(T) \cdot m_b, g^c, ssk_1 (g^c)^w (g^c)^{dH_2(T, g^{s_2})}$

$g^{fs_2}(g^a)^{ms_2}, ssk_2, g^{s_2})$

챌린지 암호문에 들어가는 서명키는 $Extract(ID_{si})$ 알고리즘을 통해서 얻을 수 있다. 위와 같이 생성한 챌린지 암호문은 키설정에 의하여 다음과 같이 유효한 챌린지 암호문이 됨을 알 수 있다.

$\phi_{ch} = ((h_1 g_1^{ID_r^*})^{s_1}, H_1(e(g_1, g_2)^{s_1}) \cdot m_b, g^{s_1},$

$g^{ab}(h_2 g_1^{ID_s^*})^{r_2}(h_4 g_3^{T_3})^{s_1}(h_3 g_1^{m})^{s_2}, g^{r_2}, g^{s_2})$

- 질의 2단계 : 공격자 F는 질의 1단계에서와 같은 질의를 다음의 경우를 제외하고 계속하여 요청할 수 있다. (ϕ_{ch}, ID_r^*)을 $Unsigncryption$ 질의를 할 수 없고, ID_r^*을 $Extract$ 질의를 할 수 없다.
- 추측($Guess$) : 공격자 F는 자신의 추측 비트값 $b' \in \{0,1\}$를 출력한다. B는 출력된 비트값 b'과 b를 비교하여 $b' = b$이면 $T = e(g,g)^{abc}$라는 의미로 1을 출력하고, 그렇지 않다면 $T \neq e(g,g)^{abc}$라는 의미로 0을 출력한다.

다음의 사항을 관찰해 보자. 만일, T가 임의의 난수값이면 공격자에게 챌린지 암호문은 난수값으로 보이므로 공격자의 이점을 이용할 수 없다. 만일 $T = e(g,g)^{abc}$이면 위의 시뮬레이션이 정상적으로 작동하였다면 완전한 공격 시뮬레이션을 제공한다. 즉, 제안 기법 IBSC의 실행환경과 동일하다.

정리.2 위조 불가능(Unforgeability) 제안한 ID 기반 사인크립션 기법 IBSC는 랜덤 오라클 모델을 사용하지 않고 CDH 가정하에서 sUF-sID-CMA 관점에서 안전하다.

증명. 제안 기법 IBSC의 sUF-sID-CMA 안전성을 의미있는(non-negligible) 확률로 깰 수 있는 알고리즘 F가 존재한다고 가정하다. 그러면 F를 이용하여 CDH 문제를 효율적으로 해결할 수 있는 알고리즘 B가 존재함을 보일 것이다. B는 임의로 선택된 $a, b \in Z_p^*$와 $g \in G_1$에 대한 CDH 문제 인스턴스(instance) (G_1, g, g^a, g^b)를 입력 받는다. B의 목적은 g^{ab}를 계산하는 것이다.

- 초기설정($Initialization$): F는 챌린지(Challenge) 할 아이디 ID_s^*, M^*를 선택한다.
- 셋업($Setup$) : 공개 상수를 생성하기 위해 B는 $g_1 = g^a$, $g_2 = g^b$, $msk = g_2^{\alpha} = g^{ab}$로 설정하고, 임의의 난수 $d, e, f, \alpha_1, \alpha_2 \in Z_p^*$를 선택해서 $g_3 = g^d$, $h_1 = g^e$, $h_2 = g^{\alpha_1} g_1^{-ID_r^*}$, $h_3 = g^{\alpha_2} g_1^{-m^*}$, $h_4 = g^f$로 설정한다. 해쉬 함수 $H_1 : G^T \rightarrow Z_p^*$과 $H_2 : G_T \times G_1 \rightarrow Z_p^*$를 선택한다. 여기서 B는 IBSC의 공개 상수 $(g, g_1, g_2, g_3, h_1, h_2, h_3, h_4, H_1, H_2)$를 F에게 준다.
- 질의 단계 : B는 F의 오라클 질의들의 응답을 다음과 같이 시뮬레이션 한다.

- $Extract(ID_{si})$: F가 ID_{si}에 대한 서명 비밀키를 요청할 때 B는 임의의 난수 $r_{1i} \in Z_p^*$를 선택하고, 마스터 비밀키 msk와 공개 상수 $param$를 가지고 서명 비밀키 $D_{ID_{si}}$를 다음과 같이 생성하여 F에게 반환한다.

$D_{ID_{si}} = (g^{ab}(h_2 g_1^{ID_{si}})^{r_{2i}}, g^{r_{2i}})$

B는 임의의 난수 $\widetilde{r_{2i}} \in Z_p^*$를 선택하여 다음과 같은 방법으로 마스터 비밀키 msk의 계산없이 정당한 서명 비밀키를 생성한다.

$r_{2i} = -b/(ID_{si} - ID_s^*) + \widetilde{r_{2i}}$

$g^{ab}(h_2 g_1^{ID_{si}})^{r_{2i}} = g^{ab}(g^{\alpha_1} g^{a(ID_{si} - ID_s^*)})^{-b/(ID_{si} - ID_s^*) + \widetilde{r_{2i}}}$

$= (g^b)^{-\alpha_1/(ID_{si} - ID_s^*)} g^{\alpha_1 \widetilde{r_{2i}}} (g^a)^{(ID_{si} - ID_s^*)\widetilde{r_{2i}}}$

- $Extract(ID_{ri})$: F가 ID_{ri}에 대한 복호화 비밀키를 요청할 때 B는 임의의 난수 $r_{2i} \in Z_p^*$를 선택하고, 마스터 비밀키 msk와 공개 상수 $param$를 가지고 복호화 비밀키 $D_{ID_{ri}}$를 다음과 같이 생성하여 F에

게 반환한다.

$$D_{ID_{ri}} = (g^{ab}(h_1 g_1^{ID_{ri}})^{r_{1i}}, g^{r_{1i}})$$

B는 임의의 난수 $\widetilde{r_{1i}} \in Z_p^*$를 선택하여 다음과 같은 방법으로 마스터 비밀키 msk의 계산 없이 정당한 복호화 비밀키를 생성한다.

$$r_{1i} = -b/(ID_{ri}) + \widetilde{r_{1i}}$$
$$g^{ab}(h_1 g_1^{ID_{ri}})^{r_{1i}} = g^{ab}(g^{\epsilon} g^{aID_{ri}})^{-b/ID_{ri}+\widetilde{r_{1i}}}$$
$$= (g^b)^{-\epsilon/ID_{ri}} g^{\epsilon \widetilde{r_{1i}}} (g^a)^{ID_{ri}\widetilde{r_{1i}}}$$

- *Signcryption*(ID_{si}, ID_{ri}, m_i): F가 ID_{si}, ID_{ri}와 m_i에 대한 암호문을 요청할 때 B는 임의의 난수 $s_i \in Z_p^*$를 선택하고, 마스터 비밀키 msk와 공개 상수 $param$를 가지고 암호문 ϕ_i를 다음과 같이 생성하여 F에게 반환한다. *Signcryption*(ID_{si}, ID_{ri}, m_i) 암호문은 공개키와 ID_{ri}를 가지고 암호 부분 (ϕ_1, ϕ_2, ϕ_3)은 쉽게 생성할 수 있으며, ID_{si}에 따라 서명 부분이 두 가지 경우로 나누어서 생성된다.

$$\phi_i = ((h_1 g_1^{ID_{ri}})^{s_{1i}}, H_1(e(g_1, g_2)^{s_{1i}}) \cdot m_i, g^{s_{1i}},$$
$$g^{ab}(h_2 g_1^{ID_{si}})^{r_{2i}} (h_4 g_3^{H_2(e(g_1,g_2)^{s_{1i}}, g^{s_{2i}})})^{s_{1i}} (h_3 g_1^{m_i})^{s_{2i}}, g^{r_{2i}}, g^{s_{2i}})$$

$ID_{si} \neq ID_s^*$ 일 때, B는 임의의 난수 $\widetilde{r_{2i}} \in Z_p^*$를 선택하여 다음과 같은 방법으로 마스터 비밀키 msk의 계산없이 정당한 서명을 생성한다.

$$r_{2i} = -b/(ID_{si} - ID_s^*) + \widetilde{r_{2i}}$$
$$(\phi_4, \phi_5, \phi_6) = (g^{ab}(h_2 g_1^{ID_{si}})^{-b/(ID_{si}-ID_s^*)+\widetilde{r_{2i}}}$$
$$(h_4 g_3^{H_2(e(g_1,g_2)^{s_{1i}}, g^{s_{2i}})})^{s_{1i}} (h_3 g_1^{m_i})^{s_{2i}}, g^{-b/(ID_{si}-ID_s^*)+\widetilde{r_{2i}}}, g^{s_{2i}})$$

$ID_{si} = ID_s^*$ 일 때, B는 임의의 난수 $\widetilde{s_{2i}} \in Z_p^*$를 선택하여 다음과 같은 방법으로 마스터 비밀키 msk의 계산없이 정당한 서명을 생성한다.

$$s_{2i} = -b/(m_i - m^*) + \widetilde{s_{2i}}$$
$$(\phi_4, \phi_5, \phi_6) = (g^{ab}(h_2 g_1^{ID_{si}})^{r_{2i}} (h_4 g_3^{H_2(e(g_1,g_2)^{s_{1i}}, g^{s_{2i}})})^{s_{1i}}$$
$$(h_3 g_1^{m_i})^{-b/(m_i-m^*)+\widetilde{s_{2i}}}, g^{r_{2i}}, g^{-b/(m_i-m^*)+\widetilde{s_{2i}}})$$

- *Unsigncryption*$(\phi_i, ID_{si}, ID_{ri})$: F가 암호문 ϕ_i에 대한 평문 m_i와 서명 σ_i을 요청할 때 B는 다음과 같이 계산하여 평문 m_i와 서명 σ_i을 구한다. 만약 *Unsigncryption*의 결과로 나온 메시지와 서명이 송신자의 아이디로 유효하게 검증이 되면 B는 F에게 평문 m_i을 반환한다. 서명이 유효하게 검증되지 않는다면 $\perp$를 반환한다.

$$\phi_i = ((h_1 g_1^{ID_{ri}})^{s_{1i}}, H_1(e(g_1, g_2)^{s_{1i}}) \cdot m_i, g^{s_{1i}},$$
$$g^{ab}(h_2 g_1^{ID_{si}})^{r_{2i}} (h_4 g_3^{T_{3i}})^{s_{1i}} (h_3 g_1^{m_i})^{s_{2i}}, g^{r_{2i}}, g^{s_{2i}})$$
$$(h_1 g_1^{ID_{ri}})^{s_{1i}} / (g^{s_{1i}})^{\epsilon} = (g^{\epsilon} g^{aID_{ri}})^{s_{1i}} / (g^{s_{1i}})^{\epsilon} = g^{as_{1i}ID_{ri}}$$
$$\Rightarrow (g^{as_{1i}ID_{ri}})^{1/ID_{ri}} = g^{as_{1i}}$$
$$e(g^{as_{1i}}, g_2) = T_{1i},\ H_1(T_{1i}) = T_{2i},$$
$$H_1(e(g_1, g_2)^{s_{1i}}) \cdot m_i / T_{2i} = m_i$$

- 위조(*Forge*(ID_s^*, ID_r^*, ϕ_f)) : F는 선택한 아이디로 위조한 서명 (ID_s^*, ID_r^*, ϕ_f) B에게 준다. B는 다음과 같은 방법으로 F가 위조한 암호문 ϕ_f에서 마스터 비밀키 msk를 추출하여 인스턴스(instance) (G_1, g, g^a, g^b)에 대한 *CDH* 값 g^{ab}를 출력한다.

$$\phi_f = ((h_1 g_1^{ID_r^*})^{s_1}, H_1(e(g_1, g_2)^{s_1}) \cdot m, g^{s_1},$$
$$g^{ab}(h_2 g_1^{ID_r^*})^{r_2} (h_4 g_3^{T_3})^{s_1} (h_3 g_1^{m^*})^{s_2}, g^{r_2}, g^{s_2})$$
$$(h_1 g_1^{ID_r^*})^{s_1} / (g^{s_1})^{\epsilon} = (g^{\epsilon} g^{aID_r^*})^{s_1} / (g^{s_1})^{\epsilon} = g^{as_1 ID_r^*}$$
$$\Rightarrow (g^{as_1 ID_r^*})^{1/ID_r^*} = g^{as_1}$$
$$e(g^{as_1}, g_2) = T_1,\ H_1(T_1) = T_2,\ H_2(T_1, g^{s_2}) = T_3$$

위와 같은 방법으로 g^{as_1}를 계산할 수 있으며, 공개키 g_2과의 페어링 연산과 해쉬함수 H_2를 통하여 T_3를 구할 수 있다. B는 T_3와 자신이 설정한 공개키를 이용해서 *CDH*값 g^{ab}를 다음과 같이 얻을 수 있다.

$$g^{ab}(h_2 g_1^{ID_s^*})^{r_2} (h_4 g_3^{T_3})^{s_1} (h_3 g_1^{m^*})^{s_2}$$
$$= g^{ab}(g^{\alpha_1} g_1^{ID_s^* - ID_s^*})^{r_2} (g^{f + dT_3})^{s_1} (g^{\alpha_2} g_1^{m^* - m^*})^{s_2}$$
$$= g^{ab}(g^{r_2})^{\alpha_1} (g^{s_1})^{f + dT_3} (g^{s_2})^{\alpha_2} \rightarrow g^{ab}$$

다음의 사항을 관찰해 보자. 만일, 유효하게 검증이 되는 정당한 서명을 위조하였다면 위조한 서명의 구조는 IBSC 기법의 서명 구조와 같을 것이고, 따라서 공격자의 이점을 이용할 수 있다. 위의 시뮬레이션이 정상적으로 작동하였다면 완전한 공격 시뮬레이션을 제공한다. 즉, 제안 기법 IBSC의 실행환경과 동일하다.

5.2. ID기반 온라인/오프라인 사인크립션 기법의 안전성

정리.3 기밀성(Confidentiality) 제안한 ID기반 온라인/오프라인 사인크립션 기법 IBOOSC는 랜덤 오라클 모델을 사용하지 않고 DBDH 가정하에서 IND-sID-CCA 관점에서 안전하다.

증명. 제안 기법 IBOOSC의 IND-sID-CCA 안전성을 의미있는(non-negligible) 확률로 깰 수 있는 알고리즘 F가 존재한다고 가정하자. 그러면 F를 이용하여 *DBDH* 문제를 효율적으로 해결할 수 있는 알고리즘 B가 존재함을 보일 것이다. B는 임의로 선택된 $a, b, c \in Z_p^*$와 $g \in G_1$에 대한 *DBDH* 문제 인스턴스(instance) $(G_1, g, g^a, g^b, g^c, T)$를 입력 받는다. B의 목적은 $T = e(g,g)^{abc}$임을 판단하는 것이다.

- 초기설정(*Initialization*): F는 챌린지(Challenge) 할 아이디 ID_r^*를 선택한다.
- 셋업(*Setup*) : 공개 상수 *param*와 마스터 비밀키 *msk*는 앞의 절에서 증명한 정리.1에서의 설정과 같다.
- 질의 1단계 : 질의 1단계의 알고리즘들은 앞의 절에서 증명한 정리.1에서의 *Extract* 알고리즘, *Signcryption* 알고리즘과 같이 시뮬레이션 된다.
- 챌린지(*Challenge*(ID_s^*, m_0, m_1)) : F는 선택한 아이디와 챌린지 메시지들의 쌍 (ID_s^*, m_0, m_1)를 B에게 준다. B는 먼저 앞의 절에서 증명한 IBSC 기법에서의 설정과 같이 암호문 ϕ_{IBSC}를 생성한다. B는 임의의 난수 $t_1, t_2, t_3, t_4 \in Z_p^*$를 선택하고, 다음과 같은 방법으로 챌린지 암호문 $\phi_{ch} = Signcrypt(ID_r^*, D_{ID_s}^*, m_b)$를 생성하여 F에게 반환한다.

$$s_1 = c, g^{s_1} = g^c, H_2(T, g^{s_2}) = T_3$$

$$\phi_{IBSC} = ((h_1 g_1^{ID_r^*})^{s_1}, H_1(e(g_1, g_2)^{s_1}) \cdot m_b, g^{s_1}, g^{ab}(h_2 g_1^{ID_s^*})^{r_2}(h_4 g_3^{T_3})^{s_1}(h_3 g_1^{m})^{s_2}, g^{r_2}, g^{s_2})$$

$$\phi_{ch} = ((h_1 g_1^{ID_r^*})^{s_1} g^{-t_1 t_2}, g^{t_1}, t_2, H_1(e(g_1, g_2)^{s_1}) \cdot m_b, g^{s_1}, g^{ab}(h_2 g_1^{ID_s^*})^{r_2}(h_4 g_3^{T_3})^{s_1}(h_3 g_1^{m^*})^{s_2} g^{-t_3 t_4}, g^{t_3}, t_4, g^{r_2}, g^{s_2})$$

B가 생성한 챌린지 암호문 ϕ_{ch}과 IBOOSC 기법의 암호문 ϕ의 구조를 비교하면 $\delta_1, \delta_2, \beta_1$와 β_2는 다음과 같이 난수성이 유지되었음을 알 수 있다.

$$\delta_1 = ID_r^* - \frac{t_1 t_2}{a s_1},\ \beta_1 = \frac{t_1}{a s_1},\ \delta_2 = m - \frac{t_3 t_4}{a s_1},\ \beta_2 = \frac{t_3}{a s_1}$$

$$\phi_{ch} = ((h_1 g_1^{\delta_1})^{s_1}, g_1^{s_1 \beta_1}, \beta_1^{-1}(ID_r - \delta_1), T_2 \cdot m, g^{s_1}, g_2^{a}(h_2 g_1^{ID_s^*})^{r_2}(h_4 g_3^{T_3})^{s_1}(h_3 g_1^{\delta_2})^{s_2}, g_3^{s\beta_2}, \beta_2^{-1}(m - \delta_2), g^{r_2}, g^{s_2})$$

- 질의 2단계 : 공격자 F는 질의 1단계에서와 같은 질의를 다음의 경우를 제외하고 계속하여 요청할 수 있다. (ϕ_{ch}, ID_r^*)을 *Unsigncryption* 질의를 할 수 없고, ID_r^*을 *Extract* 질의를 할 수 없다.
- 추측(*Guess*) : 공격자 F는 자신의 추측 비트값 $b' \in \{0,1\}$를 출력한다. B는 출력된 비트값 b'과 b를 비교하여 $b' = b$이면 $T = e(g,g)^{abc}$라는 의미로 1을 출력하고, 그렇지 않다면 $T \neq e(g,g)^{abc}$라는 의미로 0을 출력한다.

다음의 사항을 관찰해 보자. 만일, T가 임의의 난수값이면 공격자에게 챌린지 암호문은 난수값으로 보이므로 공격자의 이점을 이용할 수 없다. 만일 $T = e(g,g)^{abc}$이면 위의 시뮬레이션이 정상적으로 작동하였다면 완전한 공격 시뮬레이션을 제공한다. 즉, 제안 기법 IBOOSC의 실행환경과 동일하다.

정리.4 위조 불가능(Unforgeability) 제안한 ID기반 온라인/오프라인 사인크립션 기법 IBOOSC는 랜덤 오라클 모델을 사용하지 않고 CDH 가정하에서 sUF-sID-CMA 관점에서 안전하다.

증명. 제안 기법 IBOOSC의 sUF-sID-CMA 안전성을 의미있는(non-negligible) 확률로 깰 수 있는 알고리즘 F가 존재한다고 가정하자. 그러면 F를 이용하여 *CDH* 문제를 효율적으로 해결할 수 있는 알고리즘 B가 존재함을 보일 것이다. B는 임의로 선택된 $a, b \in Z_p^*$와 $g \in G_1$에 대한 *CDH* 문제 인스턴스(instance) (G_1, g, g^a, g^b)를 입력 받는다. B의 목적은 g^{ab}를 계산하는 것이다.

- 초기설정(*Initialization*): F는 챌린지(Challenge) 할 아이디 ID_s^*, m^*를 선택한다.
- 셋업(*Setup*) : 공개 상수 *param*와 마스터 비밀키 *msk*는 앞의 절에서 증명한 정리.2에서의 설정과 같다.
- 질의 단계 : 질의의 알고리즘들은 앞의 절에서 증명한 정리.2에서의 *Extract* 알고리즘, *Signcryption* 알고리즘 그리고 *Unsigncryption* 알고리즘과 같이 시뮬레이션 된다.
- 위조(*Forge*(ID_s^*, ID_r^*, ϕ_f)) : F는 선택한 아이

〔표 2〕 연산 비용 비교 (E: 싱글지수연산, ME: 멀티지수 연산, M: 곱 연산, Mc: 모듈라 연산, P: 페어링 연산)

	JJJ〔16〕	GMC-1〔8〕+OOIBS〔17〕	제안 IBOOSC 기법
오프라인 연산	4E+1ME	6E+2ME	11E+2ME
온라인 연산	3Mc	1M+3Mc	1M+2Mc
복호화+검증 연산	2P	9P	7P
안전성 모델	Random Oracle	without Random Oracles Selective ID	without Random Oracles Selective ID
가정	$(\ell+1)$BDHI, $(\ell+1)$SDH	DBDH, CDH	DBDH, CDH

디로 위조한 서명 (ID_s^*, ID_r^*, ϕ_f) B에게 준다. B는 다음과 같은 방법으로 F가 위조한 암호문 ϕ_f에서 마스터 비밀키 msk를 추출하여 인스턴스(instance) (G_1, g, g^a, g^b)에 대한 CDH 값 g^{ab}를 출력한다.

$$\phi_f = ((h_1 g_1^{\delta_1})^{s_1}, g_1^{s_1\beta_1}, \beta_1^{-1}(ID_r - \delta_1), T_2 \cdot m, g^{s_1},$$
$$g_2^a (h_2 g_1^{ID_s^*})^{r_2} (h_4 g_3^{T_3})^{s_1} (h_3 g_1^{\delta_2})^{s_2}, g_3^{s\beta_2}, \beta_2^{-1}(m-\delta_2),$$
$$g^{r_2}, g^{s_2})$$
$$\phi_f = (\phi_1, \phi_2, \phi_3, \phi_4, \phi_5, \phi_6, \phi_7, \phi_8, \phi_9, \phi_{10}).$$
$$\phi' = (\phi_1 \phi_2^{\phi_3}, \phi_4, \phi_5, \phi_6 \phi_7^{\phi_8}, \phi_9, \phi_{10})$$
$$= (\phi_1', \phi_2', \phi_3', \phi_4', \phi_5', \phi_6')$$

위와 같은 방법으로 위조한 암호문을 제안 IBSC 기법와 같은 암호문으로 변형할 수 있다.

$$\phi' = ((h_1 g_1^{ID_s^*})^{s_1}, H_1(e(g_1, g_2)^{s_1}) \cdot m, g^{s_1},$$
$$g^{ab}(h_2 g_1^{ID_s^*})^{r_2}(h_4 g_3^{T_3})^{s_1}(h_3 g_1^{m^*})^{s_2}, g^{r_2}, g^{s_2})$$
$$(h_1 g_1^{ID_r^*})^{s_1}/(g^{s_1})^e = (g^e g^{aID_r^*})^{s_1}/(g^{s_1})^e = g^{as_1 ID_r^*}$$
$$\Rightarrow (g^{as_1 ID_r^*})^{1/ID_r^*} = g^{as_1}$$
$$e(g^{as_1}, g_2) = T_1,\ H_1(T_1) = T_2,\ H_2(T_1, g^{s_2}) = T_3$$

위와 같은 방법으로 g^{as_1}를 계산할 수 있으며, 공개키 g_2과의 페어링 연산과 해쉬함수 H_2를 통하여 T_3를 구할 수 있다. B는 T_3와 자신이 설정한 공개키를 이용해서 CDH값 g^{ab}를 다음과 같이 얻을 수 있다.

$$g^{ab}(h_2 g_1^{ID_s^*})^{r_2}(h_4 g_3^{T_3})^{s_1}(h_3 g_1^{m^*})^{s_2}$$
$$= g^{ab}(g^{\alpha_1} g_1^{ID_s^* - ID_s^*})^{r_2}(g^{f+dT_3})^{s_1}(g^{\alpha_2} g_1^{m^* - m^*})^{s_2}$$
$$= g^{ab}(g^{r_2})^{\alpha_1}(g^{s_1})^{f+dT_3}(g^{s_2})^{\alpha_2} \rightarrow g^{ab}$$

다음의 사항을 관찰해 보자. 만일, 유효하게 검증이 되는 정당한 서명을 위조하였다면 위조한 서명의 구조는 IBOOSC 기법의 서명 구조와 같을 것이고, 따라서 공격자의 이점을 이용할 수 있다. 위의 시뮬레이션이 정상적으로 작동하였다면 완전한 공격 시뮬레이션을 제공한다. 즉, 제안 기법 IBOOSC의 실행환경과 동일하다.

VI. 분 석

본 절에서는 이전에 제안된 ID기반 사인크립션 기법과 본 논문에서 제안한 기법의 연산 비용과 안전성 모델을 비교하여 본다. 암호학에서 기법을 설계할 때 증명에 랜덤 오라클 모델을 사용하지 않았거나, 가정을 일반적으로 받아들여지는 DBDH나 CDH 문제 등과 같은 것을 썼을 때 이론적 안전성에서 우수한 기법이라고 본다. 또한 다양한 응용환경에 적용되기 위해서는 연산 효율성 또한 중요하며, 안전성 모델과 가정, 기법의 효율성 모두를 갖춘 기법이 가장 이상적인 기법이라 보며, 그만큼의 설계의 어려움이 있다.

2008년에 Liu〔16〕 등이 제안한 기법은 본 논문에서 제안한 기법보다 모든 단계에서 연산비용이 좋다. 하지만 안전성 증명을 위한 모델이 랜덤 오라클을 사용하는 모델이며, 안전성 가정 역시 $(\ell+1)$BDHI이다. Liu 등이 제안한 기법은 연산의 효율성을 높이기 위해 약한 안전성 증명 모델과 강한 가정을 사용했다고 볼 수 있다. 위 〔표 2〕의 GMC1〔8〕+OOIBS〔17〕 기법은 ID기반 온라인/오프라인 암호기법과 서명기법을 단순히 합쳐 놓은 기법이다. 특히 암호기법은 Boneh 등이 제안한 ID기반 암호 기법을 바탕으로 설계한 온라인/오프라인 기법으로서 본 논문에서 제안한 기법과 구조가 같기 때문에 본 논문에서 제안한 기법이 사인크립션으로서 효율적인 측면을 가지는지를 비교해서 알아볼 수 있다. 설계 구조가 같기 때문에 안전성 모델과 가정은 같으며 연산비용을 비교해 보았을 때, 오프라인 연산비용만이 본 논문에서 제안한 기법이 더 높다. 하지만 온라인/오프라인 기법의 특성상 미리 계산되어지는 오프라인 단계에서의 연산보다 온라인 단

계와 복호화와 검증에서의 연산이 효율적인 것이 더 의미가 있다고 본다. 결과적으로 본 논문에서 제안한 사인크립션 기법은 암호기법과 서명기법 각각을 구성하였을 때보다 효율성을 더 가지며, 기존에 Liu 등에 의해 제안된 증명시 강한 가정이 들어가는 기법보다는 효율성이 떨어지지만 랜덤오라클을 사용하지 않은 안전성 모델과 약한 가정으로 안전성 증명이 된다.

VII. 결 론

본 논문에서는 Boneh 등이 제안한 ID기반 암호기법의 구조를 이용하여 두 가지 기법을 제안하였다. 첫 번째 기법은 ID기반 사인크립션 기법으로 안전하고 신뢰할 수 있는 커뮤니케이션 환경에서 요구되는 기밀성, 무결성, 부인방지 등을 제공한다. 두 번째 기법은 첫 번째 기법에 F. Guo 등이 제안한 ID기반 온라인/오프라인 암호 기법의 구조를 적용하여 설계한 ID기반 온라인/오프라인 사인크립션 기법으로 스마트카드 같은 저전력 디바이스 등에서 유용하게 이용될 수 있다. 특히, 두 번째 기법은 최초의 안전성 증명에 랜덤오라클 모델을 사용하지 않은 ID기반 온라인/오프라인 사인크립션 기법이다. 하지만 안전성 모델이 풀 모델이 아닌 선택적인 ID 모델을 사용하였다. 향후에는 표준 모델(standard model)안에서의 풀 모델로 증명이 되는 기법의 설계가 필요하다. 또한 전방향 안전성(forward secrecy)을 제공하는 ID기반 온라인/오프라인 사인크립션 기법의 구성은 흥미로운 연구과제가 될 것이다.

참 고 문 헌

[1] D. Boneh and X. Boyeh, "Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles," In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223-238, 2004.

[2] D. Boneh, and M. Franklin, "Identity-Based Encryption from the Weil pairing," In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213-229, 2001.

[3] X. Boyen, "Multipurpose Identity-Based Signcryption A Swiss Army Knife for Identity-Based Cryptography" In: Boneh, D. (ed.) CRYPTO 2003, pp. 383-399, Aug. 2003.

[4] R. Canetti, S. Halevi and J. Katz, "Chosen-ciphertext security from udentity-based encryption," In: Proceedings of Eurocrypt 2004, LNSC, pp. 207-222, 2004.

[5] S. S. M. Chow, T. H. Yuen, L. C. K. Hui and S. M. Yiu, "Signcryption in Hierarchical Identity Based Cryptosystem," In: Security and Privacy in the Age of Ubiquitous Computing, Springer Boston, vol.181, pp. 443-457, 2005.

[6] S. Even, O. Goldreich, S. Micali, "Online/Offline Digital signature," In: Brassard, G. (eds.) CRYPTO 1989. LNCS, vol.435, pp. 263-275, 1990.

[7] C. Gentry, "Practical Identity-Based Encryption Without Random Oracles," In: Vaudenay, S. (eds.) EUROCRYPT 2006. LNCS 4004, pp. 445-464, 2006.

[8] F. Guo, Y. Mu and Z. Chen, "Identity-based online/offline encryption," In: Tsudik, G. (eds.) FC 2008. LNCS, vol.5143, pp. 247-261, 2008.

[9] J. Li, X. Chen, F. Zhang and Y. Wang, "Generalization of the Selective-ID Security Model for HIBS Protocols," In: Y. Wang, Y. Chung, and H.Liu (ed.) CIS 2003, LNAI, vol.4456, pp. 894-902, 2007.

[10] J.K. Liu and J. Zhou, "An Efficient Identity-Based Online/Offline Encryption Scheme" In: Abdalla, M. (eds.) ACNS 2009. LNCS 5536, pp. 156-167, 2009.

[11] J. Malone-Lee, "Identity-based Signcryption" In: Cryptology ePrint Archive, Report 2002-098, Jul 2002.

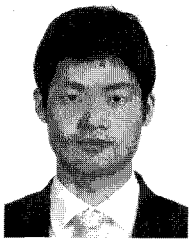
[12] S.F. Shahandashti and R. Safavi-Naini, "Theshold Attribute-Based Signatures and Their Application to Anonymous Credential systems," In: Preneel, B. (ed.) AFRICACRYPT 2009. LNCS 5580, pp. 198-216, 2009.

[13] A. Shamir, "Identity-based cryptosys-

tems and signature schemes," In: Advances in Cryptology -Crypto 1984,, LNSC 196, pp. 47-53, 1984.
[14] B. Waters, "Efficient Identity-Based Encryption without Random Oracles," In: Cramer, R.J.F. (eds.) EUROCRYPT 2005. LNCS 3494, pp. 114-127, 2005.
[15] Y. Yu, B. Yang, Y. Sun and S. Zhu, "Identity-Based Signcryption Scheme Without Random Oracles," In: CSI 2009. vol.31, pp. 56-62, 2009.
[16] J. K. Liu, J. Baek, J. Zhou, "Online/Offline Identity-Baed Signcryption Re-visited," In: Cryptology ePrint Archive, Report 2010-274, May 2010.
[17] S. Xu, Y. Mu and W. Susilo, "Online/Offline Signatures and Multisignatures for AVOD and DSR routing security," In: ACISP 06, LNCS 4058, pp. 99-110, 2006

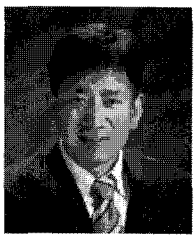
〈著者紹介〉

박 승 환 (Seunghwan Park) 학생회원
2009년 2월: 숭실대학교 수학과 학사 졸업
2009년 3월~현재: 고려대학교 정보경영공학과 석사과정
〈관심분야〉 정보보호이론, 암호 프로토콜, 프라이버시향상기술(PET)



김 기 탁 (Kitak Kim) 학생회원
2006년 8월: 고려대학교 수학과 졸업
2008년 8월: 고려대학교 정보경영공학과 공학 석사 졸업
2008년 9월~현재: 고려대학교 정보경영공학과 박사과정
〈관심분야〉 정보보호이론, 암호 프로토콜, 프라이버시향상기술(PET)

구 우 권 (Woo Kwon Koo) 학생회원
2006년 2월: 고려대학교 수학과 학사 졸업
2008년 2월: 고려대학교 정보경영공학과 공학 석사 졸업
2008년 3월~현재: 고려대학교 정보경영공학과 박사과정
〈관심분야〉 정보보호이론, 암호 프로토콜, 프라이버시향상기술(PET)



이 동 훈 (Dong Hoon Lee) 정회원
1983년: 고려대학교 경제학과 학사 졸업
1987년:Oklahoma University 전산학 석사 졸업
1992년:Oklahoma University 전산학 박사 졸업
1993년~1997년:고려대학교 전산학과 조교수
1997년~2001년:고려대학교 전산학과 부교수
2001년~현재: 고려대학교 정보경영공학전문대학원 교수
〈관심분야〉 정보보호이론, 암호 프로토콜, USN, 키 교환, 프라이버시향상기술(PET), 익명성 연구