情 報 保 護 學 會 誌
第19卷 第 6號, 2009. 12

아이디 기반 암호화 그 응용

서 재 홍*, 천 정 희*

요 약

아이디 기반 암호의 개념과 발전과정들을 소개한다. 또한, 다양한 응용들에 대해서 살펴보고 아직까지 해결되지 않은 몇 가지 문제들에 대해 소개한다.

Ⅰ. 서 론

아이디 기반 암호 시스템(ID-Based Encryption, IBE)은 1984년 Shamir가 처음 제안한 암호시스템으로 기존의 공개키 시스템에서 취약점 중 하나인 효율적인 공개키 관리에 대한 해법으로 제시되었다[33]. 즉, IBE는 임의의 비트열을 공개키로 사용하는 기존의 공개키 암호 방식과 달리 아이디를 공개키로 사용을 함으로써 공개키를 저장하기 위한 추가적인 메모리를 필요로 하지 않는 장점을 가진다. Shamir가 처음 IBE의 개념을 제안할 당시에는 구체적인 스킴을 제시하지는 않았다. 이후 2001년 Boneh와 Franklin이 페어링을 이용하여 효과적으로 구현할 수 있는 첫 번째 IBE (BF-IBE)를 제안하였다[7]. 이후 IBE는 이론적 측면과 효율성 측면에서 모두 비약적인 발전을 거듭해왔다. 특히, IBE에서 활용된 많은 기법들은 계층구조를 가지는 아이디 기반 암호(Hierarchical ID-Based Encryption, HIBE)[30], 검색 가능한 공개키 암호 시스템(Publickey Encryption with Keword Encrypton, PEKS)[6], 아이디 기반 서명(ID-Based Signature, IBS)[19] 등 다양한 응용들에도 적용이 될 만큼 아이디 기반 암호 시스템의 발전은 다른 암호 시스템에 미치는 파급이 크다고 할 수 있다.

현재까지 알려진 IBE는 크게 두 가지로 분류할 수 있다. 첫 번째. 페어링을 활용한 IBE로 BF-IBE를 시작으로 다양한 특성을 가지는 IBE 시스템이 제시가 되어왔다. 다음으로는 페어링을 활용하지 않는 IBE로 Cocks가 2002년에 제안하였고(Co-IBE)[16], 이후 2007년에 Boneh, Gentry, Hamburg 가 Co-IBE를 개선하여 암호문의 크기가 작은 IBE 시스템을 제안하였다[9]. 2008년에는 Gentry, Peikert, Vaikuntanathan이 Lattice기반의 가정 하에서 새로운 IBE를 제안하였다[28]. 페어링을 활용하지 않은 IBE는 페어링을 활용한 IBE보다 효율성 측면에서 부족한 점이 있으며 아직까지는 연구가 많이 이루어지지 않았다. 이 논문에서는 페어링을 활용한 IBE 시스템에 대해서만 상세히 다루도록 한다.

이 논문의 구성은 다음과 같다. 2절에서 IBE와 안전한 IBE에 관한 구체적인 정의, 그리고 여러 안전한 IBE의 증명을 위해 사용되는 정의 등 이 논문에서 사용하게 될 정의들을 제시한다. 3절에서는 구체적인 IBE 시스템들을 제시하고 발전해온 과정들을 비교를 통해서 설명한다. 4절에서는 다양한 IBE의 응용들을 설명한다. 마지막 5절에서는 IBE 분야에서의 미해결 문제들을 살펴봄으로써 이 논문을 마무리 한다.

Ⅱ. 정 의

이 절에서는 이 논문에서 사용할 몇 가지의 정의들을 설명한다.

1. ID-Based Encryption

IBE는 네 가지의 알고리즘으로 구성된다. 각각은 Setup, KeyGen, Enc. Dec. 알고리즘이며 정확한 정의는 아래와 같다.

본 연구는 기초기술연구회의 NAP 과제 지원으로 수행되었음.
* 서울대학교, 정보보호 및 암호연구 센터(jhsbhs@gmail.com, jhcheon@snu.ac.kr)

Setup(λ): 안전성 파라미터인 λ를 입력으로 받아서 공개정보인 시스템 파라미터 parmas와 키 생성 센터(PKG)의 비밀정보인 MK를 출력한다.

KeyGen(MK, parmas, ID): PKG의 비밀키 MK, parmas와 사용자 아이디 ID를 입력받아 ID에 해당하는 비밀키 PvkID를 출력한다.

Enc(parmas, ID, M): parmas와 사용자 아이디 ID, 메시지 M을 입력 받아서 암호문 CT를 출력한다.

Dec(PvkID, CT): 사용자의 비밀키 PvkID와 암호문 CT를 입력 받아서 평문 M 또는 실패 메시지 ⊥를 출력한다.

올바른 IBE가 되기 위해서는 다음의 조건을 만족해야한다. 모든 ID와 KeyGen 알고리즘으로 생성된 대응되는 사용자의 개인키 PvkID와 모든 메시지 M에 대해서 아래의 등식이 항상 성립해야 한다.

Dec(PvkID, Enc(parmas, ID, M)) = M

2. IBE의 안전성 모델

IBE 스킴 E의 안전성은 E를 공격하는 공격자와 E의 시스템 파라미터를 생성하는 챌린져 사이의 게임으로 정의한다.

2.1. 선택 암호문 공격에 대한 안전성 (Chosen Ciphertext Security)

보통의 공개키 시스템의 안전성 개념에서와 마찬가지로 공격자가 선택한 암호문에 대한 평문을 얻을 수 있는 상황을 고려한다. 일반적인 공개키의 안전성과의 차이점은 IBE 공격자는 공격 목표가 되는 아이디를 제외한 공격자가 선택한 아이디에 대한 비밀키는 얻을 수 있다고 가정한다. 또한, 공격 목표가 되는 아이디를 결정하는 시기는 다른 아이디들에 대한 비밀키를 얻는 시점과 무관하다.(full security) 이러한 게임을 IND-ID-CCA 게임이라고 하고 아래에 정확한 설명을 서술한다.

- Setup: 챌린져는 Setup 알고리즘을 이용하여 공격자에게 시스템 파라미터 params를 보내주고 MK는 안전하게 저장한다.
- Query1: 공격자는 반복적으로 챌린져에게 질의한다. 이때, 모든 질의를 동시에 보낼 필요는 없으며 앞선 질의에 대한 대답을 본 후에 다음 질의를 수행할 수 있다. 질의는 기본적으로 아래의 두 가지를 할 수 있다.
- KeyExt(ID): ID를 챌린져에게 보내어 대응되는 개인키를 질의한다. 챌린져는 공격자의 질의가 올 때마다 KeyGen 알고리즘을 이용하여 ID에 대응되는 개인키 PvkID를 생성하여 공격자에게 보낸다.
- Dec(ID, CT): 공격자는 반복적으로 ID와 암호문 CT를 챌린져에게 보내서 대응되는 메시지를 질의한다. 챌린져는 질의가 올 때 마다 KeyGen 알고리즘을 이용하여 PvkID를 생성하고 Dec 알고리즘을 이용하여 암호문을 복호화하여 공격자에게 보낸다.
- Challenge: Query1 이 끝난 뒤, 공격자는 같은 길이의 메시지 M0, M1과 아이디 ID*를 챌린져에게 보낸다. 단, 이전의 KeyExt 질의에서 ID*에 대응하는 비밀키를 질의한 적이 없어야한다. 챌린져는 임의의 1 비티 b를 생성하고 Enc 알고리즘을 이용하여 CT* = Enc(PK, ID*, Mb)를 공격자에게 보낸다.
- Query2: Query1과 같은 과정을 수행한다. 단, KeyExt 질의의 경우 ID*에 대한 질의는 제한된다. 또한, Dec 질의의 경우 CT*를 질의하는 것도 제한된다.
- Guess: 공격자는 b를 추측한 값인 b'을 챌린져에게 보낸다. 이때, 만약 b=b' 이라면 공격자가 게임에서 이긴다.

위에서 정의한 E를 공격하는 게임에서의 공격자 A의 advantage는 다음과 같이 정의한다.

$$Adv_{E,A}^{IND-ID-CCA} = |\Pr[b = b'] - \frac{1}{2}]|$$

정의 1. 만약 최대 t만큼의 수행시간을 가지며, qID번 이하의 KeyExt 질의, qC번 이하의 Dec 질의를 하는 임의의 공격자 A가 IBE 스킴 E에 대한 IND-ID-CCA 게임에서 ϵ이하의 advantage를 가질 때 (즉, $Adv_{E,A}^{IND-ID-CCA} \leq \epsilon$) IBE 스킴E 가 '(t, qID, qC, ϵ)-IND-ID-CCA 안전하다'고 정의한다.

2.2. 선택 평문 공격에 대한 안전성 (Chosen Plaintext Security)

선택 암호문 공격 보다 약한 개념의 안전성으로써 공격자가 IND-ID-CCA 게임에서 Dec 질의를 할 수 없도록 제한한 것과 동일하고, 이때의 게임을 IND-ID-CPA 게임이라고 한다. IND-ID-CPA게임에서의 공격자의 advantage는 IND-ID-CCA 게임과 동일하게 정의할 수 있으며 $Adv_{E,A}^{IND-ID-CPA}$로 나타낸다.

정의 2. 만약 최대 t만큼의 수행시간을 가지며, qID번 이하의 KeyExt 질의를 하는 임의의 공격자 A가 IBE 스킴 E에 대한 IND-ID-CCA 게임에서 ϵ이하의 advantage를 가질 때 (즉, $Adv_{E,A}^{IND-ID-CPA} \leq \epsilon$) IBE 스킴 E가 '(t, qID, ϵ)-IND-ID-CPA 안전하다'고 정의한다.

2.3. Selective Security 개념

앞서 설명한 안전성 모델에서 보다 공격자의 능력이 조금 더 약화된 모델로써 selective security가 있다. Selective security는 Canetti, Halevi, Katz가 처음 제안한 개념 [20]으로 앞선 안전성 모델은 selective security와 구별하기 위해 full security라고 부르겠다. Selective security에서는 공격자가 공격할 대상이 되는 아이디를 시스템 파라미터가 생성되기 이전에 미리 선택하고 챌린져에게 알리도록 제한한다. 나머지 다른 부분이 IND-ID-CCA 게임과 동일하면 IND-sID-CCA 게임, IND-ID-CPA와 동일하면 IND-sID-CPA 게임이라고 정의한다. 이때, 공격자의 advantage도 이전의 게임들과 비슷하게 정의가 가능하며 표기도 각각 $Adv_{E,A}^{IND-sID-CCA}$, $Adv_{E,A}^{IND-sID-CPA}$로 나타낸다.

정의 3. 만약 최대 t만큼의 수행시간을 가지며, qID번 이하의 KeyExt 질의, qC번 이하의 Dec 질의를 하는 임의의 공격자 A가 IBE 스킴 E에 대한 IND-sID-CCA 게임에서 ϵ 하의 advantage를 가질 때 (즉, $Adv_{E,A}^{IND-sID-CCA} \leq \epsilon$) IBE 스킴 E가 '(t, qID, qC, ϵ)-IND-sID-CCA 안전하다'고 정의한다.

정의 4. 만약 최대 t만큼의 수행시간을 가지며, qID번 이하의 KeyExt 질의를 하는 임의의 공격자 A IBE 스킴 E에 대한 IND-sID-CCA 게임에서 ϵ이하의 advantage를 가질 때 (즉, $Adv_{E,A}^{IND-sID-CPA} \leq \epsilon$) IBE 스킴 E가 '(t, qID, ϵ)-IND-sID-CPA 안전하다'고 정의한다.

3. 페어링과 암호학적 가정

3.1. bilinear 군

Bilinear map이 존재하는 군으로서 군 생성 알고리즘 g에 의해 생성이 된다. g는 안전성 파라미터 λ를 입력으로 받아서 (q, G, G_T, e)를 출력한다. q는 소수이고 G와 G_T는 위수를 q로 가지는 순환군이다. $e : G \times G \rightarrow G_T$는 non-degenerate 성질을 가지는 효율적인 계산이 가능한 bilinear map이다. 즉, e는 다음의 성질을 만족한다.

- bilinear: G의 임의의 두 원소 g_1, h_1와 임의의 정수 a, b에 대해 $e(g_1^a, h_1^b) = e(g_1, h_1)^{ab}$를 만족한다.
- non-degerate: G의 임의의 생성원 g_1에 대해 $e(g_1,g_1)$은 G_T의 생성원이 된다.
- 효율적인 계산: G의 임의의 두 원소 g_1, h_1에 대해 $e(g_1,h_1)$를 효율적으로 계산할 수 있는 알고리즘이 존재한다. 즉, λ에 대한 다항식 시간 안에 계산이 가능하다.

3.2 암호학적 가정

이 절에서는 IBE 스킴들의 안전성 증명에 사용되는 암호학적 가정들에 대해 정의한다.

3.2.1. Bilinear Diffie-Hellman (BDH)

BDH 문제: 군 생성 알고리즘 g가 주어져 있을 때 분포 $P(\lambda)$는 다음과 같이 정의한다.

$$(q, G, G_T, e) \leftarrow g(\lambda),\ g \leftarrow G,\ a, b, c \leftarrow \mathbb{Z}_q,$$
$$Z \leftarrow (g, g^a, g^b, g^c)$$

Z는 추가적으로 군에 대한 정보 (q, G, G_T, e) 를 포

함하며, 이때, Z를 BDH 문제의 challenge라고 한다. BDH 문제는 주어진 challenge로부터 $e(g,g)^{abc}$를 계산하는 것이다. BDH 문제에서를 공격하는 공격자 A의 advantage는 $\Pr[A(Z) \rightarrow e(g,g)^{abc}]$로 정의한다. 이때의 확률 공간은 분포 $P(\lambda)$에서 사용한 랜덤과 A가 사용하는 랜덤의 도메인이 된다.

정의 5. (BDH 가정) 만약 군 생성 알고리즘 g에 의해 생성된 군에서의 BDH 문제를 어떠한 알고리즘도 t 보다 작은 수행시간 내에 ϵ 보다 큰 advantage로 풀 수가 없다면, 군 생성 알고리즘 g가 '(t,ϵ)-BDH 가정을 만족한다'고 정의한다.

3.2.2. Decisional Bilinear Diffie-Hellman (DBDH)

BDH 문제: 군 생성 알고리즘 g가 주어져 있을 때 분포 $P(\lambda)$는 다음과 같이 정의한다.

$$(q, G, G_T, e) \leftarrow g(\lambda),\ g \leftarrow G,\ a,b,c \leftarrow \mathbb{Z}_q,$$
$$Z \leftarrow (g, g^a, g^b, g^c),\ Y \leftarrow e(g,g)^{abc},$$
$$R \leftarrow G_T,\ d \leftarrow 0,1,$$
$$T \leftarrow Yd + R(1-d).$$

Z는 추가적으로 군에 대한 정보 (q, G, G_T, e) 를 포함하며, 이때, (Z, T)를 BDH 문제의 challenge라고 한다. BDH 문제는 주어진 challenge로부터 d를 추측하는 것이다. BDH 문제에서를 공격하는 공격자 A의 advantage는 $\Pr[A(Z,T) \rightarrow 1|d=0]$와 $\Pr[A(Z,T) \rightarrow 1|d=1]$의 차이로 정의한다. 이때의 확률 공간은 분포 $P(\lambda)$에서 사용한 랜덤과 A가 사용하는 랜덤의 도메인이 된다.

정의 6. (DBDH 가정) 만약 군 생성 알고리즘 g에 의해 생성된 군에서의 DBDH 문제를 어떠한 알고리즘도 t 보다 작은 수행시간 내에 ϵ 보다 큰 advantage로 풀 수가 없다면, 군 생성 알고리즘 g가 '(t,ϵ)-DBDH 가정을 만족한다'고 정의한다.

Ⅲ. 아이디 기반 암호 시스템 (IBE)

이절에서는 현재까지 제안된 IBE 들에 대해 살펴볼 것이다. 앞선 절에서 설명하였듯이 IBE 스킴에서 달성하고자 하는 가장 견고한 안전성은 IND-ID-CCA이다. 하지만 많은 경우 IND-ID-CPA (혹은 IND-sID-CPA) 안전성을 만족하는 IBE가 있을 때 IND-ID-CCA (혹은 IND-sID-CCA) 안전성을 만족할 수 있도록 하는 일반화된 변형 기법들이 제안이 되어 있다[21,10,11]. 그러므로 이 논문에서는 IND-ID-CPA 또는 IND-sID-CPA 안전성에만 초점을 맞추어 각각의 스킴들을 살펴볼 것이다. 안전성은 구체적인 증명보다는 증명의 아이디어를 설명하는 데 초점을 맞추어 설명한다. 또한, 편의상 모든 IBE에서 사용하는 순환군은 곱셈 군으로 표기한다.

1. Boneh-Franklin IBE (BF-IBE)

BF-IBE는 구체적인 스킴으로 제안된 첫 번째 IBE 다. 구체적인 스킴은 다음과 같다.

- Setup(λ): $s \leftarrow \mathbb{Z}_q,\ g \leftarrow G,$
  $params \leftarrow \{g, g^s, H_1, H_2\},\ MK \leftarrow \{s\}$
  이때, $H_1 : \{0,1\}^* \rightarrow G,$
  $H_2 : G_T \rightarrow \{0,1\}^n$는 해쉬함수
- KeyGen(MK,parmas,ID): $Pvk^{ID} \leftarrow \{H_1(ID)^s\}$
- Enc(parmas, ID, M):
  $CT \leftarrow \{g^r, H_2(\ e(H_1(ID), g^s)^r\ ) \cdot M\}$
- Dec(PvkID, CT): $CT = (C_0, C_1)$일 때,
  $M \leftarrow C_1\ /\ H_2(\ e(Pvk^{ID}, C_0)\ )$

1.1. BF-IBE의 안전성

BF-IBE의 안전성은 랜덤 오라클 모델에서 BDH 가정을 기반으로 한다. (시스템 파라미터 중 H_1, H_2는 랜덤 오라클로 생각한다.) 공격자의 공격 목표가 ID^*라면 $H_1(ID^*) = g^t$라고 하자. 공격자는 ID^*에게 보내는 암호문의 첫 번째 원소로부터 g^r, 시스템 파라미터에서 g^s 그리고 아이디로부터 g^t를 얻을 수 있고, 이때 $e(g,g)^{tsr}z$를 계산할 수 있어야만 메시지에 대한 1비트 정보를 얻을 수 있다. H_2가 랜덤 오라클이기 때문에 $e(g,g)^{tsr}$를 계산하지 않고서는 메시지에 대한 1비트 정보도 얻을 수가 없다. 여기까지만 고려하면 BF-IBE의 안전성은 정확하게 BDH 문제의 안전성과 $O(1/q_{H_2})$만큼 차이가 난다고 할 수 있을 것이다. (q_{H_2}는 공격자가

H_2를 질의한 횟수.) 즉, BF-IBE를 t 간 안에 ϵ의 확률로 공격할 수 있는 공격자는 주어진 BDH의 문제의 답을 최소 1번은 H_2 오라클에 1번은 질의를 했어야 하므로 BF-IBE 공격자를 이용하여 $O(t)$ 시간 내에 $O(\epsilon/q_{H_2})$의 확률로 BDH 문제를 풀 수 있는 시뮬레이터(BDH 공격자) 를 만들 수 있다. 하지만 추가적으로 더 고려하여야 할 것이 BF-IBE 공격자는 공격 목표 아이디를 제외한 다른 선택 아이디에 대한 개인키를 추가적으로 더 가질 수가 있다. 그러므로 시뮬레이터는 공격자의 선택 아이디에 대한 개인키 질의에 대답을 할 수 있어야만 한다. 이를 해결하기 위해 Full Domain Hash와 같은 서명의 증명에 사용되던 'partitioning' 기법들을 사용하여 증명을 할 수 있다[17]. 다시 말하면, 아이디를 선택하는 공간 I를 다른 모든 랜덤과 독립적으로 교집합이 없는 두 가지 공간 $I=I_0 \sqcup I_1$으로 나눈다. 그 중 한 가지 공간 I_o은 시뮬레이터가 대응되는 비밀키를 만들 수 있는 공간이고, 다른 한 가지 공간 I_1은 시뮬레이터가 BDH 문제를 포함시킬 수 있는 공간으로 설정을 한다. BF-IBE 공격자는 q_{ID}번 KeyExt 질의 $(ID_1, ..., ID_{q_{ID}})$를 하고 공격 목표를 ID^*로 선택한다고 했을 때, $ID_1, ..., ID_{q_{ID}}$가 모두 I_o에 속하고 ID^*가 I_1에 속했을 때만 시뮬레이터는 BDH문제를 풀 수 있게 된다. I_1의 크기를 I의 $1/(q_{ID}+1)$배로 했을 때 $ID_1, ..., ID_{q_{ID}}$가 모두 I_o에 속하고 ID^*가 I_1에 포함될 확률이 $1/e(1+q_{ID})$로 최대가 된다. (이때의 e는 자연 상수) 최종적으로 위의 $O(\epsilon/q_{H_2})$와 합쳐서 $O(\epsilon/eq_{H_2}(q_{ID}+1))$의 확률로 BDH를 푸는 시뮬레이터를 만들 수 있다.

정리 1. (BF-IBE의 안전성[7]) 군 생성 알고리즘 g가 (t, ϵ)-BDH 가정을 만족할 때, g로 생성된 군에서 만들어진 BF-IBE는 $(O(t), q_{ID}, O(\epsilon e(1+q_{ID})q_{H_2})$-IND-ID-CPA 안전하다.

2. Boneh-Boyen IBE1 (BB-IBE1)

2003년 Canetti, Halevi, Katz가 selectively security 개념을 처음 소개하였다. 자세한 정의는 2절에서 설명하였다. Boneh, Boyen은 Canetti 등이 소개한 selective security 개념을 사용하여 BF-IBE의 랜덤 오라클을 제거하였다[3]. 즉, BB-IBE1은 standard 모델에서 DBDH 가정 하에 IND-sID-CPA 안전한 스킴이다. 스킴의 상세는 아래와 같으며 정확한 안전성은 정리2에 나와 있다.

- Setup(λ): $g, g_1, h, w \leftarrow G$,
  $params \leftarrow \{g, h, E=e(g,w)\}$, $MK \leftarrow \{w\}$
- KeyGen(MK, parmas, ID): $r \leftarrow \mathbb{Z}_q$,
  $$Pvk^{ID} \leftarrow \left\{w(g_1^{ID}h)^r, g^r\right\}$$
- Enc(parmas, ID, M): $s \leftarrow \mathbb{Z}_q$,
  $$CT \leftarrow \left\{M \cdot E^s, g^s, (g_1^{ID}h)^s\right\}$$
- Dec(PvkID, CT): $CT=(C, C_0, C_1)$,
  $Pvk^{ID}=(D_0, D_1)$ 일 때,
  $$M \leftarrow C \cdot e(C_1, D_1) / e(C_0, D_0)$$

2.1. BB-IBE1의 안전성

Selective security 에서는 full security와 비교하였을 때 증명이 훨씬 용이하다. 공격자는 시스템 파라미터가 결정도 되기 전에 공격 목표가 되는 아이디를 미리 정해야 하므로 시뮬레이터는 partitioning을 정확하게 할 수 있다. 다시 말하면, BF-IBE를 생각해보면 시뮬레이터가 아이디의 전체 공간을 두 부분 집합으로 나누어 놓고 공격자가 KeyExt 질의 하는 아이디들과 공격 목표로 정한 아이가 각각의 부분 집합에 포함되는 경우 시뮬레이션이 성공하도록 하였다. 하지만 selective security 모델에서는 공격 목표가 되는 아이디를 시스템 파라미터 설정 전에 미리 알기 때문에 아이디 전체 공간을 공격 목표 아이디와 그 이외의 모든 아이디들의 집합으로 둘로 나누어 놓으면 된다. 그렇게 하면 항상 시뮬레이션에서 성공할 수가 있다. 즉, 기반이 되는 DBDH 문제에 tight한 증명을 하는 것이 가능하다.

위의 스킴을 살펴보면 공격자는 시스템 파라미터의 E와 공격 목표 아이디에 대응하는 암호문의 두 번째 원소 g^s를 알 때 E^s와 랜덤한 원소를 구별할 수 있어야 한다. 이는 DBDH 문제를 푸는 것만큼의 어려움이라고 할 수 있다. 공격자는 추가적으로 자신이 선택한 아이디에 대한 개인키를 얻을 수 있지만 시뮬레이터의 정확한 partitioning에 의해서 공격자가 다른 키들로부터 아무런 정보를 얻지 못하게 할 수 있으므로 결국 DBDH에 tight한 증명을 할 수 있다.

정리 2. (BB-IBE1의 안전성[3]) 군 생성 알고리즘 g가 (t,ϵ)-DBDH 가정을 만족할 때, g로 생성된 군에서 만들어진 BB-IBE1은 임의의 q_{ID}에 대해 $(O(t),q_{ID},\epsilon)$-IND-sID-CPA 안전하다.

IND-sID-CPA 안전한 스킴은 또한 IND-ID-CPA 안전한 스킴이 되기도 한다. 하지만, 안전성의 정도가 차이가 나게 되는데, 정확히 서술하면 아래와 같다.

정리 3. ([3]) (t,q_{ID},ϵ)-IND-sID-CPA 안전한 IBE E가 N개의 서로 다른 아이디를 허용한다면, E는 $(t,q_{ID},N\epsilon)$-IND-ID-CPA 안전하다.

3. Waters IBE1 (Wa-IBE1)

Wa-IBE1은 BB-IBE1의 변형으로 아이디를 비트단위로 변동성을 부여함으로써 standard 모델에서 BDH 가정 하에 fully 안전한 IBE를 만들었다[37]. 스킴의 상세는 다음과 같다.

- Setup(λ): $g,w,u',u_1,...,u_n \leftarrow G$,
  $params \leftarrow \{g,u',(u_i),E=e(g,w)\}$,
  $MK \leftarrow \{w\}$
- KeyGen(MK, parmas, ID): n비트 ID를 비트별로 표현하면 $I_1,...,I_n$,
  $r \leftarrow \mathbb{Z}_q \quad Pvk^{ID} \leftarrow \left\{w(u' \prod_{i=1}^{n} u_i^{I_i})^r, g^r\right\}$
- Enc(parmas, ID, M): $s \leftarrow \mathbb{Z}_q$,
  $CT \leftarrow \left\{M \cdot E^s, g^s, (u' \prod_{i=1}^{n} u_i^{I_i})^s\right\}$
- Dec(PvkID, CT): $CT=(C,C_0,C_1)$,
  $Pvk^{ID}=(D_0,D_1)$ 일때,
  $M \leftarrow C \cdot e(C_1,D_1)/e(C_0,D_0)$

3.1. Wa-IBE1의 안전성

Wa-IBE1는 처음 Waters가 제안할 당시 증명과정에서 인위적인 중지를 사용하였다. 뒤에 2009년 EUROCRYPT에서 Bellare와 Ristenpart가 Wa-IBE1를 다시 증명하였는데, 증명과정에서 인위적인 중지를 없앴으며 많은 경우에 Waters의 증명보다 좋은 안전성을 제공하는 새로운 증명을 제시하였다[12]. 이 논문에서는 Bellare와 Ristenpart의 결과를 기반으로 설명한다. Wa-IBE1의 증명은 기본적으로 BF-IBE와 비슷하게 partitioning 기법을 사용한다. BF-IBE에서와 같이 해쉬함수의 출력값이 랜덤하다고 가정하는 랜덤 오라클 모델에서의 증명에서는 아이디 전체 공간 I를 다른 모든 랜덤과 독립적으로 교집합이 없는 두 가지 공간 $I=I_0 \sqcup I_1$으로 나누고 각각의 공간에 비밀키 생성 능력과 BDH 문제를 포함 시키는 것이 가능하였지만, 반면에 Wa-IBE는 랜덤 오라클 모델이 아니므로 그러한 partitioning은 어렵다. 즉, BF-IBE에서는 $H_1(ID)$를 공개키로 사용하고 H_1이 랜덤 오라클이므로 아이디마다 랜덤하게 partitioning하는 것이 가능하였지만, Wa-IBE1에서는 그러한 작업이 불가능하다. 하지만 최대한 비슷한 효과를 내기 위해 Wa-IBE1에서는 다음과 같이 $I=I_0 \sqcup I_1$를 partitioning 한다.

$ID=I[1],...,I[n]$일 때,
$\text{if } x[0]+\Sigma_{i=1}^{n} x[i]I[i] \neq 0, \ ID \in I_0,$
$otherwise, \qquad ID \in I_1$

이때, $x[1],...x[n] \in [0,m-1]$이고
$x[0] \in [-n(m-1),0]$이다. 랜덤 오라클 모델과의 차이점을 다시 한 번 살펴본다면, 랜덤 오라클 모델에서는 I를 다른 모든 랜덤과 독립적으로 두 개의 교집합 없는 집합 I_0와 I_1으로 나누었다. 그래서 각 집합 안에 속하는 원소끼리는 어떠한 연관성도 존재하지 않는다. 반면에, 위의 Wa-IBE1에서처럼 I_0와 I_1으로 나눈다면 연관성이 존재하게 된다. 예를 들어 J_1과 J_2가 모두 I_1의 원소이면서 비트 단위로 보았을 때 1이 겹쳐 나타나는 부분이 없다면, J_1+J_2도 I_1의 원소가 됨을 쉽게 보일 수 있다. 따라서 시뮬레이션의 성공확률에 공격자가 KeyExt 질의하는 아이디와 연관이 있을 수 있다. 이러한 연관성을 줄이기 위해 $x[i]$들의 크기를 키워야하며 따라서 I_0와 I_1의 크기의 불균형이 커지게 되었다. (BF-IBE의 경우 최적화된 크기로 $I_0 : I_1$의 비가 $q_{ID} : 1$인 것에 비해 Wa-IBE1의 경우 $9nq_{ID}\epsilon^{-1} : 1$이다. ϵ은 Wa-IBE1 공격자의 advantage.) 이러한 partitioning에서의 손해를 포함하여 정리하면 Wa-IBE1의 안전성은 정리4와 같다.

정리 4. (Wa-IBE1의 안전성[37]) 군 생성 알고리즘 g가 (t,ϵ)-DBDH 가정을 만족할 때, g로 생성된 군에서 만들어진 BF-IBE는($O(t), q_{ID}, 3\epsilon+\sqrt{9\epsilon^2+27q_{ID}n\epsilon}$)-IND-ID-CPA 안전하다. 단, 이때의 q_{ID}의 범위는 $[1, q\epsilon/9n]$이다.

$q_{ID}=0$인 경우에 Wa-IBE는 partitioning이 필요가 없으므로 DBDH 문제와 동일한 안전성을 증명할 수 있다.

4. 그 밖의 IBE

2003년에 Katz와 Wang은 랜덤 오라클 모델에서 기반 문제에 tight한 안전성을 가지는 서명을 제안하였다[32]. 이 논문에서 제안하는 것은 서명이지만 Katz와 Wang의 아이디어는 그 논문에서 밝혔듯이 IBE에도 적용이 가능한 기법이다. 그리고 Katz-Wang의 기법을 BF-IBE에 적용을 하면 암호문의 길이는 두 배가 되는 반면 (t,ϵ)-BDH 가정 하에서 $(O(t), q_{ID}, \epsilon q_{H_2})$-IND-ID-CPA 안전한 IBE (BF-KW-IBE)를 만들 수 있다.

2004년 Boneh와 Boyen이 BB-IBE1을 제시할 당시에 BB-IBE1 보다 효율성이 더 좋은 IBE (BB-IBE2)를 같이 제안하였는데 좀더 강한 가정을 필요로 한다[3]. 또한 같은 해에 Boneh와 Boyen은 CRYPTO에 standard 모델에서 DBDH 가정 하에 fully 안전한 IBE (BB-IBE3)를 제시하였다[4]. 하지만 암호문과 개인키의 크기가 크고 암복호화에 필요한 연산량이 Wa-IBE1에 비해 비효율적이다.

Gentry가 2006년 처음으로 standard 모델에서 기반문제에 tight한 안전성을 가지는 효율적인 IBE (Ge-IBE)를 제안하였다[25]. 기존의 partitioning과는 다른 방식의 증명을 하였는데, 이를 위해 BB-IBE2와 비슷한 강한 가정을 사용하였다. BB-IBE2와 Ge-IBE의 안전성 증명에 기반이 되는 가정들은 DBDH와 비슷하지만 공격자가 KeyExt 질의 하는 횟수만큼의 추가적인 정보를 더 주어진다. 이러한 가정들은 군의 위수가 어떠한 성질을 만족할 때 DBDH 보다 빠른 공격이 존재한다는 것이 알려져 있다[18]. Generic 모델에서의 안전성 또한 DBDH 보다 떨어진다는 것도 알려져 있다.

2009년 Waters는 standard 모델에서 DBDH와 결정적 선형 가정(Decisional Linear Assumption, DLN) 하에서 full security를 만족하는 IBE (Wa-IBE2)를 제안하였다[38]. Wa-IBE2은 기존의 증명 패러다임과는 전혀 다른 방식의 증명 방법을 제안하였는데 이 방식의 장점은 기존의 HIBE 나 BE 등과 같이 간단한 가정 하에서는 full security 증명이 어려웠던 암호시스템들은 Waters의 방식을 이용하면 DBDH와 DLN 가정 하에서 증명할 수가 있다.

5. IBE들의 비교

(표1)은 앞서서 설명한 8가지 IBE들에 대해서 효율성과 안전성을 비교한 것이다.

(표1) IBE

공개키, 비밀키, 암호문의 크기는 군 또는 군 위수 크기의 정수의 개수, n: 아이디의 길이, m<n, full: full security, selective: selective security, 안전성은 기반하는 가정의 안전성 ϵ에 대한 상대적인 안전성.

	공개키 크기	비밀키 크기	암호문 크기	기반 가정
BF-IBE	2	1	2	BDH
BF-KW-IBE	2	1	4	BDH
BB-IBE1	3	2	3	DBDH
BB-IBE2	3	2	3	Decisional q-BDHI
BB-IBE3	n+4	m+2	m+2	DBDH
Ge-IBE	3	2	3	Decisional q-ABDHE
Wa-IBE1	n+3	2	3	DBDH
Wa-IBE2	13	9	11	DBDH, DLN

	안전성		안전성 모델
BF-IBE	$O(q_{H_2}q_{ID}\epsilon)$	full	랜덤 오라클
BF-KW-IBE	$O(q_{H_2}\epsilon)$	full	랜덤 오라클
BB-IBE1	tight	selective	standard
BB-IBE2	tight	selective	standard
BB-IBE3	$O(q_{ID}\epsilon)$	full	standard
Ge-IBE	tight	full	standard
Wa-IBE1	$O(\sqrt{q_{ID}n\epsilon})$	full	standard
Wa-IBE2	$O(q_{ID}\epsilon)$	full	standard

(표1)에서 맨 좌측열의 IBE들을 나열하는 순서는 위에서부터 시간의 흐름에 따라 아래로 나열하였다. 2001년 BF-IBE가 제안된 이래로 처음에는 BB-IBE1, BB-IBE2와 같이 랜덤 오라클을 제거하기 위해 좀더 약

한 개념의 안전성인 selective security에서의 증명 가능한 IBE들이 제안이 되었고 뒤에 다시 full security를 만족하는 IBE를 설계하는 방향으로 발전을 하였다. 하지만 랜덤 오라클 가정이 없이 full security를 만족하는 첫 번째 IBE인 BB-IBE3가 효율성이 BF-IBE에 비해 너무 차이가 나므로 이를 개선하기 위해 Ge-IBE와 같이 강한 가정에서 증명을 시도하거나 혹은 안전성 증명이 tight하지 않은 Wa-IBE1과 같은 IBE들이 제안이 되었다. 최근에는 Wa-IBE1보다 안전성 증명이 tight한 Wa-IBE2가 제안이 되었지만 아직까지 BF-IBE나 BF-KW-IBE와 비교하면 랜덤 오라클 가정 하에서의 IBE 만큼의 효율성은 달성하지 못하고 있다.

Ⅳ. 아이디 기반 암호의 응용들

이 절에서는 아이디 기반 암호의 응용들에 대해 간략하게 소개한다. 아이디 기반 암호의 응용으로는 아이디 기반 암호의 확장인 '계층구조를 가지는 아이디 기반 암호(HIBE)[29]', 아이디 기반 암호의 아이디를 키워드에 대응시키는 '검색 가능한 공개키 암호(PEKS)[6]', 이전에 생성된 암호문에 대한 안전성을 보장하는 'forward secure 암호[20]', 미래에서의 복호화를 위한 'timed release 암호[22]', 암호문의 속성에 따른 접근 권한을 제한시키는 '속성 기반 암호(ABE)[35,27]', 비밀키 업데이트를 허용하는 'Key Insulated 암호[22]', 다수에게 같은 내용의 암호문을 효율적으로 전송하는 '브로드캐스트 암호[24]', 아이디 기반 암호와 서명을 합쳐놓은 '아이디 기반 signcryption[2]' 등이 있다. 또한, 기존의 공개키 암호에서 고려되던 응용들에 아이디 기반이라는 특성을 더해서 '아이디 기반 서명(IBS)[19]', '아이디 기반 그룹 서명', '아이디 기반 Blind 서명[39]', '아이디 기반 링 서명[39]', '아이디 기반 threshold 암호[15]'와 같은 좀 더 다양한 응용들을 개발할 수 있다. 우리는 지면의 제한 때문에 이 중 몇 가지에 대해서만 소개하도록 한다.

1. 계층구조를 가지는 아이디 기반 암호 (Hierarchical ID-based Encryption, HIBE)

HIBE는 Horwitz와 Lynn에 의해 정의된 개념이다 [30]. HIBE는 IBE의 확장으로 아이디가 하나의 원소가 아니라 계층구조를 가지는 벡터로 표현이 되며 위의 계층의 사용자는 아래계층의 사용자의 개인키를 생성할 수 있는 능력을 가지는 암호 시스템이다. 예를 들어, 세 단계의 계층이 있는 HIBE를 설명해보면 대학교에서 HIBE를 사용하여 구성원들에게 개인키를 할당할 경우, 아이디가 되는 벡터는 (단과대학 아이디, 학과 아이디, 직원 아이디)가 될 수 있다. 이 경우 학교의 키 생성 센터(Key Generation Center, KGC)에서 각 단과대학의 KGC에게 키를 만들어 주면 단과대학의 KGC는 각 학과의 KGC의 키를 생성해서 나누어 줄 수가 있고 최종적으로 각 학과의 KGC는 직원들의 키들을 만들어 나누어 줄 수가 있다. 암호문을 생성하는 사용자는 암호문 생성에 사용되는 아이디 벡터를 (자연과학대학, 수학과)와 같이 설정을 하게 되면 이 암호문은 (자연과학대학, 수학과) 키를 가지고 있는 사용자와 이 사용자의 상위 계층에 있는 사용자만이 복호화를 할 수가 있다.

모든 계층에서의 안전성이 증명이 되는 처음 제안된 HIBE는 2002년에 Gentry와 Silverberg가 ASIACRYPT에서 제안한 HIBE (GS-HIBE) 이다[29]. HIBE의 안전성 증명의 경우 IBE와 마찬가지로 랜덤 오라클을 없애기 위해 selective security 모델에서의 증명이 이루어 졌고[3], 뒤에 full security 모델에서 안전한 HIBE가 제안이 되었다[37]. 하지만 HIBE의 경우 IBE와 다르게 안전성 증명에서 어려운 부분이 존재를 하는데, 많은 HIBE의 안전성 증명은 랜덤 오라클 모델에서 조차 HIBE의 계층의 길이에 따라 지수적으로 안전성이 감소한다는 문제점을 가지고 있었다[29,3,5,37,23]. 2009년 Gentry와 Halivi가 계층의 길이에 따라 안전성이 지수적으로 감소하지 않은 최초의 HIBE (GH-HIBE)를 제안을 하였다[26]. GH-HIBE는 Ge-IBE의 확장으로서 Ge-IBE와 마찬가지로 강한 가정 하에서 안전성 증명을 하였다. 같은 해 CRYPTO에서 Waters가 처음으로 간단한 가정(DBDH, DLN) 하에서 안전한 HIBE를 제시하였다[38].

HIBE는 브로드캐스트 암호 SD/LSD의 공개키 버전 브로드캐스트 암호를 만드는데 사용이 될 수 있다[24]. 또한 forward secure 암호, timed release 암호 등의 암호 시스템을 만드는데 사용이 될 수 있다[20,5].

2. 검색 가능한 공개키 암호와 anonymous IBE

검색 가능한 공개키 암호(PEKS)는 Boneh, Crescenzo, Ostrovsky, Persizno 등이 처음 제안한 개념으로서 이름에서 알 수 있듯이 다량의 암호문들이 있을 때 그 중 원하는 키워드를 포함하는 암호문을 찾을 수 있도록 해주

는 공개키 암호이다. 물론, 모든 암호문을 복호화해서 찾는다면 찾을 수 있겠지만 그렇게 하면 시간이 많이 걸릴 뿐 아니라 키워드를 포함하지 않는 암호문에 대한 정보도 얻을 수 있게 된다. PEKS의 목적은 공개키에 대응되는 비밀키를 가지고 있는 사용자가 원하는 키워드에 대응되는 토큰이라는 제한된 능력의 키를 생성하여 토큰을 가진 유저는 (실제 응용에서는 메일 서버가 여기에 해당한다.) 오직 암호문들 중에서 대응되는 키워드를 가진 암호문만 골라낼 수 있게 하는 것이다. 한 가지 키워드에 대한 검색뿐만 아니라 여러 키워드들의 조합에 대한 검색을 허용하는 PEKS 등에 대한 연구가 진행 중이다[13,31].

IBE에서의 안전성은 메시지에 대한 안전성이었는데, 여기에 아이디에 대한 안전성을 추가하면, 즉, 암호문으로부터 아이디에 대한 1비트 정보도 얻을 수 없도록 만들 수만 있으면 anonymous IBE라고 부르고 이를 이용하면 PEKS를 만들 수 있음이 증명되었다[1]. BF-IBE는 제안할 당시 anoymity를 강조하지 않았는데 BF-IBE역시 anonymous IBE가 된다. Standard 모델에서의 anonymous IBE에 대한 연구도 활발히 진행이 되어 왔다.[14, 25] Anonymous IBE를 HIBE로 확장시키면 anonymous HIBE라고 부르는데 이를 이용하면 계층의 맨 마지막을 PEKS로 활용하는 것과 같이 HIBE와 PEKS를 결합하는 응용들을 개발할 수 있다[14,36,34].

3. Predicate 암호 시스템

Predicate 암호 시스템이란 암호문에 특정 함수 f를 포함시키고 개인키는 특정한 값 x를 포함시켜서 만든 뒤 f(x)=1을 만족하는 x에 대응하는 키를 가진 사용자만이 이 암호문을 복호화할 수 있도록 허용하는 암호 시스템이다. 반대로 f와 x를 키와 암호문에 바꾸어서 넣을 수도 있다. 이러한 개념의 암호 시스템은 암호화된 데이터베이스 등의 대량의 암호문들에 사용자들마다 접근권한의 능력을 제한하고자 할 때 용이하게 활용이 될 수 있다. Predicate 암호 시스템은 PEKS나 속성 기반 암호 (attribute based encryption)[35,27] 등의 암호 시스템을 포함하는 개념으로서 Katz, Sahai, Waters 등이 처음 제안하였다[31].

4. 전자 서명

IBE가 있을 때 이를 이용하면 새로운 전자 서명을 만들 수 있는데 이는 Naor가 처음 지적을 하였다. IBE의 시스템 파라미터들이 전자 서명의 공개키에 해당하고 MK가 전자 서명의 비밀키에 해당한다. IBE에서는 MK와 KeyGen 알고리즘을 사용하면 임의의 아이디에 대한 개인키를 생성할 수 있는데, 이 개인키가 전자 서명에 해당한다. 서명 검증 방법은 서명에 사용된 아이디에 대한 임의의 IBE 암호문을 생성하여 서명에 해당하는 IBE 개인키로 복호화를 해봄으로써 가능하다. 또한, 안전성 측면에서는 IBE가 IND-ID-CPA이면 EUF-CMA임을 쉽게 보일 수 있다[8].

아이디 기반 서명 (IBS)은 Cha, Cheon에 의해 처음 제안된 개념으로 IBE와 마찬가지로 공개키가 아이디라는 점에서 이전의 서명들과 차이점을 가진다[19].

V. 결론 및 미해결 문제

우리는 이 논문에서 아이디 기반 암호들을 발전 과정에 맞추어 살펴보았다. 또한, 아이디 기반 암호의 응용으로서 계층구조를 가지는 아이디 기반 암호, 검색 가능한 암호, predicate 암호, 전자 서명 등을 살펴보았다. 아이디 기반 암호의 경우 standard 모델에서 기반 가정에 tight한 full security를 가지는 것은 Ge-IBE가 유일하다. 하지만 Ge-IBE의 경우 공격자의 KeyExt 질의 횟수 능력에 따른 강한 가정을 사용하므로 BDH와 같은 간단한 가정에 tight한 full security를 만족하는 IBE를 찾는 것은 중요한 문제이고 아직까지 미해결 문제로 남아 있다. 또한, predicate 암호의 경우 복잡한 predicate에 대한 효율적인 시스템에 대한 연구가 필요하다. 마지막으로 BDH, DBDH, DLN 등의 가정들은 아직까지 CDH, DL, 인수분해, RSA 등의 가정들처럼 안전성에 대해 많은 연구가 이루어지지 않았다. 이러한 새롭게 제안되는 암호학적 가정들에 대한 검증이 필요하다.

참고문헌

[1] M. Abdalla, M. bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, “Searchable encryption re-

visited: Consistency properties, relation to anonymous ibe, and extensions" CRYPTO 2005, LNCS, vol.3621, pp.205-222, Springer-Verlag, 2005.

[2] X. Boyen, "Multipurpose Identity-Based Signcryption", CRYTO 2003.

[3] D. Boneh and X. Boyen. "Efficient selective-id identity based encryption without random oracles" EUROCRYPT 2004, volume 3027 of LNCS, pages 223-238. Springer-Verlag, 2004.

[4] D. Boneh and X. Boyen, "Secure Identity Based Encryption Without Random Oracles" CRYPTO 2004.

[5] D. Boneh, X. Boyen, and E. Goh. "Hierarchical identity based encryption with constant size ciphertexts" EUROCRYPT 2005, volume 3494 of LNCS, pages 440-456. Springer-Verlag, 2005.

[6] D. Boneh, G. Crescenzo, R. Ostrovsky, G. Persizno, "Public key encryption with keyword search", EUROCRYPT 2004.

[7] D. Boneh and M. Franklin. "Identity-based encryption from the weil pairing" CRYPTO 2001, volume 2139 of LNCS, pages 19-23. Springer-Verlag.

[8] D. Boneh and M. Franklin. "Identity-based encryption from the weil pairing" SIAM J. Comput., 32(3): 586-615, 2003.

[9] D. Boneh, C. Gentry, M. Hamburg, "Space-efficient identity based encryption without pairings" FOCS 2007.

[10] D. Boneh and J. Katz, "Improved efficiency for cca-secure cryptosystems built using identity based encryption" CT-RSA 2005, LNCS, vol.3376, pp.87-103, Springer-Verlag, 2005.

[11] X. Boyen, Q. Mei, and B. Waters, "Direct chosen ciphertext security from identity-based techniques" ACM Conference on Computer and Communications Security-CCS 2005, ACM Press.

[12] M. Bellare, T. Ristenpart, "Simulation without the Artificial Abort: Simplified Proof and Improved Concrete Security for Waters' IBE Scheme", EUROCRYT 2009.

[13] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data" TCC 2007, LNCS, vol.4392, pp.535-554, Springer-Verlag, 2007.

[14] X. Boyen and B. Waters, "Anonymous hierarchical identity-based encryption (without random oracles)" CRYPTO 2006, LNCS, vol.4117, pp.290-307, Springer-Verlag, 2006.

[15] J. Baek, Y. Zheng, "Identity-Based Threshold Decryption" PKC 2004.

[16] C. Cocks, "An identity based encryption scheme based on quadratic residues" Cryptography and Coding 2001.

[17] J. Coron, "On the Exact Security of Full Domain Hash", CRYPTO 2000.

[18] J. Cheon, "Security analysis of the strong Diffie-Hellman problem", EUROCRYPT 2006.

[19] J. Cha and J. Cheon, "An identity-based signature from gap Diffie-Hellman groups" PKC 2003.

[20] R. Canetti, S. Halevi, and J. Katz. "A forward-secure public-key encryption scheme" EUROCRYPT 2003, volume 2656 of LNCS. Springer-Verlag, 2003.

[21] R. Canetti, S. Halevi, and J. Katz, "Chosen-ciphertext security from identity-based encryption" EUROCRYPT 2004, LNCS, vol.3027, pp.207-222, Springer-Verlag, 2004.

[22] J. Cheon, N. Hopper, Y. Kim, I. Osipkov, "Timed-Release and Key-Insulated Public Key Encryption" Financial Cryptography and Data Security 2006.

[23] S. Chatterjee and P. Sarkar, "Hibe with short public parameters without random oracles" ASIACRYPT 2006, LNCS, vol.4284, pp.145-160, Springer-Verlag, 2006.

[24] Y. Dodis, N. Fazio, "Public key broadcast encryption for stateless receivers", Digital Rights Manigimant 2003.

[25] C. Gentry, "Practical identity-based encryption without random oracles" EUROCRYPT 2006, LNCS, vol.4004, Springer-Verlag, 2006.

[26] C. Gentry and S. Halevi, “Hierarchical identity base encryption with polynomially many levels” TCC 2009, LNCS, vol.5444, pp.437-456, Springer-Verlag, 2009.

[27] V. Goyal, O. Pandy, A. Sahai, B. Waters, “Attribute based encryption for fine-grained access control of encrypted data”, ACM Conference on Computer and Communications Security-CCS 2006, ACM Press.

[28] C. Gentry, C. Peikert, and v. Vaikuntanathan, “Trapdoors for hard lattices and new cryptographic constructions” STOC 2008.

[29] C. Gentry and A. Silverberg. “Hierarchical id-based cryptography” ASIACRYPT 2002, volume 2501 of LNCS, pages 149-155. Springer-Verlag, 2002.

[30] J. Horwitz and B. Lynn, “Towards hierarchical identity-based encryption” EUROCRYPT 2002, LNCS, vol.2332, pp.466-481, Springer-Verlag, 2002.

[31] J. Katz, A. Sahai, and B. Waters, “Predicate encryption supporting disjunctions, polynomial equations, and inner products” EUROCRYPT 2008.

[32] J. Katz and N. Wang. “Efficiency improvements for signature schemes with tight security reductions” In S. Jajodia, V. Atluri, and T. Jaeger, editors, ACM Conference on Computer and Communications Security-CCS 2003, pages 155-164. ACM, 200

[33] A. Shamir, “Identity-based cryptosystems and signature schemes”, CRYPTO 1984.

[34] J. Seo, T. Kobayashi, M. Ohokubo, K. Suzuki, “Anonymous HIBE with Constant Size Ciphertexts” PKC 2009.

[35] A. Sahai, B. Waters, "Fuzzy identity-based encryption" EUROCRYT 2005.

[36] E. Shi and B. Waters, “Delegating capabilities in predicate encryption systems” ICALP 2008, LNCS, vol.5126, pp.560-578, Springer-Verlag, 2008.

[37] B. Waters, “Effient identity-based encryption without random oracles” EUROCRYPT 2005, LNCS, vol.3494, pp.114-127, Springer-Verlag, 2005.

[38] B. Waters, “Dual system encryption Realizing fully secure IBE and HIBE under simple assumptions” CRYPTO 2009.

[39] F. Zhang, K. Kim, “ID-Based Blind Signature and Ring Signature from Pairings” ASIACRYPT 2002.

<著 者 紹 介>

서 재 홍 (Jae Hong Seo)
학생회원
2004년 2월 : 고려대학교 수학과 졸업
2004년 3월~현재 : 서울대학교 수리과학부 석박사통합 박사과정
<관심분야> 암호, 계산수론, 정보보호

천 정 희 (Jung Hee Cheon)
정회원
1991년 2월 : KAIST 수학과 졸업
1993년 8월 : KAIST 수학과 석사
1997년 2월 : KAIST 수학과 박사
1997년 2월~2000년 1월 : ETRI 선임연구원
2000년 1월~2000년 12월: Brown University Postdoc
2000년 12월~2003년 2월: ICU 조교수
2003년 3월~2005년 3월: 서울대학교 조교수
2005년 4월~현재: 서울대학교 부교수
<관심분야> 계산수론, 암호, 정보보호