情報保護學會論文誌
第 22 卷 第 4 號, 2012. 8

ID기반 암호시스템을 이용하여 ID기반 동적 임계 암호시스템으로 변환하는 방법*

김 미 령,† 김 효 승, 손 영 동, 이 동 훈‡
고려대학교 정보보호대학원

The Conversion method from ID-based Encryption to ID-based Dynamic Threshold Encryption*

Milyoung Kim,† Hyoseung Kim, Youngdong Son, Dong Hoon Lee‡
Graduate School of Information Security, Korea University

요 약

동적 임계 공개키 암호 시스템(dynamic threshold public-key encryption)이란 시스템을 구축하는 과정에서 전체 사용자들의 집합과 인증된 수신자 집합의 크기, 임계치를 고정값으로 설정하지 않고 유연하게 변경될 수 있는 기능을 제공하는 임계 암호 시스템을 말한다. 이와 관련하여 신원정보를 공개키로 사용하는 ID기반 암호 시스템(identity-based encryption)과 동적 임계 공개키 시스템을 결합하여 ID기반 동적 임계 암호 시스템(identity-based dynamic threshold encryption)을 설계하려는 연구가 이뤄지고 있으며, 최근 2011년 Xing과 Xu은 동적 기능을 제공하는 ID기반 임계 암호기법을 제안하였다.

본 논문에서는 Xing과 Xu가 제안한 ID기반 동적 임계 암호 시스템을 분석하고 구조적으로 문제점이 있음을 보인다. 또한 겹선형 함수를 이용한 ID기반 암호 시스템을 ID기반 동적 임계 암호 시스템으로 변환하는 방법(conversion method)를 제안한다. 마지막으로, 변환하여 설계한 기법이 완전한 풀 모델(full model)로 선택된 평문 공격(chosen plaintext attack)환경에서 안전함을 증명한다.

ABSTRACT

Dynamic threshold public-key encryption provides dynamic setting of the group of all users, receivers and the threshold value. Over recent years, there are many studies on the construction of scheme, called ID-based dynamic threshold encryption, which combines the ID-based encryption with dynamic threshold encryption.

In this paper, we analyze the ID-based dynamic threshold encryption proposed by Xing and Xu in 2011, and show that their scheme has a structural problem. We propose a conversion method from ID-based encryption which uses the bilinear map to ID-based dynamic threshold encryption. Additionally, we prove this converted scheme has CPA security under the full model.

Keywords: ID-based encryption; dynamic threshold encryprion; conversion mehtod

접수일(2012년 3월 23일), 게재확정일(2012년 5월 8일)
* 이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2011-0029831)
† 주저자, us61219@naver.com
‡ 교신저자, donghlee@korea.ac.kr

I. 서 론

1.1 개요

임계 공개키 암호 시스템(threshold public - key encryption)은 일반적인 공개키 암호 시스템을 확장한 암호 시스템으로서 임계치(threshold value)를 이용하여 수신자들의 복호화 권한을 설정할 수 있다[2,5,6]. 암호문은 송신자가 선택한 수신자들의 공개키를 이용하여 생성되고, 수신자들로 구성된 집합 중에 임계치 이상의 수신자가 모여야 암호문을 복호화 할 수 있게 된다. 이 때 복호화에 참여하지 않은 수신자는 메시지를 얻을 수 없다. 예를 들어, 전체 사용자가 20명일 때 송신자가 선택한 수신자 10명에 대하여 임계치가 4인 암호문을 전송하였을 때, 수신자 10명 중 적어도 4명이 모여야 암호문을 복호화 할 수 있다. 일반적으로 복호화 과정은 Shamir의 비밀 분산(secret sharing) 기법[10]을 이용한다. 이와 같이 임계 공개키 암호 시스템은 기존에 제시 되었던 일반적인 공개키 암호 시스템에서 지원하지 못했던 기능을 제공한다.

기본적으로 공개키 암호 시스템에서 공개키는 누구나 만들 수 있기 때문에 이것을 이용하기 위하여 신뢰할 수 있는 인증기관에 공개키를 생성한 정당한 수신자임을 인증 받아야 한다. 정당한 수신자임을 인증 받으면 인증기관에서는 수신자에게 인증서를 발급 해 준다. 하지만 이와 같은 경우 인증서 관리 문제와 인증서 검증에 따른 연산량 등 여러 문제가 생기게 된다. 이에 1985년 전자우편주소나 주민등록번호처럼 수신자의 신원정보를 공개키로 이용하는 ID기반 암호 시스템(Identity-Based Encryption:IBE)이 Shamir에 의해 처음 제안 되었다[11]. 송신자는 암호문을 만들 때 누구나 알 수 있는 수신자의 고유한 신원정보를 공개키로 이용한다. 공개키 자체로 수신자를 인증하기 때문에 공개키 암호 시스템과 달리 인증기관에 정당한 수신자임을 인증 받아야 하는 복잡함과 이에 따른 비용과 비효율성 문제를 해결하는 큰 장점을 가지게 된다.

ID기반 임계 암호 시스템(identity-based threshold encryption)은 임계 암호 시스템과 IBE를 결합한 것으로, 인증서에 대한 문제가 발생하지 않으며 임계치를 이용하여 복호화 권한을 설정할 수 있는 기능을 모두 제공 한다[9,4,12]. 이와 같이 ID기반 임계 암호 시스템은 IBE와 임계 암호 시스템의 장점을 제공한다.

1.2 관련연구

초기에 제안되었던 임계 공개키 암호 시스템에서는 암호 시스템을 초기설정 또는 키 생성 과정에서 전체 사용자들의 집합과 수신자 집합의 크기, 임계치가 고정값으로 설정 되었다. 이러한 경우 시스템이 작동한 이후로는 위에서 설정한 값들이 공개키의 입력 값이 되기 때문에 변경 할 수 없었다[5,7]. 하지만 이동 ad-hoc 네트워크와 같은 경우 수신자들의 집합이 동적으로(dynamically) 변할 수 있기 때문에 위와 같은 값들을 고정값으로 설정하지 않고 유연하게 변경할 수 있는 기능을 제공하는 동적 임계 공개키 암호 시스템(dynamic threshold public- key encryption)이 제안되었다[8].

동적 임계 공개키 암호 시스템에서는 시스템이 작동한 후에도 송신자는 인증된 수신자들의 집합을 동적으로 선택이 가능하며, 동적으로 인증된 집합 중 복호 기능에 대한 임계치가 암호문 생성 과정에서 유연하게 설정 될 수 있다. 2008년에 Cécile Delerablée 와 David Pointcheval은 동적 임계 공개키 암호 시스템이 만족해야하는 기능을 다음과 같이 제시하였다[8].

- 어떠한 사용자도 시스템에 동적으로 참여하여 수신자가 될 수 있다.
- 송신자는 암호문에 대하여 수신자들의 집합을 동적으로 선택 할 수 있다.
- 송신자는 매번 암호문을 만들 때마다 임계치를 동적으로 설정할 수 있다. 이때 임계치는 수신자 집합에서 복호화 권한이 된다.

이와 다른 연구로 Shamir에 의해 처음 제안된 IBE는 연구가 지속 되어오다, 2001년 Boneh과 Franklin에 의해 겹선형 함수(bilinear map)를 이용하여 효율적이고, 랜덤 오라클을 이용하여 안전성을 증명한 IBE가 제안 되었다[3]. 2004년에 랜덤 오라클을 이용하지 않고, 공격자가 공격 대상을 정한 뒤 공격이 시작되는 선택적인 ID 모델(sele- ctive ID model)을 이용하여 선택된 암호문 공격(Chosen Ciphertext Attack:CCA)에 안전한 기법이 Boneh과 Boyen에 의해 제안 되었다[1]. 이후 연구가 지속 되어왔지만 비효율성 문제를 가지고 있었으며, 2005년 Waters가 제안한 IBE는 선택적인 ID 모델보다 강한 개념인 풀 모델(full model)로 안전성이 증명되었다[13].

위에서 언급한 IBE와 임계 공개키 시스템의 각각의 장점을 결합한 ID기반 임계 암호 시스템(identity-based threshold encryption) 또한 하나의 연구 분야로서 활발히 연구가 이루어지고 있다. 2003년에 처음으로 구체적인 기법으로 제안되었고, 이후 여러 기법이 제안되었지만 동적인 환경에서는 적용할 수 없었다[9,4,12]. 2011년 Xing과 Xu는 ID기반 임계 암호 시스템에서 동적인 기능을 추가하여 인증된 수신자 집합의 크기, 임계치를 유연하게 변경하는 기법을 제안했다[14].

1.3 기여도

본 논문은 Xing과 Xu가 제안한 ID기반 동적 임계 암호 기법을 분석하고, 구조적인 문제가 있음을 설명한다. 또한 IBE와 Shamir 기법을 이용하여 Xing과 Xu가 제안한 기법과 같은 기능을 제공하는 기법을 설계 할 수 있는 변환 방법(conversion method)을 제시한다. 본 논문에서 제안하는 방법을 이용하면 선택된 평문 공격(Chosen Plaintext Attack:CPA)에 안전하고 겹선형 함수를 이용한 IBE의 존재 하에 CPA에 안전한 ID기반 동적 임계 암호 시스템의 설계가 가능하다. 본 논문에서는 2005년에 제안된 Waters의 IBE[13]를 기반으로 랜덤 오라클을 이용하지 않고, 완전한 풀 모델로 증명 한다[13].

논문의 구성은 다음과 같다. Ⅱ장에서는 관련 연구에 대한 배경지식을 기술하고, Ⅲ장에서는 Xing과 Xu가 제안한 ID기반 동적 임계 암호기법에 대하여 설명하고, 기법의 문제점을 분석한다. Ⅳ장에서는 변환 방법(conversion method)을 제안한다. Ⅴ장에서는 제안한 변환 방법을 이용하여 설계된 기법의 안전성을 기술한 안전성 모델로 증명한다. 마지막으로 Ⅵ장에서 결론을 맺는다.

Ⅱ. 배경 지식

2.1 겹선형 함수

G_1은 위수를 소수 q로 갖는 덧셈 연산군이라 하고, G_2는 같은 위수 q를 갖는 곱셈 연산군이라 하자. 그리고 P는 G_1의 생성원(generator)이다. 군 G_1과 G_2에서 모두 이산대수문제(discrete logarithm problem)가 어렵다고 가정할 때. 다음과 같은 조건을 만족하는 함수 $e: G_1 \times G_1 \rightarrow G_2$를 겹선형 함수라 한다.

- 겹선형성 (bilinearlity): 임의의 군 원소 $P, Q \in G_1$와 $a, b \in Z_q^*$에 대하여 $e(aP,bQ) = e(P,Q)^{ab}$을 만족한다.
- 비소실성 (non-degeneracy): $e(P,P) \neq 1$을 만족하는 $P \in G_1$이 존재한다.
- 계산 가능성 (computability): 모든 $P, Q \in G_1$에 대해서 $e(P,Q)$를 계산하는 효율적인 알고리즘이 존재한다.

2.2 Shamir의 기법[10]

라그랑지 보간법(lagrange interpolation)이란 t개의 순서쌍을 만족시키는 $t-1$차 다항식을 만족하는 순서쌍을 계산하는 방법이다. 1979년 Shamir는 라그랑지 보간법을 근거로 임계치를 이용하여 비밀 분산 기법(threshold secret sharing)을 제안하였다[10]. 비밀 분산 기법의 기본적인 조건은 분배자(dealer)는 수신자들에게 분할된 정보에 대한 비밀을 보장하여야 하며, k명의 수신자 집합에 분할된 정보 중 임의의 t명 이상이 정보를 재구성하였을 때 비밀 정보를 복원 되어야 한다. Shamir가 제안한 비밀 분산 기법은 다음과 같다.

- 분배자는 비밀 정보 $s = a_0$를 상수항으로 하는 랜덤한 $t-1$차 다항식 $f(x)$를 선택한다.

$$f(x) = a_0 + a_1 x + \cdots + a_{t-1} x^{t-1} (\mathrm{mod} p)$$

단, 유한체 $GF(p)$에서 계산이 되고, 비밀 정보 s 또한 유한체 $GF(p)$에 속해 있다. 여기서 p는 비밀 정보 s보다 큰 소수 이다.

- 분배자는 각 수신자 $i (1 \leq i \leq k)$에게 분할된 정보 $f(i)$를 준다.
- k명에게 분할된 정보 중 최소 t명이 모였을 때 라그랑지 보간법에 의해 $f(0)$값인 비밀 정보 $s = a_0$를 구할 수 있게 된다.

2.3 IBE의 형식적 정의

일반적인 IBE는 다음과 같은 4개의 다항식 시간(polynomial-time) 알고리즘들로 구성된다.

- $Setup_{IBE}(1^\lambda)$: 키 생성기관(Key Generation Center: KGC)에 의해 진행되며 보안 상수 1^λ

를 입력 받아 마스터 키 mk와 파라미터 $params$를 출력한다. 이때 mk는 KGC의 비밀 값이고 $params$는 공개된다.

- $KeyGen_{IBE}(params, ID, mk)$: KGC에 의해 진행되며 파라미터 $params$과 마스터 키 mk를 입력받아 사용자의 ID에 대응되는 개인키 sk_{ID}를 출력한다. 이때 사용자의 ID는 임의의 길이를 가지며 공개키로 이용된다.
- $Encrypt_{IBE}(params, ID, M)$: 파라미터 $params$와 사용자의 ID, 그리고 메시지 M을 입력받아 암호문 C를 출력한다.
- $Decrypt_{IBE}(params, sk_{ID}, C)$: 파라미터 $params$와 사용자의 ID에 대한 개인키sk_{ID}, 그리고 암호문 C를 입력받아 메시지 M을 출력한다.

2.4 ID기반 동적 임계 암호 시스템의 형식적 정의

ID기반 동적 임계 암호 시스템은 다음과 같은 4개의 다항식 시간 알고리즘들로 구성 된다.

- $Setup(1^{\lambda}, N)$: KGC에 의해 진행되며 보안 상수 1^{λ}와 사용자 전체 집합의 크기 N을 입력 받아 마스터 키 mk와 파라미터 $params$를 출력한다. 이때 mk는 KGC의 비밀 값이고 $params$는 공개된다.
- $KeyGen(params, ID_i, mk)$: KGC에 의해 진행되며 파라미터 $params$과 마스터 키 mk를 입력 받아 각 사용자의 ID_i에 대응되는 개인키 sk_{ID_i}를 출력한다.
- $Encrypt(params, \{ID_1, ..., ID_k\}, t, M)$: 파라미터 $params$와 그룹의 사용자 ID 집합 $\{ID_1, ..., ID_k\}$, 그리고 메시지 M을 입력받아 암호문 C를 출력한다. 이때 $k \le N$이고, t는 임계치다. 즉, k명이 구성하는 그룹에 암호문 C을 전송하여 그 중 t명이 모이면 암호문 C을 복호화 할 수 있도록 설정한다.
- $Decrypt(params, IDs, C)$: 파라미터 $params$와 사용자 집합 IDs 그리고 암호문 C를 입력받아 IDs가 암호문을 생성할 때 지정한 사용자 집합의 부분집합이 아니거나, IDs의 크기가 임계치를 넘지 않을 경우 $\perp$을 출력한다. 그렇지 않으면 메시지 M을 출력한다.

2.5 ID기반 동적 임계 암호 시스템의 안전성 모델

랜덤 오라클을 이용하지 않고, 풀 모델로 선택 평문 공격에 의한 평문 구분 불가능성(IND-CPA)을 만족하는 ID기반 동적 임계 암호 시스템의 안전성 모델은 다음과 같이 정의한다.

어떠한 다항식 시간(polynomial-time)에 ID기반 동적 임계 암호 시스템 공격자(attacker) A에 대하여 A가 다음과 같이 정의된 게임에서 이길 성공 확률이 무시할 수 있는(negligible) 값이라면 제안된 ID기반 동적 임계 암호 시스템은 IND-CPA를 만족한다고 정의한다.

- $Setup(1^{\lambda})$: 시뮬레이터(simulator) Z는 $Setup$ 알고리즘을 실행하여 마스터 키 mk와 파라미터 $params$를 얻는다. 시뮬레이터 Z는 파라미터 $params$를 공격자 A에게 준다. 이때 마스터 키 mk는 계속 비밀로 유지한다.
- $Phase1$: 공격자 A는 시뮬레이터 Z에게 다음과 같은 질의를 한다.
  - $Extract(ID = \{ID_1, ..., ID_k\})$: 공격자 A가 ID 집합에 대한 비밀키 sk를 요청할 때 시뮬레이터 Z는 $KeyGen$ 알고리즘을 이용하여 ID 집합 $\{ID_1, ..., ID_k\}$에 대응하는 비밀키 $\{sk_1, ..., sk_k\}$를 생성하여 준다.
- $Challenge$: 공격자 A는 공개키로 사용할 ID 집합 $ID^* = \{ID_1, ..., ID_l\}$과 임계치 t를 선택하고 챌린지 할 두 메시지 M_0, M_1을 선택한다. 공격자 A는 시뮬레이터 Z에게 챌린지 메시지(ID^*, t, M_0, M_1)을 준다. 시뮬레이터 Z는 $b \in \{0,1\}$을 선택하고 암호문 C_{ch}를 다음과 같이 $Encrypt(params, \{ID_1, ..., ID_i\}, t, M_b)$로 생성하여 공격자 A에게 준다. 이때 $Phase1$에서 질의하는 ID들의 색인(index) 집합 $I: \{k | ID_k \in ID\}$에 대해서 $I_1 = \bigcup I$라 하였을 때, 임계치 t는 부등식 $|I_1 \bigcap \{k | ID_k \in ID^*\}| < t$를 만족해야 한다. 즉, $Phase1$에서 질의한 모든 ID 중 t개 이상의 ID가 ID^* 집합의 원소가 될 수 없다.
- $Phase2$: 공격자 A는 시뮬레이터 Z에게 $Phase1$과 같은 질의를 한다. $Phase2$에서 질의하는 ID들의 색인 집합 $I': \{k | ID_k \in ID'\}$에 대해서 $I_2 = \bigcup I'$라 하였을 때, 부등식 $|(I_1 \bigcup I_2) \bigcap \{k | ID_k \in ID^*\}| < t$를 만족하는 ID 집합에 대해서만 질의가 가능하다. 조건을 만족하면 계속하여 질의를 요청할 수 있다.

- *Guess*: 공격자 A는 $b' \in \{0,1\}$를 출력하고 $b' = b$인 경우 공격자 A가 위의 게임에서 이긴다.

위의 공격자 A의 이점(advantage)는 다음과 같은 확률 값으로 정의 된다.

$$Adv_{IDTE}^{CPA}[A] = \left| \Pr[b' = b] - \frac{1}{2} \right|$$

따라서 공격자 A가 CPA 환경에서 ID기반 동적 임계 암호 시스템을 공격하는데 성공하였다면 A의 이점은 의미 있다고(non-negligible) 볼 수 있다.

III. Xing과 Xu의 기법[14]

본 장에서는 Xing과 Xu가 제안한 ID기반 동적 임계 암호 시스템에 대하여 설명하고 문제점을 분석한다.

3.1 Xing과 Xu의 기법

Xing과 Xu가 제안한 ID기반 동적 임계 암호기법은 다음과 같다.

- $Setup(1^{\lambda}, N)$: 위수가 소수 q인 덧셈군 $G_1 = <P>$와 곱셈군 G_2를 선택하고 겹선형 함수 $e: G_1 \times G_1 \rightarrow G_2$와 해쉬함수 $H: \{0,1\}^* \rightarrow G_1^*$를 정의한다. 임의의 $Q \in G_1^*$와 $s \in Z_q^*$를 선택하고 $T = sP$를 계산한다. 파라미터 $params = (q, G_1, G_2, e, P, Q, T, H)$와 마스터 키 $mk = s$를 출력한다.
- $KeyGen(params, ID_i, mk)$: 그룹의 각 사용자의 ID_i에 대응되는 개인키 $sk_{ID_i} = sH(ID_i)$를 계산하여 전송한다.
- $Encrypt(params, \{ID_1, ..., ID_k\}, t, M)$: 일반성을 잃지 않고 송신자가 정하는 수신자의 집합을 $\{ID_1, ..., ID_k\}$라 하였을 때, 다음 과정을 통해 메시지 M에 대한 암호문 C를 생성한다.

1. 임의의 $m \in Z_q^*$를 선택하여 $U = mP$와 $W = e(Q,T)^m \cdot M$을 계산한다.
2. $V = mQ + mH(ID_1)H(ID_2)\cdots H(ID_k)$를 계산하고 $V = f(0)$인 $t-1$차 다항식 f를 설정한다.
3. $V_i = e(H(ID_i), mT) f(H(ID_i))$를 계산한다.
4. 암호문 $C = (U, t, V_1, \cdots, V_k, W)$를 출력한다.

- $Decrypt(params, IDs, C)$: 일반성을 잃지 않고 복호화에 참여하는 t명의 수신자의 아이디 집합을 $IDs = \{ID_1, ID_2, ..., ID_t\}$라 하자. 각 수신자는 다음을 계산한다.

$$\begin{aligned} \frac{V_i}{e(U, sk_{ID_i})} &= \frac{e(H(ID_i), mT)}{e(U, sk_{ID_i})} f(H(ID_i)) \\ &= \frac{e(H(ID_i), msP)}{e(mP, sH(ID_i))} f(H(ID_i)) \\ &= f(H(ID_i)) \end{aligned}$$

t명의 수신자들이 계산한 $f(H(ID_i))$ 값들을 이용하여 V를 계산할 수 있다.

$$V = \sum_{i=1}^{t} f(H(ID_i)) \prod_{j=1, j \neq i}^{t} \frac{-H(ID_j)}{H(ID_i) - H(ID_j)}$$

다음을 통해 메시지 M을 얻을 수 있다.

$$M = \frac{e(U, S_{ID_i} \cdot \prod_{j=1, j \neq i}^{k} H(ID_j))}{e(T, V)} W$$

단, IDs가 암호문을 생성할 때 지정한 사용자 집합의 부분집합이 아니거나, IDs의 크기가 임계치를 넘지 않을 경우 $\perp$을 출력한다.

- 정확성(Correctness) 다음을 통해 기법의 정확성을 확인할 수 있다.

$$\begin{aligned} & \frac{e(U, sk_{ID_i} \cdot \prod_{j=1, j \neq i}^{k} H(ID_j))}{e(T, V)} W \\ &= \frac{e(mP, sH(ID_1)\cdots H(ID_k))}{e(sP, mQ + mH(ID_1)\cdots H(ID_k))} W \\ &= \frac{e(mP, sH(ID_1)\cdots H(ID_k))}{e(sP, mH(ID_1)\cdots H(ID_k))} \frac{e(Q, sP)^m}{e(sP, mQ)} M \\ &= \frac{e(P, H(ID_1)\cdots H(ID_k))^{sm}}{e(P, H(ID_1)\cdots H(ID_k))^{sm}} M \\ &= M \end{aligned}$$

3.2 Xing과 Xu의 기법 분석

Xing과 Xu의 기법에서 $Setup$ 알고리즘은 위수가 소수 q인 덧셈군 $G_1 = <P>$와 곱셈군 G_2를 선택하고,

겹선형 함수 $e: G_1 \times G_1 \rightarrow G_2$와 해쉬함수 $H: \{0,1\}^* \rightarrow G_1^*$를 정의하고, *Encrypt* 알고리즘에서 $V = mQ + mH(ID_1)H(ID_2)\cdots H(ID_k)$를 계산한다. 따라서 기법의 정확성을 만족하기 위해 덧셈군과 곱셈군 사이에 Z_p와 Z_p^* 같은 $G_1^* \subset G_1$의 관계가 성립해야 한다.

본래 겹선형 함수는 유한체에서 이산대수문제를 쉽게 해결하기 위해 타원곡선군의 원소를 유한체의 원소로 맵핑(maping) 시키도록 만들어진 함수이므로 G_1은 타원 곡선군이 된다. 타원 곡선상에서 원소간의 곱셈은 정의하지 않기 때문에 G_1이 포함하는 곱셈군 G_1^*는 존재하지 않는다.

이에 해쉬함수 $H: \{0,1\}^* \rightarrow G_1$로 정의를 새롭게 가정한다. G_1은 덧셈군이므로 *Encrypt* 알고리즘에서 계산하는 $V = mQ + mH(ID_1)H(ID_2)\cdots H(ID_k)$는 다음과 같이 새롭게 정의할 수 있다.

$$V = mQ + mH(ID_1) + mH(ID_2) + \cdots + mH(ID_k)$$

새롭게 정의한 V에 따라 *Decrypt* 알고리즘은 복호화 과정에서 메시지 M을 얻기 위해 다음과 같은 과정을 수행한다.

$$M = \frac{e(U,\ sk_{ID_i} \sum_{j=1, j\neq i}^{k} H(ID_i))}{e(T,\ V)} W$$

- 이에 대한 정확성은 다음과 같다.

$$\frac{e(U,\ sk_{ID_i} + H(ID_1) + \cdots + H(ID_k))}{e(T,\ V)} W$$

$$= \frac{e(mP,\ sH(ID_i) + H(ID_1) + \cdots + H(ID_k))}{e(sP,\ mQ + mH(ID_1) + \cdots + mH(ID_k))} W$$

$$= \frac{e(mP,\ sH(ID_i) + \cdots + H(ID_k))}{e(sP, mH(ID_1) + \cdots + mH(ID_k))} \frac{W}{e(sP, mQ)}$$

$$= \frac{e(mP, H(ID_1)) \cdots e(mP, H(ID_k))}{e(sP, mH(ID_1)) \cdots e(sP, mH(ID_k))} \frac{e(Q,P)^{sm}}{e(P,Q)^{sm}} M$$

$$= \frac{e(mP, H(ID_1)) \cdots e(mP, H(ID_k)}{e(sP, mH(ID_1)) \cdots e(sP, mH(ID_k))} M$$

$$= \frac{e(P, mH(ID_1)) \cdots e(P, mH(ID_k)}{e(sP, mH(ID_1)) \cdots e(sP, mH(ID_k))} M$$

위 식에 따르면 각 사용자의 개인키 $sH(ID_1)$, $sH(ID_2), \cdots, sH(ID_k)$ 값 전체를 알고 있어야 복호화 할 수 있다. 각각의 사용자는 공개된 해쉬함수를 이용하여 다른 사용자의 해쉬값 $H(ID_i)$은 알 수 있지만 자신의 개인키를 제외한 다른 사용자들의 개인키는 알 수 없다. 따라서 Xing과 Xu가 제안한 ID기반 동적 임계 암호 시스템은 구조적으로 설계가 잘못되었음을 알 수 있다.

IV. 변환 방법

본 장에서는 IBE를 ID기반 동적 임계 암호 시스템으로 변환하는 방법을 제안한다.

4.1 제안하는 변환 방법

Xing과 Xu의 기법은 ID기반 임계 암호 시스템에서 동적인 기능을 추가하여 암호화 단계에서 인증된 수신자 집합의 크기, 임계치를 유연하게 변경하고자 하였다. 겹선형 함수를 이용하는 IBE와 Shamir[8]의 기법으로 같은 기능을 제공하는 기법을 설계 할 수 있다.

겹선형 함수를 이용하면서 $Setup_{IBE}$, $KeyGen_{IBE}$, $Encrypt_{IBE}$, $Decrypt_{IBE}$ 4개의 다항식 시간 알고리즘들로 구성된 IBE가 존재한다고 가정한다.

- $Setup(1^\lambda, N)$: $Setup_{IBE}$ 알고리즘을 이용하여 파라미터 $params_{IBE}$를 생성한다. 겹선형 함수를 이용하는 IBE이므로 파라미터 $params_{IBE}$는 겹선형 함수 $e: G_1 \times G_1 \rightarrow G_2$를 원소로 갖는다. 이때 덧셈군 G_1과 곱셈군 G_2는 동일한 위수 p를 가진다. IBE의 마스터 키를 mk로 하고, 암호학적 해쉬함수 $H_1 : \{0,1\}^* \rightarrow \{0,1\}^n$과 $H_2 : G_2 \rightarrow G_1$을 정의한다. 이러한 파라미터 $params_{IBE}$를 해쉬함수 H_1, H_2와 함께 파라미터 $params = (params_{IBE}, H_1, H_2)$로 출력한다.
- $KeyGen(params, ID_i, mk)$: $KeyGen_{IBE}$ 알고리즘을 이용하여 그룹의 각 사용자의 ID_i에 대응하는 개인키 sk_i를 생성한다.
- $Encrypt(params, \{ID_1, ..., ID_k\}, t, M)$: 일반성을 잃지 않고 송신자가 정하는 수신자의 집합을 $\{ID_1, ..., ID_k\}$라 하였을 때, 다음 과정을 통해 메시지 M에 대한 암호문 C를 생성한다.

1. $t-1$차 다항식 $f: \{0,1\}^n \rightarrow G_2$를 임의로 선택한다.

2. 각 사용자의 $ID_1,...,ID_k$의 함수값 $f(H_1(ID_1)),...,f(H_1(ID_k))\in G_2$를 $Encrypt_{IBE}$ 알고리즘에 입력하여 $f(H_1(ID_{i\in\{1,\cdots,k\}}))$에 대응하는 $C_{ID_{i\in\{1,\cdots,k\}}}$를 얻는다.
3. $H_2(f(0))=H$라 할 때 임의의 $s\in Z_p$를 선택하고 $Encrypt_{IBE}$ 알고리즘을 이용하여 얻은 암호문 $C_{ID_1},...,C_{ID_k}$로 메시지 M에 대한 암호문 C를 다음과 같이 출력한다.

$$\begin{aligned}C&=\left(e(H_2(f(0)),g)^sM,g^s,C_{ID_1},...,C_{ID_k}\right)\\&=\left(e(H,g)^sM,g^s,C_{ID_1},...,C_{ID_k}\right)\\&=\left(C_1,C_2,C_{ID_1},...,C_{ID_k}\right)\end{aligned}$$

- $Decrypt(params,IDs,C)$: 다음 과정을 통해 암호문 C에 대한 메시지 M을 출력한다.

1. 일반성을 잃지 않고 복호화에 참여하는 t명의 수신자의 아이디 집합을 $IDs=\{ID_1,ID_2,...,ID_t\}$라 하자. 각 수신자는 $Decrypt_{IBE}$ 알고리즘을 이용하여 $f(H_1(ID_i))$를 얻는다.
2. t명의 수신자들이 계산한 $f(H_1(ID_i))$ 값들로 Shamir 기법을 이용하여 $f(0)$를 계산한다.

$$f(0)=\sum_{i=1}^{t}f(H_1(ID_i))\cdot\prod_{i=1,i\neq j}^{t}\frac{-H_1(ID_j)}{H_1(ID_i)-H_1(ID_j)}$$

3. 계산한 $f(0)$와 $params$에 포함된 해쉬함수 H_2를 이용하여 $H_2(f(0))$를 계산한다.
4. 다음을 통해 메시지 M을 얻을 수 있다.

$$M=C_1\frac{1}{e(H,C_2')}$$

단, IDs가 암호문을 생성할 때 지정한 사용자 집합의 부분집합이 아니거나, IDs의 크기가 임계치를 넘지 않을 경우 $\perp$을 출력한다.

- 이에 대한 정확성은 다음과 같다.

$$\begin{aligned}C_1\frac{1}{e(H,C_2')}&=e(H,g)^sM\frac{1}{e(H,g^s)}\\&=e(H_2(f(0)),g)^sM\frac{1}{e(H_2(f(0)),g)^s}\\&=M\end{aligned}$$

4.2 Waters의 IBE[13]을 이용한 ID기반 동적 임계 암호 시스템

본 절에서는 4.1의 예로서 Waters의 IBE[13]를 이용하여 ID기반 동적 임계 암호 시스템으로 변환하는 방법을 설명한다.

Waters의 IBE에 따라 위수가 소수 p인 군 $G_1=<g>$와 군 G_2를 선택하고 겹선형 함수 $e:G_1\times G_1\rightarrow G_2$를 정의한다. 군의 크기는 보안 상수에 의해 결정된다. ID의 임의의 길이를 n의 길이로 출력하기 위해 암호학적 해쉬함수 $H_1:\{0,1\}^*\rightarrow\{0,1\}^n$을 정의한다.

- $Setup(1^\lambda,N)$: Waters IBE의 공개 파라미터는 $params_{IBE}=(g,g_1,g_2,u',U,e,H_1)$로 구성되어 있다. 이때 g는 위수가 소수 p인 덧셈군 G_1의 생성원이고, IBE의 마스터 키 mk가 $\alpha\in Z_p$일 때 g_1은 g^α, $g_2\in G_1$는 임의의 값이다. 임의의 값 $u'\in G_1$과 $u_i\in G_1$에 대해 U는 길이가 n인 벡터 $U=\{u_i\}_{i=1}^n$이다. 겹선형 함수를 $e:G_1\times G_1\rightarrow G_2$라 할 때 G_2는 곱셈군이다. $H_1:\{0,1\}^*\rightarrow\{0,1\}^n$은 임의의 길이 ID를 n의 길이로 출력하기 위한 암호학적 해쉬함수이다. 마스터 키 mk를 α라 하고, 암호학적 해쉬함수 $H_2:G_2\rightarrow G_1$를 정의한 뒤 파라미터 $params_{IBE}$와 해쉬함수 H_2를 함께 파라미터 $params=(params_{IBE},H_2)$로 출력한다.
- $KeyGen(params,ID_i,mk)$: Waters IBE의 $Extract_{IBE}$ 알고리즘을 이용하여 그룹의 사용자 ID_i에 대응하는 개인키 $sk_i=\left(g_2^\alpha(u'.\prod_{j\in V}u_j)^r,g^r\right)=(d_1,d_2)$를 생성한 뒤 출력한다. $r\in Z_p$는 임의의 값이다. 이때 $H_1(ID_i)_j$는 n 비트 길이의 $H_1(ID_i)$에서 j번째 비트를 의미하고 $V\subseteq\{1,...,n\}$는 $H_1(ID_i)_j=1$을 만족하는 j로 구성된 집합이다.
- $Encrypt(params,\{ID_1,...,ID_k\},t,M)$: 일반성을 잃지 않고 송신자가 정하는 수신자의 집합을 $\{ID_1,...,ID_k\}$라 하였을 때, 다음 과정을 통해 메시지 M에 대한 암호문을 생성한다.

1. $t-1$차 다항식 $f:\{0,1\}^n\rightarrow G_2$를 임의로 선택한다.
2. 각 사용자의 $ID_1,...,ID_k$에 대한 $f(H_1(ID_1)),...,f(H_1(ID_k))\in G_2$를 Waters IBE의 $Encrypt_{IBE}$ 알고리즘에 입력하여

$f(H_1(ID_{i\in\{1,\cdots,k\}}))$에 대응하는 C_{ID_i}를 다음과 같이 $C_{ID_i}=\left(e(g_1,g_2)^{s_i}f(H_1(ID_i)),g^{s_i},\left(u'\prod_{j\in V}u_j\right)^{s_i}\right)$ $=\left(\widehat{C_1},\widehat{C_2},\widehat{C_3}\right)$를 얻는다. 이때 $s_i\in Z_p$를 만족한다.

3. $H_2(f(0))=H$라 할 때 임의의 $s\in Z_p$를 선택하고 $Encrypt_{IBE}$ 알고리즘을 이용하여 얻은 암호문 $C_{ID_1},\ldots,C_{ID_k}$로 메시지 M에 대한 암호문 C를 다음과 같이 출력한다.

$$C=\left(e(H_2(f(0)),g)^sM,g^s,C_{ID_1},\ldots,C_{ID_k}\right)$$
$$=\left(e(H,g)^sM,g^s,C_{ID_1},\ldots,C_{ID_k}\right)$$
$$=\left(C_1,C_2,C_{ID_1},\ldots,C_{ID_k}\right)$$

- $Decrypt(params,IDs,C)$: 다음 과정을 통해 암호문 C에 대한 메시지 M을 출력한다.

1. 일반성을 잃지 않고 복호화에 참여하는 t명의 수신자의 아이디 집합 IDs을 $\{ID_1,ID_2,\ldots,ID_t\}$라 하자. 각 수신자는 $Decrypt_{IBE}$ 알고리즘을 이용하여 $f(H_1(ID_i))$값을 얻는다.

$$\widehat{C_1}\frac{e(d_2,\widehat{C_3})}{e(d_1,\widehat{C_2})}$$
$$=(e(g_1,g_2)^{s_i}f(H_1(ID_i)))\frac{e(g^r,(u'\prod_{j\in V}u_j)^{s_i})}{e(g_2^{\alpha}(u'\prod_{j\in V}u_j)^r,g^{s_i})}$$
$$=f(H_1(ID_i))$$

2. t명의 수신자들이 계산한 $f(H_1(ID_i))$ 값들로 Shamir 기법을 이용하여 다음과 같이 $f(0)$를 계산한다.

$$f(0)=\sum_{i=1}^{t}f(H_1(ID_i))\prod_{i=1,i\neq j}^{t}\frac{-H_1(ID_j)}{H_1(ID_i)-H_1(ID_j)}$$

3. 계산한 $f(0)$와 $params$에 포함된 H_2를 이용하여 $H_2(f(0))$를 계산한다.
4. $H_2(f(0))=H$이므로 다음을 통해 메시지 M을 얻을 수 있다.

$$M=C_1\frac{1}{e(H,C_2)}$$

단, IDs가 암호문을 생성할 때 지정한 사용자 집합의 부분집합이 아니거나, IDs의 크기가 임계치를 넘지 않을 경우 $\perp$을 출력한다.

V. 안전성 증명

4.1에서 제안한 방법으로 변환한 ID기반 동적 임계 암호 시스템은 겹선형 함수를 이용하고 CPA에 안전한 IBE의 존재 하에 CPA 안전성을 증명 할 수 있다. Waters IBE[13]는 위의 조건을 만족하는 기법 중 하나이므로 본장에서는 [13]을 기반으로 4.2에서 설계한 ID기반 동적 임계 암호 시스템이 IND-CPA가 만족함을 보인다.

정리. 제안 방법으로 IBE를 변환하여 설계한 ID기반 동적 임계 암호 시스템이 존재 하에 CPA 환경에서 의미 있는 확률로 암호문을 구별할 수 있는 공격자 A가 존재한다고 가정한다. A의 이점이 $Adv_{IDTE}^{CPA}[A]=\epsilon$일 때 ID기반 동적 임계 암호 시스템 시뮬레이터 B가 CPA환경에서 IBE의 암호문을 구별하는데 얻을 수 있는 이점의 최솟값은 $Adv_{IBE}^{CPA}[B]\geq\frac{1}{2}\epsilon$ 로 나타낼 수 있다.

증명. CPA 환경에서 제안한 ID기반 동적 임계 암호 시스템의 암호문을 의미 있는 확률로 구별 할 수 있는 공격자 A가 존재한다고 가정한다. A를 이용하여 IBE을 효율적으로 공격할 수 있는 시뮬레이터 B가 존재함을 보일 것이다. B의 목적은 IBE 시뮬레이터 Z에게 받은 암호문에 대해서 두 메시지를 구분 하는 것이다.

- $Setup$: 파라미터 $params$를 생성하기 위해 B는 Z에게 파라미터 $params_{IBE}=(g,g_1,g_2,u',U,e,H_1)$를 받는다. g는 위수가 소수 p인 덧셈군 G_1의 생성원이고, IBE의 마스터 키 mk가 $\alpha\in Z_p$일 때 g_1은 g^{α}, $g_2\in G_1$은 임의의 값이다. 임의의 값 $u'\in G_1$과 $u_i\in G_1$에 대해서 U는 길이가 n인 벡터 $U=\{u_i\}_{i=1}^n$이다. 겹선형 함수를 $e:G_1\times G_1\rightarrow G_2$라 할 때 G_2는 곱셈군이다. $H_1:\{0,1\}^*\rightarrow\{0,1\}^n$은 임의의 길이 ID를 n의 길이로 출력하기 위한 암호학적 해쉬함수이다. B는 암호학적 해쉬함수 $H_2:G_2\rightarrow G_1$를 정의하고 Z로부터 입력 받은 파라미터 $params_{IBE}$와 해쉬함수 H_2를 함께 파라미터

$params=(params_{IBE}, H_2)$로 A에게 반환한다.

- $Phase1$: B는 A의 오라클 질의들에 대한 응답을 다음과 같이 시뮬레이션 한다.
  - $Extract(ID=\{ID_1,...,ID_k\})$: A가 사용자들의 ID 집합에 대한 비밀키 sk를 요청할 때 B는 각 사용자의 $ID_1,...,ID_k$를 Z에게 각각 $KeyGen_{IBE}$ 오라클에 질의하여 대응하는 개인키 $sk_1,...,sk_k$를 Z에게 받는다. 개인키 sk_i는 다음과 같다.

$$sk_i=\left(g_2^{\alpha}(u'\prod_{j\in V}u_j)^r, g^r\right)$$

$r\in Z_p$는 임의의 값이다. 위의 $H_1(ID_i)_j$는 n 비트 길이의 $H_1(ID_i)$에서 j번째 비트를 의미하고 $V\subseteq\{1,...,n\}$는 $H_1(ID_i)_j=1$인 j로 구성된 집합이다. B는 Z에게 받은 개인키 sk_i들을 다음과 같이 개인키 집합 $SK=\{sk_1,...,sk_k\}$로 설정하여 A에게 반환한다.

- $Challenge$: A는 공개키로 사용할 ID 집합 $ID^*=\{ID_1,...,ID_l\}$과 임계치 t를 선택하고 챌린지 할 두 메시지 M_0, M_1을 선택하여 B에게 챌린지 메시지(ID^*, t, M_0, M_1)을 준다. 이때 $Phases1$에서 질의하는 ID들의 색인(index) 집합 $I:\{k|ID_k\in ID\}$에 대해서 $I_1=\bigcup I$라 하였을 때, 임계치 t는 부등식$|I_1\bigcap\{k|ID_k\in ID^*\}|<t$ 를 만족해야 한다. 즉, $Phases1$에서 질의한 모든 ID 중 t개 이상의 ID가 ID^* 집합의 원소가 될 수 없다. B는 A의 챌린지에 대한 응답을 다음과 같이 시뮬레이션 한다.

1. B는 임의로 $t-1$차 다항식 $f:\{0,1\}^n\rightarrow G_2$를 선택한다. 각 사용자의 $ID_1,...,ID_l$에 대응하는 $f(H_1(ID_1)),...,f(H_1(ID_l))\in G_2$를 계산한다. B는 챌린지 단계에서 A에게 받은 ID 집합 $\{ID_1^*,...,ID_l^*\}$ 중 $Phase1$에서 질의하지 않은 ID_i^*를 선택하고, 이를 계산한 $f(H_1(ID_i^*))$와 임의의 값 $R\in G_2$을 선택한다. 이때 $f(H_1(ID_i^*))$와 R은 $f(H_1(ID_i^*))=M_0^*$, $R=M_1^*$으로 각각 설정한다. B는 Z에게 챌린지 메시지 (ID_i^*, M_0^*, M_1^*)를 준다.
2. 다음과 같이 B는 챌린지 암호문 $C_{ID_i}^*=Encrypt_{IBE}(params_{IBE}, ID_i^*, M_b^*)$를 Z에게 받는다.

$$C_{ID_i}^*=\left(e(g_1,g_2)^{\beta}M_b^*), g^{\beta}, (u'\prod_{j\in V}u_j)^{\beta}\right)$$

이때 b^*는 $b^*\in\{0,1\}$이고, $\beta\in Z_p$는 임의의 값이다.

3. B는 ID 집합 $ID^*=\{ID_1^*,...,ID_l^*\}$ 중 ID_i^*를 제외한 나머지 $ID_{k\neq i}^*$에 대해 $f(H_1(ID_{k\neq i}^*))$의 암호문을 다음과 같이 시뮬레이션 한다. B는 임의의 $\gamma_k\in Z_p$를 선택하고 파라미터 $params$와 사용자의 $H_1(ID_k^*)$에 대한 $f(H_1(ID_k^*))$를 이용하여 암호문 $C_{ID_k^*}$를 다음과 같이 생성한다.

$$C_{ID_k^*}=\left(\begin{matrix}e(g_1,g_2)^{\gamma_k}f(H_1(ID_k^*)),\\ g^{\gamma_k}, (u'\prod_{j\in V}u_j)^{\gamma_k}\end{matrix}\right)$$

4. B는 $b\in\{0,1\}$와 임의의 $s\in Z_p$를 선택하고 Z에게 받은 암호문 $C_{ID_i}^*$와 B'가 생성한 암호문 $C_{ID_1^*},...,C_{ID_l^*}$으로 챌린지 메시지 M_b에 대한 암호문 C을 다음과 같이 생성하여 A에게 반환한다.

$$C=\left(\begin{matrix}e(H_2(f(0)),g)^sM_b, g^s,\\ C_{ID_1^*},...,C_{ID_l^*}^*,...,C_{ID_l^*}\end{matrix}\right)$$

- $Phase2$: 공격자 A는 시뮬레이터 Z에게 $Phase1$과 같은 질의를 한다. $Phase2$에서 질의하는 ID들의 색인 집합 $I':\{k|ID_k\in ID'\}$에 대해서 $I_2=\bigcup I'$라 하였을 때, 부등식$|(I_1\bigcup I_2)\bigcap\{k|ID_k\in ID^*\}|<t$를 만족하는 ID 집합에 대해서만 질의가 가능하다. 이와 같은 조건을 만족하면 A는 계속하여 질의를 요청할 수 있다.
- $Guess$: A는 자신이 추측한 비트값 $b'\in\{0,1\}$를 출력한다. B는 출력된 비트값 b'와 b를 비교하여 $b'=b$이면 Z에게 $b''=0$을 출력하고, 그렇지 않으면 $b''=1$를 출력한다.

위의 ID기반 동적 임계 암호 시스템 공격자 A의 이점을 $Adv_{IDTE}^{CPA}[A]=\epsilon$이라고 할 때, 가정에 의하여 A가 출력하는 b'와 ID기반 동적 임계 암호 시스템의 시뮬레이터 B'가 설정한 b가 서로 같거나 다를 경우에 대한 확률은 다음과 같다.

$$\Pr[b'=b]=\frac{1}{2}+\epsilon,\ \Pr[b'\neq b]=\frac{1}{2}-\epsilon$$

IBE 시뮬레이터 Z가 $b^* = 1$로 설정했을 때, B가 A에게 주는 암호문 C에 $|ID^*|-1$개의 IBE 암호문과 임의의 R값이 하나 포함되어 있다. 만약 $t = 1$일 때 확률 $1/|ID^*|$로 B는 A에게 실제와 같은 환경으로 시뮬레이션 할 수 없으며, 이 때 A의 이점을 모두 손실하게 된다. 따라서 A가 출력하는 b'와 B가 설정한 b가 서로 다를 경우에 대한 확률의 최솟값은 다음과 같다.

$$\Pr[b' \neq b | b^* = 1] \geq \left| \frac{|ID^*|-1}{|ID^*|}\left(\frac{1}{2}-\epsilon\right) + \frac{1}{|ID^*|}\frac{1}{2} \right| \geq \left| \frac{1}{2} - \left(\frac{1}{|ID^*|}-1\right)\epsilon \right|$$

Z가 $b^* = 0$으로 설정했을 때, B가 A에게 주는 암호문 C는 IBE 암호문 C^*_{ID}가 포함한 IBE 암호문으로 구성되어 있다. 따라서 B는 확률 $1/|ID^*|$로 A의 이점을 손실 없이 이용할 수 있다. 따라서 A가 출력하는 b'와 B가 설정한 b가 서로 같을 경우에 대한 확률의 최솟값은 다음과 같다.

$$\Pr[b' = b | b^* = 0] \geq \left| \frac{1}{2} + \frac{1}{|ID^*|}\epsilon \right|$$

시뮬레이터 B가 IBE 시뮬레이터 Z에게 받은 암호문에 대해서 두 메시지를 구분 하는데 얻을 수 있는 이점은 다음과 같은 확률 값으로 계산된다.

$$\begin{aligned} Adv^{CPA}_{IBE}[B] &= \left| \Pr[b'' = b^*] - \frac{1}{2} \right| \\ &= \left| \frac{1}{2}\Pr[b'' = b^* | b^* = 1] + \frac{1}{2}\Pr[b'' = b^* | b^* = 0] - \frac{1}{2} \right| \\ &= \left| \frac{1}{2}\Pr[b' \neq b | b^* = 1] + \frac{1}{2}\Pr[b' = b | b^* = 0] - \frac{1}{2} \right| \\ &\geq \frac{1}{2}\epsilon \end{aligned}$$

VI. 결 론

본 논문에서는 Xing과 Xu가 제안한 ID기반 동적 임계 암호 시스템을 분석하고 구조적인 문제점에 대해 설명했다. IBE와 Shamir의 기법을 이용하여 ID기반 동적 임계 암호 시스템으로 변환할 수 있는 방법을 제안하였다. 이는 CPA에 안전한 IBE의 존재 하에 CPA에 안전한 ID기반 동적 임계 암호 시스템을 설계 할 수 있음을 의미한다. 일반적인 임계 암호 시스템에서 암호문의 길이는 인증된 수신자의 집합 크기에 비례하여 선형적으로 증가하게 된다. 겹선형 함수 연산은 일반 곱 연산보다 몇 배의 계산량을 필요로 하기 때문에, 기법의 효율성을 증가시키는 것에 대한 연구는 임계 암호 시스템 분야에서 떠오르는 이슈라 할 수 있다. 특히 인증된 수신자의 집합 크기와 상관없이 암호문 길이가 항상 상수가 되도록 하는 기법은 향후 흥미로운 연구과제가 될 것이다.

참고문헌

〔1〕 Dan Boneh and Xavier Boyen, "Efficient selective-ID secure identity -based encryption without random oracles," Advances in Cryptology, EUROCRYPT '04, LNCS 3027, pp. 223-238, 2004.

〔2〕 Dan Boneh, Xavier Boyen, and Shai Halevi. "chosen ciphertext secure public-key threshold encryption without random oracles," CT-RSA'06, LNCS 3860, pp. 226-243, 2006.

〔3〕 Dan Boneh and Matt Franklin, "identity-based encryption from the weil pairing," Advances in Crypto- logy, CRYPT'01, LNCS 2139, pp. 213-229, 2001.

〔4〕 J. Baek and Y. Zheng, "identity-based threshold decryption," public-key Cryptography, PKC'04, LNCS 2947, pp. 262-276, 2004.

〔5〕 R. Canetti and S. Goldwasser, "An efficient threshold public-key cryptosystem secure against adaptive chosen ciphertext attack," Advances in Cryptology, EUROCRYPT'99, LNCS 1592, pp. 90-106, 1999.

〔6〕 Yvo Desmedt and Yair Frankel. "Threshold cryptosystems," Advances in Cryptology, CRYPTO'89, LNCS 435, pp. 307-315, 1990.

〔7〕 V. Daza, J. Herranz, P. Morillo, and C. Rtextmdafols, "CCA2-secure thre- shold broadcast encryption with shorter ciphertexts," Provable Sec- urity'07,

LNCS 4784, pp. 35-50, 2007.
〔8〕 Cécile Delerablée and David Pointcheval, "Dynamic threshold public-key encryption," Advances in Cryptology, CRYPTO'08, LNCS 5157, pp. 317-334, 2008.
〔9〕 B. Libert and J.-J. Quisquater, "Efficient revocation and threshold pairing based cryptosystems," ACM Symposium on Principles of Distributed Computing - PODC'03, pp. 163-171, July, 2003.
〔10〕 Adi Shamir, "How to share a secret." Communications of the ACM, pp. 612-613, Nov, 1979.
〔11〕 Adi Shamir, "Identity-based cryptosystems and signature schemes," Advances in Cryptology, LNCS 196, pp. 47-53, 1985.
〔12〕 Amit Sahai and Brent Waters, "Fuzzy identity-based encryption," Advances in Cryptology, EUROCRYPT'05, LNCS 3494, pp. 457-473, 2005.
〔13〕 Brent Waters, "Efficient identity- based encryption without random oracles," Advances in Cryptology, EUROCRYPT '05, LNCS 3494, pp. 114-127, 2005.
〔14〕 Jinghao Xing, Qiuliang Xu, "An identity-based group-oriented thresh- old encryption scheme," Anti- Counterfeiting, Security and Identification (ASID), 2011 IEEE, pp. 30-33, June, 2011.

〈著者紹介〉

김 미 령 (Milyoung Kim) 학생회원
2011년 2월: 숭실대학교 수학과 학사 졸업
2011년 2월~현재: 고려대학교 정보보호대학원 정보보호학과 석사과정
〈관심분야〉 정보보호이론, 암호 프로토콜, 프라이버시향상기술(PET)

김 효 승 (Hyoseung Kim) 학생회원
2010년 2월: 고려대학교 수학과 학사 졸업
2010년 2월~현재: 고려대학교 정보보호대학원 정보보호학과 석박사 통합과정
〈관심분야〉 정보보호이론, 암호 프로토콜, 경량인증 프로토콜

손 영 동 (Youngdong Son) 정회원
1986년: 한국경제신문 정보통신전문기자
2003년: KTH 상무이사/상임감사
2008년: 국가보안기술연구소 소장
2011년: 숭실대학교 IT정책경영학(박사)
2011~현재: 고려대학교 정보보호대학원 초빙교수
〈관심분야〉 사이버테러, 사이버전, 사이버심리전

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 정보보호대학원 교수
〈관심분야〉 정보보호이론, 암호 프로토콜, USN, 키 교환, 프라이버시향상기술(PET), 익명성 연구