효율적인 퍼지 아이디 기반 암호화 방법

Efficient Fuzzy Identity-Based Encryption Scheme

이 광 수*, 이 동 훈
(Kwangsu Lee and Dong-Hoon Lee)

Abstract: In this paper, we construct an efficient fuzzy identity-based encryption scheme in the random oracle model. The fuzzy identity-based encryption is an extension of identity-based encryption schemes where a user's public key is represented as his identity. Our construction requires constant number of bilinear map operations for decryption and the size of private key is small compared with the previous fuzzy identity-based encryption of Sahai-Waters. We also presents that our fuzzy identity-based encryption can be converted to attribute-based encryption schemes.

Keywords: Fuzzy identity-based encryption, Bilinear map

I. 서론

퍼지 아이디 기반 암호화(Fuzzy Identity-Based Encryption) 기법은 Sahai와 Waters에 의해서 소개 되었다 [5]. 퍼지 아이디 기반 암호화는 기존의 아이디 기반 암호화 기법 [2]을 확장한 것으로, 사용자의 아이디가 다수의 속성의 집합으로 구성되고 송신자가 선택한 속성과 수신자의 비밀키에 포함된 속성간의 공통값이 특정 임계치 이상인 경우 수신자가 암호문을 복호화하는 것이 가능한 기법이다.

Sahai와 Waters의 퍼지 아이디 기반 암호화 기법 이후, 퍼지 아이디 기반 암호화 기법에 대한 많은 연구가 진행되었다. Goyal 등은 퍼지 아이디 기반 암호화 기법을 확장하여 접근 권한 구조를 지원하는 속성 기반 암호화(Attribute-Based Encryption) 기법을 제시하였다 [3]. Bethencourt 등은 기존의 속성 기반 암호화가 사용자의 비밀키에 접근 권한 구조를 지정하는 것과 달리 암호문에 접근 권한 구조를 지정하는 것이 가능한 암호문-정책 속성 기반 암호화(Ciphertext-Policy Attribute-Based Encryption) 기법을 제안하였다 [1]. Ostrovsky 등은 속성 기반 암호화의 접근 권한 구조에 NOT 연산을 지원하도록 속성 기반 암호화를 확장하였다 [4].

본 논문에서는 효율적인 퍼지 아이디 기반 암호화 기법을 제시한다. 기존에 제시된 다양한 퍼지 아이디 기반 암호화 기법들의 경우 대부분 효율성에 가장 큰 영향을 미치는 bilinear 함수 연산의 횟수가 시스템 파라미터 값에 선형적으로 비례하여 증가했다. 하지만 본 논문의 기법은 고정된 횟수의 bilinear 함수 연산만을 이용하여 효율적으로 퍼지 아이디 기반 암호화 기법을 구성하는 것이 가능하다. 또한 사용자 비밀키 길이 역시 기존 기법에 비하여 더욱 짧다.

본 논문의 구성은 다음과 같다. 먼저 2절에서는 본 논문을 이해하는데 도움이 되는 배경 지식을 살펴본다. 3절에서는 본 논문에서 제안하는 퍼지 아이디 기반 암호화 기법을 설명하고 제안된 기법의 효율성을 분석한다. 4절에서는 퍼지 아이디 기반 암호화 기법을 확장하여 속성 기반 암호화 기법을 구성하는 것이 가능함을 보인다. 그리고 5절에서는 결론을 맺도록 한다.

* 책임저자(Corresponding Author)
논문접수 : 20xx. x. x., 채택확정 : 200x. x. xx.
이광수, 이동훈 : 고려대학교 정보경영공학전문대학원
(guspin@korea.ac.kr, donghlee@korea.ac.kr)
※ 본 연구는 지식경제부 및 정보통신연구위원회의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (IITA-2008-(C1090-0801-0025))

II. 배경 지식

이 절에서는 본 논문을 이해하기 위해서 필요한 배경 지식으로 bilinear 함수, lagrange 보간법에 대해서 설명한다.

1. Bilinear 함수

먼저 G 와 G_T 는 소수 위수 g 를 갖는 곱셉 순환군(multiplicative cyclic group)이다. 그리고 g 는 G 의 생성원이고 e 는 bilinear 함수로 $e: G \times G \rightarrow G_T$ 로 정의되고 다음의 성질을 가지는 함수이다.

- Bilinearity: 모든 $u, v \in G$ 와 $a, b \in Z_p^*$ 에 대해, $e(u^a, v^b) = e(u, v)^{ab}$ 가 성립한다.
- Non-degeneracy: 모든 $u, v \in G$ 에 대해, $e(u, v) \neq 1$ 이 성립한다.

만일 G 에서의 그룹 연산과 bilinear 함수 e 의 연산을 효율적으로 계산 가능한 경우 G 를 bilinear 그룹이라고 한다.

2. Lagrange 보간법

Lagrange 보간법은 주어진 $k+1$ 개의 좌표 정보 $(1, y_1)$, $(2, y_2)$, $\cdots$, $(k+1, y_{k+1})$ 를 이용하여 이들 점을 지나는 k 차 이하의 다항식을 다음과 같은 식으로 계산할 수 있다는 것이다.

$$q(x) = \sum_{1 \le i \le k+1} y_i \cdot \Delta_{i,N}(x)$$

이때 $N = \{1, 2, \cdots, k+1\}$ 이고 Lagrange 상수는 $\Delta_{i,N}(x) = \prod_{j \in N, j \neq i} \frac{x-j}{i-j}$ 와 같이 정의된다.

3. 퍼지 아이디 기반 암호화 보간법

퍼지 아이디 기반 암호화 기법은 다음과 같은 4가지 알고리즘으로 구성되어 있다.

- Setup: 보안 파라미터를 입력으로 받아 KGC의 공개 파라미터 PP와 마스터 비밀키 MK를 생성한다.
- KeyGen: 사용자의 속성 집합 w, 마스터 비밀키 MK를 입력으로 받아서 사용자의 비밀키 SK를 생성한다.
- Encrypt: 수신자의 속성 집합 w', 메시지 M, 공개 파라미터 PP를 입력으로 받아서 암호문 CT를 생성한다.
- Decrypt: 수신자의 속성이 w'으로 설정된 암호문 CT와 사용자 속성이 w인 비밀키 SK를 입력으로 받아서, $|w' \cap w| \geq d$ 경우 암호문을 복호화하여 메시지 M을 출력한다.

III. 퍼지 아이디 기반 암호화 기법

이 절에서는 효율적인 퍼지 아이디 기반 암호화 기법을 설명하고 기존에 제시된 다른 기법과 효율성을 비교한다.

1. 기법 설명

먼저 G 는 소수 위수 p 를 가지는 bilinear 그룹이고, $e: G \times G \rightarrow G_T$ 는 bilinear 함수로 정의된다. 이 경우 퍼지 아이디 기반 암호화 기법은 다음과 같다.

Setup(d): 설정 알고리즘은 시스템 파라미터 d 값을 입력으로 받고, 랜덤 $s \in Z_p^*$, $g_2 \in G$ 를 선택하고 해쉬 함수 $H: \{0,1\}^* \rightarrow G$ 를 선택한다. 이 경우 공개키 파라미터 PP 와 마스터 비밀키 MK 는 다음과 같이 설정된다.

$$PP = (g,\ g_1 = g^s,\ g_2,\ H)$$
$$MK = s$$

KeyGen(w, MK, PP): 비밀키 생성 알고리즘은 속성 집합 w, 마스터 비밀키 MK, 그리고 공개 파라미터 PP 를 입력으로 받는다. 먼저 $d-1$ 차 다항식 $q(x)$ 를 랜덤하게 선택하고 $q(0) = s$ 값이 되도록 설정한다. 이때 비밀키는 다음과 같이 계산된다.

$$SK_w = (w,\ \{D_{1,i} = g_2^{q(i)} H(i)^r\}_{i \in w},\ D_2 = g^r)$$

그리고 이때 r 은 Z_p 상의 랜덤 값이다.

Encrypt(w', M, PP): 암호화 알고리즘은 수신자의 속성 집합 w', 메시지 M 그리고 공개 파라미터 PP 를 입력으로 받는다. 메시지를 암호화하기 위해서 먼저 랜덤 값 $t \in Z_p$ 를 선택한 후 다음과 같이 암호문을 생성한다.

$$CT = (w',\ C_1 = g^t,\ \{C_{2,i} = H(i)^t\}_{i \in w'},$$
$$C_3 = M \cdot e(g_1, g_2)^t)$$

Decrypt(CT, SK_w, PP): 복호화 알고리즘은 암호문 $CT = (w', C_1, \{C_{2,i}\}, C_3)$, 속성 집합 w 에 대한 비밀키 $SK_w = (w, \{D_{1,i}\}, D_2)$, 그리고 공개 파라미터 PP 를 입력으로 받는다. 암호문을 복호화 하기 위해서 $|w' \cap w| \geq d$ 조건을 만족하는 집합 S 를 선택한다. 그런 뒤 복호화는 다음과 과정으로 이루어진다.

$$C_3 \cdot \frac{e(D_2, \prod_{i \in S} (C_{2,i})^{\Delta_{i,S}(0)})}{e(C_1, \prod_{i \in S} (D_{1,i})^{\Delta_{i,S}(0)})} = M$$

2. 올바름

제안된 퍼지 아이디 기반 암호화 기법이 올바르게 동작하는 것은 다음의 수식을 통해서 파악할 수 있다.

$$C_3 \cdot \frac{e(D_2, \prod_{i \in S} (C_{2,i})^{\Delta_{i,S}(0)})}{e(C_1, \prod_{i \in S} (D_{1,i})^{\Delta_{i,S}(0)})}$$
$$= C_3 \cdot \prod_{i \in S} \left(\frac{e(D_2, C_{2,i})}{e(C_1, D_{1,i})}\right)^{\Delta_{i,S}(0)}$$
$$= M \cdot e(g_1, g_2)^t \cdot \prod_{i \in S} \left(\frac{e(g^r, H(i)^t)}{e(g^t, g_2^{q(i)} H(i)^r)}\right)^{\Delta_{i,S}(0)}$$
$$= M \cdot e(g_1, g_2)^t \cdot \prod_{i \in S} \left(\frac{e(g^r, H(i)^t)}{e(g^t, g_2^{q(i)}) e(g^t, H(i)^r)}\right)^{\Delta_{i,S}(0)}$$
$$= M \cdot e(g, g_2)^{ts} \cdot \prod_{i \in S} e(g, g_2^{tq(i)\Delta_{i,S}(0)})^{-1}$$
$$= M$$

먼저 첫번째 등식은 bilinear 함수의 성질에 의해서 얻어진다. 그리고 마지막 등식은 lagrage 보간법에 의해서 숨겨진 다항식을 복원하는 것이 가능하기 때문에 성립한다.

3. 효율성 및 키 길이

퍼지 기반 암호화 기법의 효율성을 결정하는 것은 암호화 및 복호화 과정에서 사용되는 bilinear 함수 연산의 횟수이다. 본 논문에서 제안하는 기법은 암호화 과정의 경우, 미리 $e(g_1, g_2)$ 값을 계산해 두면 bilinear 함수 연산이 필요하지 않는다. 복호화 과정의 경우에는 단 두 번의 bilinear 함수 연산으로 복호화가 가능하다.

퍼지 기반 암호화 기법의 비밀키는 기존의 Sahai-Waters 기법의 경우 $2|w|$ 개의 비밀키 요소가 필요하다. 하지만 본 논문에서 제안하는 기법의 경우 $|w|+1$ 개의 비밀키 요소만 필요하다.

암호화 및 복호화시 필요한 bilinear 함수의 연산 횟수 그리고 비밀키 길이 두 가지 측면에서 본 논문에서 제안하는 기법은 기존 기법들 보다 더욱 우수함을 알 수 있다. 표 1은 기존 퍼지 아이디 기반 암호화 기법과 본 논문의 기법을 비교하고 있다.

Table 1. 효율성과 비밀키 길이 비교

	본 논문	SW05
bilinear 함수 연산	2	2d
비밀키 길이	$\|w\|+1$	$2\|w\|$

IV. 속성 기반 암호화 확장

속성 기반 암호화 기법은 퍼지 아이디 기반 암호화 기법을 확장하여 사용자의 비밀키에 접근 권한 구조를 지정하는 것이 가능한 암호화 기법이다. 퍼지 아이디 기반 암호화 기법 역시 속성 기반 암호화 기법의 특별한 형태로 하나의 임계치 노드만을 포함하는 속성 기반 암호화라고 볼 수 있다.

일반적인 접근 권한 구조를 지정하는 것이 가능한 속성 기반 암호화 기법은 Goyal 등에 의해서 소개되었다. Goyal 등이 제안한 방법은 접근 권한 구조를 접근 트리로 표현하고 개별 접근 트리의 노드 부분에 기존 퍼지 아이디 기반 암호화 기법과 유사하게 다항식을 랜덤하게 선택하여 전체 접근 트리의 잎 노드 부분에 해당하는 비밀키를 구성하여 속성 기반 암호화 구성이 가능하다고 보였다.

본 논문의 효율적인 퍼지 아이디 기반 암호화 기법 역시 Goyal 등이 제시한 방법을 이용하면 동일하게 속성 기반 암호화 기법으로 변환이 가능하다.

V. 결론

본 논문에서는 효율적인 퍼지 아이디 기반 암호화 기법을 제시하였다. 제시된 암호화 기법은 고정된 횟수의 bilinear 함수 연산만을 이용하는 최초의 퍼지 아이디 기반 암호화 기법이고 비밀키 길이 역시 기존의 기법에 비하여 더욱 작다. 또한 제안된 기법은 속성 기반 암호화 기법으로 변환이 가능하다.

참고문헌

[1] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," *IEEE Symposium on Security and Privacy*, pp. 321-334, 2007.

[2] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *CRYPTO*, pp. 213-229, 2001.

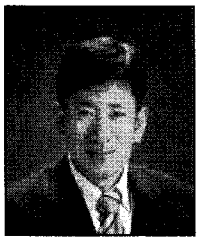
[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," *ACM Conference on Computer and Communications Security*, pp. 89-98, 2006.

[4] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," *ACM Conference on Computer and Communication Security*, pp. 195-203, 2007.

[5] A. Sahai and B. Waters, "Fuzzy identity-based encryption," *EUROCRYPT*, pp. 457-473, 2005.

이 광 수

1998년 연세대학교 컴퓨터과학과 졸업. 2000년 한국과학기술원 전산학과 석사 졸업. 2007년~현재 고려대학교 정보경영공학전문대학원 박사과정 재학중. 관심분야는 암호이론, 정보보호.



이 동 훈

1983년 고려대학교 경제학과 졸업. 1987년 University of Oklahoma, 전산학과 (공학석사). 1992년 University of Oklahoma, 전산학과 (공학박사). 1993년~현재 고려대학교 정보경영공학전문대학원 교수. 관심분야는 프로토콜 이론, 정보보호.