Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.1, Feb. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.1.17

ABE 스킴을 활용한 효율적인 공모자 추적 및 제외 스킴*

이 문 식,[1†] 이 주 희,[2‡] 홍 정 대[3]
[1]공군사관학교, [2]이화여자대학교 수리과학연구소, [3]국군기무사령부

An Efficient Public Trace and Revoke Scheme Using Augmented Broadcast Encryption Scheme*

MoonShik Lee,[1†] Juhee Lee,[2‡] JeoungDae Hong[3]
[1]Korea Air Force Academy,
[2]Institute of Mathematical Sciences, Ewha Womans University,
[3]Defense Security Command, Korea

요 약

본 논문에서는 효율적인 공개키 기반 공모자 추적 및 제외 스킴을 제안하고자 한다. 공모자 추적 및 제외 스킴은 암호 전송 스킴(Broadcast encryption scheme)에 공모자 추적과 제외 기능을 추가한 것으로 악의적인 사용자들이 유출한 개인키 또는 공모한 해적판 키를 시스템에서 제외함으로서 스킴의 안전성을 유지하는 것이다. 또한 제외 기능은 일부 사용자만을 위한 암호문을 만들 수 있어 다양한 응용 환경에 적용할 수 있는 스킴이다. 본 논문에서는 합성수 위수의 겹선형 군을 기반으로 설계된 스킴〔Augmented broadcast encryption scheme〕을 소수 위수의 겹선형 군을 기반으로 하는 스킴으로 변화시켰고, 효율성의 척도인 공개키, 개인키, 암호문의 크기를 크게 개선했다. 또한 제외 기능에 대한 분석을 통해 기존 논문의 제한적인 제외 기능을 충분한 제외 기능으로 확장하는 결과를 얻을 수 있었다. 본 논문에서 제안하는 스킴의 구조는 계층적 구조 또는 피라미드 구조를 갖는 우리나라 정부, 군 조직 등에 쉽게 적용 가능하다.

ABSTRACT

In this paper, we propose an efficient public key trace and revoke scheme. An trace and revoke scheme is a broadcast encryption scheme which has a tracing and revocation algorithm. It would maintain security of the scheme to revoke pirate keys which are colluded by malicious users. In addition, property of revocation can be applied to various circumstances because it can help cipher text delivered to certain users who are supposed to. In this paper, we would change the scheme[Augmented broadcast encryption scheme] based on the bilinear groups of the composite order into that of prime order and we can improve the size of public key, secret key, ciphertext considerably. Furthermore, we define property of revocation precisely, so we can obtain the result that the scheme with limited revocation can be expanded to have a full revocation. This paper can be easily applied to the organization such as government, military, which has a hierarchical structure.

Keywords: Broadcast Encryption Scheme, Traitor Tracing Scheme, Trace and Revoke Scheme, Augmented Broadcast Encryption Scheme, Bilinear map

Received(12. 18. 2015), Modified(02. 15. 2016), Accepted(02. 19. 2016)
* 본 연구는 한국연구재단 연구과제 (No.NRF-2012R1A1A3015819) 지원으로 수행하였습니다.
† 주저자, kafa0443@gmail.com
‡ 교신저자, juhee1108@ewha.ac.kr (Corresponding author)

I. 서 론

일반적으로 네트워크상에서는 디지털 콘텐츠 배포자(distributor)는 요금을 지불한 정당한 사용자만이 콘텐츠를 받아 볼 수 있도록 전송하고자 한다. 이를 위해 정당하지 않은 사용자의 콘텐츠에 대한 접근을 방지하기 위해 배포자는 콘텐츠를 암호화해서 전송하고, 복호화 키를 가지는 정당한 사용자만이 복호화 해서 콘텐츠를 감상, 청취 등을 할 수 있다. 이것을 가능하게 하는 암호학적 알고리즘을 암호 전송(Broadcast encryption)스킴이라 한다. 하지만 악의적인 사용자가 자신의 복호화(개인키)키를 이용하여 콘텐츠를 복호화 할 수 있는 다른 키를 만들거나, 서로 공모하여 복호화 할 수 있는 키를 만들어 이를 저장한 해적판 디코더(pirate decoder)를 만들 경우가 있다. 공모자 추적 알고리즘(Traitor Tracing Scheme 이하 : TT 스킴)의 목적은 해적판 디코더가 발견되었을 때, 해적판 디코더를 만들기 위해서 공모한 사용자(Traitor)를 찾아내는 것이다. TT 스킴이 "l-collusion resilient"라는 것은 l명 이하의 공모자가 해적판 디코더를 만들었을 때 적어도 한 명의 공모자를 추적할 수 있다는 것을 의미한다. 공모자의 수가 제한된 스킴 [2,4,8,13,15,17]들은 초기 연구에서 많이 제안되었는데 그 이유는 스킴을 다항식 기반으로 설계했기 때문이며, 이러한 다항식 기반 스킴들 중 일부 [17]는 선형 공격(linear attack)[14]에 의해 안전하지 않음이 증명되었다. 선형 공격은 공모자들의 개인키를 선형 결합(linear combination)해서 추적 알고리즘을 피할 수 있는 해적판 키(pirate key)를 생성하는 것이다. 최근에는 겹선형 함수(bilinear map)를 기반으로 스킴 [1,5,6,7,11,16]을 설계하여 공모자 수가 제한된 스킴의 문제점을 해결하였다. 이러한 스킴은 모든 사용자가 공모하더라도 적어도 한명은 추적할 있는 "*fully*-collusion resilient" 성질을 갖는다. 또한 대부분 스킴에서는 소수 위수의 겹선형 군을 사용하고 있으며, 몇몇 스킴[5,6]에서는 합성수 위수의 겹선형 군을 사용해서 설계되었다.

또한 TT 스킴의 공모자를 추적할 수 있는 추적 알고리즘에는 초기의 Black box confirmation 또는 Black box list의 방법을 사용해서 공모자로 예상되는 집합을 확인했으나 최근에는 적어도 한명을 반드시 추적할 수 있는 Black box tracing 알고리즘(이하 : 추적 알고리즘)을 사용하고 있다.

이러한 이유로 공모자 추적 개념에 유출되었을 거라 판단되는 키를 저장한 사용자는 복호화 할 수 없도록 제외해서 암호문을 전송하는 스킴이 연구되었다. 이러한 스킴에서는 해적판 키(pirate key)를 저장하고 있는 해적판 디코더는 더 이상 암호문을 복호화 할 수 없어 시스템의 안전성을 유지할 수 있다. 이러한 스킴을 Trace & Revoke 스킴(이하 : TR 스킴)[6,12,15,18]이라 한다. 즉 TR 스킴은 공모자의 키를 추적할 수도 있고, 추적된 키를 시스템으로부터 제거할 있는 스킴이며, 일부의 사용자들만을 위한 암호문을 만들 수 있는 스킴이다.

TR 스킴 중에서도 Binary tree를 사용한 D. Naor, M. Naor, Lotspiech[12]의 2001년 Crypto에서 발표된 "Revocation and tracing schemes for stateless receivers" 논문은 complete subtree method 방법을 사용해서 개인키는 $\log n$, 암호문은 $r\log(n/r)$의 크기를 갖고, subset difference method 방법을 사용해서 개인키는 $\log^2 n$, 암호문은 최대 $2r-1$의 크기를 갖는다. (여기서 n은 총 사용자 수이고, r은 제외하고 하는 사용자의 수이다.) 효율성이 상당히 좋음에도 불구하고 이 스킴은 공개키 스킴이 아닌 비밀키 스킴이라는 단점을 가지고 있어, 이를 공개키로 전환한 논문이 Y. Dodis, N. Fazio [18]의 "Public Key Broadcast encryption for stateless receivers"이다. 하지만 [18]논문은 공개키로 전환하기 위해 HIBE(Hierarchical ID- based encryption) 스킴을 사용했는데 이는 공개키를 third party라 할 수 있는 Public Key File(PKG)에 저장하고, 이를 HIBE 스킴이 크기를 $O(1)$으로 줄임으로써 가능하게 한 것이다.

Binary tree 구조를 사용하지 않는 이 분야(TT 스킴, TR 스킴)의 대표적인 논문은 D. Boneh, C. Gentry, B. Waters[7]가 2005년 Crypto에서 발표한 "Collusion resistant broadcast encryption with short ciphertexts and private keys" 와 D. Boneh, A. Sahai, B. Waters[5]가 2006년 Eurocrypt에서 발표한 "Fully collusion resistant traitor tracing with short ciphertexts and private keys"가 있다. 최근에는 A. Lewko, A. Sahai, B. Waters[1]가 2010년 IEEE Symposium on Security and Privacy에서 발표한 "Revocation Systems with Very Small Private Keys"와

D. Boneh, B. Waters, M. Zhandry[9]가 2014년 Crypto에서 발표한 "Low Overhead Broadcast encryption from Multi-linear maps" 이 있다.

이 중, D. Boneh, C. Gentry, B. Waters[7]가 2005년 Crypto에서 발표한 "Collusion resistant broadcast encryption with short ciphertexts and private keys"는 제안 논문과 같은 l-BDHE 복잡도 가정을 사용해서 암호문의 크기는 $O(\sqrt{N})$, 개인키 크기는 1개, 공개키는 $O(\sqrt{N})$, 복호화 연산량은 2번의 pairing 연산을 갖는다. 하지만 이 스킴은 TT 스킴이 아니라 Broadcast encryption 스킴이므로 해적판 디코더(pirate decoder)가 발견되었을 때 추적을 할 수 없는 단점을 가지고 있다.

또한 D. Boneh, A. Sahai, B. Waters[5]가 2006년 Eurocrypt에서 발표한 "Fully collusion resistant traitor tracing with short ciphertexts and private keys"는 본 논문에서 개선하고자 했던 [6]논문("A fully collusion resistant broadcast, trace and revoke system")의 기초가 되는 논문으로 Private linear broadcast encryption이란 이름으로 암호문의 크기는 $O(\sqrt{N})$, 개인키의 크기는 1개, 공개키의 크기는 $O(\sqrt{N})$, 복호화 연산량은 3번의 pairing 연산을 갖는다. 합성수 위수의 겹선형 군을 활용한 단점을 가지고 있지만 새로운 개념인 index hiding을 도입하고 스킴을 증명했다. 구체적으로 index hiding은 사용자마다 주어진 고유 위치를 index(예를 들면, i행, j열)로 표현하고, 암호문 생성할 때, 또는 추적 알고리즘을 적용할 때, 수신자 집합에 포함되는 사용자 index를 숨김으로써 악의적인 사용자 또는 해적판 디코더가 전송되는 암호문이 추적을 위한 암호문이라는 것을 알 수 없게 하는 것이다. 즉, 어느 index부터 복호화가 가능한지를 알 수 없게 하는 것이다.

그리고 [5]스킴을 [6]스킴으로 변화시키기 위해서는 revocation기능이 필요한데, 이를 위해서는 각 행과 열을 control 할 수 있어야 하기에 [5]스킴의 Private linear broadcast encryption개념을 확장해서 [6]의 Augmented broadcast encryption (ABE)개념으로 바꾼 것이다. Revocation기능을 추가함으로서 개인키의 크기는 $O(\sqrt{N})$으로 증가되었지만 복호화 연산량은 변함없이 3번의 pairing 연산을 갖는다. 하지만 [5]와 마찬가지로 합성수 위수의 겹선형 군을 사용함으로써 현실적으로 적용하기 어렵다는 문제를 가지고 있어 그 후, 합성수 위수의 겹선형 군을 소수 위수의 겹선형 군으로 바꾸려는 연구가 2010년 ACM CCS에서 발표된 "Building Efficient Fully Collusion- Resilient Traitor Tracing and Revocation Schemes"[16]이다. 이 스킴은 소수 위수의 겹선형 군을 사용하면서도 [6]의 암호문 크기를 1/2로 줄임으로써 암호화/복호화 연산속도를 더욱 빠르게 했다. 또한 2010년 Eurocrypt에서 발표된 "Converting Pairing-Based Cryptosystems from Composite-Order Groups to Prime-Order Groups"[11] 논문에서도 합성수 위수의 겹선형 군을 활용한 모든 스킴을 소수 위수의 겹선형 군으로 변환 할 수 있음을 보였으며, 그 중 [5]를 개선한 스킴도 포함하고 있다.

최근에는 A. Lewko, A. Sahai, B. Waters[1]가 2010년 IEEE Symposium on Security and Privacy에서 발표한 "Revocation Systems with Very Small Private Keys" 논문으로 효율성으로는 암호문의 크기는 $O(r)$, 공개키, 개인키의 크기는 모두 $O(1)$, 복호화 연산량은 $O(r)$번의 pairing 연산을 갖는다. 이 스킴은 Naor, Pinkas[15]가 2000년에 발표한 "Efficient Trace and Revoke Schemes"스킴을 응용해서 설계했는데 이는 라그랑주 보간법을 사용하는 것이다. 그리고 D. Boneh, B. Waters, M. Zhandry[9]가 2014년 Crypto에서 발표한 "Low Overhead Broadcast encryption from Multi - linear maps" 논문은 bilinear map이 아니라 multi - linear map을 사용해서 개인키와 암호문의 크기는 $O(1)$, 공개키의 크기는 $O(\log N)$, 복호화 연산량은 2번의 pairing 연산이 필요하게 되는 좋은 효율성에 도달했다.

결론적으로 제안하는 기법은 ABE 스킴[6]을 개선한 효율적인 공모자 추적 및 제외 스킴으로 우리나라의 sky-life와 같은 위성방송 또는 위성통신에 활용할 수 있는 응용 기법이다. ABE의 장점은 사용자 위치를 i행과 j열로 표현해서 개인키를 생성하고 수신자는 $(x > i \text{ or } x = i) \text{ and } y \geq j$ 인 위치의 사용자들만 복호화 할 수 있는 기법으로, 공개키, 개인키와 암호문 크기를 $O(\sqrt{N})$으로 기존 결과에 비해 크게 줄인 기법이다. 하지만 이러한 장점을 갖기 위

해 앞서 언급한 합성수 위수의 겹선형 군이 필요하고 연산량도 지수승 연산에 비해 훨씬 크기에 현실적으로 응용할 수 없는 기법이다. 따라서 제안하는 기법은 ABE스킴의 장점, 즉 공개키, 개인키, 암호문의 크기를 좀 더 줄이면서 소수 위수의 겹선형 군으로 설계한 스킴이다.

앞서 언급에서와 같이 [11,16]은 각각 [5,6]스킴을 개선한 논문이다. 이와 마찬가지로 제안 논문은 [6]를 개선한 논문으로 [16]과는 달리 가장 simple하고 새로운 복잡도 가정 없이 안정성을 증명할 수 있고 효율성을 개선한 스킴이다.

구체적으로 효율성 척도로는 [6]의 공개키, 암호문 크기를 절반 이상 줄였으며, [16]의 암호문 크기를 절반 이상 줄였다. 또한 복호화 연산량은 4번에서 3번의 pairing 연산으로 줄였다. 또한 본 논문에서는 [6,16]스킴이 가지는 제외 기능이 제한적인 제외(limited-revocation)기능을 갖고 있으므로 이를 간단히 언급하고 이를 개선한 충분한 제외(fully-revocation)기능을 갖는 스킴으로 설계했다.

II. 배경 지식

2.1 공모자 추적 및 제외 스킴의 정의(Definition)

일반적으로 TR 스킴은 초기화, 암호화, 복호화, 추적 알고리즘으로 구성되어 있으며, 세부 구조는 다음과 같다. 여기서 N은 총 사용자 수, S는 수신자 집합, $U=\{1,...,N\}$은 총 사용자 집합, 자연수 $i\ (1 \le i \le N)$는 각 사용자의 고유 인덱스(index)를 의미한다.

2.1.1 초기화(Set-up)

Set-up(N,λ) : N과 보안 파라미터 λ를 입력받아 공개키 PK와 마스터키 MK, 개인키 $SK_1,...,SK_N$를 출력하는 알고리즘이다. 여기서 공개키 PK는 시스템 서버에 저장하고 사용자가 암호화 과정에서 PK를 서버로부터 받는다.

2.1.2 암호화(Enc)

Enc(S,PK,M) : 수신자 집합 $S(\subset U)$, 공개키 PK, 메시지 M를 입력받아 암호문 CT_S을 출력하는 알고리즘이다. 암호문 CT_S은 집합 S에 포함되어 있는 사용자들만 복호화 할 수 있는 암호문이다.

2.1.3 복호화(Dec)

Dec(S,SK_j,CT_S) : 수신자 집합 S, 개인키 SK_j, 암호문을 입력받아 메시지 M 또는 임의의 값을 출력하는 알고리즘이다. 즉 사용자가 집합 S에 속한다면 자신의 개인키 SK_j를 가지고 암호문을 복호화 할 수 있다.

2.1.4 추적(Trace)

TR(X,PK,i,M) : 추적용 수신자 집합 $X(\subset U)$, 공개키 PK, 메시지 M, 인덱스 $i\ (1 \le i \le N)$를 입력받아 추적용 암호문 TR_X을 만드는 알고리즘이다. 추적용 암호문 TR_X은 $X=\{i,...,N\}$에 포함되어 있는 사용자만이 복호화 할 수 있는 암호문이다. 추적용 암호문과 일반 암호문의 차이점은 수신자 집합의 개념에 대한 차이로서 일반 암호문의 수신자 집합은 임의의 집합 S이고, 추적용 암호문의 수신자 집합은 인덱스 i에 대한 집합 $\{i,...,N\}$이다. 그리고 추적용 암호문 TR_X 은 추적 알고리즘에 입력된다.

따라서 TR 스킴은 임의의 사용자
$i \in \{1,...,N\}$와 메시지 M에 대해서
Set-up$(N,\lambda) \rightarrow PK, MK, SK_1,...,SK_N$ 출력하고,
Enc$(S,PK,M) \rightarrow$ 암호문 CT_S 출력하고,
Dec$(S,SK_j,CT_S)=M$ 을 만족한다.

2.2 겹선형 함수(Bilinear map)

G_1와 G_2는 위수를 소수 p로 갖는 곱셈 순환군이다. 그리고 g는 G_1의 생성원이고, e는 다음 조건을 만족하는 함수로 $e: G_1 \times G_1 \rightarrow G_2$ 를 겹선형 함수라 한다.

- **Bilinearity** : 임의의 $a, b \in Z_p^*$에 대해 $e(g^a,\ g^b)=e(g,\ g)^{ab}$ 가 성립한다.
- **Non-degeneracy** : $e(g,\ g) \neq 1$ 이 성립한다.
- **Efficient computability** : $e(g,\ g)$를 효율적으로 계산할 수 있는 알고리즘이 존재한다.

2.3 복잡도 가정(Complexity Assumption)

· Bilinear Diffie-Hellman Exponent Assumption

l-BDHE 문제는 $T=(h,g,g^{\alpha},...,g^{\alpha^{l-1}},g^{\alpha^{l+1}},...,g^{\alpha^{2l}})$ 가 주어졌을 때, $e(h,g)^{\alpha^{l}} \in G_2$을 계산하는 것이다. 여기서 $h,g \in G_1$ 이다. l-BDHE 문제를 푸는 알고리즘 A가 $|\mathbf{Pr}[A(T)=e(h,g)^{\alpha^{l}}]| \geq \epsilon$ 을 만족하면 ϵ 이익을 갖는다고 한다. 그리고 $g_i = g^{\alpha^i}, i=1,...,2l$ 와 $g_{\alpha,l}=(g_1,...,g_{l-1},g_{l+1},...,g_{2l})$ 라 정의하자. 또한 $T=(h,g,g_{\alpha,l},e(g,h)^{\alpha^{l}})$, $W=(h,g,g_{\alpha,l},w)$일 때, decision l-BDHE 문제를 푸는 알고리즘 B가 $|\mathbf{Pr}[B(T)=0]-\mathbf{Pr}[B(W)=0]| \geq \epsilon$ 을 만족하면 ϵ 이익을 갖는다고 한다. 여기서 $w=e(g,h)^{z} \in G_2$ 이고 임의의 $z \in Z_p$이다.

정의 1. 다항식 t시간 안에 적어도 이익 ϵ을 갖고 decision l-BDHE 문제를 푸는 알고리즘이 존재하지 않는다면, decision (t,ϵ,l)-BDHE 가정은 유효하다.

2.4 안전성 게임(Security Game)

제안하는 알고리즘은 다음 게임을 사용해서 안전성을 정의한다.

· Semantic Security Game

이 게임은 개인키가 없는 사용자는 암호문을 복호화하지 못한다는 기본적인 게임이다.

- **초기화** : 도전자는 **Set-up**알고리즘을 수행해서 공격자 A에게 PK와 개인키 $SK_1,...,SK_N$ 준다.
- **도전** : 공격자 A는 메시지 M_0, M_1을 만들어 도전자에게 준다. 도전자는 $b \in \{0,1\}$을 선택해서 공격자 A에게 암호문 $\mathbf{Enc}(S,PK,M_b)$ 준다. 여기서 수신자 집합 $S \cap U = \{\varnothing\}$ 이다.
- **추측** : 공격자 A는 $b' \in \{0,1\}$을 추측한다.

이 게임에서 공격자 A의 이익을
$Adv_{SS} = |\mathbf{Pr}|b'=b| - 1/2|$ 이라 하자.

Semantic Security Game은 제안 스킴의 안전성을 공격하려는 공격자에게 시스템의 모든 정보(파라미터, 공개키, 모든 개인키)를 다 주어도 공격자는 수신자 집합이 $S \cap U = \{\varnothing\}$인 암호문을 복호화 할 수 없다는 것을 증명하는 것이다.

예를 들어 $S=\{u\}, u \notin U$ 이고, 도전자가 u에게 개인키 SK를 주었다고 가정하고 수신자 집합 S를 위한 암호문을 만들었다면 이는 오직 u만이 복호화 할 수 있다는 것이다. 만일 공격자의 능력이 대단해서 주어진 공개키 PK, 개인키 $SK_1,...,SK_n$를 이용해서 암호문을 복호화 할 수 있는 $SK \notin \{SK_1,...,SK_n\}$을 만든다면 제안하는 기법은 안전하지 않다. 그러한 경우, 공격자의 이익은 1/2보다 많다고 정의한다.

· 추적성 게임(Traceability Game)

이 게임은 해적판 디코더(pirate decoder)에 저장되어 있는 공모자의 키를 찾는 게임이다.

- 도전자는 **Set-up** 알고리즘을 수행해서 공격자 A에게 PK와 개인키 집합 $\{SK_1,...,SK_N\}$ 준다.
- 공격자 A는 공모자 집합 $S_D=\{i_1,...,i_t\} \subseteq U$을 생성한다.
- 공격자 A는 공모자 키가 저장된 해적판 디코더 D 를 생성한다.
- 도전자는 추적 알고리즘을 수행해서 집합 $T \subseteq \{1,...,N\}$ 를 얻는다.
  만일 다음 두 조건을 만족하면 공격자 A는 위의 게임에서 이겼다고 한다.

  i. 임의의 메시지 M에 대해서 $\mathbf{Pr}[D(Enc(S_D,PK,M))=M] \geq \epsilon$ 만족한다.

  ii. $T=\{\varnothing\}$ 이거나 $T \not\subset S_D \cap \{1,...,N\}$이다.

  공격자 A가 이길 확률을 Adv_{TR} 이라 하자.

일반적으로 TT 스킴에서는 암호문 $\mathrm{Enc}(S,PK,M)$과 추적용 암호문 $\mathrm{TR}(X,PK,i,M)$의 구별 불가능을 증명해야 하지만 TR 스킴은 암호문에 제외 기능을 포함하고 있어, 해적판 디코더의 입장에서는 추적 과정과 정상적인 암호문 전송 과정을 구별할 수 없으므로 구별 불가능(indistinguishability)은 증명할 필요가 없다.

정의 2. 다항식 시간 동안과 $\epsilon > 0$에 대해서 공격자의 Adv_{TR} 과 Adv_{SS} 이 λ에 대해서 무시할 만 한 정도(negligible)라면 제안하는 스킴은 안전하다.

III. 제안 스킴

3.1 초기화(Set-up)

시스템 매니저는 총 사용자를 $N=m^2$ 명이라고 가정하고 사용자 집합을 $U=\{1,...,N\}$ 이라 하자. 그리고 소수 p의 위수를 가지는 그룹 G_1, G_2에 대해서 겹선형 사상 $e: G_1 \times G_1 \rightarrow G_2$ 가 있다고 가정하자. 임의의 생성원 $g \in G_1$과 임의의 $\alpha \in Z_p$를 생성하고 또한 임의의 $u_1,...,u_m, v_1,...,v_m \in G_1$과 $r_1,...,r_m, c_1,...,c_m \in Z_p$를 선택하여 다음과 같이 공개키 PK, 마스터키 MK를 생성한다.

$$PK = \begin{bmatrix} u_1,...,u_m,\ v_1,...,v_m, \\ g^{r_1},...,g^{r_m}, g^{c_1},...,g^{c_m}, \\ g,\ e(g,g)^{\alpha} \end{bmatrix},\ MK=\{\alpha\}$$

본 알고리즘에서 필요로 하는 공개키 PK의 크기는 $4m+2$이다. 여기서 $m=\sqrt{N}$이다.

개인키를 생성하기 위해서 먼저 $m \times m$ 행렬을 만들고 각 사용자를 행렬에서 $1 \le x, y \le m$ 을 만족하는 (x,y)위치에 일대일 대응시킨다. 즉 첫 번째 사용자는 $(1,1)$위치에 마지막 사용자는 (m,m)에 대응시킨다. 그리고 자연수 $i=(x-1)m+y$ 을 만족하는 i를 인덱스(index)라 정의하면 사용자는 인덱스 i 또는 순서쌍 (x,y)을 갖는다. 인덱스 i를 갖는 사용자의 개인키 SK_i는 임의의 $ID_i \in Z_p$ 을 선택하여 다음과 같이 생성한다.

$$SK_i = \begin{bmatrix} K_i = g^{\alpha}\, g^{r_x c_y} (u_x v_y)^{ID_i},\ I_i = g^{ID_i}, \\ V_i = \left\{ v_1^{ID_i}, ..., v_{y-1}^{ID_i}, v_{y+1}^{ID_i}, ..., v_m^{ID_i} \right\} \end{bmatrix}$$

여기서 V_i의 원소들은 제외 기능에 필요한 역할을 한다. 각 사용자들이 저장해야 하는 개인키 SK의 크기는 $m+1$이다.

예를 들면, 사용자 i의 인덱스를 $(2,3)$이라 가정하면 $i=(2-1)m+3=m+3$ 이므로 사용자 i의 개인키는 다음과 같다. 여기서 $m=10$이라 가정한다.

$$SK_i = \begin{bmatrix} K_i = g^{\alpha}\, g^{r_2 c_3} (u_2 v_3)^{ID_i},\ I_i = g^{ID_i}, \\ V_i = \left\{ v_1^{ID_i}, v_2^{ID_i}, v_4^{ID_i}, ..., v_{10}^{ID_i} \right\} \end{bmatrix}$$

K_i에는 v_3만 곱해져 있고, V_i에는 v_3만 없다.

3.2 암호화(Enc)

먼저 수신자 집합 $S=U=\{1,...,N\}$ 인 경우, 즉 수신자의 집합이 모든 사용자인 경우는 임의의 $s, t \in Z_p$ 를 선택해서 암호문 CT_S 를 다음과 같이 생성한다.

$$\begin{bmatrix} R_1 = g^{r_1 s},..., \ R_m = g^{r_m s}, \\ C_1 = g^{c_1 t},..., \ C_m = g^{c_m t}, D = g^{st}, \\ B_1 = \left(u_1 \prod_{j \in S_1} v_j\right)^{st}, ..., B_m = \left(u_m \prod_{j \in S_m} v_j\right)^{st}, \\ A = M \cdot e(g,g)^{\alpha st} \end{bmatrix}$$

$$= \begin{bmatrix} R_1,...,R_m, C_1,...,C_m, D, \\ B_1,...,B_m, A \end{bmatrix}$$

수신자 집합 $S \subset U$ 인 경우, 즉 제외하고자 하는 수신자가 있는 경우는 다음과 같은 절차를 따른다. 먼저 집합 $U_i \subset U (1 \le i \le m)$ 를 $m \times m$ 행렬의 i번째 행에 포함된 사용자들의 부분집합이라 하자. 메시지 M을 수신자 집합 S 에게 전송하기 위해서 집합 $S_i = S \cap U_i$ ($1 \le i \le m$) 를 찾는다.

만약 $S_i=\{\varnothing\}$ 이면 임의의 $s, t, z_i \in Z_p$ 를 선택해서 먼저 $R_i = g^{z_i s}$ 를 생성한다. 그리고 B_i를 생성하기 위해서 $U_i=\{(i,j_1),...,(i,j_m)\}$순서쌍 중에서 임의의 열 원소를 선택한 집합 $\widetilde{S}_i=\{(i,j_1),...,(i,j_k)\}$ 를 선택해서 $B_i=(u_i \prod_{j \in \widetilde{S}_i} v_j)^{st}$ 를 생성한다. $|\widetilde{S}_i| \neq 0$이다. 즉, 집합 전체를 제외시키기 위해서는 R_i, B_i를 임의의 값으로 대체하면 된다.

만약 $S_i=\{(i,j_1),...,(i,j_k)\} \neq \{\varnothing\}, (k<m)$ 이

면 임의의 $s, t \in Z_p$ 를 선택해서 $R_i = g^{r_i s}$ 를 생성한다. 순서쌍의 S_i의 열 원소 $j_1, ..., j_k$에 대응하는 공개키 $v_{j_1}, ..., v_{j_k}$를 이용하여 $B_i = (u_i v_{j_1} \cdots v_{j_k})^{st}$ 를 생성한다.

$S_i = \{\varnothing\}$ 인 경우를 집합 제외(set revocation)라 하고 $S_i \neq \{\varnothing\}$ 인 경우를 열 원소 제외(column revocation)이라 하자. 본 논문에서 집합 제외 기능은 암호문에서 $R_i = g^{r_i s}$를 임의의 $R_i = g^{z_i s}$으로 교체함으로 얻어지고, 열 원소 제외 기능은 암호문 중 B_i의 v_i $(i \in S_i)$ 원소를 포함/제외함으로서 얻어진다. 암호문의 크기는 $3m+2$개의 크기를 갖는다.

3.3 복호화(Dec)

인덱스 $i = (x-1)m + y$를 가진 사용자가 수신자 집합 $S_x = \{(x, j_1), ..., (x, j_k)\}$에 포함된다면 S_x의 열 원소 $j_1, ..., j_k$에 대응하는 개인키의 $v_{j_1}^{ID_i}, ..., v_{j_k}^{ID_i}$ 를 이용해서 다음을 먼저 계산한다.

$$K_i' = K_i \cdot \prod_{j \in S_x} v_j^{ID_i} = g^{\alpha + r_x c_y} (u_x v_y)^{ID_i} \prod_{j \in S_x} v_j^{ID_i}$$

그리고 자신의 행, 열에 해당하는 암호문 속의 원소 $R_x = g^{r_x s}$, $C_y = g^{c_y t}$, $B_x = \left(u_x \prod_{j \in S_x} v_j\right)^{st}$ 를 이용하여, 다음 복호화 식을 통해 메시지 M을 구한다.

$$M = A \cdot \frac{e(R_x, C_y) \cdot e(B_x, I_i)}{e(K_i', D)}$$

위의 식에서 겹선형 부분만 계산하면 다음과 같다.

$$\frac{e(R_x, C_y)\ e(B_x, I_i)}{e(K_i', D)}$$

$$= \frac{e(g^{r_x s}, g^{c_y t})\ e((u_x \prod_{j \in S_x} v_j)^{st}, g^{ID_i})}{e(g^{\alpha + r_x c_y} (u_x v_y)^{ID_i} \prod_{\substack{j \in S_x \\ y \notin S_x}} v_j^{ID_i}, g^{st})}$$

$$= \frac{e(g,g)^{r_x c_y st}\, e((u_x \prod_{j \in S_x} v_j), g)^{st\, ID_i}}{e(g,g)^{\alpha st}\, e(g,g)^{r_x c_y st}\, e((u_x \prod_{j \in S_x} v_j), g)^{st\, ID_i}}$$

$$= \frac{1}{e(g,g)^{\alpha st}}$$

따라서 $M = M \cdot e(g, g)^{\alpha st} \cdot \frac{1}{e(g, g)^{\alpha st}}$

복호화에 필요한 연산량은 3번의 pairing 연산과 K_i'를 계산하기 위해 $S_x = \{(x, j_1), ..., (x, j_k)\}$의 열 원소 정보$(j_1, ..., j_k)$를 알고 있다는 가정 하에 최대 $m-1$번의 곱셈 연산이 필요하다.

예를 들어, 사용자 i의 인덱스를 $(2,3)$이라 가정하면 개인키는 다음과 같고

$$SK_i = \left[\begin{array}{l} K_i = g^{\alpha}\, g^{r_2 c_3} (u_2 v_3)^{ID_i},\ I_i = g^{ID_i}, \\ V_i = \left\{ v_1^{ID_i}, v_2^{ID_i}, v_4^{ID_i}, ..., v_{10}^{ID_i} \right\} \end{array} \right]$$

만일 암호문 중 B_2가 다음과 같다면

$$\left[B_2 = \left(u_2 \prod_{j \in S_1} v_j\right)^{st} = (u_2 v_1 v_2 v_3 v_4)^{st} \right]$$

사용자 i는 자신의 V_i에 있는 $v_1^{ID_i}, v_2^{ID_i}, v_4^{ID_i}$를 가지고 $\prod_{j \in S_x} v_j^{ID_i} = v_1^{ID_i} v_2^{ID_i} v_4^{ID_i}$ 을 계산하고, 자신의 개인키 중 $K_i = g^{\alpha + r_2 c_3} (u_2 v_3)^{ID_i}$와 곱해서 K_i'을 계산한다. 즉,

$$K_i \cdot \prod_{j \in S_x} v_j^{ID_i} = g^{\alpha + r_2 c_3} (u_2 v_3)^{ID_i} v_1^{ID_i} v_2^{ID_i} v_4^{ID_i}$$

$$= g^{\alpha + r_2 c_3} (u_2 v_1 v_2 v_3 v_4)^{ID_i} = K_i'$$

하지만 암호문 중 B_2에 v_3원소가 없다면, 즉

$$\left[B_2 = \left(u_2 \prod_{j \in S_1} v_j\right)^{st} = (u_2 v_1 v_2 v_4)^{st} \right]$$

라면, 사용자 i는 K_i에 v_3원소를 포함하고 있어 v_3

를 삭제할 방법이 없어 메시지 M을 복호화 할 수 없다.

3.3.1 [6] 스킴의 제한적인 제외 기능

스킴이 충분한 제외 기능을 갖는다는 것은 임의의 수신자 집합 $S(\subseteq U)$ 에 대한 암호문을 생성할 수 있다는 것을 의미한다. 본 논문에서는 수신자 집합 S를 $S_i = S \cap U_i \ (1 \le i \le m)$ 로 분리해서 각 S_i에 해당하는 암호문 B_i를 생성함으로서 임의의 사용자를 제외하는 암호문을 생성할 수 있어 충분한 제외 기능을 달성 할 수 있었다. 하지만 본 논문이 개선하려는 [6]스킴은 충분한 제외 기능이 아닌 제한적 제외 기능임을 간단히 설명한다.

[6]스킴과 본 스킴은 사용자 집합을 $m \times m$ 행렬로 대응시켜 행렬의 원소마다 서로 다른 사용자를 대응시킨다. [6]스킴의 암호문 $CT_{(i,j)}$는 $x > i$ 또는 $x = i$와 $y \ge j$을 만족하는 인덱스 $u = (x-1)m + y$인 사용자들만, 즉 수신자 집합 $S = \{u, u+1, ..., n\}$만이 복호화 할 수 있는 암호문을 의미한다.

만일 암호문 $CT_{(i,j)}$에 수신자 집합 S를 설정한다면 복호화 할 수 있는 사용자 집합은 $S \cap \{u, ...N\}$이다. 결국 인덱스로 정해진 집합 $\{u, ..., N\}$중에서 몇몇 사용자를 제외 할 수 있는 제한적인 제외 기능을 갖는 스킴이다. 하지만 제한적인 제외 기능은 암호문을 항상 $CT_{(1,1)}$로 설정한다면 해결할 수 있다. 이는 [6]스킴에서 언급하고 있다. 즉, 암호문 $CT_{(1,1)}$은 수신자 집합 S와 인덱스 집합 $\{1, ..., N\}$과의 교집합 $S \cap \{1, ...N\}$이므로 충분한 제외 기능을 갖는다. 하지만 [6]스킴의 암호화 알고리즘을 따라 암호문 $CT_{(1,1)}$을 생성하면 다음과 같다.

$$CT_{(1,1)} = \left[\begin{array}{l} x > 1 : T_x = \left(\prod_{k \in S_x} U_{q,k} \right)^{s_x t}, \cdots, \\ \\ x = 1 : T_1 = \left(\prod_{k \in S_1} U_k \right)^{s_1 t} \ , \cdots \end{array} \right]$$

여기서 T_x를 생성하는데 사용되는 U_k 또는 $U_{q,k}$ 원소는 본 논문의 열 원소를 제어하는 v_k 역할과 같다. 따라서 사용자가 암호문을 복호화하기 위해서는 T_x 원소 내에 어떤 U_k 또는 $U_{q,k}$ 원소가 사용되었는지 알아야 자신의 개인키 원소 V_i 중 다음을

$$K_i' = K_i \cdot \prod_{j \in S_x} U_j^{ID_i} \quad \text{또는} \quad K_i' = K_i \cdot \prod_{j \in S_x} U_{q,j}^{ID_i}$$

을 계산할 수 있다. 하지만 T_x를 생성하는데 어떤 U_k 또는 $U_{q,k}$ 원소가 사용되는지 정보가 없다면 사용자는 자신의 개인키 $m-1$개의 v_i원소 중 몇 개가 T_x를 생성하는데 사용되었는지 알기 위해 최대 ${}_{m-1}C_{m-2} + {}_{m-1}C_{m-3} + \cdots + {}_{m-1}C_1$ 의 곱셈 연산과 이에 따르는 겹선형 연산을 반복해야 한다. 따라서 암호문에는 사용자 집합 S와 S_x에 대한 정보가 반드시 포함되어야 한다. 즉, 어떤 U_k, $U_{q,k}$가 사용되었는지 반드시 알아야 한다.

만일 수신자 집합 $S_x = \{\varnothing\}$이라면 S_x에 포함되는 U_k 또는 $U_{q,k}$ 원소가 없기 때문에 T_x는 항상 고정된 값($\perp$)을 갖는다. 즉 고정된 T_x의 값은 [6]스킴에서 사용자에 대한 정보(행렬의 위치와 집합 $S_x = \{\varnothing\}$)를 노출 할 수 있다.

더욱이 [6]스킴에서 추적 알고리즘을 사용하기 위해 암호문 $CT_{(i,j)}$을 생성한다면 T_x는 $x > i$ 또는 $x = i$와 $y \ge j$을 만족하는 사용자가 복호화 하도록 $T_x = (U_{q,1} \cdots U_{q,m})^{s_x t}$ 또는 $T_x = (U_1 \cdots U_m)^{s_x t}$ 와 같이 생성해야 한다. 즉, 집합 $U_i, U_{q,i} (1 \le i \le m)$의 모든 원소를 T_x에 포함시켜야 한다. 그렇지 않으면 추적 알고리즘의 출력값에 대한 올바른 분석이 어렵다. 따라서 추적 알고리즘 과정 중 수신자 집합에 대한 정보가 노출될 수 있다는 것은 [6]스킴에서 가정한 statelss 디코더가 아닌 stateful 디코더의 경우에는 anti -detectable 한 방법을 적용해서 추적을 회피할 수도 있다는 것을 의미한다.

결국 암호문을 복호화 할 때에는 어떤 U_k 또는 $U_{q,k}$ 원소가 T_x를 생성하는데 사용되는지의 정보와 추적 알고리즘에서는 모든 U_k 또는 $U_{q,k}$가 T_x를 생성하는데 반드시 포함되어야 한다는 사실을 통해 해적판 디코더는 추적 중이라는 사실을 판단 또는 유추 할 수 있어, 결과적으로 [6]스킴은 인덱스 숨김(index hiding) 기능은 유지하고 있지만 추적 중이라는 사실을 부분적으로 노출하는 문제를 갖고 있다.

3.4 추적(Tracing)

추적 알고리즘은 악의적인 사용자가 자신의 개인

키를 유출 또는 공모해서 복호화 할 수 있는 해적판 디코더를 만들었을 때, 이를 분해하지 않고 추적용 암호문 TR_X을 추적 알고리즘에 입력해서 나온 출력을 분석함으로써 저장된 키를 찾는 것으로 절차는 다음과 같다.

Step 1. 모든 $u,(1 \le u \le N+1)$에 대해서 다음 과정을 반복한다.
- **Step 1.1**. 먼저 $ctr_u = 0$으로 초기화한다.
- **Step 1.2**. $X := \{u,...,N\}$ 를 수신자 집합이라 한다.
- **Step 1.3**. 다음 과정을 m번 테스트 한다.
  - ⅰ. 암호문 TR_X을 만든다.
  - ⅱ. 암호문 TR_X을 해적판 디코더에 입력한다.
  - ⅲ. 해적판 디코더가 올바르게 M을 구하면 ctr_u를 ctr_u+1로 증가시킨다.
  - ⅳ. $\widehat{p_u} = ctr_u/m$ 로 정의한다.

Step 2. $\widehat{p_u} - \widehat{p}_{u+1} \ge \epsilon/(4N)$ 을 만족하는 집합 $T \subseteq \{1,...,N\}$ 를 찾고, 이 중에 $\widehat{p_u} - \widehat{p}_{u+1}$가 최대가 되는 인덱스 $u \in T$가 해적판 디코더에 저장되어있는 공모자의 개인키라는 것을 확인한다.

여기서 m은 대략 $8\lambda(N/\epsilon)^2$임을 의미한다. 또한 추적용 암호문 TR_X는 다음과 같이 생성한다. 먼저 인덱스 $u=(i-1)m+j$라면 각 행(row)에 대하여 임의의 $s, t, z_1, ..., z_{i-1} \in Z_p$ 를 선택하여 다음을 생성한다.

- $x < i$ 인 경우, $R_x = g^{z_x s}$,
- $x \ge i$ 인 경우, $R_x = g^{r_x s}$,

- $x \ne i$ 인 경우, B_x는 U_x에 있는 모든 열 원소로 $B_x = \left(u_x v_1 v_2 \cdots v_m\right)^{s t}$ 를 생성,
- $x = i$ 인 경우, B_x는 $S_x = X \cap U_x$ 에 있는 모든 열 원소로 $B_x = \left(u_x v_j v_{j+1} \cdots v_m\right)^{s t}$ 를 생성한다.

따라서 추적용 암호문 TR_X는 위의 원소를 모두 포함한 형태로서 다음과 같다.

$$TR_X = \begin{bmatrix} R_1, ..., R_m, C_1, ..., C_m, D, \\ B_1, ..., B_m, A \end{bmatrix}$$

일반 암호문은 전체 사용자 집합 U에서 임의의 수신자 집합 $S(\subseteq U)$을 위한 암호문이며, 추적용 암호문은 해적판 디코더가 발견되었을 때, 디코더를 분해하지 않고 그 속에 저장되어 있는 유출된 키를 확인하기 위한 추적 알고리즘 속에 입력하는 암호문을 만드는 것이다.

예를 들어, 사용자 집합 $U=\{1,2,3,...,n\}$이라고 가정하면, 추적 알고리즘의 핵심은 수신자 집합을 $S=U$, $S=U-\{1\}$, $S=U-\{1,2\}$,⋯, $S=U-\{1,2,3,...,n-1\}$, $S=\{\varnothing\}$으로 변화하면서 S에 해당하는 추적용 암호문을 알고리즘에 입력하고 출력을 통해서 유출된 키를 찾는 것이다.

만일 해적판 디코더에 저장되어 있는 키가 $\{SK_7\}$이라면, 즉 사용자 7의 개인키 SK_7이 저장되어 있다면, 해적판 디코더는 분명 $S=U-\{1,2,3,4,5,6\}$에 대한 암호문에서는 정상적으로 복호화 하다가 $S=U-\{1,2,3,4,5,6,7\}$ 에서는 복호화 하지 못할 것이다. 이러한 확률적인 차이로 인해 디코더 내의 키가 $\{SK_7\}$이라는 것을 추적하는 것이다. 따라서 추적용 암호문은 순차적으로 수신자 집합 $S=U-R=\{u,u+1,....,n\}$을 대상으로 만드는 암호문이고 일반적인 암호문은 임의의 부분집합 $S \subseteq U$에 대한 것이다.

3.5 안전성 증명

제안하는 스킴의 안전성은 다음 정리에 기초를 한다.

정리 1. 결정적 $(t,\epsilon,l+1)$-BDHE 가정이 유효하다면, 제안하는 스킴은 (t',ϵ,l)-BDHE 가정에 근거하여 semantic secure하다.

증명. ϵ의 이익을 가지고 제안하는 스킴을 공격하는 공격자 A가 있다고 가정하고 공격자 A를 이용해서 결정적 $(l+1)$문제를 해결하는 알고리즘 B를 다음과 같이 생성한다. 먼저 생성원 $g \in G_1$, $\alpha \in Z_p$를 선택하고 $g_i = g^{\alpha^i} \in G_1$이라 두고, 다음 입력 쌍 $(g, g_1, ..., g_l, g_{l+2}, ..., g_{2l+2}, T)$ 대해서 $T = e(g,g)^{\alpha^{l+1}}$

을 만족하면 알고리즘 B는 1을 출력하고, 만족하지 않으면 0을 출력하는 알고리즘으로 공격자 A와는 다음과 같이 상호 작용한다.

먼저 공격자 A가 공격하려는 집합 $S \subset U$을 생성해서 알고리즘 B에게 주면 알고리즘 B는 집합 S를 부분집합 $S = S_1 \cup \cdots \cup S_m$으로 나눈다. 공개키를 생성하기 위해서 임의의 $\delta_1,...,\delta_m, \gamma_1,...,\gamma_m \in Z_p$에 대하여 $u_i = g^{\delta_i} \cdot \left(\prod_{k \in S_i} g_k\right)^{-1}$, $(i=1,...,m)$, $v_j = g^{\gamma_j} g_j$ $(j=1,...,m)$을 생성한다. 그리고 임의의 $r_1,...,r_m, c_1,...,c_m \in Z_p$를 선택해서 공개키 PK를 다음과 같이 생성한다.

$$PK = \begin{bmatrix} u_1,...,u_m,\ v_1,...,v_m, \\ g_l^{r_1},...,g_l^{r_m}, g_l^{c_1},...,g_l^{c_m} \\ g_l,\ e(g_l,\ g_l)^{\alpha} \end{bmatrix}$$

알고리즘 B는 개인키 SK_i, $i \notin S$를 다음과 같이 생성한다. 먼저 사용자의 인덱스가 다음과 같이 $i=(x-1)m+y$ 라면, 임의의 $\widetilde{ID}_i \in Z_p$를 선택해서 $\widetilde{ID}_i = ID_i - \alpha^{(l+1-y)}$ 으로 설정한다. 공개키 PK를 이용해서 생성한 개인키는 다음과 같다.

$$SK_i = \begin{bmatrix} K_i = g_l^{\alpha + r_x c_y} (u_x v_y)^{\widetilde{ID}_i},\ I_i = g_l^{\widetilde{ID}_i}, \\ V_i = \left\{ v_1^{\widetilde{ID}_i},..., v_{y-1}^{\widetilde{ID}_i}, v_{y+1}^{\widetilde{ID}_i},..., v_m^{\widetilde{ID}_i} \right\} \end{bmatrix}$$

개인키가 잘 정의되었는지 확인하면 다음과 같다.

$$(u_x v_y)^{\widetilde{ID}_i} = (g^{\delta_x} (\prod_{k \in S_x} g_k)^{-1} g^{\gamma_y} g_y)^{\widetilde{ID}_i}$$

$$= (g^{\delta_x} (\prod_{k \in S_x} g_k)^{-1} g^{\gamma_y} g_y)^{ID_i} (g^{\delta_x} (\prod_{k \in S_x} g_k)^{-1} g^{\gamma_y} g_y)^{-a^{l+1-y}}$$

$$= (g^{\delta_x} (\prod_{k \in S_x} g_k)^{-1} g^{\gamma_y} g_y)^{ID_i} \cdot$$

$$(g_{l+1-y}^{\delta_x} (\prod_{k \in S_x} g_{l+1-y+k})^{-1} g_{l+1-y}^{\gamma_y})^{-1} g_{l+1}^{-1}$$

따라서 $g_l^{\alpha + r_x c_y} (u_x v_y)^{\widetilde{ID}_i}$ 는 다음과 같다.

$$g_l^{\alpha + r_x c_y} (u_x v_y)^{\widetilde{ID}_i} = g_l^{r_x c_y} (g^{\delta_x} (\prod_{k \in S_x} g_k)^{-1} g^{\gamma_y} g_y)^{ID_i}$$

$$\cdot (g_{l+1-y}^{\delta_x} (\prod_{k \in S_x} g_{l+1-y+k})^{-1} g_{l+1-y}^{\gamma_y})^{-1}$$

여기에 $g_l^{\alpha + r_x c_y}$을 곱함으로서 $(u_x v_y)^{\widetilde{ID}_i}$의 계산할 수 없는 g_{l+1}^{-1} 원소를 제거할 수 있다.

그리고 개인키의 다른 원소는 $g_l^{\widetilde{ID}_i} = g_l^{ID_i} g_{2l+1-y}^{-1}$, $v_i^{\widetilde{ID}_i} = (g^{\gamma_i} g_i)^{ID_i} (g_{l+1-y}^{\gamma_i} g_{l+1-y+i})^{-1}$ 으로 생성할 수 있다. 여기서 $i=1,...,y-1,y+1,...,m$ 이다.

알고리즘 B는 공개키를 생성하기 위해서 $\rho, \gamma_1,...,\gamma_m, \delta_1,...,\delta_m$를 임의의 Z_p에서 선택했기에 위의 알고리즘 B가 생성한 공개키와 시스템이 생성한 공개키와는 구별 할 수 없다.

알고리즘 B는 SK_i, $i \notin S$, $i=(x-1)m+y$ 를 생성했기에 $y \notin S_x$이고, 이는 S_x를 생성할 때 포함되는 k에 대해서 $k-y \neq 0, (k \in S_x)$ 임을 의미한다. 그렇기 때문에 위의 개인키를 생성하는 과정에서 유도되는 $g_{l+1-y+k}$의 아래첨자는 $l+1-y+k \neq l+1$ 이다. 또한 $i \neq y$이기 때문에 $g_{l+1-y+i} \neq g_{l+1}$이다. 즉, 알 수 없는 g_{l+1}원소는 개인키를 만드는데 사용되지 않았고, 오직 알고 있는 원소를 사용해서 만들었으므로 정상적인 개인키로서 작동을 한다.

이제 집합 S를 위한 암호문을 다음과 같이 생성하면 일반 암호문과는 구별 불가능하다.

$$CT_S = \left\{ \begin{array}{l} g_l^{r_1 s},..., g_l^{r_m s}, \\ g_l^{c_1 t},..., g_l^{c_m t}, g_l^{s t} \\ B_1^{\delta_1 + \sum_{k \in S_1} \gamma_k},..., B_m^{\delta_m + \sum_{k \in S_m} \gamma_k}, \\ M \cdot e(g_l, g_l)^{\alpha s t} \end{array} \right\}$$

임의의 $s, t \in Z_p$에 대해서 $B_i = g^{s t}$ $(i=1,...,m)$ 라고 두면

$$B_i^{\delta_i + \sum_{k \in S_i} \gamma_k} = (g^{\delta_i} (\prod_{k \in S_i} g_k)^{-1} \prod_{k \in S_i} g^{\gamma_k} g_k)^{s t} = (u_i \prod_{k \in S_i} v_j)^{s t}$$

위 식을 자세한 계산은 다음과 같다.

$$(u_i \prod_{k\in S_i} v_y) = (g^{\delta_i}(\prod_{k\in S_i} g_k)^{-1} \prod_{k\in S_i}(g^{\gamma_k} g_k))$$

$$= (g^{\delta_i}(\prod_{k\in S_i} g_k)^{-1} \prod_{k\in S_i}(g_k) \prod_{k\in S_i} g^{\gamma_k})$$

$$= (g^{\delta_i} \prod_{k\in S_i} g^{\gamma_k}) = g^{\delta_i + \sum_{k\in S_i}\gamma_k}$$

암호문 CT_S에 대해서 만약 $T = e(g,g)^{\alpha^{l+1}}$라면 $e(g_l, g_l)^{\alpha st} = e(g,g)^{\alpha^{2l+1} st} = T \cdot e(g, g_l^{st})$이 므 로 암호문 CT_S는 올바른 암호문이고, T가 임의의 값이면 공격자 입장에서는 CT_S와 메시지 M의 관계가 서로 의미 없게 보일 것이다.

알고리즘 B는 암호문을 공격자 A에게 주고 공격자 A는 $b' \in \{0,1\}$을 추측한다. 만약 $b' = 1$이면 이것은 $T = e(g,g)^{\alpha^{l+1}}$임을 의미하고 그렇지 않으면 $T \neq e(g,g)^{\alpha^{l+1}}$을 의미한다. $T \neq e(g,g)^{\alpha^{l+1}}$이면 $\mathbf{Pr}[B(g, g_{\alpha,l+1}, T) = 0] = 1/2$이고 $T = e(g,g)^{\alpha^{l+1}}$이면 B는 올바른 암호문 CT_S를 공격자에게 줄 수 있어 $|\mathbf{Pr}[b' = b] - 1/2| \geq \epsilon$이다. 즉, 알고리즘 B는 $|\mathbf{Pr}[B(g, g_{\alpha,l+1}, e(g, g_{l+1})) = 0]$ $- \mathbf{Pr}[B(g, g_{\alpha,l+1}, T) = 0]| \geq \epsilon$ 이므로 결정적 $(l+1)$ 문제를 해결하는 알고리즘 B를 만들 수 있다. □

정리 2. 제안하는 공모자 추적 및 제외 스킴이 안전하다면, 다항식 시간 안에 공격이 가능한 Adv_{TR}의 이익 ϵ은 λ에 대해서 무시할 만하다.

증명. 먼저 추적성 게임에서 이길 확률이 무시할 만하다는 것을 보인다. 공격자는 수신자 집합 S_D, 해적판 디코더 D를 생성한다.

그리고 $p_i = \Pr[D(TR(S_D, PK, i, M)) = M]$ 이라 정의하자. 여기서의 p_i는 임의의 메시지 M을 선택한 것에 대한 확률이다. 해적판 디코더 D는 제외하는 집합이 없을 경우, $X = \{1,...,N\}$, $i = 1$에서는 당연히 $D(TR(S_D, PK, 1, M)) = M$이므로 $p_1 \geq \epsilon$이다. 모든 사용자를 제외할 경우는 $i = N+1$로 정하면 $D(TR(S_D, PK, N+1, M)) = \perp$이므로 p_{N+1}은 무시할 만하다. 따라서 Chernoff bound에 의해서 반드시 $j \in \{1,...,N\}$인 $p_j - p_{j+1} \geq \epsilon/(4N)$가 존재한다. 따라서 $D(TR(S_D, PK, i, M)) = M$을 만족하는 추적 알고리즘의 출력 집합 $T \neq \{\varnothing\}$이다.

이제 $j \in U$ 임을 보인다. 왜냐하면 추적 알고리즘으로 찾은 인덱스 j의 개인키 SK_j가 총 사용자 집합 U에 포함되어 있다는 것은 SK_j의 사용자가 공모자 중 한명이라는 것을 의미한다. 만일 찾은 인덱스 j가 $j \notin U$ 라고 가정하면 D는 개인키 SK_j 없이 $p_j = \mathbf{Pr}[D(TR(S_D, PK, j, M)) = M]$ 와 $p_{j+1} = \mathbf{Pr}[D(TR(S_D, PK, j+1, M)) = M]$ 를 반드시 구분 할 수 있다는 것을 의미한다. 이는 〔정리 1〕에서의 증명했던 것처럼 제안하는 스킴이 semantic secure 하다는 것에 모순이 된다. 따라서 $j \in U$ 이고, $j \in S_D \cap U$ 이다. □

3.6 효율성 비교

먼저 TR 스킴〔6〕, 〔6〕의 기초가 되었던 TT 스킴〔5〕, 〔6〕을 다른 방법으로 개선한 TR 스킴〔16〕과 〔5〕를 개선한 TT 스킴〔11〕의 효율성을 제안 스킴과 비교하면 다음과 같다. 효율성은 공개키의 크기, 암호문의 크기, 개인키의 크기, 복호화의 복잡도로 척도를 구분한다. 〔표 1〕에서의 비교를 통해 제안하는 논문이 〔5,6,16〕에 비해서 공개키, 암호문의 크기가 대폭 줄였음을 확인할 수 있고, 소수 위수의 겹선형군을 사용하는 〔16〕스킴에 비해 암호문의 크기가 절반 정도이지만, 〔16〕스킴의 암호문을 생성하는 단계에서 암호문의 크기만큼의 지수승 연산이 필요하기 때문에, 제안하는 논문과의 암호문 생성 속도에서는 절반 이상의 연산 속도 차이를 예상할 수 있다.

앞 절 3.3.1에서 〔6,16〕스킴은 제한적인 제외 기능이라 언급했지만 본 논문은 〔6,16〕스킴과는 달리 인덱스 숨김(index hiding)기능은 없지만 충분한 제외 기능의 장점을 가지고 있다. 즉, 본 스킴에서는 암호문과 추적용 암호문과의 구별 불가능성으로 인해 인덱스 숨김 기능과 충분한 제외 기능을 서로 trade-off 했다고 할 수 있다. 추가적으로는 〔6,16〕의 제한적인 제외 기능으로 수신자 집합에 대한 정보가 유출될 수 있어 〔6,16〕스킴이 가정하고 있는 stateless 디코더가 아닌 stateful 디코더를 가정한 스킴에서는 안전하지 않을 수 있다.

Table 1. Efficiency comparison between [5,6,11, 16] and ours [N: the total number of users]

	public key size	ciphertext size	private key size
[5]	$9\sqrt{N}$	$6\sqrt{N}$	1
[6]	$9\sqrt{N}$	$7\sqrt{N}$	$\sqrt{N}$
[11]	$4\sqrt{N}$	$6\sqrt{N}$	1
[16]	$4\sqrt{N}$	$7\sqrt{N}$	$\sqrt{N}$
Ours	$4\sqrt{N}$	$3\sqrt{N}$	$\sqrt{N}$

	decryption complexity	revocation	group order
[5]	3 pairings	NO	composite
[6]	4 pairings	limited	composite
[11]	3 pairings	NO	prime
[16]	4 pairings	limited	prime
Ours	3 pairings	fully	prime

또한 이 분야에서의 최근 연구 흐름을 간단히 살펴보면 대표적인 연구로는 A. Lewko, A. Sahai, B. Waters가 2010년 IEEE Symposium on Security and Privacy에서 발표한 "Revocation Systems with Very Small Private Keys"[1] 스킴과 D. Boneh, B. Waters, M. Zhandry가 2014년 Crypto에서 발표한 "Low Overhead Broadcast encryption from Multi-linear maps"[9]이 있다. 위 스킴들의 효율성을 정리하면 아래 표와 같다.

[1,9]스킴은 TT 스킴, TR 스킴이 아닌 Broadcast encryption 스킴이지만 [표 2]에서와 같이 연구 결과는 매우 효율적이다. 제안 논문의 효율성은 [1,9]스킴의 효율성에는 크게 미치지 못하지만, 제안 논문의 장점은 [6]스킴의 장점을 살리면서 가장 간단하고, 새로운 복잡도 가정 없이 안전성을 증명한 것이고, 이를 통해 [표 1]에서의 비교와 같이 [6]의 효율성을 개선한 것이다. 더욱이 [6]스킴을 개선한 [16]스킴 보다도 암호문의 크기를 절반 이상으로 줄인 장점도 가지고 있다.

Table 2. Efficiency of recently representative results [r: the number of revoked users]

	public key size	ciphertext size	private key size
[1]	$O(1)$	$O(r)$	$O(1)$
[9]	$O(\log N)$	$O(1)$	$O(1)$

	decryption complexity	system type
[1]	$O(r)$ pairings	Broadcast encryption
[9]	2 pairings	Broadcast encryption

IV. 결 론

본 논문에서는 ABE 스킴[6]을 개선한 효율적인 TR 스킴을 제안했다. 제안 스킴은 암호 전송 스킴에 공모자의 키를 추적할 수 있는 기능과 이를 시스템에서 제외할 수 있는 기능을 갖고 있는 스킴이다. [6] 스킴은 합성수 위수의 겹선형 군을 사용함으로서 암호학 분야에 비약적인 발전을 가져왔으나, 소수 위수의 군을 사용하는 것에 비해서 복호화 연산량이 비교할 수 없을 만큼 크기 때문에 현실적으로는 사용할 수 없는 단점을 가지고 있다. [16]은 이러한 단점을 개선하기 위해 유사한 구조로 소수 위수의 겹선형 군을 사용하는 스킴을 제안했다. 본 논문도 소수 위수의 겹선형 군을 사용하면서, 효율성 측면으로는 공개키, 개인키, 암호문의 크기를 [6]스킴과 이를 개선한 [16]스킴보다 부분적으로 개선한 논문이며 [6,16]스킴이 가지는 제한적인 제외 기능의 문제점을 분석한 후, 충분한 제외 기능을 갖는 스킴이다. 또한 [6]스킴의 제한적인 제외 기능은 전체적인 스킴의 안전성에 문제점을 야기하지 않지만 스마트한 해적판 디코더를 가정하는 경우에는 [6]스킴의 인덱스 숨김(index hiding) 기능에 대한 문제점을 야기할 수 있다. 비록 최근 연구 결과의 효율성에는 미치지 못하지만 제안 스킴은 피라미드 구조와 같은 계층적(hierarchical)구조를 갖고 있는 정부, 관공서, 군과 같은 상위계층으로 오를수록 책임/권한(즉, 복호화 권한)이 증대되는 조직 구조에 적용할 수 있는 스킴이다.

References

[1] A. Lewko, A. Sahai and B. Waters, "Revocation systems with very small private keys," IEEE Symposium on Security and Privacy 2010, pp. 273-285, May 2010.

[2] A. Kiayias and M. Yung, "Traitor tracing with constant transmission rate,"

Eurocrypt 2002, LNCS vol. 2332, pp. 450-465, Apr.-May 2002.
〔3〕 A. Sahai and B. Waters, "Fuzzy identity-based encryption," Eurocrypt 2005, LNCS vol. 3494, pp. 457-473, May 2005.
〔4〕 B. Chor, A. Fiat and M. Naor, "Tracing traitors," Crypto 1994, LNCS vol. 839, pp. 257-270, Aug. 1994.
〔5〕 D. Boneh, A. Sahai and B. Waters, "Fully collusion resistant traitor tracing with short ciphertexts and private keys," Eurocrypt 2006, LNCS vol. 4004, pp. 573-592, May-Jun. 2006.
〔6〕 D. Boneh and B. Waters, "A fully collusion resistant broadcast, trace and revoke system," ACM CCS 2006, pp. 211-220, Oct.-Nov. 2006.
〔7〕 D. Boneh, C. Gentry and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys," Crypto 2005, LNCS vol. 3621, pp. 258-275, Aug. 2005.
〔8〕 D. Boneh and M.K. Franklin, "An efficient public key traitor tracing scheme," Crypto 1999, LNCS vol. 1666, pp. 338-353, Aug. 1999.
〔9〕 D. Boneh, B. Waters and M. Zhandry, "Low overhead broadcast encryption from multi-linear maps," Crypto 2014, LNCS vol. 8616, pp. 206-223, Aug. 2014.
〔10〕 D. Boneh, X. Boyen and E. J. Goh, "Hierarchical identity based encryption with constant size ciphertext," Eurocrypt 2005, LNCS vol. 3494, pp. 440-456, May 2005.
〔11〕 D. M. Freeman, "Converting pairing-based cryptosystems from composite- order groups to prime-order groups," Eurocrypt 2010, LNCS vol. 6110, pp. 44-61, May-Jun. 2010.
〔12〕 D. Naor, M. Naor and Lotspiech, "Revocation and tracing schemes for stateless receivers," Crypto 2001, LNCS vol.2139, pp. 41-62, Aug. 2001.
〔13〕 K. Kurosawa and Y. Desmedt, "Optimum traitor tracing and asymmetric schemes," Eurocrypt 1998, LNCS vol. 1403, pp. 145-157, May-Jun. 1998.
〔14〕 M. Lee, D. Ma and M. Seo, "Breaking Two k-resilient Traitor Tracing Schemes with Sublinear Ciphertext Size," ACNS 2009, LNCS vol. 5536, pp. 238-252, Jun. 2009.
〔15〕 M. Naor and B. Pinkas, "Efficient trace and revoke schemes," Financial Cryptography 2001, LNCS vol. 1962, pp. 1-20, Oct. 2001.
〔16〕 S. Garg, A. Kumarasubramanian, A. Sahai and B. Waters, "Building efficient fully collusion-resilient traitor tracing and revocation schemes," ACM CCS 2010, pp. 121-130, Oct. 2010.
〔17〕 T. Matsushita and H. Imai, "A public key black box traitor tracing scheme with sublinear ciphertext size against self defensive pirates," Asiacrypt 2004, LNCS vol. 3329, pp. 260-275, Dec. 2004.
〔18〕 Y. Dodis and N. Fazio, "Public key broadcast encryption for stateless receivers," DRM 2002, LNCS vol. 2696, pp. 61-80, Nov. 2002.

〈저자소개〉

이 문 식 (MoonShik Lee) 정회원
2001년 2월: 서울대학교 수리과학부 졸업
2004년 2월: 서울대학교 수리과학부 석사
2010년 2월: 서울대학교 수리과학부 박사
2010년 2월~현재: 공군사관학교 기초과학과 수학 교수
〈관심분야〉 정보보호, 암호학

이 주 희 (Juhee Lee) 정회원
1996년 2월: 한남대학교 수학과 졸업
2002년 2월: 이화여자대학교 수학과 석사
2010년 8월: 이화여자대학교 수학과 박사
2010년 9월~2012년 5월: 이화여자대학교 수리과학연구소 연구원
2012년 6월~2012년 12월: 국가수리과학연구소 연구원
2012년 12월~현재: 이화여자대학교 수리과학연구소 연구교수
〈관심분야〉 정보보호, 암호학

홍 정 대 (JeoungDae Hong) 정회원
1993년 2월: 육군사관학교 기계공학과 졸업
2005년 2월: 서울대학교 전기·컴퓨터공학부 석사
2010년 2월: 서울대학교 전기·컴퓨터공학부 박사
2010년 2월~현재: 국군기무사령부
〈관심분야〉 암호학, 군사보안