The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 19, No. 2, pp.9-17, Apr. 30, 2019. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2019.19.2.9
JIIBC 2019-2-2

위성방송에 적용 가능한 속성기반 암호전송 알고리즘

Attribute-based Broadcast Encryption Algorithm applicable to Satellite Broadcasting

이문식*, 김득수**, 강순부***

Moon-Shik Lee*, Deuk-Su Kim, Sun-Bu Kang***

요 약 본 논문에서는 위성방송의 네트워크에 적용 가능한 속성기반 암호전송 알고리즘을 제안하고자 한다. 암호전송 알고리즘은 위성을 통해 사업자(송신자)가 다수의 정당한 사용자에게 콘텐츠를 효율적이며 안전하게 전송할 수 있는 기법이며, 속성기반 암호 알고리즘은 콘텐츠 또는 사용자가 지닌 속성에 따라 콘텐츠를 암호화하고, 그 속성의 일정 부분을 만족하면 복호화가 가능한 알고리즘으로 본 논문에서는 두 알고리즘의 효율적인 결합을 통해 위성방송 네트워크의 안전성과 운용성을 높인 알고리즘이다. 즉, 다수의 사용자에게 효율적으로 암호문을 전송할 수 있으며, 다양한 속성의 결합으로 복호화를 제어할 수 있는 장점을 가진 알고리즘이다. 제안 알고리즘은 효율성 측면에서 공개키, 개인키, 암호문의 크기를 크게 감소시켜 위성방송의 네트워크 부하를 줄일 수 있으며, 복호화 연산량을 절반으로 줄여 빠른 복호화를 가능하게 함으로서 사용자의 운용성을 높인 특징을 지닌다.

Abstract In this paper, we propose an attribute-based broadcast encryption algorithm that can be applied to satellite broadcasting network. The encryption algorithm is a cryptographic method by which a carrier(sender) can transmit contents efficiently and securely to a plurality of legitimate users through satellites. An attribute-based encryption algorithm encrypts contents according to property of contents or a user, In this paper, we combine effectively two algorithms to improve the safety and operability of satellite broadcasting network. That is, it can efficiently transmit ciphertexts to a large number of users, and has an advantage in that decoding can be controlled by combining various attributes. The proposed algorithm reduces the network load by greatly reducing the size of the public key, the private key and the cipher text in terms of efficiency, and the decryption operation amount is reduced by half to enable fast decryption, thereby enhancing the operability of the user.

Key Words : Cryptograpy, Attribute-based Encryption, Broadcast Encryption, Satellite Broadcasting, Bilinear map

Ⅰ. 서 론

1. 개요

일반적으로 위성을 통한 방송 사업자(예 : Skylife)는 요금을 지불하고 가입한 정당한 사용자만이 디지털 콘텐츠를 받아 볼 수 있도록 콘텐츠를 전송하고 있다. 이를 위해 사업자(송신자)는 콘텐츠를 암호화(Encryption 또는 Scramble)해서 전송하고, 정당한 사용자는 개인키를 가지고 있어, 복호화(Decryption)를 통해 콘텐츠를 감상, 시청, 청취한다. 이를 가능하게 하는 것은 암호전송

*정회원, 공군사관학교 기초과학과
**정회원 공군사관학교 기초과학과(교신저자)
***정회원 공군사관학교 기초과학과
접수일자 2019년 3월 4일, 수정완료 2019년 4월 3일
게재확정일자 2019년 4월 5일

Received: 4 March, 2019 / Revised: 3 April, 2019 / Accepted: 5 April, 2019
**Corresponding Author: deuksu@gmail.com
Dept. of Natural Science, Republic of Korea Air Force Academy, Korea

(Broadcast Encryption : 이하 BE) 알고리즘을 적용하는 것이다. BE의 암호문은 대칭키를 암호화하는 헤더(Header)와 대칭키(예 : AES, ARIA 등)를 이용하여 콘텐츠를 암호화하는 바디(Body)로 구성된다. 따라서 송신자가 위성을 이용하여 암호문을 전송하면, 정당한 사용자는 개인키를 이용하여 대칭키를 구하고, 콘텐츠를 얻는 구조이다. 또한 BE는 한명의 송신자만 전송할 수 있는 비밀키 기반 BE와 공개키를 이용하여 사용자 누구나 암호문을 만들어서 전송할 수 있는 공개키 기반 BE로 구분한다. 기술 발전으로 위성방송의 사업영역이 확대된다면 공개키 기반 BE의 응용분야가 더욱 많은 장점을 가지므로 공개키 기반 BE의 연구가 더욱 활발히 진행되고 있다. BE의 효율성은 공개키와 개인키, 암호문의 크기, 복호화에 필요한 연산량으로 크게 구분한다. 위 효율성 중 위성방송의 네트워크 트래픽에 가장 큰 영향을 주는 암호문 전송량이 가장 중요하다고 할 수 있다.

속성기반 암호(Attribute-based Encryption : 이하 ABE) 알고리즘은 콘텐츠가 갖는 속성에 따라 콘텐츠를 암호화하고, 그 속성 중 일정부분 이상의 속성을 사용자가 만족할 때, 복호화가 가능한 기법으로 속성에 따라 복호화를 효과적으로 제어할 수 있는 장점이 있다. 일반적으로 ABE는 암호문 속성기반(Ciphertext-Policy) ABE와 키 속성기반(Key-Policy) ABE로 구분하며, 전자는 콘텐츠의 속성에 따라서 암호문을 생성하는 것이고, 후자는 사용자가 지닌 속성에 따라 개인키를 생성하는 것이다.

최근에는 ABE와 BE를 대수적으로 결합한 속성기반 암호전송(이하 ABBE) 알고리즘이 활발히 연구되고 있으며, 이는 위성방송 뿐만 아니라 군사/통신위성과 같은 일 대 다수(one-to-many)의 네트워크 시스템에 적용 가능한 알고리즘이다.

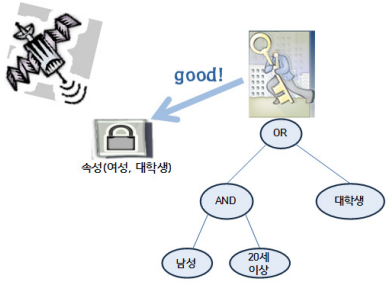

그림 1. 속성기반 암호전송 알고리즘(ABBE)
Fig. 1. Attribute-based Broadcast Encryption Algorirthm (ABBE)

2. 관련 연구

가장 대표적인 BE는 이진트리(Binary tree) 기반의 Complete Subtree(CS)와 Subset Difference(SD) 기법이다[16]. CS의 암호문 크기는 $r\log(n/r)$, 개인키는 $\log n$ 이고, SD의 암호문 크기는 최대 $2r-1$, 개인키는 $\log^2 n$ 으로 가장 효율성이 좋지만 비밀키 기반 BE라는 단점을 가지고 있다. (여기서 n은 총 사용자 수이고, r은 제외하고자 하는 사용자 수이다.) 이를 공개키 기반으로 전환하는 기법이 제안되었고[15], 이를 위해 Hierarchical ID-based encryption 기법을 적용한 것이다. 이진트리 기반을 사용하지 않고 겹선형 사상을 이용한 대표적인 BE는 D. Boneh 등이 제안한 기법이 있다[12,13,14]. 비록 합성수 위수의 겹선형 군을 활용함으로서 현실적으로 적용하기에는 한계가 있지만 Subgroup decision 가정 및 Index hiding과 같은 독창적인 아이디어를 사용하여 공개키의 크기는 $O(\sqrt{n})$, 암호문의 크기는 $O(\sqrt{n})$, 개인키의 크기는 $O(\sqrt{n})$, 복호화 연산량은 4번의 겹선형 연산을 갖게 하였다. 또한 합성수 위수의 겹선형 군을 소수 위수의 겹선형 군으로 전환함과 동시에 효율성을 개선한 기법이 제안되었다[7]. 또한 이러한 기법과 별개로 ElGamal 암호로 다수의 수신자 환경에 대한 Universal re-encryption(URM) 기법이 제안되기도 했다[11].

ABE의 가장 대표적인 알고리즘은 [10]이며, “AND, OR, Threshold, NOT” 의 속성에 대한 논리구조를 갖는 장점을 가지고 있다. 또한 격자(Lattices)를 이용한 기법이 제안되었다[5]. 또한 ABE의 하나의 시스템 사업자가 아닌 다중 시스템 사업자(Multi-authority)가 존재하는 환경에서의 ABE가 제안 되어 시스템 사용자 누구라도 자신 스스로 사업자가 될 수 있어 콘텐츠의 속성과 사용자의 개인키를 생성하고 암호문을 전송할 수 있는 장점을 가진다.

최근에는 ABE와 BE의 대수적으로 결합한 ABBE가 활발히 연구되고 있다[6,8,9]. 이는 다수의 사용자에게 효율적인 전송이 가능한 BE의 장점과 속성에 따라 복호화가 가능한 ABE의 장점을 결합한 기법으로 위성방송과 같은 시스템의 효율성과 운용성을 증대할 수 있는 알고리즘이다. 위성을 통한 디지털 콘텐츠를 전송하는 네트워크 전송 방식(예 : Transport Stream Packet) 등의 물리적 계층 향상과 관련된 연구[2]는 지속되고 있으나, 여기서는 소프트웨어 계층의 암호 알고리즘에 집중하고자 한다.

3. 연구 의의

본 논문에서는 ABE와 BE의 효율적인 결합을 통해 위성방송 등에 적용할 수 있는 암호학적인 알고리즘인 ABBE 알고리즘을 제안하고자 한다. ABE는 이론적으로는 활발히 연구가 진행되고 있으나, 현실에 적용하기에는 부가가치가 높은 기술은 아니다. 그 이유는 ABE의 응용범위가 넓지 않기 때문이다. 많은 콘텐츠를 보유하고 있는 위성방송 사업자 입장에서는 단순한 암호기법을 사용하여 시스템을 구현하는 것이 유지, 운용비가 적기 때문이다. 또한 BE와 ABE의 암호학적 기반이 겹선형 사상이므로 복호화 시에 지수승 연산보다 약 10배정도의 연산량을 요구하고 있어, 빠른 암/복호화에 걸림돌로 작용하고 있기 때문이다. 그러나 향후 과학기술의 발전으로 위성의 데이터 전송 네트워크 시스템이 크게 향상된다면 이에 적용 가능한 ABBE 알고리즘을 제안하고자 한다.

본 논문에서는 기존의 대표적인 알고리즘 [1, 3, 6, 7, 8, 12]에 비해 효율성의 척도인 공개키, 암호문, 개인키의 크기와 복호화 연산량을 개선하였고, 이는 논문의 Ⅳ장의 효율성 비교에서 구체적으로 설명하겠다.

Ⅱ. 배경 지식

1. 속성기반 암호전송(ABBE) 알고리즘의 정의

ABBE는 다음과 같이 4개의 단계로 구성된다. 여기서 n은 총 사용자 수, U는 총 사용자 집합을 의미한다.

가. 초기화

- Set-up$(\lambda; PK, MK, \Gamma)$: 시스템 매니저가 실행하는 단계로 보안 파라미터 λ를 입력하면 공개키 PK, 마스터키 MK, 시스템에서 사용할 속성 집합 Γ를 출력하는 알고리즘으로 공개키 PK, Γ는 서버에 저장하며, 송신자는 다음 암호화 단계에서 공개키 PK, Γ를 서버에서 가져온다.

나. 키 생성

- Key-gen$(PK; \tau, SK)$: 시스템 매니저가 실행하는 단계로 공개키 PK를 입력하면 사용자의 속성에 따른 접근 트리 τ와 사용자의 개인키 SK를 출력하는 알고리즘으로 개인키 SK는 안전한 채널을 통해 사용자에게 전송한다.

다. 암호화

- Enc$(PK, M, S; CT, \omega)$: 송신자가 실행하는 단계로 공개키 PK와 콘텐츠 M, 사용자 중 보내고자 하는 수신자 집합 $S(\subseteq U)$ 를 입력하면 콘텐츠 M의 암호문 CT과 콘텐츠 속성 ω를 출력하는 알고리즘이다. 따라서 암호화 단계에서는 사용자 중 수신자 집합 S에 포함시키지 않으므로 사용자를 제외(Revocation)할 수 있는 기능을 포함한다.

라. 복호화

- Dec$(CT, SK_u; M, \perp)$: 사용자 u가 실행하는 단계로 암호문 CT와 개인키 SK_u를 입력하면 콘텐츠 M 또는 임의의 값 $\perp$을 출력하는 알고리즘이다. 즉 사용자 u가 수신자 집합 S에 포함되고, 암호문의 속성에 해당하는 속성을 지닌다면 암호화된 콘텐츠 M을 복호화 할 수 있고, 그렇지 않으면 임의의 값을 출력하는 알고리즘이다.

2. 수학적 배경

가. 겹선형 함수(Bilinear map)

G_1, G_2는 소수 p 위수를 갖는 곱셈 순환군이라 하자. $g \in G_1$는 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 : $e(g, g) \neq 1$ 을 만족한다.
- Efficient computability : $e(g, g)$를 효율적으로 계산할 수 있는 알고리즘이 존재한다.

겹선형 함수는 소수 위수의 타원곡선 암호에서 구현되는데, 이를 실수체 기반의 타원곡선 암호시스템으로 확장하여 안전도를 높이는 방법도 연구되고 있다[4].

나. 라그랑주 보간법(Lagrange interpolation)

차수가 d인 다항식 $f(x)$는 $d+1$개의 서로 다른 원소들의 집합 $S = \{(x_0, f(x_0)), ..., (x_d, f(x_d))\}$가 주어지면 만들 수 있는 방법으로 다음과 같다.

$f(x) = \sum_{i=0}^{d} (f(x_i) \cdot \triangle_{i,S}(x))$, 여기서

$\triangle_{i,S}(x) = \prod_{\substack{j \in S \\ j \neq i}}^{d} \frac{x - x_j}{x_i - x_j}$ 는 라그랑주 계수이다.

3. 복잡도 가정(Complexity assumption)

· B-Bilinear Diffie Hellman Exponent(BDHE) 가정

$h, g \in G_1$에 대해서 $(h, g, g^{\alpha},...,g^{\alpha^B}, g^{\alpha^{B+2}},...,g^{\alpha^{2B}})$이 주어졌을 때, $T = e(h, g)^{\alpha^{B+1}} \in G_2$을 의미 있는(non-negligible) 확률로 계산할 수 있는 알고리즘 Λ가 존재하지 않는다는 것이 B-BDHE 문제이다.

$g_i = g^{\alpha^i}$ 와 $g_{\alpha, B} = (g_1,...,g_B, g_{B+2},..., g_{2B})$ 라 정의하면, $(g_{\alpha,B}, T = e(g,h)^{\alpha^{B+1}})$, $(g_{\alpha,B}, W = e(g,h)^{z})$를 의미 있는(non-negligible) 확률로 구분할 수 있는 알고리즘 Λ가 존재하지 않는다는 것이 결정적 B-BDHE 가정이다. 결정적 B-BDHE 가정을 푸는 알고리즘 Λ가 $|\mathbf{Pr}[\Lambda(g_{\alpha,B}, T) = 1] - \mathbf{Pr}[\Lambda(g_{\alpha,B}, W) = 1]| \geq \epsilon$ 을 만족하면 알고리즘 Λ는 ϵ이익을 갖는다고 한다.

4. 안전성 모델(Security model)

제안하는 알고리즘의 안전성을 공격자와 시뮬레이터 사이의 다음 challenge와 response게임으로 정의한다.

- Int : 제안 알고리즘에 대한 공격자는 수신자 집합 S를 선택해서 시뮬레이터에게 준다.
- Set-up : 시뮬레이터는 초기화, 키 생성 단계를 수행해서 공개키 PK와 사용자 $u(\notin S)$ 의 개인키 SK_u를 생성하여 공격자에게 준다.
- Challenge : 공격자는 두 콘텐츠 M_0, M_1을 시뮬레이터에게 주고, 시뮬레이터는 $b \in \{0,1\}$를 선택해서 M_b의 암호문 CT를 생성해서 공격자에게 준다.
- Guess / Response : 공격자는 암호문에 대해서 $b' \in \{0,1\}$을 추측하고 b'을 시뮬레이터에게 준다.

만일 $b' = b$ 이면 공격자가 이기는 게임으로 공격자의 이익을 $Adv = |\mathbf{Pr}[b' = b] - 1/2|$ 이라 한다.

즉, 공격자의 능력이 대단해서 시뮬레이터에게 받은 공개키, 개인키를 이용하여 $u \notin S$ 의 개인키 SK_u를 가지고 알고리즘을 공격할 수 있다면, 제안하는 알고리즘은 안전하지 않다는 것이다. 그러한 경우 공격자의 이익 ϵ은 $1/2$보다 많다고 정의한다.

정의 1. 다항식 시간 안에 $\epsilon > 0$에 대해서 공격자의 Adv가 무시할 만한 정도(negligible)라면 제안 알고리즘은 안전하다.

5. 접근 트리 τ (Access tree)

사용자가 지닌 속성 사이의 관계를 “AND, OR, Threshold”를 사용해서 트리(tree)로 표현하는 것을 접근 트리 τ라 부른다. 접근 트리 τ의 모든 내부 노드는 한계치 게이트(Threshold gate)를 가지고 있다. num_x는 x 노드의 자식 노드 수, k_x는 한계치 값(Threshold value)이라 정의하면 $0 \leq k_x \leq num_x$을 만족한다. 그리고 $k_x = 1$이면, 한계치 게이트는 OR 게이트로, $k_x = num_x$이면 한계치 게이트는 AND 게이트라 한다. 또한 노드 x의 부모 노드를 $parent(x)$라 하고, 노드 x가 잎 노드라면 잎 노드 x에 대응되는 속성이 부여되어 있다. 그리고 접근 트리 τ의 모든 노드에 대해서는 루트 노드부터 자식 노드에 이르기까지 1부터 num까지 순서를 정하고, 노드 x에 대한 이 순서 값을 $index(x)$라 정의한다. 예를 들면 다음과 같다.

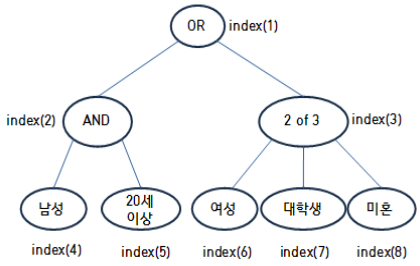

그림 2. 사용자 개인키에 대한 접근 트리 τ
Fig. 2. Private key for user with access tree τ

Ⅲ. 제안 알고리즘

제안 알고리즘은 속성기반 암호(ABE) 알고리즘과 암호전송(BE) 알고리즘의 효율적인 결합으로 ABE는 [1, 10], BE는 [3, 12]를 기초로 하여 설계하여, 공개키, 암호문, 개인키의 크기와 복호화 연산량을 크게 개선하였다.

먼저 총 사용자를 $n = m^2$명 이라고 가정하고, 사용자 집합을 $U = \{1,...,n\}$라 한다. $m \times m$ 행렬을 만들고, 각 사용자를 행렬에서 $1 \leq x, y \leq m$ 을 만족하는 x 행, y 열의 좌표 (x, y)와 일대일 대응시킨다. 그리고 집합 $U_i (\subset U), (1 \leq i \leq m)$ 를 $m \times m$ 행렬의 i번째 행에 포함된 사용자 집합이라 정의한다. 간단히 표현하면 사용자 u는 $u = (x-1)m + y$를 만족하는 고유의 자연수 u 또는 (x, y)를 가지며, 이를 공개한다.

1. 초기화(Set-up)

소수 p 위수를 갖는 군 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 원소 $r_1,...,r_m, c_1,...,c_m \in G_1$, 임의의 $\alpha, t_1,...,t_l \in Z_p$를 선택한다. 여기서 시스템 속성 집합을 $\Gamma = \{\omega_1,...,\omega_l\}$이라 하고, ω_i :={남성}, ω_j:= {20세 이상}과 같은 속성을 의미하며 이는 속성 값은 t_i와 t_j에 대응된다. 공개키 PK와 마스터키 MK는 다음과 같다.

$$PK = \left\{ r_1,...,r_m, c_1,...,c_m, \Gamma, \quad g, g^{t_1},..., g^{t_l}, e(g,g)^{\alpha} \right\} \quad MK = \{\alpha\} \qquad (1)$$

2. 키 생성(Key-Gen)

시스템 매니저는 사용자 u가 지닌 속성 집합 $\Upsilon = \{\delta_i,...,\delta_j\}$에 따른 접근 트리 τ를 생성하기 위해, 접근 트리 τ의 모든 노드 x마다 다항식 p_x를 아래와 같이 루트 노드에서 잎 노드 순으로 생성한다. 각 노드 x에 대해서 다항식 p_x의 차수는 $d_x = k_x - 1$이다. 먼저 루트 노드 r에 대해서 $p_r(0) = \alpha$로 설정한다. 그리고 다항식 p_r의 서로 다른 d_r개의 점들을 선택해서 다항식 p_r을 생성한다. 그 이외의 노드 x에 대해서 $p_x(0) = p_{parent(x)}(index(x))$로 설정하고 다항식 p_x의 서로 다른 d_x개의 점들을 선택해서 다항식 p_x를 생성한다.

마지막으로 잎 노드 x는 사용자 u가 지닌 속성과 대응시킨다. 만일 사용자 u가 j개의 속성 $t_{i1},...,t_{ij}$를 지닌다면 임의의 $r \in Z_p$를 선택하고, 공개키 PK를 이용해서 개인키 SK_u를 다음과 같이 생성한다. 논문의 기술상 편의를 위해 $t_{i1} := t_1,...,t_{ij} := t_j$라 표현한다.

$$SK_u = \left\{ \Upsilon = \{\delta_1,..,\delta_j\},\ g^{t_1 r},....,g^{t_j r}, \quad g^{p_1(0)/t_1}(r_x c_y)^r,...,g^{p_j(0)/t_j}(r_x c_y)^r, \quad c_1^r,..., c_{y-1}^r, c_{y+1}^r,...,c_m^r \right\} \qquad (2)$$

예를 들면, 사용자 개인키에 대한 다항식 p_x는 다음과 같이 생성한다.

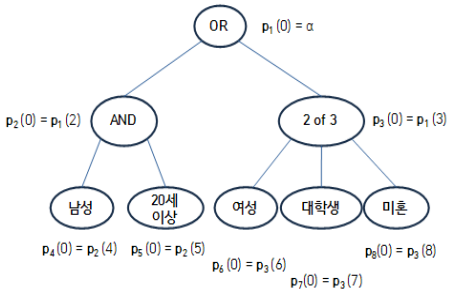

그림 3. 사용자 개인키에 대한 다항식 p_x
Fig. 3. Private key for user with polynomial p_x

3. 암호화

송신자는 수신자 집합 $S(\subseteq U)$에 속한 사용자만이 콘텐츠 M의 암호문을 복호화 하도록 다음과 같이 암호문을 생성한다. 먼저 콘텐츠 M이 지닌 속성 집합 $\Gamma_{CT} = \{w_i,...,w_j\}$라 하고, $S_i = S \cap U_i \ (1 \le i \le m)$이라 하자. 그리고 임의의 $\beta \in Z_p$를 선택하여 암호문 CT를 생성한다.

$$CT = \left\{ g^{t_i \beta},..., g^{t_j \beta}, \Gamma_{CT} = \{w_i,...,w_j\}, \quad B_1 = (r_1 \prod_{j \in S_1} c_j)^{\beta},..., B_m = (r_m \prod_{j \in S_m} c_j)^{\beta}, \quad M \cdot e(g,g)^{\alpha\beta}, \right\} \qquad (3)$$

만약 $S_i = \{\varnothing\}$이면 $B_i = (r_i \prod_{j \in S_i} c_j)^{\beta}$대신 임의의 $z_i \in G_1$를 선택해서 $B_i = (z_i \prod_{j \in \tilde{S}_i} c_j)^{\beta}$로 생성한다. 여기서 $\tilde{S} = \{c_i,...,c_k\}$ 은 $\{c_1,...,c_m\}$에서 임의로 선택한다. 즉, U_i에 속해있는 사용자를 제외(revocation)하는 방법이다.

또한 $S_i \neq \{\varnothing\}$이면, 해당하는 열 원소 $c_j,...,c_k$를 이용하여 $(r_i \prod_{j \in S_i} c_j)^{\beta}$를 생성한다. 즉, $U_i - S_i$에 속하는 사용자를 제외하는 방법이다. 이를 통해 암호문 생성단계는 시스템 사용자를 완전히(fully) 제외(revocation)할 수 있는 기능을 포함한다.

4. 복호화

암호문 속의 $\Gamma_{CT} \cap \Upsilon \neq \{\varnothing\}$이고, 사용자의 접근

트리 τ가 Γ_{CT} 을 만족한다면 $K_{u,i},...,K_{u,j}$를 다음과 같이 계산한다. 또한 (x,y)위치에 있는 사용자 u가 수신자 집합 S_x에 포함된다면, S_x에 포함되는 열 원소 $\{c_{q_i},...,c_{q_j}\}$에 대응되는 개인키 $c_{q_i}^r,...,c_{q_j}^r, (q_k \neq y)$를 이용하여

$$K_{u,i} = g^{p_i(0)/t_i}(r_x c_y)^r \cdot \prod_{\substack{q_k \in S_x \\ q_k \neq y}} c_{q_k}^r \quad (4)$$

$$\vdots \qquad\qquad \vdots$$

$$K_{u,j} = g^{p_i(0)/t_j}(r_x c_y)^r \cdot \prod_{\substack{q_k \in S_x \\ q_k \neq y}} c_{q_k}^r$$

까지 계산한다. 그리고 다음을 계산한다.

$$\frac{e(K_{u,i}, g^{t_i\beta})}{e(B_x, g^{t_i r})} = \frac{e(g^{p_i(0)/t_i}(r_x \prod_{j \in S_x} c_y)^r, g^{t_i\beta})}{e((r_x \prod_{j \in S_x} c_y)^\beta, g^{t_i r})} = \quad (5)$$

$$\frac{e(g^{p_i(0)/t_i}, g^{t_i\beta}) \cdot e((r_x \prod_{j \in S_x} c_y)^r, g^{t_i\beta})}{e((r_x \prod_{j \in S_x} c_y)^\beta, g^{t_i r})} =$$

$$e(g^{p_i(0)/t_i}, g^{t_i\beta}) \cdot e((r_x \prod_{j \in S_x} c_y), g)$$

계산된 $e(g,g)^{p_i(0)\beta},...,e(g,g)^{p_j(0)\beta}$과 사용자의 속성에 대한 접근 트리 τ의 노드 x에 대해서 다항식 $p_x(0) = p_{parent(x)}(index(x))$와 루트 노드 r에 대해서 $p_r(0) = \alpha$이므로, 라그랑주 보간법을 사용하면 다음을 계산할 수 있다.

$$e(g,g)^{\beta(p_i(0)\cdot\triangle + \cdots + p_j(0)\cdot\triangle)} = e(g,g)^{\beta\alpha} \quad (6)$$

여기서 $\triangle$은 간단한 표현으로 라그랑주 계수를 의미한다. 그리고 $M = M \cdot e(g,g)^{\alpha\beta} \cdot \frac{1}{e(g,g)^{\alpha\beta}}$을 계산하면 콘텐츠 M을 복구할 수 있다.

Ⅳ. 안전성 증명 및 효율성 비교

1. 안전성 증명

ϵ의 이익을 가지고 제안하는 알고리즘을 공격하는 공격자 A가 있다고 가정하고, 공격자 A를 이용하여 결정적 B-BDHE문제를 해결하는 알고리즘 Ω을 다음과 같이 생성한다. 여기서 $g_i = g^{\alpha^i}$라 두고 다음 입력 쌍 $(g, g_1,...,g_B, g_{B+2},...,g_{2B})$에 대해서 $T = e(g,g)^{\alpha^{B+1}}$을 만족하면 알고리즘은 1을 출력하고, 만족하지 않으면 0을 출력하는 알고리즘으로 공격자와 다음과 같이 상호작용한다.

- Int : 먼저 A는 집합 $S \subset U$를 Ω에게 준다.
- Set-up : Ω는 A에게 받은 집합 S를 부분집합 $S = S_1 \cup \cdots \cup S_m$ 으로 나눈다. 그리고 Ω는 임의의 $c \in Z_p$를 선택하여 $h = g_B g^c$로 정의하고, 임의의 $\delta_1,...,\delta_m, \gamma_1,...,\gamma_m \in Z_p$ 을 선택하여,
  $r_i = g^{\delta_i} \cdot \left(\prod_{k \in S_i} g_k\right)^{-1}$, $c_j = g^{\gamma_j} g_j$, $(i,j = 1,...,m)$
  을 생성한다. 또한 속성 값에 해당하는 임의의 $t_1,...,t_l \in Z_p$을 선택해서, 속성 집합 Γ와 함께 공개키 PK와 마스터키 MK를 다음과 같이 생성한다.

$$PK = \begin{bmatrix} r_1,\ldots,r_m, c_1,\ldots,c_m, \Gamma, \\ g_B, g_B^{t_1},\ldots,g_B^{t_l}, e(h, g_1) \end{bmatrix}, \; MK = \{\alpha\} \quad (7)$$

Ω는 개인키 SK_u, $(u \notin S)$를 다음과 같이 생성한다. 사용자의 인덱스가 다음과 같이 $u = (x-1)m + y$ 라면, 임의의 $\tilde{r} \in Z_p$를 선택해서 $\tilde{r} = r - \alpha^{(B+1-y)}$ 으로 설정한다. 그리고 임의의 다항식 $p_i(0)$를 생성하고, 공개키 PK를 이용해서 개인키를 다음과 같이 생성한다. 또한 안전성 증명의 편의를 위해 사용자가 지닌 속성은 하나라고 가정한다.

$$SK_u = \begin{Bmatrix} \Upsilon = \{\delta_i\}, \; g_B^{t_i\tilde{r}}, \\ g_B^{p_i(0)/t_i}(r_x c_y)^{\tilde{r}}, \\ c_1^{\tilde{r}},\ldots,c_{y-1}^{\tilde{r}}, c_{y+1}^{\tilde{r}},\ldots,c_m^{\tilde{r}} \end{Bmatrix} \quad (8)$$

여기서 $g_B^{t_i\tilde{r}} = (g_B^r g_{B+1-y}^{-1})^{t_i}$ 과
$c_i^{\tilde{r}} = (g^{\gamma_i} g_i)^r (g_{B+1-y}^{\gamma_i} g_{B+1-y+i})^{-1}$ 은 공개키를 이용해서 생성할 수 있으며,

$$g_B^{\alpha}(r_x\, c_y)^{\tilde{r}} = g_B^{\alpha}(g^{\delta_x}(\prod_{k\in S_x} g_k)^{-1} g^{\gamma_y} g_y)^r \cdot (g_{B+1-y}^{\delta_x}(\prod_{k\in S_x} g_{B+1-y+k})^{-1} g_{B+1-y}^{\gamma_y})^{-1} \quad (9)$$

을 의미한다. $i=1,...,y-1,y+1,...,m$ 이다.

Ω는 공개키를 생성하기 위해서 $\gamma_1,...,\gamma_m,\delta_1,...,\delta_m$를 Z_p에서 임의로 선택했기에, Ω가 생성한 공개키와 시스템 매니저가 생성한 공개키와는 구별 할 수 없다.

· Challenge : Λ는 M_0, M_1를 Ω에게 주고, Ω은 $b\in\{0,1\}$을 선택해서 M_b의 암호문을 다음과 같이 생성하면 일반 암호문과는 구별 불가능하다.

$$CT=\left\{ g_B^{t_i\beta}, \Gamma_{CT}=\{w_i\}, \; B_1^{\delta_1+\sum_{k\in S_1}\gamma_k}, ..., B_m^{\delta_m+\sum_{k\in S_m}\gamma_k}, \; M_b\cdot e(h,g_1)^{\beta} \right\} \quad (10)$$

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

$$B_i^{\delta_i+\sum_{k\in S_i}\gamma_k}=(g^{\delta_i}(\prod_{k\in S_i} g_k)^{-1}\prod_{k\in S_i} g^{\gamma_k} g_k)^{\beta}=(r_i\prod_{k\in S_i} c_j)^{\beta} \quad (11)$$

이므로 일반 암호문과 구별 불가능하다.

만약 $T^{\beta}=e(g,g)^{\alpha^{B+1}\beta}$라면, 암호문 CT에 대해서 $e(h,g_1)^{\beta}=T^{\beta}\cdot e(g^c,g_1)^{\beta}$ 이므로 암호문은 올바른 암호문이고, T가 임의의 값이면 공격자 입장에서 암호문과 콘텐츠 M_b의 관계가 서로 의미 없게 보일 것이다. Ω는 암호문 CT를 Λ에게 준다.

· Guess / Response : Λ는 $b'\in\{0,1\}$을 추측해서 b'을 Ω에게 준다.

만약 $b'=1$이면 이것은 $T=e(g,g)^{\alpha^{B+1}}$ 임을 의미하고 $b'=0$이면 $T\neq e(g,g)^{\alpha^{B+1}}$ 을 의미한다. $b'=0$이면 $\mathbf{Pr}[\Lambda(g,g_{\alpha,B+1},T)=0]=1/2$ 이므로, Ω는 Λ를 이용하여 결정적 $(B+1)$문제를 해결할 수 있다는 결론을 얻는다.

2. 효율성 비교

먼저 대표적인 BE 알고리즘[3,7,12]과 제안 알고리즘의 효율성을 비교하면 다음 표와 같다. BE의 효율성은 공개키, 암호문, 개인키의 크기와 복호화 연산량으로 구분하며, 추가해서 사용자를 수신자 집합에서 제외할 수 있는 제외 기능과 군의 위수를 비교하였다. BE와의 정확한 비교를 위해 제안 알고리즘의 복호화 연산량은 속성에 관련된 연산은 제외하고 비교하였다.

표 1. 제안 알고리즘과 BE와의 효율성 비교
Table 1. Comparison of Efficiencies among BE

구 분	공개키	암호문	개인키
[12]	$9\sqrt{n}$	$7\sqrt{n}$	$\sqrt{n}$
[7]	$4\sqrt{n}$	$7\sqrt{n}$	$\sqrt{n}$
[3]	$4\sqrt{n}$	$3\sqrt{n}$	$\sqrt{n}$
제안	$2\sqrt{n}$	$\sqrt{n}$	$2\sqrt{n}$

구 분	복호화 연산량	제외 기능 (revocation)	group order
[12]	4 pairings	제한적	합성수
[7]	4 pairings	제한적	소수
[3]	3 pairings	완전	소수
제안	2 pairings	완전	소수

비교를 통해 제안 알고리즘은 [3, 7, 12]에 비해서 공개키, 암호문의 크기는 대폭 개선이 되었으나, 개인키의 크기는 증가하였다. 이는 제안 알고리즘이 완전한 제외기능을 갖기 위해서 행렬 $m\times m$에 따른 사용자의 행, 열 정보를 추가했기 때문이다. 따라서 완전한 제외기능을 갖기 위해 개인키의 크기를 trade-off 했다고 볼 수 있다. 또한 복호화 연산량이 감소되었기에 빠른 복호화 연산속도와 암호문 크기 감소로 인해 빠른 암호문 생성이 가능한 장점을 가진다.

제안 알고리즘과 대표적인 ABBE[1,6,8]과 비교하면 다음과 같다. [6, 8]는 이미 오래전에 제안되었지만, 현재까지 알고리즘의 수준, 효율성과 독창성을 뛰어넘는 기법이 없기에 비교 대상에 포함시켰다.

표 2. 제안 알고리즘과 ABBE와의 효율성 비교
Table 2. Comparison of Efficiencies among ABBE

구 분	공개키	암호문	개인키
[8]	$O(n+l_{\max})$	$O(l)$	$O(l)$
[6]	$O(n+l_{\max})$	$O(n+l)$	$O(n\cdot l)$
[1]	$O(\sqrt{n}+l_{\max})$	$O(\sqrt{n}+l)$	$O(\sqrt{n}+l)$
제안	$O(\sqrt{n}+l_{\max})$	$O(\sqrt{n}+l)$	$O(\sqrt{n}+l)$

여기서 $l_{\max}$는 시스템에서 사용하는 총 속성수를 의미하고, l은 암호문 생성 시에 포함되는 속성 수와 사용자가 지닌 속성 수를 의미한다. ($l \ll n$)

제안 알고리즘의 가장 큰 장점은 공개키의 크기가 [6, 8]에 비해 $O(n)$에서 $O(\sqrt{n})$으로 크게 감소하였다는 점과 암호문, 개인키의 크기는 [6]에 비해 마찬가지로 sublinear하게 감소한 장점이 있으나, [8]에 비해서는 크게 증가한 단점을 가지고 있다. 이는 앞서의 언급에서와 마찬가지로 완전한 제외기능을 갖기 위해 관련된 파라미터가 필요했기 때문이다. [1]에 비해서는 큰 차이는 없으나, 사용자가 지닌 각 속성마다 수행해야할 복호화 연산량이 4번에서 2번의 겹선형 연산으로 감소하였기에, 사용자의 속성이 많을수록 복호화 속도를 크게 향상할 수 있는 결과를 얻을 수 있었다.

제안 알고리즘의 사용 환경을 구체적으로 기술하기 위해, 총 사용자 수를 $n=2^{20}$, 속성 수 $l_{\max}=2^5$이라 가정할 때, $|G_1|$ =160 bits, $|G_2|$ =1024 bits 으로 설정하면, 시스템 설계에 필요한 공개키는 40 kbyte, 암호문은 20 kbyte, 개인키는 20 kbyte의 저장량으로 현실적으로 위성방송의 네트워크 시스템에 적용 가능한 파라미터이다.

V. 결 론

본 논문에서는 속성기반 암호 알고리즘과 암호전송 알고리즘을 효율적으로 결합한 알고리즘을 제안하였다. 제안 알고리즘은 위성방송/통신과 같은 다수의 사용자에게 암호화된 콘텐츠를 전송하는 기법에 추가적으로 사용자가 지닌 속성들로 개인키를 만들어서 암호문의 속성과 일정부분을 만족하면 복호화를 할 수 있는 알고리즘이다.

제안 알고리즘은 기존에 제시된 암호전송 알고리즘과 속성기반 알고리즘에 비해서 부분적으로 공개키, 암호문, 개인키의 크기를 줄여, 위성방송의 네트워크 시스템 부하를 감소시켰으며, 복호화 연산량의 감소로 사용자의 복호화 속도를 향상시켰다. 또한 암호문 크기의 감소로 암호화 단계에서의 암호문 생성 속도를 향상시켜 시스템 운용성을 증대할 수 있는 장점을 가진다. 다만 제안 알고리즘은 비밀키 기반이 아닌 공개키 기반으로 설계되었기에, 현재는 응용분야가 넓지 않지만 향후 과학기술의 발전으로 인해 다양한 응용분야가 생기면 적용 가능한 알고리즘이라 할 수 있다.

References

[1] MoonShik Lee, “Multi-Authority with Access Policy Attribute-based Broadcast Encryption Algorithm”, Korean Journal of Military Arts and Science, Vol 74., No 3, pp. 269-294, 2018.
DOI : http://doi.org/10.31066/kjmas.2018.74.3.010

[2] Jang-Won Kim, “A Study on Transport Stream Analysis and Parsing Ability Enhancement in Digital Broadcasting and Service”, JKIIECT, Vol 10, No 6, pp. 552-557. 2017.
DOI : https://doi.org/10.17661/jkiiect.2017.10.6.552

[3] MoonShik Lee, Juhee Lee and JeoungDae Hong, “An Efficient Public Trace and Revoke Scheme Using Augmented Broadcast Encryption Scheme”, JKIISC, Vol 26, No 1. pp. 17-30. 2016.
DOI : https://doi.org/10.13089/JKIISC.2016.26.1.17

[4] Chan-Il Woo, Eun-Hee Goo, “Study of the Real Number Field Extension Operand of Elliptic Curve Cryptography”, JKAIS, Vol 15, No 9. pp. 5790-5795. 2014.
DOI : http://dx.doi.org/10.5762/KAIS.2014.15.9.5790

[5] X. Boyen, “Attribute-based functional encryption on lattices”, TCC 2013. LNCS Vol. 7785. pp. 122-142. 2013.
DOI : https://doi.org/10.1007/978-3-642-36594-2_8

[6] P. Junod and A. Karlov, “An efficient public-key attribute-based broadcast encryption scheme allowing arbitrary access policies”, DRM 2010. pp. 13-24. 2010.

DOI : https://doi.org/10.1145/1866870.1866875

[7] S. Garg, A. Kumarasubramanian, A. Sahai and B. Waters, "Building efficient fully collusion-resilent traitor tracing and revocation schemes", ACM CCS 2010, pp. 121-130. 2010.
DOI : https://doi.org/10.1145/1866307.1866322

[8] N. Attrapadung and H. Imai, "Conjunctive broadcast and attribute-based encryption", Pairing 2009. LNCS Vol. 5671. pp. 248-265. 2009.
DOI : https://doi.org/10.1007/978-3-642-03298-1_16

[9] N. Attrapadung and H. Imai, "Attribute-based encryption supporting direct/indirect revocation", Cryptography and Coding 2009. LNCS 5921. pp. 278-300. 2009.
DOI : https://doi.org/10.1007/978-3-642-10868-6_17

[10] R. Ostrovsky, A. Sahai and B. Waters, "Attribute-based encryption with non-monotonic access structure". ACM CCS 2007. pp. 195-203. 2007.
DOI : https://doi.org/10.1145/1315245.1315270

[11] Jin-Wook Byun, Jun-Ha Cho and Dong-Hoon Lee, "Efficient and Provably Secure Universal Re-Encryption for Multi-recipient", JIIBC 2006, Vol 6, No 4, pp. 39-47. 2006.

[12] D. Boneh and B. Waters, "A fully collusion resistant broadcast trace and revoke system", ACM CCS 2006, pp. 211-220. 2006.
DOI : https://doi.org/10.1145/1180405.1180432

[13] 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. 2006.
DOI : https://doi.org/10.1007/11761679_34

[14] 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. 2005.
DOI : https://doi.org/10.1007/11535218_16

[15] Y. Dodis and N. Fazio, "Public key broadcast encryption for stateless receivers", DRM 2002, LNCS, Vol. 2696, pp. 61-80. 2002.
DOI : https://doi.org/10.1007/978-3-540-44993-5_5

[16] D. Naor, M. Naor and Lotspiech, "Revocation and tracing schemes for stateless receivers", Crypto 2001, LNCS, Vol. 2139, pp. 41-62. 2001.
DOI : https://doi.org/10.1007/3-540-44647-8_3

저자 소개

이 문 식(정회원)

- 2004년 2월 : 서울대학교 대학원 수리과학부(이학석사)
- 2010년 2월 : 서울대학교 대학원 수리과학부(이학박사)
- 2014년 8월 ~ 현재 : 공군사관학교 기초과학과 부교수

• 주관심분야 : 정보보호, 암호 알고리즘, 브로드캐스팅 암호

김 득 수(정회원)

- 2001년 2월 : 서울대학교 대학원 자연과학대학(이학석사)
- 2009년 1월 : 한국과학기술원 물리학과(이학박사)
- 2013년 7월 ~ 현재 : 공군사관학교 기초과학과 부교수
- 주관심분야 : 양자암호, 원자물리, 광학

강 순 부(정회원)

- 2004년 2월 : 서울대학교 대학원 수리과학부(이학석사)
- 2010년 2월 : 서울대학교 대학원 수리과학부(이학박사)
- 2010년 2월 ~ 현재 : 공군사관학교 기초과학과 부교수

• 주관심분야 : 정보보호, 암호 알고리즘, 브로드캐스팅 암호