Bilinear Pairing을 이용한 효율적인 신원기반 다중 수신자 암호 기법

정채덕* · 윤석봉** · 서 철*** · 이경현****

Efficient Multi-receiver Identity-Based Encryption Scheme from Bilinear Pairing

Chae Duk Jung* · Suk Bong Yoon** · Chul Sur*** · Kyung Hyune Rhee****

본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음
(IITA-2006-C1090-0603-0026)

요 약

본 논문에서는 Bilinear Paring을 사용한 효율적인 신원기반 다중 수신자 암호 기법을 제안한다. 제안 기법은 암호화 과정에서 Pairing 연산을 필요로 하지 않으며 복호화 과정에서 단 한번의 Pairing 연산만을 요구한다. 뿐만 아니라, 제안 기법을 이용하여 Subset-Cover framework 기반의 효율적인 스테이트리스 (stateless) 공개키 브로드캐스트 암호 기법을 제시한다.

ABSTRACT

In this paper, we propose a new efficient multi-receiver identity-based encryption scheme from Bilinear Pairing. The proposed scheme eliminates pairing computation to encrypt a message for multiple receivers and only need one pairing computation to decrypt the ciphertext. Moreover, we show how to properly transform our scheme into a highly efficient stateless public key broadcast encryption scheme based on the subset-cover framework.

키워드

다중 수신자 암호, 신원기반 암호, 브로드캐스트 암호, Bilinear Pairing

I. 서 론

송·수신자간 안전한 통신을 위하여 공개키 암호 기술을 사용할 경우 송신자는 수신자의 공개키로 메시지를 암호화하여 암호문을 수신자에게 전송한다. 수신자는 전송받은 암호문을 자신이 소유하고 있는 비밀키로 복호화하여 평문을 획득한다. 이와 같은 환경을 단일 수신자 환경이라고 한다.

* 부경대학교 정보보호학협동과정
** 동의대학교 수학과
*** 부경대학교 전자계산학과
**** 부경대학교 전자컴퓨터정보통신공학부(교신저자)

접수일자 : 2006. 11. 17

이에 반하여, 다중 수신자 환경에서는 송신자가 다중 수신자들에 해당하는 공개키들로 메시지를 암호화하여 다중 수신자들에게 브로드캐스트한다. 이와 같은 환경에서는 수신자마다 각각 다른 메시지를 암호화 할 수도 있고, 단일 메시지를 암호화할 수도 있다. 본질적으로, 다중 수신자 암호 기술은 브로드캐스트 암호 기술로 변형되어질 수 있어 최근 효율적인 다중 수신자 암호화 기법 및 안전성에 대한 연구가 활발하게 이루어지고 있다 [1,2,3].

브로드캐스트 암호 기술은 메시지 송신자인 그룹 관리자 또는 브로드캐스터 (Broadcaster)가 암호문을 공개된 채널상에서 특정 그룹의 수신자들에게 전송하며, 전송된 암호문은 단지 정당한 수신자들만이 복호화가 가능한 암호 기법이다. 최근 디지털 컨텐츠의 안전한 분배, 위성 기반의 비즈니스, 그룹 통신 및 PayTV 시스템등 여러 응용 분야에 대한 브로드캐스트 암호 기법의 적용성이 폭 넓게 연구되고 있다.

다중 수신자 암호화 기법은 Baudron, [4]와 Bellare[5]에 의해 정형화되었으며, 최근 Baek등에 의하여 효율적인 신원기반 다중 수신자 암호 기법이 제안되었다[1].

본 논문에서는 Bilinear Paring을 사용한 효율적인 신원기반 다중 수신자 암호 기법을 제안한다. 제안 기법은 암호화 과정에서는 Pairing 연산을 필요로 하지 않으며 복호화 과정에서는 단 한번의 Pairing 연산만을 요구한다. 뿐만 아니라, 제안 기법을 기반으로 효율적인 스테이트리스 브로드캐스트 암호 기법을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서는 새로운 기법 설계를 위한 암호학적 기반 기술을 소개하고, 3장에서 효율적인 신원기반 다중 수신자 암호 기법을 제안한 후, 4장에서 제안 기법을 분석한다. 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 새로운 기법 설계를 위한 기반 기술

2.1 Bilinear Pairing

G_1을 위수가 q인 덧셈군이라 두고 G_2를 동일한 위수 q를 가지는 곱셈군이라 할 때, bilinear pairing $e: G_1 \times G_1 \rightarrow G_2$는 다음과 같은 성질을 만족한다.

① Bilinearity : $P, Q \in G_1$와 $a, b \in Z_q^*$에 대해,

$e(P, Q+R) = e(P,Q)e(P,R)$,

$e(P, Q+R) = e(P,Q)e(P,R)$,

$e(aP, bQ) = e(P,Q)^{ab}$

이다.

② Non-degeneracy : $e(P,Q) \neq 1$을 만족하는 $P, Q \in G_1$가 존재한다.

③ Computability : 모든 $P, Q \in G_1$에 대해 $e(P,Q)$를 효율적으로 계산할 수 있는 알고리즘이 존재한다.

- p-Bilinear Diffie-Hellman Inversion (p- BDHI) 문제.

  어떤 $\alpha \in Z_q^*$에 대해,

  $P, \alpha P, \alpha^2 P, \ldots, \alpha^p P \in G_1^{p+1}$이 주어졌을 때, $e(P, P)^{1/\alpha} \in G_2$를 계산한다.

- p-BDHI 가정.

  다항식 실행 시간내에 상당한 확률을 가지고 p-BDHI 문제를 해결할 수 있는 알고리즘은 존재하지 않는다.

2.2 신원기반 공개키 암호 기술

신원 기반 암호 기술은 사용자의 신원을 나타낼 수 있는 e-mail주소, IP주소, 주민등록번호등을 이용하여 공개키를 사용함으로써 공개키에 대한 사용자의 인증을 생략하는 암호 기술로써 사전에 분배된 공개키 없이도 수신자의 알려진 신원정보를 활용하여 수신자에게 평문에 대한 암호문을 전송하고, 수신자는 비밀키 생성 센터 (PKG, Private Key Generation Center)에게 비밀키를 전송받아 암호문을 복호화하는 암호 기술이다.

신원 기반 암호 기술은 공개키 인증서를 통하여 공개키를 인증하는 방식을 대체하기 위하여 1984년에 Shamir에 의하여 제안되었다[6]. 제안된 방식의 핵심적인 요소는 신원 정보를 사용자의 공개키로 활용하는 것으로 기존의 공개키 방식의 복잡한 키 값을 대체하는 것이다. 사용자의 신원 정보를 이용하여 신뢰기관이 신원정보에 대응한 개인키를 생성하고 이를 사용자에게 안전하게 전송한다. 이 때 신뢰기관은 절대적으로 신뢰되어야하며 대칭키 방식에서 시스템의 안전성을 키 값에 의존하는 것과 같이 신원 정보로부터 개인키를 유도하는 과정은 전적으로 신뢰기관에 의해서 수행되어야 한다.

Shamir의 제안에서는 전자서명에 대한 방식은 제안

이 되었으나 신원정보 기반의 암호 알고리즘은 제안이 되지 못하고 단지 개념만이 제시되었다. 이후 많은 신원 기반의 암호 방식이 제시가 되었으나 실용화 할 수준의 제안이 없었다. 그러나, 2001년에 Boneh와 Franklin이 타원 곡선에 기초한 Weil Pairing 구조를 제안함으로써 Shamir의 제안에 대한 실질적인 구현 방안을 제시하게 되었다[7].

일반적인 공개키 시스템에 대비한 신원 기반의 암호 시스템의 이점은 공개키 인증서가 필요 없다는 것이다. 공개키 인증서가 필요 없다는 것은 이의 발행과 저장 그리고 검증을 위한 제반의 자료 저장과 관련 처리 기능의 표준화등이 불필요하다는 것을 의미한다.

신원정보를 기반으로 한 암호학적 기법에는 ID를 이용한 개인 식별(Identity based identification), ID를 이용한 서명(Identity based signature), ID를 이용한 키 분배(Identity based key distribution), ID를 이용한 암호화(Identity based encryption) 등이 있다.

2.3 다중 수신자 암호 기법

다중 수신자 환경에서는 송신자가 다중 수신자에 해당하는 공개키들로 메시지를 암호화하여 다중 수신자에게 전송(브로드캐스트 형태)한다. 수신자마다 다른 메시지를 암호화 할 수도 있고, 단일 메시지를 각각 수신자에 해당하는 키로 암호화 할 수도 있다. 본질적으로, 다중 수신자 암호 기술은 브로드캐스트 암호 기술로 변형되어질 수 있다.

대칭키 기반의 다중 수신자 암호화 기법은 각각의 사용자의 대칭키를 가지고 있는 신뢰센터만이 브로드캐스터가 될 수 있다. 반면에, 공개키 기반의 다중 수신자 암호 기법은 각각의 사용자에 대응하는 공개키를 이용하여 암호문을 생성하므로 각각의 사용자들 또한 브로드캐스터가 될 수 있는 장점을 가진다.

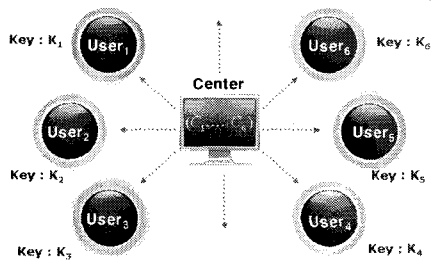

그림 1. 다중 수신자 암호
Fig. 1. Multi-receiver Encryption

그림. 1은 다중 수신자 암호 기법의 일반적인 모델을 보여주고 있으며 신뢰센터와 사용자로 구성되어진다. 브로트캐스터는 각각의 수신자들이 가지고 있는 공개키들로 평문을 암호화하여 브로드캐스트 형태로 암호문을 전송한다. 각각의 수신자들은 자신이 소유하고 있는 개인키를 이용하여 암호문을 복호화하여 평문을 획득한다. 각각의 수신자 개인키에 해당하는 암호문을 찾기 위해 추가적으로 라벨(label)이 암호문과 함께 전송되어질 수 있다.

다중 수신자 암호 기법에서는 단일 평문 또는 각각의 수신자들마다 다른 평문이 암호화되어질 수 있다. 일반적인 공개키 기반 브로드캐스트 암호 기법은 평문에 대응되는 세션 키를 각각의 수신자들의 공개키로 암호화하여 전송하기 때문에 다중 수신자 암호 기법은 브로드캐스트 암호 기법에 적용되어질 수 있다.

신원기반 다중 수신자 암호화 기법은 아래와 같은 4단계로 구성되며, 설정 및 개인키 추출 단계는 키 생성 센터(PKG)에 의해서 수행된다.

- 설정단계 : 보안 매개변수 k가 주어졌을 때, 시스템 변수와 마스터 키를 출력한다.
- 개인키 추출 단계: 키 생성 센터 (PKC)는 사용자 A의 신원정보와 마스터 키를 입력값으로 신원정보에 대한 개인키를 생성하고 사용자 A의 신원정보 검증을 거친 뒤 사용자 A에게 전송한다.
- 암호화 단계: 다중 수신자의 신원 정보, 시스템 변수와 평문 메시지를 입력값으로 암호문을 생성한다.
- 복호화 단계: 각각의 수신자는 수신자의 신원정보, 개인키와 암호문을 입력값으로 평문 메시지를 출력한다.

2.4 효율적인 신원기반 다중 수신자 암호 기법[1]

2005년 Baek 외 저자들은 신원기반 다중 수신자 암호 기법을 제안하였다[1]. 제안 기법은 기존의 신원기반 암호 기법을 다중 수신자 암호 기법에 적용했을 때보다 Pairing 연산을 줄인 다중 수신자 환경에서의 효율적인 암호 기법이다. 기존의 신원기반 암호 기법을 다중 수신자 환경에 적용하였을 경우와 제안 기법에 대한 연산량 및 전송 데이터량의 비교는 아래 표. 1과 같다.

표 1. 연산량 및 전송 데이터량 비교
table 1. Comparisons of Computational and Communication costs

	[1]	기존의 신원기반 기술
Pairing	1(or 0)	n
덧셈 (in G_1)	n	0
곱셈 (in G_1)	$n+2$	n
지수연산 (in G_2)	1	n
전송 데이터	$(n+1)l_1+l_2$	nl_1+nl_3

- n : 사용자 수 - l_1 : G_1의 원소 비트 길이
- l_2 : G_2의 원소 비트 길이
- l_3 : 메시지의 비트 길이

Baek 외 저자들이 제안한 신원기반 다중 암호 기법의 구체적인 절차는 다음과 같다.

- 설정단계 : 보안 매개변수 k가 주어졌을 때, 설정 알고리즘은 다음과 같이 수행되어지며 시스템 변수와 마스터 키를 출력한다.

(1) 보안 매개변수 k를 입력받아 소수 q, 소수 위수 q를 갖는 군 G_1, G_2, 허용 가능한 겹선형 사상 (Bilinear Map) $e : G_1 \times G_1 \rightarrow G_2$를 출력한다.

(2) 임의의 G_1의 생성자 P와 임의의 G_1의 원소 Q를 선택한다.

(3) 랜덤하게 마스터 키 $s \in Z_q^*$를 선택하고, $T = sP$라고 둔다. 그리고 암호학적 해쉬 함수 $H_1 : \{0, 1\}^* \rightarrow G_1^*$를 선택한다.

- 개인키 추출 단계: 키 생성 센터 (PKG)는 사용자 A의 신원정보(ID_A)와 마스터 키를 입력값으로 신원정보 (ID_A)에 대한 개인키 (S_A)를 아래와 같이 생성하고 사용자 A의 신원정보 검증을 거친 뒤 사용자 A에게 전송한다.

1) $Q_A = H_1(ID_A)$
2) 개인키: $S_A = sQ_A$

- 암호화 단계: 다중 수신자의 신원 정보와 시스템 변수를 입력값으로 아래와 같은 암호문을 생성한다.

1) 임의의 $r \in Z_q^*$ 선택
2) 암호문 C:

$$C = < U, V_1, \ldots, V_n, W, \Delta > \\ < rP, rH_1(ID_1) + rQ, \ldots, rH_1(ID_n) + rQ, e(Q, T)^r M, \Delta >$$

Δ는 암호문에서 V_i에 대한 수신자 신원정보를 나타냄.

암호화 단계에서 $e(Q, T)$를 계산하기 위해 한번의 Pairing 연산을 수행하지만, 두 변수 Q, T는 시스템 변수로서 시스템 변수가 변하지 않으면 초기에 한번의 Pairing 연산을 수행으로 이후 암호화를 위한 Pairing 연산을 제거할 수 있다.

- 복호화 단계: 수신자 i는 수신자의 신원정보 (ID_i)와 개인키 (S_{ID_i})를 입력값으로 평문 메시지를 출력한다.

$$M = \frac{e(U, S_{ID_i})}{e(T, V_i)} W$$

복호화 알고리즘에 대한 적합성은 다음과 같이 증명할 수 있다.

$$\begin{aligned} \frac{e(U, S_{ID_i})}{e(T, V_i)} W &= \frac{e(rP, sH_1(ID_i))}{e(sP, rH_1(ID_i) + rQ)} W \\ &= \frac{e(rP, sH_1(ID_i))}{e(rP, sH_1(ID_i) + sQ)} W \\ &= \frac{e(rP, sH_1(ID_i))}{e(rP, sH_1(ID_i))e(rP, sQ)} e(Q, T)^r M \\ &= M \end{aligned}$$

Ⅲ. 효율적인 신원기반 다중 수신자 암호 기법

본 논문에서 제안하는 효율적인 신원기반 다중 수신

자 암호 기법은 Bilinear pairing을 사용하여 구성되어지며 제안 기법의 자세한 설명은 아래와 같다.

[설정단계] : 보안 매개변수가 주어졌을 때, 설정 알고리즘은 다음과 같이 수행되어지며 시스템 변수와 마스터 키를 출력한다.

(1) 보안 매개변수 k, k_1를 입력받아 소수 q, 소수 위수 q를 갖는 군 G_1, G_2, 허용 가능한 겹선형 사상 $e: G_1 \times G_1 \rightarrow G_2$를 출력한다.

(2) 임의의 G_1상의 생성자 P를 선택한다.

(3) 랜덤하게 마스터 키 $s \in Z_q^*$를 선택하고, $P_0 = sP \in G_1$라고 둔다. 그리고 암호학적 해쉬 함수 $H_1: \{0,1\}^* \rightarrow Z_q^*$, $H_2: G_2 \rightarrow \{0,1\}^{k_1}$를 선택한다.

[개인키 추출 단계] : 키 생성 센터(PKG)는 사용자 i의 신원정보(ID_i)와 마스터 키를 입력값으로 신원정보(ID_i)에 대한 개인키(d_i)를 아래와 같이 생성하고 사용자 i의 신원정보 검증을 거친 뒤 사용자 i에게 전송한다.

$$d_i = \frac{1}{s + sH_1(ID_i)} P$$

[암호화 단계] : 다중 수신자의 신원 정보와 시스템 변수를 입력값으로 평문 $M \in \{0,1\}^*$에 대한 암호문을 아래와 같이 생성한다.

(1) 임의의 $r \in Z_q^*$ 선택

(2) 암호문 C:

$$C = < U, V_1, \ldots, V_n, W, \Delta > = < rP_0, rH_1(ID_1)P_0, \ldots, rH_1(ID_n)P_0, M \oplus H_2(g^r), \Delta >$$

Δ는 V_i에 대응되는 사용자에 대한 정보를 나타내는 라벨(label).

[복호화 단계] : 각각의 수신자 $i \in [1, n]$는 자신이 소유하고 있는 개인키(d_i)와 암호문을 입력값으로 평문 메시지를 출력한다.

$$M = W \oplus H_2(e(d_i, V_i + U))$$

Ⅳ. 제안 기법 분석 및 응용

본 장에서는 제안 기법의 암/복호화 알고리즘의 일치성 및 효율성을 분석하고, 제안 기법을 기반으로 효율적인 스테이트리스 브로드캐스트 암호화 기법을 제시한다.

4.1 일치성

복호화 알고리즘에 대한 일치성은 다음과 같이 증명할 수 있다.

$$\begin{aligned} e(d_i, V_i + U) &= e\left(\frac{1}{s + sH_1(ID_i)} P, rP_0 + rH_1(ID_i)P_0\right) \\ &= e\left(\frac{1}{s + sH_1(ID_i)} P, r(s + sH_1(ID_i))P\right) \\ &= g^r \end{aligned}$$

4.2 효율성

제안 기법은 암호화 단계에서는 Pairing연산을 요구하지 않으며 복호화 단계에서만 한번의 Pairing연산을 요구한다. 뿐만 아니라, 기 제안된 효율적인 신원기반 암호 기법[1]에서는 수신자의 수가 증가함에 따라 G_1상의 덧셈과 스칼라 곱셈이 증가하지만 제안 기법은 스칼라 곱셈만이 수신자의 수에 비례하여 증가한다.

표 2. 제안 기법과 Baek[1]의 제안 기법 비교
table 2. Comparison Proposed scheme with Baek[1]

	제안 기술	[1]
Pairing (암호화/복호화)	0/1	1/2
덧셈 (in G_1)	0	n
곱셈 (in G_1)	n	$n+2$
지수연산 (in G_2)	1	1

기 제안된 효율적인 신원기반 암호 기법[1]과 제안 기법의 효율성에 대한 자세한 비교는 표. 2와 같다.

4.3 스테이트리스 브로드캐스트 암호 기법

브로드캐스트 암호 기술은 메시지 송신자인 그룹 관리자 또는 브로드캐스터가 암호화 된 데이터를 공개된 채널 상에서 특정 그룹의 수신자들에게 전송하며, 전송된 암호문은 단지 정당한 수신자들만이 복호화가 가능한 암호 기법이다. 최근 브로드캐스트 암호 기법은 디지털 컨텐츠의 분배 및 보호, 위성 기반의 비즈니스, 그룹 통신, CD/DVD 로 저작권이 있는 컨텐츠의 분배 등 여러 가지 응용 분야에 그 적용성이 폭 넓게 연구되고 있다. 이와 같은 어플리케이션에서의 주요 안전성 문제는 그룹에 가입한 정당한 구성원만이 그룹 통신에 접근할 수 있도록 하는 접근권한이다. 이러한 안전성 문제를 해결하기 위한 단순한 방법 중 하나는 그룹 구성원들에게 전달 할 데이터를 정당한 그룹 구성원들만이 공통적으로 얻을 수 있는 그룹키로 암호화해서 전달하는 것이다. 즉, 그룹 데이터를 보호하기 위한 기술중의 하나로 암/복호화 메커니즘을 사용하는 것이다.

스테이트리스 브로드캐스트 암호 기법은 메시지 수신자가 초기 설정된 키 정보를 가지고 과거의 송신자와의 상태에 무관하게 현재의 수신된 브로드캐스트 메시지만으로 새롭게 변경된 그룹 키를 획득할 수 있는 브로드캐스트 암호 기법이다[8,9].

스테이트리스 브로드캐스트 암호 기법을 위해 논리적 트리 구조에 기반한 Complete Subtree (CS) 기법, Subset Difference(SD) 기법등의 효율적인 Subset-Cover Framework 기법이 제안되었다[8].

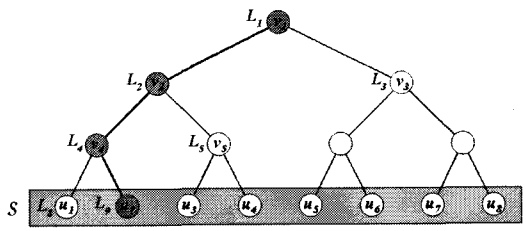

그림 2. Complete Subtree의 키 설정
Fig. 2. Key assignment of Complete Subtree

그림. 2는 CS의 키 분배 기법으로서 사용자 u_2는 자신의 노드와 상위 노드에 해당하는 키 집합 $\{L_1, L_2, L_4, L_9\}$을 할당받는다. 만약 사용자 u_2가 수신 대상자에서 제외되면 브로드캐스터는 사용자 u_2가 가지고 있지 않은 키를 이용하여 메시지를 암호화하여야 한다. 즉, 사용자 u_5, u_6, u_7, u_8를 위하여 L_3키로 세션키 K를 암호화하고, 사용자 u_3, u_4를 위하여 L_5키로 세션키 K를 암호화하고, 마지막으로 u_1을 위하여 L_8키로 세션키 K를 암호화한다. 브로드캐스터는 메시지 M에 대해 아래와 같이 암호문을 구성하여 브로드캐스트 형태로 전송한다.

$$C=<3, 5, 8, E_{L_3}(K), E_{L_5}(K), E_{L_8}(K), F_K(M)>$$

대칭키 암호에서 SD 기법은 CS 기법보다 각각의 사용자가 보유해야 비밀키는 증가하지만 브로드캐스터가 생성해야 되는 암호문의 수가 줄어 상대적으로 CS 기법보다 효율적인 Subset-Cover framework 기법이지만, 공개키 암호에서는 사용자의 공개키 저장 공간 및 공개키 검증에 관한 문제가 야기되었다. 이러한 문제를 해결하기 위하여 Naor외 저자들은 신원기반 암호를 이용하여 CS 기법의 키 설정문제에 대해서는 해결하였지만, 아직까지 SD 기법의 효율적인 키 설정기법이 제안되지 않았다.

스테이트리스 성질은 모바일 환경과 같이 낮은 배터리 용량으로 인해 장기간 온라인 상태를 유지할 수 없는 환경에 유용하게 사용되어질 수 있다.

본 논문에서 제안된 효율적인 신원기반 다중 수신자 암호 기법에 기반한 브로드캐스트 암호 기법의 비밀키 추출 및 키 암호화 단계는 다음과 같다.

[비밀키 추출] 키 생성 센터 (PKG)는 3장에서 제안된 "개인키 추출 알고리즘"을 이용하여 각각 사용자들의 상위 노드에 대한 비밀키(L_i)를 생성하고 그 노드의 하위에 있는 사용자 부분 집합(S_i)에 속한 각각의 사용자들에게 안전한 채널로 전송한다.

$$KGC \rightarrow j \in S_i: \quad L_i = \frac{1}{s + sH(ID(S_i))} P$$

[키 암호화 단계] 브로드캐스터는 PKG의 공개키와 각각의 부분 집합의 신원정보를 입력값으로 암호문을 복호화하기 위한 키(K)를 3장에서 제안된 "암호화 알고리즘"을 이용하여 아래와 같이 암호화한다.

$C=<1,\cdots,n,rP_0,rH_1(ID(S_1))P_0,\cdots,rH_1(ID(S_n))P_0$
$,K\oplus H_2(g^r)>$

정당한 수신자는 자신이 가지고 있는 비밀키(L_i) 집합에서 하나의 비밀키를 입력값으로 암호문을 복호화하기 위한 키(K)를 3장에서 제안된 "복호화 알고리즘"을 이용하여 추출한다.

Baek 외 저자들이 제안한 브로드캐스트 암호 기법의 이점은 암호화 단계에서 모든 사용자의 공개키를 이용하는 것이 아니라, 단지 신뢰센터의 공개키만을 이용하여 암호문을 생성하는 것이다. 제안된 브로드캐스트 암호 기법에서도 신뢰센터의 공개키(P_0)만을 이용하여 암호문을 생성하였으며, 추가적으로 암호화 단계에서 Pairing연산을 제거하였기 때문에 낮은 계산능력을 가진 장치에서도 암호문을 생성하여 브로드캐스트 할 수 있다.

V. 결 론

본 논문에서는 Bilinear Paring을 사용한 효율적인 신원기반 다중 수신자 암호 기법을 제안하였다. 제안 기법은 암호화 과정에서는 Pairing 연산을 필요로 하지 않으며 복호화 과정에서는 단 한번의 Pairing 연산만을 요구한다. 기 제안된 효율적인 신원기반 암호 기법[1]에서는 수신자의 수가 증가함에 따라 G_1상의 덧셈과 스칼라 곱셈이 증가하지만 제안 기법은 스칼라 곱셈만이 수신자의 수에 비례하여 증가한다. 뿐만 아니라, 제안 기법을 활용하여 모바일 환경과 같이 낮은 배터리 용량으로 인해 장기간 온라인 상태를 유지할 수 없는 환경에 유용한 효율적인 스테이트리스 브로드캐스트 암호 기법을 소개하였다.

참고문헌

[1] J. Baek, R. Safavi-Naini, and W. Susilo, "Efficient multi-receiver identity-based encryption and its application to broadcast encryption," Public Key Cryptography - PKC 2005, LNCS 3386, pp. 380-397, 2005.

[2] M. Bellare, A. Boldyreva, and D. Pointcheval, "Multi-recepient encryption schemes: Security notions and randomness re-use," Public Key Cryptography - PKC 2003, LNCS 2567, pp. 85-99, 2003.

[3] K. Kurosawa, "Multi-Recipient Public-Key Encryption with Shortened Ciphertext," Public Key Cryptography - PKC 2002, LNCS 2274, pp. 48-63, 2002.

[4] O. Baudron, D. Pointcheval, and J. Stern, "Exteded Notions of Security for Multicast Public Key Cryptosystems," In ICALP 2000, LNCS 1853, pp. 499-511, 2000

[5] M. Bellare, A. Boldyreva, and S. Micali, "Public-key encryption in a multi-user setting: Security proofs and improvements," Advances in Cryptology - Eurocrypt 2000, LNCS 1807, pp. 259-274, 2000.

[6] A. Shamir, "Identity-based cryptosystems and signature schemes," Advances in Cryptology - Crypto 1984, LNCS 196, pp. 47-53, 1985

[7] D. Boneh and M. Franklin, "Identity-based encryption from the weil paring," Advances in Cryptology - Crypto 2001 , LNCS 2139, pp. 213-229, 2001.

[8] Y. Dodis and N. Fazio, "Public Key Broadcast Encryption for Stateless Receivers," ACM-DRM, 2002.

[9] D. Naor, M. Naor, and J. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," Advances in Cryptology - Crypto 2001, LNCS 2139, pp.41-62, 2001

저자소개

정 채 덕 (Chae Duk Jung)

2005년 동의대학교 수학과 학사
2005년 - 현재: 부경대학교
정보보호학 석사과정

※관심분야 : 암호 프로토콜, 공개키 암호, 신원기반 암호

윤 석 봉 (Suk Bong Yoon)

1985년 동의대학교 수학과 학사
1988년 동국대학교 수학과 석사
1992년 동국대학교 수학과 박사수료
1999년 : 경북대학교 수학과 박사
2000년 - 현재 : 동의대학교 수학과 교수
※관심분야 : 정수론, 공개키 암호, 암호 프로토콜

서 철 (Chul Sur)

2000년 부경대학교 전자계산학과 학사
2004년 부경대학교 전자계산학 석사
2004년 - 현재: 부경대학교
전자계산학과 박사과정

※관심분야 : 암호 프로토콜, 공개키 암호, 신원기반 암호

이 경 현 (Kyung Hyune Rhee)

1982년 경북대학교 수학교육과 학사
1985년 한국과학기술원 응용수학과 석사
1992년 한국과학기술원 수학과 박사
1993년 - 현재 : 부경대학교 전자컴퓨터 정보통신공학부
교수
※관심분야 : 정보보호론, 멀티미디어 정보보호, 네트워크 성능 평가, 그룹키 관리, 재시도 대기체계론