효율적인 인증서기반 다중수신자 암호 기법 및 응용

서철* · 정채덕** · 이경현***

Efficient Multi-Receiver Certificate-Based Encryption Scheme and Its Application

Chul Sur* · Chae Duk Jung** · Kyung Hyune Rhee***

이 논문은 2006년도 정부(과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임
(No. R01-2006-000-10260-0)

요 약

본 논문에서는 다중수신자 환경에서 신원기반 암호 기법의 키 위탁 문제를 해결함과 동시에 묵시적인 공개키 인증을 유지하기 위하여 인증서기반 (certificate-based) 다중수신자 암호 기법을 소개한다. 제안 기법은 다중수신자에 대하여 메시지를 암호화하는 단계에서 Pairing 연산을 제거하였을 뿐만 아니라 복호화 단계에서 단 한번의 Pairing 연산만을 요구한다. 또한, Baek등에 의해 제안되었던 다중수신자 환경에서 가장 효율적인 신원기반 암호 기법[1]과의 계산량 비교를 통하여 제안 기법이 보다 효율적임을 보인다. 마지막으로 제안 기법을 이용하여 Subset-Cover 프레임워크 기반의 새로운 스테이트리스 공개키 브로드캐스트 암호 기법을 제시한다.

ABSTRACT

In this paper, we introduce the notion of certificate-based encryption in multi-receiver environment, which avoids the inherent key escrow problem while preserving the implicit certification in identity-based encryption. We also construct a highly efficient certificate-based encryption scheme for multi-receiver environment, which eliminates pairing computation to encrypt a message for multiple receivers. Moreover, the proposed scheme only needs one pairing computation for decrypting the ciphertext. We compare our scheme with the most efficient identity-based encryption scheme for multi-receiver environment proposed by Baek et.al.[1] in terms of the computational point of view, and show that our scheme provides better efficiency than Baek's scheme. Finally, we discuss how to properly transform our scheme into a new public key broadcast encryption scheme based on subset-cover framework.

키워드

다중수신자 암호, 인증서기반 암호, Key Escrow Free, 공개키 브로드캐스트 암호, Bilinear Pairing

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

접수일자 : 2007. 6. 19

Ⅰ. 서 론

일반적으로, 다중수신자 환경에서 공개키 암호 기법은 다음과 같다. n명의 수신자들은 각각 자신의 공개키 pk_i와 이와 대응하는 개인키 sk_i를 생성한다 $(i=1,\ldots,n)$. 송신자는 다중수신자 암호 기법 및 수신자의 공개키 집합 $(pk_1,\ldots,pk_n)$과 메시지 집합 $(M_1,\ldots,M_n)$을 이용하여 암호문 집합 $(C_1,\ldots,C_n)$을 생성한다. 각각의 수신자 i들은 개인키 sk_i와 암호문 C_i을 입력값으로 메시지 M_i를 복호화한다.

이러한 다중수신자 암호 기법의 특성을 고려할 때, 암호문을 공개된 채널상에서 특정 그룹의 수신자들에게 전송하는 디지털 컨텐츠의 안전한 분배 및 PayTV 시스템등 여러 응용 분야에 활용되어질 수 있다. 이러한 응용 시스템에서, 다중수신자 암호 기법은 메시지 M을 보호하기 위하여 사용되어지는 세션 키 K에 대한 암호화를 위하여 사용되어지며, 전체 암호문은 세션 키 K를 암호화한 암호문과 메시지 M를 암호화한 암호문으로 구성되어진다.

또한, 다중수신자 암호 기법은 일반적인 브로드캐스트 암호 기법으로 변형되어질 수 있다[2]. 브로드캐스트 암호 기법은 송신자가 큰 그룹으로 데이터를 전송하더라도 특정 그룹만이 데이터를 복호화 할 수 있는 암호 기법이다. 특히, 최근에 연구된 신원기반 다중수신자 암호 기법에 기반한 공개키 브로드캐스트 암호 기법은 공개키에 대한 묵시적인 인증을 통하여 인증서 관리의 문제점을 해결하였다[1,3].

하지만, 신원기반 설정은 본질적으로 키 위탁 문제를 내포하고 있기 때문에, 다중수신자 환경에서 신원기반 암호 기법은 저작권 요소의 분배와 같은 다양한 활용에 제한점을 지닌다. 그러므로, 다중수신자 환경에서 신원기반 설정에서의 장점을 유지하면서 키 위탁 문제를 해결할 수 있는 암호 기법에 대한 연구가 필요하다.

본 논문에서는 신원기반 다중수신자 암호 기법의 키 위탁 문제를 해결함과 동시에 묵시적인 공개키 인증을 유지하기 위하여 인증서기반 (Certificate-Based) 다중수신자 암호 기법을 소개한다. 제안 기법은 다중수신자에 대하여 메시지를 암호화하는 단계에서 Pairing 연산을 제거하였을 뿐만 아니라 복호화 단계에서 단 한번의 Pairing 연산만을 요구한다. 또한, Baek등에 의해 제안되었던 다중수신자 환경에서 가장 효율적인 신원기반 암호 기법[1]과의 계산량 비교를 통하여 제안 기법이 보다 효율적임을 보인다. 마지막으로, 제안 기법을 이용하여 Subset-Cover 프레임워크 기반의 새로운 공개키 브로드캐스트 암호 기법을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서는 본 논문의 사전연구를 소개하고, 3장에서 Bilinear Pairing 기반의 다중수신자 환경에서 인증서기반 암호 기법을 제안한 후, 4장에서 제안 기법을 이용하여 스테이트리스 수신자를 위한 새로운 공개키 브로드캐스트 암호 기법을 제시한다. 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 사전연구

2.1 다중수신자 암호 기술

다중수신자 암호 기술의 개념은 Baudron[4]와 Bellare[5]에 의해서 독립적으로 정의되었다. 그들의 주요 결론은 단일수신자 환경에서 안전한 공개키 암호 기법은 다중수신자 환경에서도 안전성을 보장한다는 것이다. 따라서, 안전한 다중수신자 암호 기술은 단일수신자 환경에서 안전한 암호 기술의 서로 다른 n개의 공개키로의 암호화로 구성되어질 수 있다. 예를 들어, ElGamal[6] 암호 기법을 이용한 다중수신자 암호 기법은 다음과 같다.

1. 각 수신자 i의 개인키 $x_i \in Z_q^*$와 공개키를 g^{x_i}라고 가정한다.
2. Z_q^*에서 임의의 $r_1, \cdots, r_n$를 선택한다.
3. 암호문 $C_i=(g^{r_i}, g^{x_i r_i} M_i), (i=1, \cdots, n)$를 계산한다.

Kurosawa[7]는 위 암호 기술보다 계산량과 데이터 전송량을 향상시키기 위하여 "randomness re-use"라고 불리는 기술을 제안하였다. [8]에서는 Kurosawa의 제안 기술을 재정의하고 randomness re-use를 이용하여 단일수신자 공개키 암호기술이 다중수신자 공개키 암호기술의 구성에 적합한 일반적인 방법을 제안하였다.

Boneh와 Franklin의 실용적인 신원기반 암호 기술[9]의 제안으로 인하여, 다양한 신원기반 다중수신자 암호 기술이 제안되었으며[10,11], 최근 Bilinear Pairing을 기반하여 암호화 단계에서 한번의 Pairing 연산을 요구하

고 복호화 단계에서 두 번의 Pairing 연산을 요구하는 효율적인 신원기반 다중수신자 암호기술이 제안되었다[1].

2.2 인증서기반 암호 기술

전통적인 공개키기반 구조 (PKI, Public Key Infrastructure)에서는 사용자의 공개키와 신원정보간의 연관성을 명확하게 인증하기 위하여 신뢰기관 (CA, Certificate Authority)에 의해 전자서명된 인증서를 사용하였다. 하지만, 공개키기반 구조에서 사용자는 메시지를 수신자의 공개키로 암호화하기 전에 수신자의 인증서 상태 검증을 위한 질의 (Third-Party Queries)를 요청해야 된다. 이러한 인증서 상태 검증을 위하여 CRL (Certificate Revocation List) 또는 OCSP (Online Certificate Status Protocol)와 같은 기술들이 사용되어지고 있지만 이러한 대응 방안은 신뢰기관에게 많은 계산량과 통신량을 요구한다.

위에서 기술한 전통적인 공개키기반 구조의 문제점을 해결하기 위하여, 신원기반 암호 기법이 제안되었다. 신원기반 암호 기법은 사용자의 신원을 나타낼 수 있는 e-mail주소, IP주소, 주민등록번호등을 이용하여 공개키를 사용하여 공개키에 대한 인증을 생략하는 암호 기법으로써 사전에 분배된 공개키 없이도 수신자의 알려진 신원정보를 활용하여 수신자에게 평문에 대한 암호문을 전송할 수 있다. 그러나, 신원기반 암호 기법에서는 수신자가 비밀키 생성 센터 (PKG, Private Key Generation Center)로부터 비밀키를 전송받아야 하므로 본질적인 키 위탁 문제를 내포하고 있다. 따라서, 비밀키 생성 센터는 사용자의 모든 암호문을 복호화 할 수 있다. 또한, 사용자에 해당하는 비밀키를 안전한 채널을 통해 전송해야 되는 키 분배 문제점을 가지고 있다.

2003년 Gentry[12]는 전통적인 공개키기반 암호 기법과 신원기반 암호 기법의 장점을 유지하면서 단점을 보완하는 새로운 인증서기반 암호 (CBE, Certificate-Based Encryption) 기법을 제안하였다. 인증서기반 암호 기법은 인증서 상태 검증을 위한 질의 문제의 해결방안인 묵시적 인증 기법과 키 위탁 문제의 해결방안인 사용자가 직접 개인키를 생성하는 기법을 융합한 새로운 암호 기법이다.

Ⅲ. 인증서기반 다중수신자 암호

3.1 정의

본 절에서는 단일수신자 환경에서 기 정의 되었던 인증서기반 암호 기법[12]을 다중수신자 환경으로 확장하기 위하여 새로운 인증서기반 다중수신자 암호 기법을 정의한다. 인증서기반 다중수신자 암호 기법의 일반적인 모델은 다음과 같다.

정의1. 인증서기반 다중수신자 암호(MR-CBE)

단일 메시지 브로드캐스팅을 위한 일반적인 인증서기반 다중수신자 암호 기법은 6단계로 구성되어지며, 수행절차는 다음과 같다.

- **설정단계.** 신뢰기관 (CA, Certificate Authority)에서 수행되는 확률적인 알고리즘으로써, 보안 매개변수 k를 입력값으로하여, CA의 마스터 키 SK_{CA}와 시스템 변수 params를 출력한다.

- **키 설정단계.** 사용자 i에서 수행되는 확률적인 알고리즘으로써, 시스템 변수 params를 입력값으로 사용자 i의 공개키 pk_i와 개인키 sk_i를 출력한다.

- **인증서 생성단계.** CA에서 수행되는 결정적인 알고리즘으로써, CA의 마스터 키 SK_{CA}, 시스템 변수 params, 사용자 i의 공개키 pk_i, 시간구간 τ_i, 사용자의 추가정보 (신원정보등) λ_i를 입력값으로 하여 사용자 i의 인증서 $Cert'_{\tau_i}$를 출력한다.

- **통합단계.** 결정적인 알고리즘으로써 시스템 변수 params, 사용자 i의 τ_i, λ_i, $Cert'_{\tau_i}$와 $Cert_{\tau_i-1}$ (optionally)을 입력값으로, 사용자 i의 시간구간 τ_i에서의 인증서 $Cert_{\tau_i}$를 출력한다.

- **암호화단계.** 확률적인 알고리즘으로써, 메시지 M, 시스템 변수 params, 다중수신자의 시간구간 집합 $(\tau_1,\cdots,\tau_n)$, 추가정보 집합 $(\lambda_1,\cdots,\lambda_n)$, 공개키 집합 $(pk_1,\cdots,pk_n)$을 입력값으로, 메시지 M에 대한 암호문 C를 출력한다.

- **복호화단계.** 결정적인 알고리즘으로써, 수신된 암호문 C, 시스템 변수 params, 수신자 i의 인증서 $Cert_{\tau_i}$와 개인키 sk_i를 입력값으로, 메시지 M또는 $\perp$를 출력한다.

기 제안된 인증서기반 암호 기법[12]과 같이 인증서 기반 다중수신자 암호 기법에서는 인증서 통합단계를 포함할 필요가 없으며, 이러한 경우 통합단계는 간략하게 $Cert_{\tau_i} = Cert'_{\tau_i}$으로 설정된다.

제안 기법이 기반하고 있는 Bilinear Pairing과 관련 계산상의 어려운 문제에 대한 정의는 다음과 같다.

정의2. 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, $e(aP, bQ) = e(P, Q)^{ab} = e(abP, Q)$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.

정의3. p-BDHI (p-Bilinear Diffie-Hellman Inversion) 가정

어떤 $\alpha \in Z_q^*$에 대하여,

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

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

3.2 Bilinear Pairing기반의 효율적인 인증서기반 다중수신자 암호 기법

본 절에서는 키 위탁문제를 해결함과 동시에 묵시적인 공개키 인증을 제공하는 효율적인 다중수신자 암호 기술을 제안한다. 제안 기술은 5단계로 구성되어 있으며, 각 단계별 수행절차는 다음과 같다.

[설정단계] 신뢰기관 (CA)는 보안 매개변수 k, k_0를 입력 값으로 하여 다음과 같은 절차를 수행한 후 시스템 변수 params와 마스터 키 s를 출력한다.

1. 보안 매개변수 k, k_0를 입력받아 k-비트 소수 q, 위수 q를 갖는 군 G_1, G_2, 허용 가능한 Bilinear Pairing $e : G_1 \times G_1 \rightarrow G_2$를 출력하고 임의의 G_1의 생성자 P를 선택한다.
2. CA의 마스터 키 $SK_{CA} = s \in Z_q^*$를 선택하고, CA의 공개키는 $PK_{CA} = P_0 = sP$로 설정한다.
3. 암호학적 해쉬함수 $H_1 : \{0,1\}^* \rightarrow Z_q^*$, $H_2 : G_2 \rightarrow \{0,1\}^{k_0}$, $H_3 : \{0,1\}^* \rightarrow Z_q^*$, $H_4 : \{0,1\}^{k_0} \rightarrow \{0,1\}^{k_1}$를 설정한 후, $g = e(P,P) \in G_2$를 선택한다.

시스템 변수 params 는 다음과 같이 구성된다.

$$\{q, k, k_0, k_1, G_1, G_2, P, P_0, g, e, H_1, H_2, H_3, H_4, M, C\}$$

또한, 평문(M)과 암호문(C)의 크기는 다음과 같다.

$$M = \{0,1\}^{k_1},$$
$$C = G_1 \times \cdots \times G_1 \times \{0,1\}^{k_0} \times \{0,1\}^{k_1} \times \{0,1\}^*$$

[키 설정단계] 시스템 변수를 이용하여 사용자 i는 개인키 $sk_i = x_i \in Z_q^*$를 선택하고, 공개키 pk_i를 다음과 같이 설정한다.

$$pk_i = (x_i P, x_i P_0) = (P_i, P_i') \in G_1 \times G_1$$

[인증서 생성단계] 사용자 i는 CA로 부터 다음과 같은 절차를 통해서 인증서를 획득한다.

1. 사용자 i는 자신의 공개키(pk_i)와 신원정보와 같은 사용자 추가정보(λ_i)를 포함하는 $UserInfo_i$를 CA에게 전송한다.
2. CA는 사용자의 정보 $UserInfo_i$를 검증한다.
3. CA는 검증된 사용자의 정보에 대하여 구간 τ_i에 해

당하는 h_i를 다음과 같이 계산한다.

$$h_i = H_1(PK_{CA}, \tau_i, UserInfo_i) \in Z_q^*$$

4. CA는 사용자 i의 인증서 $Cert_i = \frac{1}{s+h_i}P$를 생성한 후 사용자 i에게 전송한다.

[암호화단계] 송신자는 메시지 M을 다중수신자들의 정보 $UserInfo_i (i = 1, \cdots, n)$를 이용하여 다음과 같은 절차를 통해서 암호문 C를 생성한다.

1. 송신자는 $h_i, h'_i (i = 1, \cdots, n)$를 계산한다.

$$h_i = H_1(PK_{CA}, \tau_i, UserInfo_i) \in Z_q^*$$
$$h'_i = H_1(UserInfo_i) \in Z_q^*$$

2. 임의의 $\sigma \in \{0, 1\}^{k_0}$를 선택하고, $r = H_3(M \| \sigma \| L) \in Z_q^*$를 계산한 후, 암호문 C을 계산한다.

$$C = (U_1, \cdots, U_n, V, W, L)$$
$$= (rh'_1(h_1P_1 + P_1'), \cdots, rh'_n(h_nP_n + P_n'), \sigma \oplus H_2(g^r), M \oplus H_4(\sigma), L)$$

L은 U_i에 대응되는 사용자에 대한 정보를 나타내는 라벨 (label)이다.

[복호화단계] 수신자 i는 다음과 같은 절차를 통하여 암호문 C를 복호화한다.

1. 암호문내의 L을 이용하여 수신자 i에 해당하는 U_i를 찾는다.
2. $\sigma' = V \oplus H_2(e(Cert_i, U_i)^{1/h'_i x_i})$를 계산한다.
3. $M' = W \oplus H_4(\sigma')$, $r' = H_3(M' \| \sigma' \| L)$를 계산한다.
4. 만약 $U_i \neq r'h'_i(h_iP_i + P_i')$이면, $\perp$를 출력하고, 그렇지 않으면 M'를 평문으로 출력한다.

제안 기법의 일치성은 다음과 같이 증명된다.

$$e(Cert_i, U_i)^{1/h'_i x_i}$$
$$= e(Cert_i, rh'_i(h_iP_i + P_i'))^{1/h'_i x_i}$$
$$= e(\frac{1}{s+h_i}P, rh'_i(x_ih_iP_i + sx_iP))^{1/h'_i x_i}$$
$$= e(\frac{1}{s+h_i}P, rh'_i x_i(s+h_i)P)^{1/h_i' x_i}$$
$$= g^r$$

3.3 효율성

기 제안된 효율적인 신원기반 다중수신자 암호 기법 [1]과 제안 기법의 효율성에 대한 자세한 비교는 표. 1과 같다. 제안 기법은 암호화 단계에서는 Pairing연산을 요구하지 않으며 복호화 단계에서만 한번의 Pairing연산을 요구한다.

표 1. 제안 기술과 [1]의 계산량 비교
Table 1. Comparisons of Computational Costs

	제안 기술	[1]
Pairing (암호화/복호화)	0 / 1	1 / 2
덧셈연산 (in G_1)	n	n
지수연산 (in G_2)	1	1

비록, 제안 기법이 Pairing 연산을 제외한 연산에서는 [1]와 비슷하지만, Bilinear Pairing 기반의 암호시스템에서 Pairing 연산을 줄이는 것은 매우 중요하다. 왜냐하면, Pairing 연산은 아직까지 유한체상에서의 지수연산과 같은 일반적인 연산보다 많은 계산을 요구하기 때문이다. 최근의 MIRACL[13]에 따르면 512-비트 Tate Pairing은 20ms 시간이 소요되는 반면, 1024-비트 법(modular)상에서 지수연산은 8.80ms 시간이 소요된다.

Ⅳ. 브로드캐스트 암호 기법으로의 응용

4.1 공개키 브로드캐스트 암호와 Subset -Cover 프레임워크

브로드캐스트 암호 기법[2]은 메시지 송신자인 그룹 관리자 또는 브로드캐스터 (Broadcaster)가 암호화된 데이터를 공개된 채널 상에서 특정 그룹의 수신자들에게 전송하며, 전송된 암호문은 단지 정당한 수신자들만이 복호화가 가능한 암호 기법이다. 최근 브로드캐스트 암

호 기법은 디지털 컨텐츠의 분배 및 보호, 위성 기반의 비즈니스, 그룹 통신등 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 전송 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.

기존에는 대칭키 브로드캐스트 암호 기법[14]이 소개되었지만, 최근에는 공개키 브로드캐스트 암호 기법[3]이 많은 주목을 받고 있다. 대칭키 브로드캐스트 암호 기법에서는 그룹 관리자만이 데이터를 암호화하여 브로드캐스트 할 수 있지만, 공개키 브로드캐스트 암호 기법은 그룹 관리자 뿐만 아니라 그룹내 사용자들도 암호화된 데이터를 브로드캐스트할 수 있다. 최근, 컴퓨터 및 기타 장치의 발달과 보편화로 인하여 일반 사용자들이 쉽게 콘텐츠를 만들 수 있게 되어, 공개키 브로드캐스트 암호 기법의 연구가 더욱 필요하다.

브로드캐스트 암호에서의 또 다른 중요한 이슈는 스테이트리스 (Stateless) 수신자 환경을 위한 브로드캐스트 암호 기법에 관한 연구이다. 스테이트리스 수신자 환경이란 시스템 설정단계에서 시스템 사용자들에게 분배된 그룹키들이 시스템의 라이프타임동안 변경되지 않는 환경이다. 이러한 환경에서의 브로드캐스트 암호 기법을 위하여 논리적 트리 구조에 기반한 Subset-Cover 프레임워트가 제안되었으며, Subset-Cover 프레임워크를 실현하기 위하여 Complete Subtree (CS) 기법과 Subset Difference(SD) 기법이 제안되었다[14].

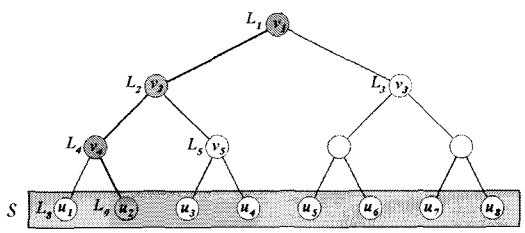


그림 1. CS 기법의 키 설정
Fig. 1. The key tree topology of the CS method

그림. 1는 CS 기법의 키 분배 방식으로서 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 암호화한다. 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.

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

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

4.2 제안 기법기반 공개키 브로드캐스트 암호

본 절에서는 제안 기법을 기반하여 스테이트리스 수신자 환경을 위한 새로운 공개키 브로드캐스트 암호 기법을 소개한다. [14]에서는 CS 기법이 공개키 브로드캐스트 암호에 적용되어질 수 있음을 보였으며, [3]에서는 신원기반 암호 기법을 이용하여 CS 기법에 기반한 스테이트리스 공개키 브로드캐스트 암호 기법을 제안하였다.

본 논문에서는 [3]의 적용 방법을 이용하여 제안 기법을 CS 기법에 기반한 공개키 브로드캐스트 암호 기법으로 확장한다.

먼저, 각 부분집합 S_i에 대한 신원정보 $ID(S_i)$는 최상위노드로부터 하위노드로 내려오면서 왼쪽의 자식노드는 부모노드의 신원정보에 0을 추가하고, 오른쪽에 있는 자식노드는 1을 추가하도록 정의한다. 이후, 센터는 제안 기법의 설정단계를 수행하여 시스템 변수를 생성 및 공개하고, 각 부분집합의 신원정보를 나타내는 매핑 함수를 공개한다.

설정단계 이후, 각 사용자는 제안 기법의 키 설정단계를 수행하여 자신의 공개키/개인키 쌍을 생성한다. 또한 각 사용자들은 자신이 포함된 부분집합들의 공개키/개인키 쌍들을 생성하기 위하여 자신의 개인키와 이웃노

드의 공개키를 이용하여 각 부분집합들의 개인키들을 생성한다.

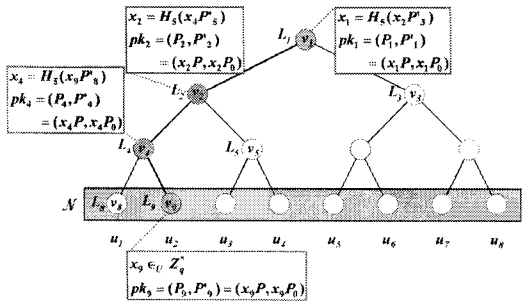


그림 2. 제안 기법의 키 설정
Fig. 2. Our key tree topology

예를 들어, 그림 2.에서와 같이 사용자 u_2는 $x_9 \in Z_q^*$를 선택하고 상위 노드(v_4, v_2, v_1)들의 개인키를 암호학적 해쉬함수 $H_5 : G_1 \rightarrow Z_q^*$를 이용하여 다음과 같이 계산한다.

$$\begin{cases} x_4 = H_5(x_9 P_8') \\ x_2 = H_5(x_4 P_5') \\ x_1 = H_5(x_2 P_3') \end{cases} \quad (1)$$

위의 식 (1)의 결과로, 사용자 u_2만이 개인키 집합 (x_1, x_2, x_4, x_9)를 계산할 수 있다.

키 설정단계 이후, 암호화 된 세션키 K를 복호화하기 위해 각 부분집합에 해당하는 인증서를 생성하고 부분집합에 속하는 각 사용자들에게 분배되어야 된다. 부분집합의 인증서 L_j^{Cert}를 생성하기 위하여 부분집합의 정보 $SubsetInfo_j$을 생성하여, 구간 τ_j에 해당하는 인증서를 제안 기법의 인증서 생성단계를 아래와 같이 수행한다($SubsetInfo_j$는 부분집합의 공개키 pk_i와 부분집합의 신원정보 $ID(S_j)$로 구성된다).

$$L_j^{Cert} \leftarrow Certify(params, SubsetInfo_j, \tau_j, s)$$

센터 또는 사용자가 정당한 다중수신자에 대하여 메시지를 암호화 할 때, 정당한 수신자들의 부분집합들에 해당하는 부분집합의 정보 $SubsetInfo_j$와 공개키 pk_j를 이용하여 메시지 암호화에 사용된 세션키 K를 제안 기법의 암호화단계 절차에 따라 수행하고, 그 결과로서 암호문을 출력하고 브로드캐스트 형태로 전송한다.

$$C_j \leftarrow Encrypt(params, SubsetInfo_j, pk_j, \tau_j, K)$$

정당한 각 수신자들은 자신의 개인키 집합에서 암호화에 사용된 공개키에 대응하는 개인키를 이용하여 암호문을 복호화한다.

4.3 새로운 공개키 브로드캐스트 암호 기법 분석

기 제안되었던 스테이트리스 수신자 환경을 위한 공개키 브로드캐스트 암호 기법[1,3]에서는 센터가 공격자에 의해 손상되었을 경우, 키 위탁문제로 인하여 시스템 내의 모든 개인키들이 손상된다. 그러므로, 시스템을 복구하기 위해서는 모든 부분집합에 해당하는 새로운 개인키를 생성해야 하고, 사용자들에게 새롭게 생성된 개인키 집합을 안전한 채널을 통해서 전송하여야 한다. 하지만, 스테이트리스 수신자 환경의 경우 수신자가 항상 온라인 상태를 유지하기 힘들므로 새로운 개인키 집합의 재분배에 많은 제약이 따른다. 하지만, 본 논문에서 제안된 새로운 공개키 브로드캐스트 암호 기법은 신원기반 암호 기법에서의 키 위탁문제를 해결한 인증서기반 암호 기법을 사용하였기 때문에, 위와 같은 상황이 발생하더라도 새로운 개인키 집합을 재분배할 필요가 없고, 또한 암호문 복호화를 위한 새로운 인증서 분배가 필요한 경우에도 안전한 채널을 요구하지 않는다.

또한, 제안 기법은 기 제안되었던 스테이트리스 수신자 환경을 위한 공개키 브로드캐스트 암호 기법[1,3]보다 계산량 측면에서도 보다 효율적이며, 제안 기법의 브로드캐스트 메시지에 대한 전송량은 기존의 기법[14]과 동일하다(즉, $\mu \log N/\mu$, μ는 탈퇴자 수, N는 총 사용자 수).

V. 결 론

본 논문에서는 신원기반 다중수신자 암호 기법에서의 키 위탁 문제를 해결한 인증서기반 다중수신자 암호 기법을 소개하였으며, Bilinear Pairing을 이용한 기 제안된 신원기반 다중수신자 암호 기법[1]보다 효율적인 인증서기반 다중수신자 암호 기법을 제안하였다. 제안 기

법은 암호화 과정에서는 Pairing 연산을 필요로 하지 않으며 복호화 과정에서는 단 한번의 Pairing 연산만을 요구하는 효율적인 기법이다. 뿐만 아니라, 제안 기법을 활용하여 모바일 환경과 같이 낮은 배터리 용량으로 인해 장기간 온라인 상태를 유지할 수 없는 환경에 유용한 새로운 스테이트리스 공개키 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] A. Fiat and M. Naor, "Broadcast Encryption," Advances in Cryptology - Crypto 1994, LNCS 773, pp. 480-491, 1994.

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

[4] O. Baudron, D. Pointcheval, and J. Stern, "Exteded Notions of Security for Multicast Public Key Cryptosystems," 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] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Transactions on Information Theory, Vol.31, pp. 469-472, 1985.

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

[8] 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.

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

[10] L. Chen, K. Harrison, D. Soldera, and N. P. Smart, "Applications Multiple Trust Authorities in Pairing Based Cryptosystems," InfraSec 2002, LNCS 2437, pp. 260-275, 2002.

[11] N. P. Smart, "Access Control Using Pairing Based Cryptography," CT-RSA 2003, LNCS 2612, pp. 111-121, 2003.

[12] C. Gentry, "Certificate-Based Encryption and the Certificate Revocation Problem," Advances in Cryptology - Eurocrypt 2003, LNCS 2656, pp. 272-293, 2003.

[13] MIRACL, Multiprecision Integer and Rational Arithmetic C/C++ Library, http://indigo.ie/mscott

[14] 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.

[15] S. S. Al-Riyami and K. G. Paterson. "Certificateless Public Key Cryptography," Advances in Cryptology-Asiacrypt 2003, LNCS 2894, pp. 452-473, 2003.

[16] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," ACM CCS'93, pp. 62-73, 1993.

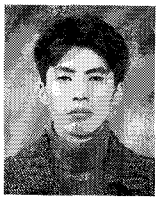
[17] D. Boneh and X. Boyen, "Efficient selective-id secure identity based encryption without random oracles," Advances in Cryptology - Eurocrypt 2004, LNCS 3027, pp. 223-238, 2004

[18] D. Boneh and X. Boyen, "Short signatures without random oracles," Advances in Cryptology - Eurocrypt 2004, LNCS 3027, pp. 56-73, 2004

[19] L. Chen and Z. Chen, "Security proof of Sakai-Kashahara's identity-based encryption scheme," Cryptography ePrint Archive, Report 2005/226, 2005.

[20] E. Fujisaki and T. Okamoto, "Secure integration of asymmetric and symmetric encryption schemes," Advances in Cryptology - Crypto'99, LNCS 1666, pp.535-554, 1999.

저자소개



서 철 (Chul Sur)

2000년 부경대학교 전자계산학과 학사
2004년 부경대학교 전자계산학과 석사
2004년 - 현재: 부경대학교
전자계산학과 박사과정
※관심분야 : 암호 프로토콜, 공개키 암호, 신원기반 암호

정 채 덕 (Chae Duk Jung)

2005년 동의대학교 수학과 학사
2007년 부경대학교 정보보호학과 석사
2007년 - 현재: 부경대학교
정보보호학과 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, 공개키 암호, 신원기반 암호, 멀티미디어 정보보호, 그룹 키 관리,