# 브로드캐스트 암호화에서의 효율적인 키 갱신 방법에 관한 연구

이덕규, 이임영*

*순천향대학교, 정보기술공학부

# A Study on Efficient Key Renewal for Broadcast Encryption

Deok-Gyu Lee, Im-Yeong Lee*

*Division of Information Technogy Engineering Soonchunhyang Univ.

## 요 약

브로드캐스트 암호화 기법은 공개된 네트워크 상에서 멀티미디어, 소프트웨어, 유료 TV 등의 디지털 정보들을 전송하는데 적용되고 있다. 브로드캐스트 암호화 기법에서는 중요한 것은 오직 사전에 허가된 사용자만이 디지털 정보를 얻을 수 있어야 한다는 것이다. 브로드캐스트 메시지가 전송되면 권한이 있는 사용자들은 자신이 사전에 부여받은 개인키를 이용하여 먼저 세션키를 복호화하고 이 세션키를 통하여 디지털 정보를 얻게 된다. 이와 같이 사용자는 브로드캐스터가 전송하는 키를 이용하여 메시지나 세션키를 획득하게 되는데, 이러한 과정에서 브로드캐스터가 키를 생성하고 분배하는 과정이 필요하다. 또한 사용자가 탈퇴나 새로운 가입시에 효율적인 키 갱신이 필요하게 된다. 본 논문에서는 효율적인 키 생성과 분배, 키 갱신 방법에 대해 소개한다.

## I. 서론

최근 브로드캐스트 암호화 기법은 공개된 네트워크 상에서 멀티미디어, 소프트웨어, 유료 TV 등의 디지털 정보들을 전송하는데 적용되고 있다.

키를 제공하는 방식 중에 하나인 공개키 방식은 세션키를 암호화하기 위한 그룹의 암호화키는 하나이고 이를 복호하기위한 키는 여러개의 무수히 많은 키를 이용함으로써 서버는 세션키를 암호화하고 각 사용자에게는 서로 다른 키를 이용하여 복호화 할수 있도록 되어 있다.

브로드캐스트 암호화 기법에서 중용한 것은 오직 사전에 허가받은 사용자만이 디지털 정보를 얻을 수 있어야 한다는 것이다. 브로드캐스트 메시지가 전달되면 권한이 있는 사용자들은 자신이 사전에 부여받은 개인키를 이용하여 먼저 세션키를 복호화하고 이 세션키를 통하여 디지털 정보를 얻게 된다. 브로드 캐스트 암호화에 있어 가장 중요한 것은 키 생성, 분배, 갱신이다.

제안 방식에서는 빠른 키 갱신을 위한 키 갱신 인자를 첨가하고 이 인자를 통해 새로운 신규 가입자 혹은 탈퇴자가 발생하더라도 기존의 사용자에게 갱신값을 제공함으로써 쉽게 키 갱신이 간능해지도록 설계하였다.

본 논문은 Broadcast Encryption의 개요 중에서 적용방식에 대해 간략히 설명하고 제안방식의 각 단계에 관하여 살펴본다. 각 단계에 관한 프로토콜을 살펴본 마지막으로 결론으로써 끝을 맺도록 한다.

## II. Broadcast Encryption 개요

### 1. 적용 방식

브로드캐스트 암호화는 다음과 같이 2가지 모델을 기반으로 할 수 있다. 적용모델간의 차이점이 있지만 각각에 대하여 살펴보면 다음과 같다. 우선 첫 번째 모델은 아래의 그림과 같다.

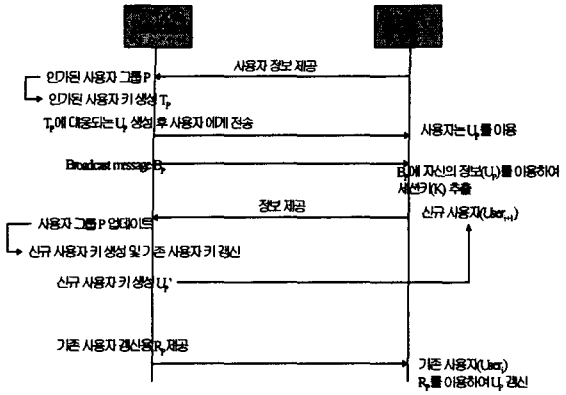


그림 1. 적용모델 1

사용자와 서버간의 정보를 이용하여 키를 생성/분배하는 방식이다. 다음은 기존의 멀티캐스트 방식과 유사하다. 이는 전송되는 방식에서 차이가 존재할 뿐 제공되는 베시지가 이전의 사용 그룹에 의해 결정되는 점에서 유사하다.

키 생성과정에서 사용자가 참여하여야 하므로 생성시간에 사용자의 참여 시간이 포함될 수 있다. 키 갱신과정에서도 기존 사용자의 탈퇴/신규 사용자의 참여 시 키 갱신에 따른 소요시간이 많이 발생하게 된다.

위 방식과 다르게 서버가 키를 생성하는 방식으로 두 번째 적용 모델을 살펴볼 수 있다.

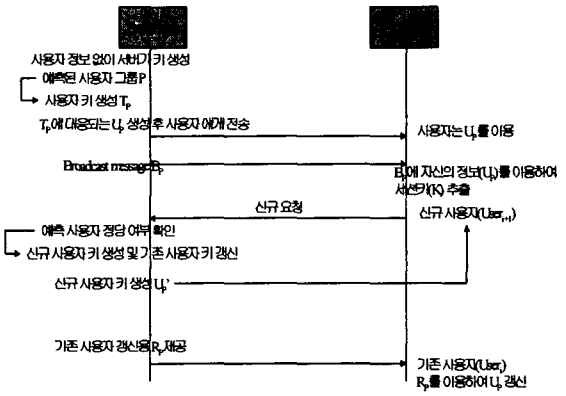


그림 2 적용 모델 2

서버가 단독으로 참여할 사용자를 예측하여 키를 생성한다. 이러한 방법은 사용자의 동의 없이 서버가 모든 사용자의 키를 생성하게 됨으로써 빠른 생성과 빠른 갱신이 가능하다. 하지만 서버가 악의적인 목적 혹은 서버가 공격의 대상이 되었을 경우 많은 취약점을 내포하고 있다.

# III. 제안방식

기존 사용자등의 탈퇴 혹은 신규사용자의 가입에 따른 효율적인 키 갱신을 위해 다음 방식을 제안한다.

## 1. 제안방식 개요

다음은 제안방식의 전체적인 개요에 대하여 살펴본다. 다음 그림은 본 제안방식에서 나타날 수 있는 시나리오를 구분한 것이다. 다음의 시나리오를 살펴보면 기본적인 흐름, 갱신 흐름, 신규과정 흐름, 탈퇴흐름, 사용자 예측 오류 흐름등으로 볼 수 있다. 아래의 시나리오에 따라 제안 방식은 크게 세부분으로 구분된다. 첫째 키 생성 및 분배 부분, 브로드캐스트 메시지 생성 부분, 마지막으로 키 갱신 부분으로 나뉠 수 있다.

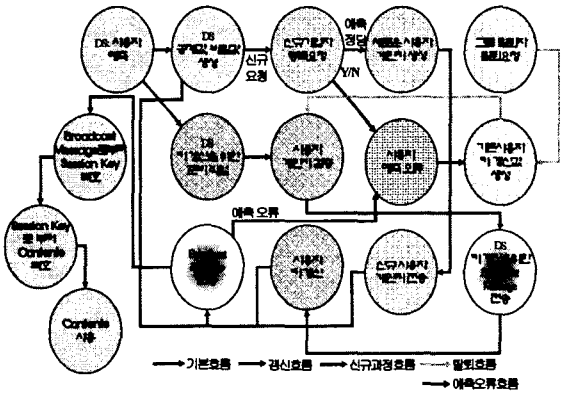


그림 3. 제안방식 전체 흐름도

또한 본 제안방식은 다음과 같은 특징을 가지고 있다. 사용자의 개인키는 서버가 생성하며, 사용자 이외의 사람은 브로드캐스팅되는 메시지에 대해 복호할 수 없다. 신규가입자, 사용자 탈퇴 등에 따른 키 갱신이 용이하다.

## 2. 시스템 계수

다음은 본 방식에서 사용되는 시스템 계수를 기술한 것이다.

- p : 소수 ≥512 bit
- q : 소수 ≥160 bit (q | p-1)
- l : 개인키 생성을 위한 수
- e : 공개 암호화 키
- $d_1, \ldots, d_k$ : 개별 복호화키 리스트

· M : 메시지 · S : 세션 키

· k : 사용자

· $r_i$ : 랜덤 수 집합($r_i \in Z_p$) ($r_1, \ldots, r_k$)

· $h_i = g^{r_i}$ · $<y, h_1, \ldots, h_k>$ : 공개키

· $y = \Pi\ h_i^{a_i}$

· $a_i$ : 랜덤수 ($a_i \in Zq$) $\{a_1, \ldots, a_k\}$

· $d_i = \theta_i \cdot \gamma^{(i)}$ ($\gamma^{(i)} \in \Gamma$)

· $\Gamma = \gamma_1, \gamma_k$

· a: 랜덤 요소($a \in Z_q$)

· C: 방송 메시지(Broadcast message)

· $C = <M(or\ S)y^{aT}, h_1^a, \ldots, h_k^a>$

$= <B, H_1, \ldots, H_k>$

· $B = M(or\ S)\ y^a$

· $H_i = \Pi h_i^a$

· T : 키 갱신을 위한 인자 ($t_1, \ldots, t_k \in Z_q$), $T = t_1 \cdot \ldots \cdot t_k$

## 3. 프로토콜

### 1) 키 생성 및 분배 단계

키 생성은 서버의 담당이며, 개인키와 공개키를 생성하고 전달하기 위해 다음의 일련의 과정을 거친다.

(1) 서버는 사용자를 예측하여 이를 바탕으로 열을 랜덤하게 선택한다.

$i = 1, \ldots, k$ 예측 $\Rightarrow r_i$열 선택

(2) 이 선택된 랜덤열을 바탕으로 공개키 작성에 필요한 값을 생성한다.

$h_i = g^{r_i} \bmod q$ 계산

공개키 $<y, h_1, \ldots, h_k>$

갱신을 위해 T생성 : $T = t_1 \cdot \ldots \cdot t_k$

(3) 생성된 값 h를 이용하여 공개키를 작성한 후 이를 바탕으로 개인키를 계산한다.

$\theta i = (\sum rj\alpha jtj)/(\sum rj\gamma j) \bmod q$

(4) 생성된 개인키 di를 사용자에게 전송한다.

$di = \theta i \cdot \gamma i$

(5) 사용자는 전송받은 di에서 θi를 획득한다.

$di = \theta i \cdot \gamma i\ /\ \gamma i$

### 2) 브로드캐스트 메시지 생성 단계

브로트캐스트 메시지를 전송하는데 있어 메시지를 암호화한 세션키를 암호화하여 전송할 수 있고 메시지 자체를 암호화하여 전송할 수 있다. 다음에서는 두가지 모두를 고려하여 기술한다.

(1) 메시지 M 혹은 세션키 S를 암호화하여 계산하다.

(2) 랜덤 요소 a를 선택하고 키 갱신 요소 T를 연산하여 랜덤요소와 갱신요소를 같이 메시지 작성에 사용한다.

(3) 브로드캐스트 메시지를 작성하여 전송한다.

$C = <M(or\ S)yaT, h1a, , h2ka>$

(4) 전송받은 메시지는 개인키를 이용하여 메시지 M이나 세션키 S를 획득한다.

$M(or\ S) = B/U^{\theta i},\ U = \Pi Hj^{\gamma j}$

$U^{\theta i} = (\Pi Hj^{\gamma j})^{\theta i} = (\Pi g^{\alpha rj \gamma j})^{\theta i} = (g^{rj \gamma j})^{\theta ia} = (g^{rj \alpha j})^a = (hj^{\alpha jT})^a = y^{aT}$

$M(or\ S) = M(or\ S) \cdot y^{aT}/y^{aT}$

### 3) 키 갱신 단계

사용자의 탈퇴 혹은 신규 가입자가 발생한 경우 다음과 같은 과정을 거친다.

(1) 사용자 i가 탈퇴를 요청

(2) 서버는 기존 사용자의 개인키를 갱신하기 위해 갱신요소인 T에서 사용자 i의 갱신요소를 제거한다.

(3) 제거한후 개인키를 갱신하고 사용자에게 전송한다.

$\theta i \cdot \gamma(i) \cdot ti\text{-}1 = di'$

(4) 갱신된 키를 이용하여 사용자들은 브로드캐스트 메시지를 전송받고 다음과 같이 암호화된 메시지를 복호화하여 메시지를 획득하게 된다.

$(C=<B, H1, \ldots, H2k>) = (C = <M(or\ S) \cdot yaTti\text{-}1, h1a, \ldots, h2ka>)\ \theta i$이용 계산

$M(or\ S) = B/U^{\theta iti\text{-}1},\ U = \Pi Hj^{\gamma j}$

$U^{\theta iti\text{-}1} = (\Pi Hj^{\gamma j})^{\theta iti\text{-}1} = (\Pi g^{\alpha rj \gamma j})^{\theta iti\text{-}1} = (g^{rj \gamma j})^{\theta iati\text{-}1} = (g^{rj \alpha jti})^{ati\text{-}1} = (H^{j \alpha jti})^a = y^{aTti\text{-}1}$

$M(or\ S) = M(or\ S) \cdot y^{aTti\text{-}1}/y^{aTt\text{-}1}$

| 데이터제공자(DS) | 공개정보 (p,q, r) ($\Gamma$, <y,h1,...,h2k>,) | 사용자 |
|---|---|---|
| 1. hi=gri mod q계산<br>2. <y,h1,...,h2k>,y=$\Pi$ i=12khi $\alpha$ i,<br>3. $\gamma$(i)=($\gamma$1,..., $\gamma$2k) $\in\Gamma$><br>4. $\theta$i • $\gamma$(i)=di<br>5. $\theta$i=($\Sigma$rj $\alpha$ jtj)/($\Sigma$rj $\gamma$j) mod q | | |
| Broadcast Message 작성 | | C=<B, H1,...,H2k> |
| | | 1. M(or S)=B/$U^{\theta i}$<br>2. U=$\Pi$Hj$^{rj}$<br>3. $U^{\theta i}$ = ($\Pi$Hj$^{\gamma j}$)$^{\theta i}$ = ($\Pi g^{\alpha j \gamma j}$)$^{\theta i}$ = $(g^{\gamma j \gamma j})^{\theta i \alpha}$ = $(g^{\gamma j \alpha})^{a}$=$(hj^{\alpha jT})^{a}$= $y^{aT}$<br>4. M(or S) = M(or S) • $y^{aT}/y^{aT}$ |
| 1. 기존개인키갱신<br>2. 개인키갱신에해당하는ti-1계산 전송<br>3. $\theta$i • $\gamma$(i) • ti-1=di'<br>4. 브로드캐스트메시지 생성후전송 | 사용자탈퇴요청<br>di'전송 | 1. 전송받은 di'로부터 $\theta$i • ti-1획득<br>2. (C=<B, H1,...,H2k>) = (C = <M(or S)· y a T t i - 1 , h 1 a ,...,h2ka>) $\theta$ i이용계산<br>3. M(or S)=B/$U^{\theta iti-1}$<br>4. U=$\Pi$Hj$^{rj}$<br>5. $U^{\theta iti-1}$ = ($\Pi$Hj$^{\gamma j}$)$^{\theta iti-1}$ = ($\Pi g^{\alpha j \gamma j}$)$^{\theta iti-1}$ = $(g^{\gamma j \gamma j})^{\theta iati-1}$ = $(g^{\gamma j \alpha jti})^{ati-1}$ = $(H^{i\alpha jti})^{a}$= $y^{aTti-1}$<br>7. M(or S) = M(or S) • $y^{aTti-1}/y^{aTt-1}$ |

## IV. 결론

브로드캐스트 암호화는 공개된 네트워크 상에서 인가된 사용자에게만 컨텐츠를 제공하는데 사용한다. 인가된 사용자이외에는 브로드캐스트되는 메시지에 대해 아무런 정보를 얻어낼 수 없으며, 인가된 사용자는 사전에 전송된 개인키를 이용하여 세션키를 취득할 수 있게된다. 본 논문은 사용자에게 개인키의 생성, 분배와 갱신에 이르는 방법을 제안하고 있다. 본 방식의 방법은 갱신을 위한 특별한 값을 제공하고 있으며, 사용자의 탈퇴 요청 혹은 서버의 사용자 탈퇴 처리가 있은 후에 기존 사용자들에 대해 보다 쉽게 갱신을 할 수 있도록 제안하고 있다. 본 연구는 사용자 추적, 키 주기등을 위한 연구가 필요하리라 본다.

## 참고문헌


[1] Amos Fiat, and Moni Naor, *"Broadcast Encryption"*, Crypto'93, LNCS 773, 480-491

[2] C. Blundo, Luiz A. Frota Mattos, D.R. Stinson, *"Generalized Beimel-Chor schemes for Broadcast Enryption and Interactive Key Distribution"*, Crypto'96, LNCS 1109

[3] Carlo Blundo, Luiz A. Frota Mattos, and Douglas R. Stinson, *" Trade-offs Between Communication and Storage in Unconditionally Secure Schemes for Broadcast Encryption and Interactive Key Distribution"*, Crypto 98

[4] Juan A. Garay, Jessica Staddon, and Avishai Wool, *"Long-Lived Broadcast Encryption"*, Crypto'00, LNCS 1880, 333-352

[5] Ignacio Gracia, Sebastia Martin, and Carles Padro, *"Improving the Trade-off Between Storage and Communication in Broadcast Encryption Schemes"*, 2001

[6] Dani Halevy, and Adi Shamir, *"The LSD Broadcast Encryption Scheme"*, Crypto'02, LNCS 2442, 47-60

[7] Yevgeniy Dodis and Nelly Fazio, *"Public Key Broadcast Encryption for Stateless Receivers"*, DRM2002, 2002. 11. 18

[8] Donald Beaver, and Nicol So, *"Global, Unpredictable Bit Generation Without Broadcast"*, 1993

[9] Michel Abdalla, Yucal Shavitt, And Avishai Wool, *"Towards Marking Broadcast Encryption Practical"*, FC'99, LNCS 1648

[10] Dong Hun Lee, Hyun Jung Kim, and Jong In Lim, *"Efficient Public-Key Traitor Tracing in Provably Secure Broadcast Encryption with Unlimited Revocation Capability"*, KoreaCrypto 02', 2003