효율적인 키 갱신 주기를 적용한 Traitor Tracing

이덕규* · 한종욱*

*한국전자통신연구원

Traitor Tracing using an Efficient Key Renewal

Deok Gyu Lee* · Jongwook Han*

*Electronics and Telecommunications Research Institute

E-mail : deokgyulee@etri.re.kr

요 약

브로드캐스트 암호화 기법은 공개된 네트워크상에서 멀티미디어, 소프트웨어, 유료 TV 등의 디지털 정보들을 전송하는데 적용되고 있다. 브로드캐스트 암호화 기법에서 중요한 것은 오직 사전에 허가된 사용자만이 디지털 정보를 얻을 수 있어야 한다는 것이다. 본 논문에서는 공격자 확인과, 추적을 행할 수 있으며, 키 생성에서 각 사용자의 키가 효율적인 갱신 주기를 가질 수 있도록 Proactive 방식을 이용하여 제안한다.

ABSTRACT

Broadcast encryption has been applied to transmit digital information such as multimedia, software and paid TV programs on the open networks. This paper presents a method called Traitor Tracing to solve all these problems. Traitor tracing can check attackers and trace them. It also utilizes a proactive way for each user to have effective renewal cycle to generate keys.

키워드

Traitor Tracing, 키 갱신, Broadcast Encryption

Ⅰ. 서 론

디지털 기술이 발달함에 따라 많은 수의 디지털 콘텐츠가 생겨나고 보급되고 있다. 이러한 디지털 정보들은 컴퓨터 및 기타 장치를 사용하여 쉽게 복제할 수 있고 그에 따른 피해가 발생하고 있다. 예를 들어, CD나 디스켓 안에 저장되어 있는 디지털 정보들은 CD writer나 디스켓을 통해 쉽게 복제할 수 있으며, 인터넷을 통해 디지털 정보에 관련하여 쉽게 다운로드 받고 이 정보들을 쉽게 다른 사람에게 줄 수 있다. 이러한 상황에 대해 브로드캐스트 암호화 기법은 공개된 네트워크상에서 멀티미디어, 소프트웨어, 유료 TV 등의 디지털 정보들을 전송하는데 적용되고 있다.[3][4][7][8].

브로드캐스트 암호화 기법에서도 사용자가 키를 악의적인 목적을 가지고 이용하였을 경우에는 불법적인 사용자가 누구인지 추적이 어렵게 된다. 불법사용자의 추적은 사용자가 알 수 없는 간단한 디지털 정보를 숨겨서 불법 복제자가 누구인지를 추적하게 하는 기법이다. 본 논문에서는 불법 복제를 하기 위해 결탁하거나 기타 행위를 하는 사용자를 불법 사용자라고 부르고 이러한 불법 사용자를 찾아내는 기법을 불법 사용자 추적 기법이라 하겠다.

본 논문에서는 불법 사용자를 추적함에 있어 사전에 최대한 사용자의 불법 행위를 방지하기 위해 사용자에게 제공되는 키에 proactive 방식을 적용하였으며, 이를 바탕으로 사용자가 불법적인 행위를 하였을 경우 효율적으로 불법 사용자를 추적할 수 있도록 제안하였다. 또한 사용자가 등록과 더불어 개인키를 제공 받음에 있어 공격자로부터 효율적으로 키를 변형하고 후에 불법 사용자 추적에 있어 고유한 사용자에서 불법 사용자를 추출하는데 더욱 효과적이도록 설계하였다.

본 논문은 제안 방식의 각 단계에 관하여 살펴

본다. 또한 제안 방식 분석을 통하여 제안 방식에 대해 고찰하며, 마지막으로 결론을 맺도록 한다.

II. 제안 방식

제안방식은 콘텐츠 제공자와 n명의 사용자로 구성되어 있다. 각 사용자들은 개인키를 전송받게 되는데, 개인키는 권한 블록에 포함된 세션키를 복호화 하는데 필요하며, 개인키는 각 사용자에게 3개씩 전송되며 이는 사용자가 콘텐츠 제공자간에 동기화를 통해 브로드캐스트 메시지를 해당 개인키로 복호화하게 된다. 사용자에게 키를 3쌍씩 나눠주는 것은 두 가지의 목적을 가진다. 우선 각 사용자의 키를 주기적으로 반복시켜 공격자로부터 사용자의 키를 동일하게 사용하지 않는 목적을 가지고, 다음은 사용자가 불법적인 목적으로 사용되었을 경우 키 쌍은 전체적으로 이동하게 된다. 이 때 불법적인 목적을 가지고 사용되었다면 불법적으로 사용된 키가 교집합으로 형성되게 되며, 이에 대한 정확한 불법 사용자를 추적할 수 있게 된다. 다음은 제안 방식의 단계와 가정에 대해 살펴본다.

초기 단계 : 시스템 변수를 설정하는 단계로써 콘텐츠 제공자는 참여할 사용자 수를 예측하고 공개키와 개인키를 생성하게 되는데, 사용자의 수보다 3배 많은 키를 구성한다.

등록 단계 : 콘텐츠 제공자와 디지털 정보를 수신하기 원하는 사용자 사이에 진행되는 프로토콜로써 이때 사용자는 콘텐츠 제공자로부터 키 쌍을 받게 된다.

브로드캐스트 메시지 암호화 단계 : 브로드캐스트 암호화 메시지를 생성하는 단계로서 사용자는 콘텐츠 제공자와 우선 사용할 키에 대해 동기화를 한다. 전송되는 브로드캐스트 메시지가 불법적으로 사용되어졌다면, 불법 디코더 내에 포함되는 복호화 키는 콘텐츠 제공자가 각 사용자에게 분배한 개인키 중 하나일 것이다.

복호화 단계 : 각 사용자는 자신의 개인키를 이용한 복호화 과정을 통하여 브로드캐스트 메시지로부터 디지털 정보를 획득하게 된다. 이때 사용자는 자신이 가진 키에 대해 분별할 수 없으며 사용자는 자신의 키 쌍을 이용하여 복호만 가능하다.

키 갱신 단계 : 콘텐츠 제공자는 새로운 다항식을 값을 이용하여 키 변경과 관련된 정보를 브로드캐스트하고 각 사용자는 전송받은 값을 이용하여 자신의 개인키를 변경한다. 이때 사용자는 자신이 가지고 있는 3개에 키 쌍에 대해 각각 수행되며, 사용자가 선택할 수 없고 자동적으로 진행된다.

불법 사용자 추적 및 사용자 탈퇴 단계 : 콘텐츠 제공자가 불법 디코더를 발견하면 불법 사용자를 찾기 위해 브로드캐스트 메시지를 디코더에 입력하여 키 갱신이 진행되도록 한다. 불법 디코더는 키 갱신을 위한 것인지 불법 사용자 추적을 위한 것인지 구별 할 수 없으며, 불법 사용자의 키 쌍 중에서 2개가 동시에 나타나는 사용자는 불법 사용자임을 확실히 알 수 있게 된다.

2.1 제안 방식 적용 및 가정 사항

본 제안방식은 방송, 콘텐츠 제공과 같은 콘텐츠 유포에 있어 다수에 전송하는 시나리오를 토대로 진행된다. 콘텐츠를 제공하고 이를 암호화한 후 사용자에게 제공하는 방식은 기존의 방식과 동일하게 진행된다. 하지만 여기서 불법 사용자 추적에 있어 두 사용자로 나뉘어 질수 있는데, 우선 첫 번째 불법 사용자는 불법 디코더를 획득하여 이를 통해 불법적인 행위를 하는 사용자이고, 두 번째 사용자는 불법 디코더를 사용하지 않고 획득한 콘텐츠를 이용하여 불법적인 유통시킨 사용자로 분리할 수 있다. 우선 앞서 언급한 불법 사용자의 경우는 다시 2부분으로 분리할 수 있다. 하나의 경우는 불법 디코더 제작자와 사용자가 결탁하여 불법 디코더를 만드는 경우이고, 다른 하나의 경우는 불법 사용자가 통신로상의 정보를 획득하여 이를 바탕으로 제작하는 경우이다. 결탁의 경우 본 제안방식에서 사용자에게 키를 3개씩 나눠줌으로써 이를 이용하여 결탁 공모자를 추적할 수 있으며, 통신로상의 정보를 계속적으로 변화시키기 위해 3개의 키를 이용하여 사용자와 콘텐츠 제공자 사이에 동기화를 통해 키를 변경 시킬 수 있다. 이러한 경우를 제외하고 불법 사용자가 콘텐츠를 획득하여 이를 이용하여 불법적인 유통을 시키는 경우는 본 제안방식에서 설명하지 않고 기존 DRM(Digital Rights Management)등과 같은 콘텐츠 보안에서 참조하는 것으로 한다.

2.2 제안방식 흐름

본 제안 방식은 다음과 같은 특징을 가지고 있다. 우선 콘텐츠 제공자는 시스템 알고리즘과 그와 관계된 변수를 설정하는데 사용자의 키를 쉽게 갱신하고 불법 사용자로부터 사용자의 키를 안전하게 보관할 수 있도록 갱신 인자를 삽입하고 사용자들은 후에 콘텐츠 제공자에 등록하며 이때 할당되어있는 개인키를 전송받게 된다. 후에 콘텐츠 제공자는 메시지를 브로드캐스트 하고자 할 때 브로드캐스트 될 데이터를 세션키로 암호화한 암호문과 정당한 개인키를 가지고 있는 사용자만이 세션키를 획득하도록 권한블록을 구성한다. 사용자는 메시지를 획득하기 위해 자신이 가지고 있는 개인키를 이용하여 복호화할 수 있다. 브로드캐스트 암호화 메시지를 전송하고 복호화하는 단계에서는 사용자와 서버간의 키 사용에 따른 동기를 맞추도록 한다. 콘텐츠 제공자가 불법 사용자를 발견하였을 경우, 사용된 개인키에 발급받은 사용자를 결정하고자 한다면, 정당한 사용자들이 자신들의 개인키를 조합해서 정당하지 않은 개인키를 만들어서 브로드캐스트 된 데이터

를 복호화 할 수 있는 경우 콘텐츠 제공자는 새롭게 만들어진 메시지의 입력과 출력사이의 관계를 살핌으로써 사용된 캐인키를 알 수 있다.

사용자들의 최대 불법 수는 k이고 발견된 불법 사용자자들에 대한 추출 임계치는 z(즉, 불법 사용자의 개인키가 3개씩 설정되어 있으므로 사용자를 확실히 구분지을 수 있다.) 큰 소수인 위수 q를 갖는 그룹 G_q 이다.

2.2.1 초기화 단계 및 브로드캐스트 메시지 암호화/복호화 단계

Step 1. 콘텐츠 제공자는 사용자$(i=1,\cdots,2u+2)$를 예측하여 이에 대해 랜덤수(β)를 선택한다. 이때 사용되는 랜덤수는 사용자의 키를 갱신하기 위한 갱신인자로 사용된다.

Step 2. 콘텐츠 제공자는 Z_q상에서 계수 z를 갖는 다항식 $f(x)=\sum_{i=0}^{z}\beta_i a_i x^i$를 선택한다. 콘텐츠 제공자는 다항식을 비밀키로 하고 공개키를 다음과 같이 설정하고 모든 사용자들에게 공개한다.

$\langle g, g^{\beta_0 a_0}, g^{f(1)}, \cdots, g^{f(2z+2)}\rangle$ 공개

Step 3. 콘텐츠 제공자는 사용자가 등록할 때 콘텐츠 제공자는 사용자에게 개인키 $((i,f(i-1)),(i,f(i)),(i,f(i+1)))$를 전송한다. 사용자는 자신이 받은 키가 정확한 값인지 검증을 시행한다. 이때 콘텐츠 제공자는 첫 번째 키로서 검증을 수행하도록 유도한다. 사용자에게 키와 함께 동기화 과정에서 갱신할 수 있는 값 $\beta_{2u+3},\beta_{2u+4},\beta_{2u+5}$을 같이 전송한다.

$g^{\beta_0 a_0}=\prod_{i=0}^{z} g^{f(x_i)\lambda_i}$, 단 $x_0=1, x_2=2, \cdots, x_{2z+1}=z, x_{2z+2}=i$이다.

이 식을 검증하게 되면 사용자는 개인키를 획득하게 된다.

Step 4. 콘텐츠 제공자는 사용자와 통신을 개시하기 전에 사용자와의 동기화 과정을 행하고, 이에 사용자는 최초 받은 갱신값을 이용하여 자신의 개인키를 갱신하고 이를 바탕으로 사용하게 된다. 이와 같은 과정이 종료되면, 콘텐츠 제공자는 사용되지 않은 정보를 선택하고 랜덤수 $r\in Z_q$를 선택한 뒤 권한 블록을 계산한다.

$\langle j_1, f(j_1)\rangle, \langle j_2, f(j_2)\rangle \cdots \langle j_{2u+2}, f(j_{2u+2})\rangle$, $C=\langle sg^{r\beta_0 a_0}, g^{r}\langle j_1, g^{rf(j_1)}\rangle, \cdots g^{r}\langle j_u, g^{rf(j_{2u+1})}\rangle\rangle$

그리고 메시지를 세션키로 암호화 한 뒤 C와 암호화한 메시지를 전송한다.

Step 5. 사용자는 콘텐츠 제공자로부터 받은 C와 암호화한 메시지로부터 세션키를 획득하는 과정은 다음과 같다.

$s=sg^{r\beta_0 a_0}/\left[(g^{r})^{f(0)\lambda_0}\cdot\prod_{i=0}^{z+1}(g^{rf(x_i)})\right]$, 단 $x_0=j_1, x_2=j_2\cdots, x_{2z+1}=j_{2z+2}, x_{2z+2}=i$이다.

2.2.2 키 갱신 단계

Step 1. 사용자 j가 콘텐츠 제공자에게 탈퇴 요청

Step 2. 콘텐츠 제공자는 기존 사용자의 개인키를 갱신하기 위해 갱신요소인 β에서 사용자 j의 갱신요소를 제거한다.

Step 3. 콘텐츠 제공자는 탈퇴 사용자의 갱신요소를 제거한 후 개인키를 갱신하고 사용자에게 전송한다. 각 사용자에게 키 쌍 3개를 전송하였으므로 갱신에 해당하는 $B=(\beta_{i-1},\beta_i,\beta_{i+1})$의 3개에 해당하는 공유정보들을 고정하고 사용되지 않은 공유정보를 이용하여 권한 블록을 구성하게 되면 사용자 j는 사용할 수 없게 된다.

$\langle\beta_{i-1}, g^{rf(\beta_{i-1})}\rangle,\ldots,\langle\beta_{i+1}, g^{rf(\beta_{i+1})}\rangle \Rightarrow \langle j_1, g^{rf(j_1)}\rangle,\ldots,\langle j_{z-3}, g^{rf(j_{z-3})}\rangle$

2.2.3 공모자 추적 단계

공모자 추적은 키 갱신 과정에서 WGT가 제안한 방법을 적용한다 WGT에서는 두가지 공모자 추적 방식을 제안하고 있는데 이 방식을 제안 방식에 맞추어 설명한다.

Step 1. 콘텐츠 제공자는 불법 사용자로 추정되는 사용자 집합 $\{c_1, c_2, \cdots, c_m\},(m\le k)$를 구성한다.

Step 2. 불법 사용자를 추적하기위해 정보를 권한블록에 다음과 같이 첨부한다.

$\langle sg^{r\beta_0 a_0}, g^{r}\langle c_1, g^{rf(c_1)}\rangle, \cdots g^{r}\langle c_m, g^{rf(c_m)}\rangle\rangle$

다른 방법은 불법 사용자만이 권한 블록을 복호화 할 수 있는 방식으로 콘텐츠 제공자는 $\{(c_1,f(c_1)),\ldots,(c_m,f(c_m))\}$를 해의 일부로 하고 나머지 근들은 $f(x)$와 일치하지 않는 새로운 다항식 $h(x)$를 선택한다.

이렇게 하고 불법 사용자가 발견된 후에 콘텐츠 제공자는 불법 사용자의 키를 사용해서 만들어진 불법 개인키들이 브로드캐스트 된 데이터를 복호화 할 수 없게 할 수 있다. $\{c_1, c_2, \cdots, c_m\},(m\le k)$가 콘텐츠 제공자에 의해 찾아진 공모자들이라 하고 그들의 공유 정보를 다른 사용자들의 개인키들을 바꾸지 않으면서 다음과 같은 방법에 의해 추출할 수 있다. 콘텐츠 제공자는 권한 블록의 처음 m개의 공유정보들을 $\langle c_1, g^{rf(c_1)}\rangle,\ldots,\langle c_m, g^{rf(c_m)}\rangle$으로 고정하고 나머지 $z-m$개의 사용되지 않은 공유정보 $\langle j_1, g^{rf(j_1)}\rangle,\ldots,\langle j_{z-m}, g^{rf(j_{z-m})}\rangle$로 권한 블록을 구성한다.

III. 제안 방식 분석

본 논문에서는 기존의 방식보다 효율적인 키 생성과 키 갱신을 위한 브로드캐스트 암호화 방식과 함께 사용자 추적을 위해 사용자에게 키 쌍을 제공하는 방식을 제안하였다. 본 제안 방식들의 안전성은 이산대수의 문제에 기반을 두고 있다. 기존의 방식에 비해 사용자의 참여, 키 갱신, 사용자의 탈퇴에 있어 효율성을 나타내고 있다. 본 장에서는 제안 방식에 대해 고찰한다.

3.1 키 갱신

기존 KPS(Key Predistribution Scheme)에서는 키가 생성되고 분배가 되어진 후 이를 이용하여 암호화하여 메시지를 전송하게 된다. 전송된 메시지를 사용자가 확인한 후 한 세션이 종료되면 키를 새로 생성하여 전송되거나, 키에 대하여 공격이 이루어진 경우 키를 갱신하지 아니하고 전체

적으로 다시 생성하게 된다. 하지만 제안 방식들에서는 사용자의 가입 혹은 탈퇴가 발생하면 기존 사용자들의 키를 갱신하고 사용이 가능하다. 키 갱신은 초기 키 생성 시에 키 갱신 요소인 β 인자를 삽입하게 된다. 차후 사용자 탈퇴/강제 탈퇴 등과 같은 상황이 발생되면 서버는 탈퇴자의 키 갱신 정보인 β 인자를 삭제하고 제공함으로써 사용자는 간단한 연산으로 키 갱신을 마치게 된다.

3.2 초기 예측 오류에 따른 재연산

제안 방식의 경우 서버가 시스템을 설정하고 관리해야한다. 만일 서버가 유동적인 사용자를 관리한다면 사용자에 대한 예측이 올바르게 이뤄져야한다. 그러므로 서버는 초기 예측에 대한 오류가 발생하였을 경우 재연산이나 혹은 추가 연산을 실시해야 한다. 하지만 기존 방식의 경우에서는 이러한 사용자 예측 오류에 대하여 수행할 수 있는 연산이 없다. 본 논문에서 제공하는 방식에서는 서버가 시스템을 설정하는데 사용자에 대한 예측 연산을 원활히 할 수 있도록 r과 같이 연산을 통해 이뤄질 수 있도록 제안하였다. 또한 랜덤한 수 r에 대해서는 Z_q상에서 생성하게 되며 r에 대해서 사전에 예측 사용자보다 많은 수를 만들면 해결할 수 있다.

3.3 선택 암호문 공격에 대한 안전한 스킴

적응적 선택 암호문 공격에 안전한 암호시스템을 설계할 수 있는 것은 매우 좋은 성질로써 본 절에서는 Boneh와 Franklin의 방식과 유사한 방식으로 제안방식의 변형을 가함으로써 적응적 선택 암호문 공격에 안전한 불법 사용자 추적 스킴을 제안한다.

콘텐츠 제공자는 Z_q위에서 z를 갖는 다항식 $f(x)=\sum_{i=0}^{z}\beta_i a_i x^i$를 선택하며, $a, b, x_1, x_2, y_1, y_2 \in Z_q$를 선택한다 콘텐츠 제공자의 비밀키는 $\langle f(x), a, b\rangle$이고 공개키는 $\langle g, g^{\beta a a_0}, g^{f(1)}, \ldots, g^{f(z)}, g^{r\beta a}, g^{r\beta b}, c, d, H\rangle$로 모든 사용자에게 공개한다. 사용자가 콘텐츠 제공자에게 등록할 때 콘텐츠 제공자는 사용자에게 개인키를 제공한다. 사용자는 받은 키가 정확한 값인지 앞 장과 동일한 방법으로 검증한다. 콘텐츠 제공자는 랜덤하게 z개의 사용되지 않은 공유정보를 선택하고 이를 바탕으로 권한 블록을 계산한다. 사용자는 브로드캐스트된 권한 블록으로부터 개인키를 이용해 세션키를 획득한다. 검증이 성공하면 선택 암호문 공격에 안전함을 알 수 있다.

IV. 결 론

인가된 사용자이외에는 브로드캐스트 되는 메시지에 대해 아무런 정보를 얻어낼 수 없으며, 인가된 사용자는 사전에 전송된 개인키를 이용하여 세션키를 취득할 수 있게 된다. 본 논문에서는 불법 사용자를 추적함에 있어 사전에 최대한 사용자의 불법 행위를 방지하기 위해 사용자에게 제공되는 키에 proactive 방식을 적용하였으며, 이를 바탕으로 사용자가 불법적인 행위를 하였을 경우 효율적으로 불법 사용자를 추적할 수 있도록 제안하였다. 이는 새로운 형태의 불법 사용자 추적 기법을 제안을 의미한다. 제안 방식에서 브로드캐스트 메시지는 권한블록, 갱신블록, 암호블록으로 구성된다. 또한 사용자가 등록과 더불어 개인키를 제공 받음에 있어 공격자로부터 효율적으로 키를 변형하고 후에 불법 사용자 추적에 있어 고유한 사용자에서 불법 사용자를 추출하는데 더욱 효과적이도록 설계하였다.

참고문헌

[1] Amos Fiat and Moni Naor, "Broadcast Encryption", Crypto'93, pp. 480-491, 1993

[2] A. Narayana, "Practical Pay TV Schemes", to appear in the Proceedings of ACISP03, July, 2003

[3] C. Blundo, Luiz A. Frota Mattos and D.R. Stinson, "Generalized Beimel-Chor schemes for Broadcast Enryption and Interactive Key Distribution", Theoretical Computer Science, vol. 200, pp. 313-334, 1998.

[4] 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", In Advances in Cryptology - Crypro '96, Lecture Notes in Computer Science 1109, pp. 387-400.

[5] Carlo Blundo and A. Cresti, "Space Requirements for Broadcast Encryption", EUROCRYPT 94, LNCS 950, pp. 287-298, 1994

[6] Donald Beaver and Nicol So, "Global, Unpredictable Bit Generation Without Broadcast", EUROCRYPT 93, volume 765 of Lecture Notes in Computer Science, pp. 424-434. Springer-Verlag, 1994, 23-27 May 1993.

[7] 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

[8] D. Boneh and M. Franklin, "AN Efficient Public Key Traitor Tracing Scheme", CRYPTO 99, LNCS 1666, pp. 338-353, 1999

[9] Dani Halevy and Adi Shamir, "The LSD Broadcast Encryption Scheme", Crypto '02, Lecture Notes in Computer Science, vol. 2442, pp. 47-60, 2002.