제 18 회 한국정보처리학회 추계학술발표대회 논문집 제 9 권 제 2 호 (2002.11)

연산비용 향상을 제공하는 Revocation 기법의 제안

강현선*, 정종필**, 박창섭*
*단국대학교 전자계산학과
**MISecurity, Inc.
e-mail : sshskang@dankook.ac.kr

Revocation Schemes Reducing the Computational Overhead

Hyun-Sun Kang*, Jong-Pil Jung**, Chang-Seop Park*
*Dept. of Computer Science, Dan-Kook University
**MISecurity, Inc.

요 약

Revocation 기법은 멀티캐스트 환경에서 그룹의 동적인 변화에 대한 그룹키의 갱신을 의미한다. 키갱신을 위해서는 키갱신 메시지의 전송이 필요하며 키갱신 메시지의 효율적인 분배를 위해서 트리를 이용한 방식과 비밀공유를 이용한 방식이 제안되었다. 이 논문에서는 키 갱신에서의 연산비용을 줄이기 위해 이전에 제안 되었던 비밀공유 기반의 revocation 기법의 두가지 변형을 제안한다.

1. 서론

멀티캐스트(Multicast) 통신에서는 하나의 복사본만을 전송함으로써 일대다 통신이 가능하다. 그래서 멀티미디어, 뮤직, 비디오, 소프트웨어, 유료 TV 등의 디지털 정보들을 전송하는데 멀티캐스트가 응용되어질 수 있다. 이와 같은 멀티캐스트 응용환경에서 중요한 것은 오직 사전에 허가를 받은 사용자만이 디지털 정보를 얻을 수 있어야 한다는 점이다. 이를 위해 디지털 정보는 그룹키(Group Key)로 암호화되어 전달되고 이 메시지를 전달 받은 권한이 있는 사용자들은 자신이 사전에 부여 받은 개인키를 이용하여 그룹키를 복호화 하고 이로써 디지털 정보를 얻게 된다. 여기에서 사용되는 그룹 멤버들(Group Members) 간의 공통된 그룹키를 설정하고 관리하는 것이 키관리이며 사용자의 가입 또는 탈퇴 등으로 인해 멤버쉽에 변화가 생길 때 마다 그룹 관리자(Group Manager)는 그룹키를 변경하기 위한 키갱신 메시지를 전송해 주어야만 한다. 즉, 그룹에서 탈퇴한 사용자들이 계속해서 그룹 통신에 참여하는 것을 방지하고 또한 새로운 사용자들이 이전의 그룹 통신 메시지에 접근할 수 없도록 하기 위함이다. 초기에 제안된 많은 키관리 프로토콜들은 탈퇴한 사용자를 기존의 그룹에서 제거하기 위해 새로운 그룹키를 생성한 후, 이를 각 사용자들과 공유하고 있는 비밀키를 이용해 대칭형 암호화하여, 사용자에게 전달해 주는 방식을 사용하였다. 그러나 이러한 방식은 확장성의 문제를 가지고 있다. 이를 해결하기 위해 트리 구조를 이용한 방식과 비밀공유를 이용한 방식이 제안되었다. 트리를 이용한 방식은 키의 길이가 짧고 속도가 빠른 반면 사용자가 저장하고 있어야할 개인키의 개수가 많고, 비밀공유를 이용한 방식은 이산대수 문제에 기반을 두고 있기 때문에 키의 길이를 줄이면서 계산량을 향상시킬 수 있다. 비밀공유 방식을 이용한 기법은 Anzai et.al [1] 의 "A Quick Group Key Distribution Scheme"(QGKDS), Naor, M. and Pinkas, B.[2]의 "Efficient Trace and Revoke Schemes", Tzeng, W. and Tzeng, Z.J.[4]의 "A Public-Key Traitor Tracing Scheme with Revocation Using Dynamic Shares" 등에서 소개되었다. 이 논문에서는 이들 중 Anzai et.al [1] 의 "A Quick Group Key Distribution Scheme"(QGKDS)을 소개할 것이며 이를 기반으로 한 새로운 두가지 변형된 기법들을 제안할 것이다. 또한 기존 기법과 새롭게 제안하는 기법들과의 연산비용과 확장성 등의 비교를 통해 제안 기법들의 효율성의 향상됨을 보이고자 한다.

2. 기존기법 (QGKDS)

QGKDS 은 이산대수 문제의 어려움에 기반을 두고 있으며 Shamir[3]의 threshold scheme 을 이용하여 그룹 키 관리를 한다. 그룹 멤버쉽의 변화에 따른 키갱신 메시지와 연산 등의 오버헤드는 동시에 탈퇴할 수 있는 최대 사용자 수에 따라 결정되며 사용자가 저장하고 있어야 하는 개인키의 길이는 전체 사용자수와는 독립적이며, 한 개의 개인키 만을 저장하고 있으면 된다. 앞서 서론에서 언급되었던 비밀공유 방식을 이용한 여러 기법들의 키갱신 메시지와 연산 등의 오버헤드는 QGKDS 와 거의 동일하며 단계별 구성 역시 유사하다. 이 장에서는 여러 기법들 중 특히 QGKDS 의 단계별 구성, 오버헤드, 안전성에 관해 간략히 설명 하고자 한다.

2.1 단계별 구성

QGKDS 은 그룹 관리자(Group Manager) GM 과 n 명의 사용자 집합 $U = \{ 1, 2, \ldots, n \}$로 구성되어 있다. 사전에 허가를 받은 각 사용자들은 그룹키를 복호화 하기 위한 개인키를 가지고 있다. GM 은 그룹 멤버쉽에 변화가 있을 때 키갱신 메시지를 멀티캐스트로 전달하게 되며, 사용자는 수신된 메시지와 자신의 개인키를 이용하여 새로운 그룹키를 얻게 된다. 과정을 살펴보면 다음과 같다.

[초기화]

p, q 는 $q \mid (p\text{-}1)$을 만족하는 큰 소수이고, g 는 위수가 q 인 $GF(p)$상의 원소라고 하자. GM 은 $0 \le t\text{-}1 < n$ 을 만족하는 임의의 t 를 선정한 후 임의의 난수 $a_1, a_2, \ldots, a_{t-1} \in Z_q$ 를 기반으로 t-1 차 다항식 $f(x)$를 생성한다. 그 후 GM 은 $n+t$-1 개의 i 에 대한 $f(i)$와 y_i 값을 계산하여 둔다. 여기서 t-1 은 동시에 탈퇴 가능한 최대 사용자 수로, a_0는 시스템 비밀키(System Secret Key)로 사용되게 된다.

$$f(x) = a_0 + a_1 x + \ldots + a_{t-1} x^{t-1} \bmod q$$
$$y_i = g^{f(i)} \bmod p \ (1 \le i \le n+t-1)$$

[사용자 가입시]

GM 은 그룹에 참여를 원하는 사용자 i 에게 그룹키를 복호화할 수 있는 개인키 $f(i)$를 안전한 채널을 통해 제공한다. $(1 \le i \le n)$

[키갱신 암호화]

만약 사용자의 탈퇴요청 등의 이유로 권한을 취소해야 할 사용자들이 있을 경우, 이 사용자들의 집합을 Λ라 하고 $|\Lambda| = d$ 라고 하자. 우선 GM 은 Z_q–U–Λ에서 임의로 t-d-1 개의 정수를 선택한다. 이때 선택된 정수의 집합을 θ 라고 하자. GM 은 임의의 난수 $r \in Z_q$ 을 선택하여 X 와 M_j 를 계산하고, *Message* 를 작성한 후 작성된 *Message* 를 멀티캐스트 한다.

$$X = g^r \bmod p$$
$$M_j = y_j^r \bmod p \ (j \in \Lambda \cup \theta)$$
$$Message = < X, \{ (j, M_j) \mid j \in \Lambda \cup \theta \} >$$

[키갱신 복호화]

Revocation 집합 Λ에 포함되지 않은 사용자 i 는 수신한 멀티캐스트 메시지와 자신의 개인키 $(i, f(i))$를 이용하여 그룹키를 복원하게 된다. 이때 Langrange 보간법이 사용된다.

$$L(\psi, \omega) = \sum_{k \in \psi - \{\omega\}} (k / k\text{-}\omega) \bmod q \quad \text{이면}$$

$$GK = X^{f(0)} = X^{f(i) \times L(\Lambda \cup \theta \cup \{i\}, i)} \times \prod_{j \in \Lambda \cup \theta} M_j^{L(\Lambda \cup \theta \cup \{i\}, j)} \bmod p$$

2.2 오버헤드

사용자는 한 개의 개인키를 저장하고 있으면 된다. 멀티캐스트 될 메시지의 갯수는 $2t$–1 개이고, $2t(t$-1)번의 곱셈과 t 번의 지수승과 t 번의 역원계산이 필요하게 된다.

2.3 안전성

그룹키의 복원을 위해서는 적어도 t 개의 점이 필요하다. 사전에 허가를 받은 사용자는 전달 받은 메시지로부터 얻은 t-1 개의 점과 자신이 가지고 있는 하나의 점을 이용하여 그룹키를 복원할 수 있지만, Λ에 포함된 사용자들은 t–1 개의 점만을 가지게 되므로 새로운 그룹키를 복원하는 것은 불가능하다.

3. 제안기법

이 장에서 소개할 기법들은 기존의 QGKDS 기법에서 사용자 측면의 연산비용을 줄이고자 하는 목적으로 새롭게 제안된 그 변형들이다. 그 결과 기존 기법에 비해 상당한 연산비용의 향상을 가져온다. 제안기법 Ⅰ은 Revocation 집합 Λ에 포함되지 않은 사용자들의 공통된 계산을 GM 이 미리 계산하여 보냄으로써, 제안기법 Ⅱ는 새로운 다항식을 이용함으로써 사용자 측면에서의 연산비용을 향상시켜 준다. 이처럼 그룹 멤버가 수행해야 할 연산비용을 향상시키는 것은 그룹 멤버가 PDA(Personal Digital Assistants), 스마트 폰(Smart Phone)과 같이 계산 능력이 제한적인 단말기인 경우에 매우 중요한 요인으로 작용할 수 있다. 앞으로 소개할 새로운 기법들은 QGKDS 에서 뿐만 아니라 다른 기법들[2][4]에서도 적용 가능하며 이장에서는 QGKDS 에 적용한 제안기법들의 단계별 구성, 오버헤드, 안전성에 관해 간략히 설명하고자 한다.

3.1 제안기법 Ⅰ

3.1.1 단계별 구성

QGKDS 에서 계산적 오버헤드가 가장 큰 부분은 그룹멤버가 수신한 키갱신 메시지를 이용해서 $L(\psi, \omega)$를 계산하는 부분이다. 제안기법 Ⅰ은 Revocation 집합 Λ에 포함되지 않은 사용자들이 그룹키의 갱신을 위해 $L(\psi, \omega)$를 계산함에 있어 공통된 부분을 GM 이

미리 계산하여 보냄으로써 연산비용을 줄일 수 있다는 제안으로 다음과 같은 과정으로 구성되어 진다.

[초기화]

p, q는 $q \mid (p\text{-}1)$을 만족하는 큰 소수이고, g는 위수가 q인 $GF(p)$상의 원소라고 하자. GM은 $0 \le t\text{-}1 < n$을 만족하는 임의의 t를 선정한 후 임의의 난수 $a_1, a_2, \ldots, a_{t-1} \in Z_q$를 기반으로 t-1 차 다항식 $f(x)$를 생성한다. 그 후 GM은 $n+t$-1 개의 i에 대한 $f(i)$와 y_i 값을 계산하여 둔다. 여기서 t-1 은 동시에 탈퇴 가능한 최대 사용자 수로, a_0는 시스템 비밀키(System Secret Key)로 사용되게 된다.

$$f(x) = a_0 + a_1 x + \ldots + a_{t-1}x^{t-1} \bmod q$$
$$y_i = g^{f(i)} \bmod p \ (1 \le i \le n+t-1)$$

[사용자 가입시]

GM은 그룹에 참여를 원하는 사용자 i에게 그룹키를 복호화할 수 있는 개인키 $f(i)$를 안전한 채널을 통해 제공한다. $(1 \le i \le n)$

[키갱신 암호화]

만약 사용자의 탈퇴요청 등의 이유로 권한을 취소해야 할 사용자들이 있을 경우, 이 사용자들의 집합을 Λ라고 하고 $|\Lambda| = d$ 라고 하자. 우선 GM은 Z_q-U-Λ에서 임의로 t-d-1 개의 정수를 선택한다. 이때 선택된 정수의 집합을 θ 라고 하자. GM은 임의의 난수 $r \in Z_q$을 선택하여 X와 N_j를 계산하고, $Message$를 작성한 후 작성된 $Message$를 멀티캐스트 한다.

$$X = g^r \bmod p$$
$$N_j = (y_j)^{L(\Lambda \cup \theta, j)} \bmod p \ (j \in \Lambda \cup \theta)$$
$$Message = \langle X, \{ (j, N_j) \mid j \in \Lambda \cup \theta \} \rangle$$

[키갱신 복호화]

Revocation 집합 Λ에 포함되지 않은 사용자 i는 수신한 멀티캐스트 메시지와 자신의 개인키 $(i, f(i))$를 이용하여 그룹키를 복원하게 된다. 이때 Langrange 보간법과 새로 정의한 함수 $l(i,j)$가 사용된다.

$$L(\psi, \omega) = \prod_{k \in \psi - \{\omega\}} (k / k-\omega), \ l(i,j) = (i / i-j) \text{ 이면}$$

$$GK = X^{f(0)} = X^{f(i) \times L(\Lambda \cup \theta \cup \{i\}, i)} \times \prod_{j \in \Lambda \cup \theta} N_j^{l(i,j)} \bmod p$$

3.1.2 오버헤드

사용자는 한 개의 개인키를 저장하고 있으면 된다. 멀티캐스트 될 메시지의 갯수는 $2t$-1 개이고 $4(t\text{-}1)$번의 곱셈과 t 번의 지수승과 t 번의 역원 계산이 필요하게 된다.

3.1.3 안전성

그룹키의 복원을 위해서는 적어도 t 개의 점이 필요하다. 사전에 허가를 받은 사용자는 전달 받은 메시지로부터 얻은 t-1 개의 점과 자신이 가지고 있는 하나의 점을 이용하여 그룹키를 복원할 수 있지만, Λ에 포함된 사용자들은 t-1 개의 점만을 가지게 되므로 새로운 그룹키를 복원하는 것은 불가능하다.

3.2 제안기법 II

3.2.1 단계별 구성

제안기법 II는 새로운 그룹키의 갱신을 위한 계산 중 $L(\psi, \omega)$의 계산으로 인한 오버헤드를 줄이기 위한 것으로 새로운 다항식을 생성, 이용하게 된다. 다음과 같은 과정으로 구성되어 진다.

[초기화]

p, q는 $q \mid (p\text{-}1)$을 만족하는 큰 소수이고, g는 위수가 q인 $GF(p)$상의 원소라고 하자. GM은 $0 \le t\text{-}1 < n$을 만족하는 임의의 t를 선정한 후 임의의 난수 $a_1, a_2, \ldots, a_{t-1} \in Z_q$를 기반으로 t-1 차 다항식 $f(x)$를 생성한다. 여기서 t-1 은 동시에 탈퇴 가능한 최대 사용자 수로 사용되게 된다.

$$f(x) = a_0 + a_1 x + \ldots + a_{t-1}x^{t-1} \bmod q$$

[사용자 가입시]

GM은 그룹에 참여를 원하는 사용자 i에게 그룹키를 복호화할 수 있는 개인키 $f(i)$를 안전한 채널을 통해 제공한다. $(1 \le i \le n)$

[키갱신 암호화]

만약 사용자의 탈퇴요청 등의 이유로 권한을 취소해야 할 사용자들이 있을 경우, 이 사용자들의 집합을 Λ라고 하고 $|\Lambda| = d$ 라고 하자. 우선 GM은 Z_q-U-Λ에서 임의로 t-d-1 개의 정수를 선택한다. 이때 선택된 정수의 집합을 θ 라고 하자. GM은 $\{ (j, f(j)) \mid j \in \Lambda \cup \theta \}$와 임의로 선택한 한점 $\{ (j_1, j_2) \mid j_1 \notin U \cup \Lambda, j_2 \notin f(j_1) \}$을 지나는 t-1 차의 다항식 $v(x) = v_0 + v_1 x + \ldots + v_{t-1}x^{t-1}$를 생성하고 $h(x) = f(x) - v(x)$를 생성한다. GM은 임의의 난수 $r \in Z_q$을 선택하여 X와 W_k를 계산하고, $Message$를 작성한 후 작성된 $Message$를 멀티캐스트 한다.

$$X = g^r \bmod p$$
$$W_k = X^{*k} \bmod p \ (0 \le k \le t\text{-}1)$$
$$Message = \langle X, \{ W_k \mid 0 \le k \le t\text{-}1 \}, \{ j \mid j \in \Lambda \cup \theta \} \rangle$$

[키갱신 복호화]

Revocation 집합 Λ에 포함되지 않은 사용자 i는 수신한 멀티캐스트 메시지와 자신의 개인키 $(i, f(i))$를 이용하여 그룹키를 복원하게 된다. 그룹키를 복원하기 위해 사용자 i는 우선 $X^{v(i)}$와 $X^{h(i)}$를 계산한다. 이 계산 과정에서 필요한 i에 대한 거듭제곱 값은 사용자가 미리 구해 놓는다고 가정한다. 그 다음 Langrange 보간법을 이용하여 그룹키를 복원할 수 있게 된다.

$$X^{v(i)} = W_0 \times (W_1)^i \times (W_2)^{i^2} \times \ldots \times (W_{t-1})^{i^{t-1}}$$
$$X^{h(i)} = X^{f(i)} \times (X^{v(i)})^{-1} = (X)^{f(i)-v(i)}$$

$L(\psi, \omega) = \underset{k \in \psi - \{\omega\}}{(k / k-\omega)}$ 이면

$$GK = X^{h(0)} = X^{h(i) \times L(\Lambda \cup \theta \cup \{i\}, i)} \times \underset{j \in \Lambda \cup \theta}{M_j^{L(\Lambda \cup \theta \cup \{i\}, j)}}$$

하지만 위의 식에서 $j \in \Lambda \cup \theta$ 은 $h(j) = f(j) - v(j) = 0$ 이므로 위의 식은 $X^{h(i) \times L(\Lambda \cup \theta \cup \{i\}, i)}$로 감소될 수 있다.

3.2.2 오버헤드

사용자는 한 개의 개인키를 저장하고 있으면 된다. 멀티캐스트 될 메시지의 갯수는 $2t$ 개이고 $3(t\text{-}1)$번의 곱셈과 $t+1$ 번의 지수승과 2 번의 역원계산이 필요하게 된다.

3.2.3 안전성

사전에 허가를 받은 사용자 i 는 전달받은 메시지와 그 메시지로부터 계산한 값인 $X^{h(i)}$를 이용하여 그룹키 $GK = X^{h(0)} = X^{h(i) \times L(\Lambda \cup \theta \cup \{i\}, i)}$ 를 구할 수 있다. 하지만 Λ 에 포함된 사용자 j 는 $h(j) = f(j) - v(j) = 0$ 이므로 새로운 그룹키를 복원하는 것은 불가능하다.

4. 기존기법과 제안기법의 비교

우리는 앞에서 기존기법과 새롭게 제안하는 기법들에 대한 오버헤드와 안전성에 관하여 다루었다. 이 장에서는 앞에서 소개한 기법들의 확장성과 사용자 측면에서의 연산비용을 비교 분석해 보고자 한다.

4.1 확장성 측면

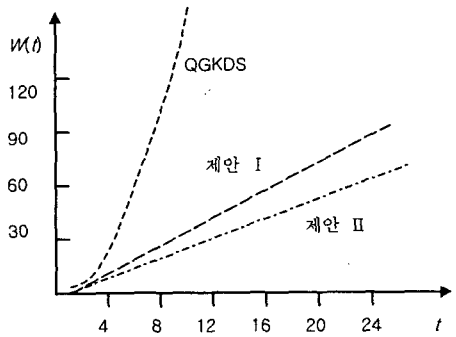
먼저 시스템 확장성을 보면 기존기법은 한번에 탈퇴 시킬 수 있는 사용자의 수가 개인키를 구성하는 다항식 $f(x)$의 차수에 제약을 받는다. 따라서 한번에 탈퇴 시키고자 하는 사용자의 수를 증가시켜 주기 위해서는 시스템을 다시 초기화 해주어야 하기 때문에 확장성에 문제가 있다. 그러나 제안기법 II에서는 한번에 탈퇴 시킬 수 있는 사용자 수가 GM 에 의해 유동적으로 증가될 수 있기 때문에 시스템 확장성을 향상시켜 준다.

4.2 연산비용 측면

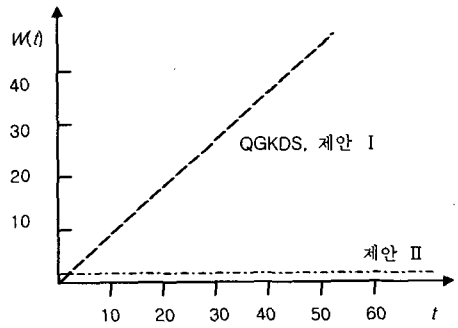
사용자측의 연산비용에서도 기존기법에 비해 새롭게 제안하는 기법들이 향상되었음을 알 수 있다. 곱셈연산의 경우 기존기법은 $2t^2$ 2t 인 것에 비해 새로운 제안기법은 4t 4 와 3t 3 으로 감소하였으며, 역원연산의 경우 기존기법은 t 인 것에 비해 제안기법 II는 2 로 감소하였음을 볼 수 있다. 즉, 곱셈연산의 경우 $O(t^2)$에서 $O(t)$로 줄어들었으며 역원연산의 경우는 $O(t)$에서 $O(1)$로 현저히 줄어들었음을 알 수 있다. 효율성의 향상을 한눈에 보기 위해 여러 기법의 전체 연산비용에 대한 비교는 <표 1>로 정리 하였으며, 그 중 탈퇴자수에 의한 곱셈 연산비용 비교는 (그림 1)로, 역원 연산비용 비교는 (그림 2)로 정리하였다.

<표 1> 여러기법의 연산비용 비교

구 분	QGKDS	제안 I	제안 II
곱 셈	2t^2 2t	4t 4	3t 3
지수승	t	t	$t+1$
역 원	t	t	2



(그림 1) 탈퇴자수에 의한 곱셈 연산비용 비교



(그림 2) 탈퇴자수에 의한 역원 연산비용 비교

참고문헌

[1] Anzai, J., Matsuzaki, N., and Matsumoto, T. "A Quick Group Key Distribution Scheme with Entity Revocation", Advances in Cryptology – Asiacrypt'99, LNCS 1716, Springer, pp. 333-347, 1999.

[2] Naor, M. and Pinkas, B. "Efficient Trace and Revoke Schemes", In Proc. Financial Crypto' 2000, Anguilla, Feb. 2000.

[3] Shamir, A. "How to share a Secret", Comm. ACM, vol. 22, no. 11, pp. 612-613, 1979.

[4] Tzeng, W. and Tzeng, Z.J. "A Public-Key Traitor Tracing Scheme with Revocation Using Dynamic Shares", In Proc. Int'l Workshop on Practice and Theory in Public-Key Cryptography, LNCS 1992, Springer, pp. 207-224, 2001.