情報保護學會論文誌
第13券 第2號, 2003. 4

멀티캐스트 환경에서의 계산비용 향상을 제공하는 사용자 취소 기법*

강 현 선**, 박 철 훈**, 이 병 선**, 박 창 섭***

User Revocation Scheme for Reducing the Computational Overheads in Multicast Environment

Hyun-Sun Kang**, Chul-Hoon Park**, Byung-Seon Lee**, Chang-Seop Park***

요 약

사용자 취소 기법은 멀티캐스트 환경에서 그룹의 동적인 변화에 대한 그룹키의 갱신을 의미한다. 이 논문에서는 그룹 사용자의 그룹키 복호화 계산 비용을 줄이기 위해, 이전에 제안되었던 사용자 취소 기법의 두 가지 변형을 제안한다. 또한 제안된 기법은 무제한 사용자 취소를 위한 방법이기도 하다.

ABSTRACT

Revocation scheme is a re-keying scheme for dynamically changing group in multicast environment. In this paper, we propose two variants of the previously proposed revocation scheme, on the purpose of reducing the amount of computations group members should perform. Also proposed is a method of allowing unlimited number of member revocations.

Keyword : *multicast, revocation scheme, unlimited revocation*

Ⅰ. 개 요

멀티미디어, 뮤직, 비디오, 소프트웨어 등 멀티캐스트(Multicast) 응용 환경에서 서비스되는 디지털 데이터들은 복사나 조작이 용이하며, 인터넷 기반에서 서비스되기 때문에 상당한 문제점을 가지고 있다. 즉, 디지털 데이터들의 무단 불법 복제, 무단 배포 혹은 사용자 정보의 유출, 서비스되는 정보의 도청 등의 여러 가지 공격에 노출될 수 있다. 이와 같은 문제점으로 인해 멀티캐스트 환경에서는 정보보호가 반드시 필요하며 그 근본적인 해결 방법이 데이터의 암호화(Encryption)이다.

일반적으로 멀티캐스트 암호화 기법이란 서비스되는 디지털 데이터를 그룹키(Group Key)를 이용하여 대칭키 방식으로 암호화하여 전달되고, 해당 그룹키는 정당한 사용자만이 복호화(Decryption) 할 수 있도록 공개키로 암호화되어 사용자에게 전달되는 방식을 말한다. 멀티캐스트 메시지를 전달 받은 정당한 사용자는 자신의 개인키로 그룹키를 복호화하고 복호화된 그룹키로 멀티캐스트된 데이터를 복호화하여 서비스를 제공받게 된다. 이와 같은 방식으로 오직 사전에 권한이 부여된 정당한 사용자만이 서비스되는 디지털 정보를 제공받을 수 있게 되며, 여기에서 사용되는 그룹 멤버들(Group Members)간의 공통된

* 본 연구는 2001학년도 단국대학교 대학연구비의 지원으로 연구되었습니다.
** 단국대학교 전자계산학과 대학원(sshskang@dankook.ac.kr)
*** 단국대학교 전자컴퓨터학부 교수(csp0@dankook.ac.kr)

그룹키를 설정하고 변경하는 것이 키관리이다. 키관리는 멤버에 동적인 변화가 생길 때마다 그룹 관리자에 의해 새로운 그룹키 메시지를 전송해 주는 것으로, 이는 그룹에서 탈퇴한 사용자들이 계속해서 그룹 통신에 참여하는 것을 막고 새로운 사용자들이 이전의 그룹 통신에 접근할 수 없도록 하기 위한 것이다.

초기에 제안된 많은 키관리 프로토콜은 탈퇴한 사용자를 기존의 그룹에서 제거하기 위해 새로운 그룹키를 생성한 후 이를 각 사용자들과 공유하고 있는 비밀키를 이용해 대칭키 방식으로 암호화하여 사용자에게 전달하는 방식을 사용하였다. 그러나 이러한 방식은 큰 그룹으로의 확장에 문제가 있으며, 이를 해결하기 위해 제안된 방식으로는 트리(Tree) 방식과 비트리(non-Tree) 방식이 있다. 트리를 이용한 방식은 멀티캐스트 그룹을 이진 트리에 적용한다. 즉, 이진 트리의 루트(root) 노드는 그룹키가 되고 새로운 멤버의 가입 시 사용자를 말단(leaf) 노드에 지정하고 트리의 말단 노드에서 루트 노드까지의 키를 제공하게 된다. 멤버의 탈퇴 등의 이유로 사용자의 권한을 취소해야 할 경우에는 사용자가 저장하고 있던 경로의 모든 키를 변경하게 된다. 이러한 방식은 키의 길이가 짧고 속도가 빠른 반면에 저장해야 할 키의 개수가 많다는 단점이 있다. 비트리 방식은 [1,2,4]에서 소개되었다. [1,2,4]에서는 Shamir의 다항식 기반의 비밀 정보 분할 기법을 사용하여 그룹키를 암호화하는 기법을 사용하였으며 이산대수문제(Discrete logarithm problem)의 어려움에 기반을 두고 있다. 본 논문에서는 기존의 비트리 방식 중 [1]에서 제안된 "A Quick Group Key Distribution Scheme"(QGKDS) 기법을 간단히 소개할 것이며 기존의 비트리 방식에서 계산량과 확장성을 개선한 새로운 두 가지 형태의 기법을 제안할 것이다.

본 논문에서 새롭게 제안되는 기법들은 [1,2,4]에 비해 사용자 측면에서의 복호화에 필요한 계산 비용의 향상을 가져왔다. 이는 클라이언트가 PDA(Personal Digital Assistants), 스마트 폰(Smart Phone)과 같이 계산 능력이 제한적인 단말기인 경우에 매우 중요한 요인으로 작용할 수 있다. [1,2,4]에서는 사용자의 취소가 다항식의 차수인 $t-1$에 기반하며 취소할 수 있는 사용자수는 $t-1$명까지 가능하다. 반면 제안기법 Ⅱ에서는 무제한 사용자 취소 기법을 제안하여 확장성 측면에서의 향상을 가져왔다. [5]에서도 무제한 사용자 취소 기법이 제안되었는데 기존의 메시지 블록에 갱신블록을 따로 추가하여 사용자 취소 기능을 수행하며 [1,2,4]와 같이 한번에 취소 가능한 사용자수는 $t-1$명까지이나 $t-1$명 이상일 경우에는 사용자 취소 알고리즘을 여러 번 반복 수행하여 무제한 사용자 취소를 가능하게 한다. 앞으로 2장에서는 기존 기법에 대해 간략히 설명하고 3장에서는 새로운 제안 기법들에 대해 소개하고 4장에서는 기존 기법과 제안 기법들의 성능비교 및 효율성의 향상됨을 보이고자 한다.

Ⅱ. 기존기법 (QGKDS)

QGKDS은 이산대수 문제의 어려움에 기반을 두고있으며 Shamir[3]의 threshold scheme을 이용하여 그룹키 관리를 한다. 그룹 멤버쉽의 변화에 따른 키 갱신 메시지와 계산 등의 오버헤드는 동시에 탈퇴할 수 있는 최대 사용자 수에 따라 결정되며 사용자가 저장하고 있어야 하는 개인키의 길이는 전체 사용자 수와는 독립적이며, 한 개의 개인키만을 저장하고 있으면 된다. 앞서 개요에서 언급되었던 비밀공유 방식을 이용한 여러 기법들의 키갱신 메시지와 계산등의 오버헤드는 QGKDS와 거의 동일하며 단계별 구성 역시 유사하다. 이 장에서는 여러 기법들 중 특히 QGKDS의 단계별 구성, 오버헤드에 관해 간략히 설명하고자 한다.

2.1 단계별 구성

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

2.1.1 초기화

p,q는 $q|(p-1)$을 만족하는 큰 소수이고, g는 위수가 q인 $GF(p)$상의 원소라고 하자. GM은 $0\le t-1<n$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, a_0는 시스템 비밀키(System

Secret Key)로 사용되게 된다. 그 후 GM은 $n+t-1$개의 i에 대한 $f(i)$와 y_i 값을 계산하여 보관한다. 이 중에서 n개는 그룹에 참여를 원하는 사용자에게 할당하기 위한 것이며, 나머지 $t-1$개는 사용자의 탈퇴 요청 등의 이유로 새로운 그룹키의 갱신이 필요한 경우에 사용하기 위한 것이다.

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

2.1.2 사용자 가입

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

2.1.3 사용자 탈퇴

만약 사용자의 탈퇴 요청 등의 이유로 권한을 취소해야 할 사용자들이 있을 경우 이 사용자들의 집합을 Λ라하고 $|\Lambda| = d$라고 하자. GM $Z_q - U - \Lambda$에서 임의로 $t-d-1$개의 정수를 선택한다. 이때 선택된 정수의 집합을 θ라고 하자. GM은 임의의 난수 $r \in Z_q$을 선택하여 X와 M_j를 계산하고, 메시지(Message)를 작성한 후 작성된 메시지를 멀티캐스트 한다.

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

2.1.4 그룹키 복호화

취소되어야 할 사용자들의 집합 Λ에 포함되지 않은 사용자 i는 수신한 멀티캐스트 메시지와 자신의 개인키 $(i, f(i))$를 이용하여 그룹키 $GK = X^{f(0)}$를 복원하게 된다. 이때 Lagrange 보간법이 사용된다.

$$L(\psi, \omega) = \prod_{k \in \psi - \{\omega\}} (k/(k-\omega)) \bmod q \text{ 라 하면}$$
$$GK = X^{f(0)}$$
$$= X^{f(i) \times L(\Lambda \cup \theta \cup \{i\}, i)} \times \prod_{j \in \Lambda \cup \theta} M_j^{\,L(\Lambda \cup \theta \cup \{i\}, i)} \bmod p$$

2.2 오버헤드

사용자는 한 개의 개인키를 저장하고 있어야 하며, 멀티캐스트 되어야 할 메시지의 개수는 $2t-1$개이고, $2t(t-1)$번의 곱셈과 t번의 지수승, 그리고 t번의 역원 계산이 필요하게 된다.

Ⅲ. 새로운 사용자 취소 기법의 제안

이 장에서는 앞장에서 소개한 QGKDS 기법에서 사용자 측면의 계산 비용을 줄이고자 하는 목적으로 새롭게 제안된 그 변형들에 대해 소개한다. 제안기법 Ⅰ은 취소되어야 할 사용자들의 집합 Λ에 포함되지 않은 사용자들의 공통된 계산을 GM이 미리 계산하여 보냄으로써, 그리고 제안기법 Ⅱ에서는 탈퇴자에 대한 정보를 담고 있는 새로운 다항식을 정의하고 이용함으로써 사용자 측면에서의 계산 비용을 절감시켜 준다. 이처럼 사용자 측면에서의 계산 비용의 향상은 그룹의 클라이언트(Client)가 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 뿐만 아니라 다른 기법들[2,4]에도 적용 가능하다. 이장에서는 QGKDS 유형의 사용자 취소 기법에 적용 가능한 새로운 제안 기법들의 단계별 구성, 오버헤드, 안전성에 관해 간략히 설명한다.

3.1 제안기법 Ⅰ

사용자 측면에서 계산적 오버헤드가 가장 큰 부분은 그룹의 사용자가 수신한 키갱신 메시지를 이용해서 $L(\psi, \omega)$을 계산하는 부분이다. 제안기법 Ⅰ은 취소되어야 할 사용자들의 집합 Λ에 포함되지 않은 사용자들이 그룹키의 갱신을 위해 $L(\psi, \omega)$을 계산함에 있어서 공통된 부분을 GM이 미리 계산하여 보냄으로써 계산 비용을 줄일 수 있다는 제안이다. 그룹 멤버쉽의 변화에 따른 키갱신 메시지와 계산 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.

3.1.1 단계별 구성

[초기화]

p, q는 $q|(p-1)$을 만족하는 큰 소수이고, g는 위수가 q인 $GF(p)$상의 원소라고 하자. GM은 $0 \le t-1 < n$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, a_0는 시스템 비밀키(System Secret Key)로 사용되게 된다. 그 후 GM은 $n+t-1$개의 i에 대한 $f(i)$와 y_i값을 계산하여 둔다. 이 중에서 n개는 그룹에 참여를 원하는 사용자에게 할당하기 위한 것이며, 나머지 $t-1$개는 사용자의 탈퇴 요청 등의 이유로 새로운 그룹키의 갱신이 필요한 경우에 사용하기 위한 것이다.

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

[사용자 가입]

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

[사용자 탈퇴]

만약 사용자의 탈퇴 요청 등의 이유로 권한을 취소해야 할 사용자들이 있을 경우 이 사용자들의 집합을 Λ라하고 $|\Lambda| = d$라고 하자. GM은 $Z_q - U - \Lambda$에서 임의로 $t-d-1$개의 정수를 선택한다. 이때 선택된 정수의 집합을 θ라고 하자. GM은 임의의 난수 $r \in Z_q$을 선택하여 X와 N_j를 계산하고, 메시지(Message)를 작성한 후 작성된 메시지를 멀티캐스트 한다.

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

[그룹키 복호화]

취소되어야 할 사용자들의 집합 Λ에 포함되지 않은 사용자 i는 수신한 멀티캐스트 메시지와 자신의 개인키 $(i, f(i))$를 이용하여 그룹키 $GK = X^{f(0)}$ 를 복원하게 된다. 이때 Lagrange 보간법과 새로 정의한 함수 $I(i,j)$가 사용된다.

$L(\phi, \omega) = \prod_{k \in \phi - \{\omega\}} (k/(k-\omega)) \mod q$ 이고
$I(i,j) = (i/(i-j))$ 이면,

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

3.1.2 오버헤드

사용자는 한 개의 개인키를 저장하고 있어야 하며, 멀티캐스트 되어야 할 메시지의 개수는 $2t-1$개이고, $4(t-1)$번의 곱셈과 t번의 지수승, 그리고 t번의 역원 계산이 필요하게 된다.

3.1.3 안전성

그룹키의 복원을 위해서는 적어도 t개의 점이 필요하다. 만약 권한이 취소된 사용자가 공개된 데이터 y_j나 혹은 N_j로부터 그룹키 GK를 복호화 하려고 한다고 가정할 때 사용자는 복호화에 필요한 정당한 사용자 i의 개인키 $f(i)$ 혹은 GM의 임의의 난수 r을 알아야 한다. 여기서 만약 멀티캐스트 그룹의 정당한 사용자 중에 자신의 개인키를 탈퇴자에게 제공하는 사용자(Traitor)가 없다고 가정한다면, $f(i)$나 r을 구하는 문제는 이산대수문제이므로 구하기는 어렵게 된다. 즉, 사전에 허가를 받은 사용자는 전달받은 메시지로부터 얻은 $t-1$개의 점과 자신이 가지고 있는 하나의 점을 이용하여 그룹키를 복원할 수 있지만, Λ에 포함된 사용자들은 결국 $t-1$개의 점만을 가지게 되므로 새로운 그룹키를 복원하는 것은 불가능하게 된다.

3.2 제안기법 II

제안기법 II는 그룹 멤버가 수신한 키갱신 메시지를 이용해서 새로운 그룹키의 복호화를 위한 계산 중에서 $L(\phi, \omega)$의 계산으로 인한 오버헤드를 줄이기 위한 것으로, 새로운 다항식을 생성, 이용하게 된다. 이 기법 또한 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 개인키만을 저장하고 있으면 된다.

3.2.1 단계별 구성

[초기화]

p, q는 $q|(p-1)$을 만족하는 큰 소수이고, g는 위수가 q인 $GF(p)$상의 원소라고 하자. GM은 $0 \le t-1 < n$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 가입]

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

[사용자 탈퇴]

만약 사용자의 탈퇴 요청 등의 이유로 권한을 취소해야 할 사용자들이 있을 경우, 이 사용자들의 집합을 Λ라하고 $|\Lambda| = d$라고 하자. GM은 $Z_q - U - \Lambda$에서 임의로 $t-d-1$개의 정수를 선택한다. 이때 선택된 정수의 집합을 θ라고 하자.

GM은 $\{(j, f(j)) \mid j \in \Lambda \cup \theta\}$와 임의로 선택한 한 점 $\{(j_1, j_2) \mid j_1 \notin U \cup \Lambda,\ j_2 \neq f(j_1)\}$을 지나는 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 Y_k를 계산하고, 메시지(Message)를 작성한 후 작성된 메시지를 멀티캐스트 한다.

$$X = g^r \bmod p$$

$$Y_k = X^{v_k} \bmod p \quad (0 \le k \le t-1)$$

$$Message = \langle X, \{Y_k \mid 0 \le k \le t-1\}, \{j \mid j \in \Lambda \cup \theta\} \rangle$$

[그룹키 복호화]

취소되어야 할 사용자들의 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 거듭 제곱값은 사용자가 미리 구해 놓는다고 가정한다. 그 다음 Lagrange 보간법을 이용하여 그룹키 GK를 다음과 같이 복원할 수 있게 된다.

$$X^{v(i)} = (Y_0)^{i^0} (Y_1)^{i^1} \ldots (Y_{t-1})^{i^{t-1}}$$

$$X^{h(i)} = X^{f(i) - v(i)}$$

$$L(\psi, \omega) = \prod_{k \in \psi - \{\omega\}} (k/(k-\omega)) \bmod q \text{ 라 하면}$$

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

$$\text{where } W_j = X^{h(j)}$$

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

3.2.2 오버헤드

사용자는 한 개의 개인키를 저장하고 있으면 된다. 멀티캐스트 될 메시지의 수는 $2t$개이고 $3(t-1)$번의 곱셈과 $t+1$번의 지수승과 2번의 역원 계산이 필요하게 된다.

3.2.3 안전성

사전에 허가를 받은 사용자 i는 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 만약 멀티캐스트 그룹의 정당한 사용자 중에 자신의 개인키를 탈퇴자에게 제공하는 사용자(Traitor)가 없다고 가정한다면, Λ에 포함된 사용자 j는 $h(j) = f(j) - v(j) = 0$으로 새로운 그룹키를 복원하는 것은 불가능하다.

Ⅳ. 기존 기법과 제안 기법의 성능 비교

우리는 앞에서 기존 기법과 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

기존 기법에서는 취소 가능한 사용자의 수는 개인키를 구성하는 다항식 $f(x)$의 차수 $(=t-1)$에 제약을 받는다. 하지만, 제안기법 Ⅱ에서 정의된 다항식을 사용한다면 한번에 취소 가능한 사용자의 수는 n까지 증가시킬 수 있다. 만약 $|\Lambda| = d$이고 $t \le d \le n$이라면, GM은 $\{(j, f(j)) \mid j \in \Lambda\}$와 임의로 선택한 한

점 $\{(j_1, j_2) \mid j_1 \notin U, j_2 \notin f(j_1)\}$을 지나는 d차 다항식 $v(x) = v_0 + v_1 x + \ldots + v_d x^d$를 생성하고 메시지를 멀티캐스트 한다. $h(x) = f(x) - v(x)$를 기반으로, 새로운 그룹키 $GK = X^{h(0)} = X^{h(i) \times L(A \cup \theta \cup \{i\}, i)}$가 생성될 수 있다. 물론 $d = n$일 경우는 기존의 모든 사용자들이 취소되는 경우를 의미한다.

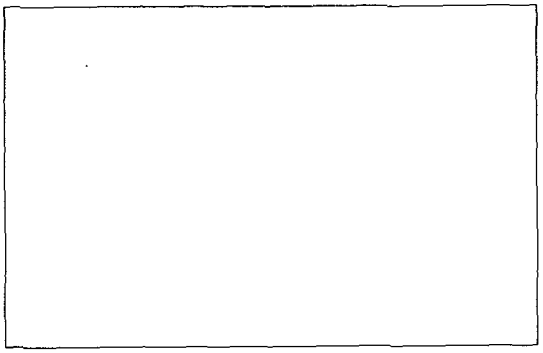
4.2 계산비용 측면

사용자측의 계산 비용에서도 기존 기법에 비해 새롭게 제안하는 기법들이 향상되었음을 알 수 있다. 곱셈 계산의 경우 기존 기법은 $2t^2 - 2t$인 것에 비해 새로운 제안 기법은 $4t-4$와 $3t-3$으로 감소하였으며, 역원 계산의 경우 기존 기법은 t인 것에 비해 제안 기법 II는 2로 감소하였음을 볼 수 있다. 즉, 곱셈 계산의 경우 $O(t^2)$에서 $O(t)$로 줄어들었으며 역원 계산의 경우는 $O(t)$에서 $O(1)$로 현저히 줄어들었음을 알 수 있다. 효율성의 향상을 확인하기 위해 여러 기법의 전체 계산 비용에 대한 비교는 표 1로 정리하였다.

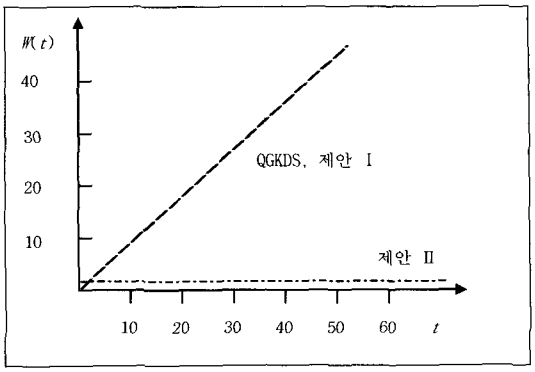
여러 기법의 계산 비용 중 두드러지게 향상된 연산에 대한 계산비용을 [그림 1]과 [그림 2]로 나타냈다. [그림 1]은 탈퇴자수에 의한 곱셈 계산비용 비교이고, [그림 2]는 탈퇴자수에 의한 역원 계산비용 비교이다.

〔표 1〕 여러 기법의 계산비용비교

구 분	QGKDS	제안기법 I	제안기법 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 계산비용 비교



〔그림 2〕 탈퇴자수에 의한 역원 계산비용 비교

참 고 문 헌

[1] J. Anzai, N. Matsuzaki and T. Matsumoto, "A Quick Group Key Distribution Scheme with Entity Revocation", Proc. Advances in Cryptology-Asiacrypt' 99, Vol. 1716 of Lecture Notes in Computer Science, pp. 333~347, Springer Verlag, 1999.

[2] M. Naor and B. Pinkas, "Efficient Trace and Revoke Schemes", Proc. Financial Cryptography 2000,Anguilla, February 2000.

[3] A. Shamir, "How to share a Secret", Comm. ACM, Vol. 22, No. 11, pp. 612~613, 1979.

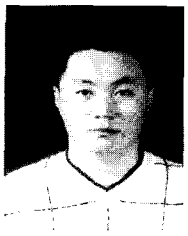
[4] W. Tzeng and Z. J. Tzeng, "A Public-Key Traitor Tracing Scheme with Revocation Using Dynamic Shares", International Workshop on Practice and Theory in Public-Key Cryptography-PKC' 01, Vol. 1992 of Lecture Notes in Computer Science, pp. 207~224, Springer Verlag, 2001.

[5] 김현정, 이동훈, "Efficient Public-Key Traitor Tracing with Unlimited Revocation Capability", 한국정보보호학회 논문지, Vol. 11, No. 5, pp. 31~41, 2001.

〈著者紹介〉

강 현 선 (Hyun-Sun Kang) 학생회원
2002년 2월 : 단국대학교 전자계산학과 졸업
2002년 3월~현재 : 단국대학교 전자계산학과 석사과정
<관심분야> 부호이론, 암호학

박 철 훈 (Chul-Hoon Park) 학생회원
2002년 2월 : 단국대학교 전자계산학과 졸업
2002년 3월~현재 : 단국대학교 전자계산학과 석사과정
<관심분야> 부호이론, 암호학



이 병 선 (Byung-Seon Lee) 학생회원
2002년 2월 : 단국대학교 전자계산학과 졸업
2002년 3월~현재 : 단국대학교 전자계산학과 석사과정
<관심분야> 부호이론, 암호학

박 창 섭 (Chang-Seop Park) 정회원
1983년 : 연세대학교 경제학과 졸업
1983년 : 한국 IBM 근무
1990년 : LEHIGH Univ. 전자계산학 박사
1990년~현재 : 단국대학교 전자컴퓨터학부 교수
<관심분야> 부호이론, 암호학