자가 치료 기능과 취소 능력을 가진 효율적인 그룹키 분배 기법

강 주 성[†] · 홍 도 원[††]

요 약

자가 치료 기능을 가진 그룹키 분배 기법은 신뢰성이 약한 네트워크 환경에서 특정 세션의 그룹키 정보를 수신하지 못한 사용자가 그룹 매니저와의 추가적인 통신 없이 스스로 세션키를 복구할 수 있도록 해주는 방식이다. 본 논문에서는 자가 치료 기능을 가진 새로운 그룹키 분배 기법을 제안한다. 여기에서 제안하는 방식은 취소 능력을 가지며, 사용자의 저장 메모리 관점에서 최적이고, 통신 복잡도 측면에서는 기존의 방법들 보다 효율적이다. 최근에 제안된 Blundo 등[13]과 Liu 등[14]의 방식에서 사용한 브로드캐스트 방법을 적절히 원용함으로써 메모리 정장소는 최적이고, 통신 복잡도 관점에서는 기존 두 방식들보다 약 2배 정도 개선된 결과를 얻는다. 또한, 제안한 프로토콜이 t-차 순방향 및 역방향 기밀성을 만족한다는 사실을 증명하고, 단일 브로드캐스트 메시지를 통해서 그룹세션키를 복구할 수 있는 보다 효율적인 자가 치료 기능을 가진 그룹키 분배 기법도 가능함을 보인다.

키워드 : 그룹키 분배, 자가 치료 기능, 취소 능력

An Efficient Variant of Self-Healing Group Key Distribution Scheme with Revocation Capability

Ju-Sung Kang[†] · Dowon Hong[††]

ABSTRACT

In the self-healing group key distribution scheme, users are capable of recovering lost group keys on their own without requesting additional transmission from the group manager, where there is no reliable network infrastructure. In this paper, we propose a new self-healing group key distribution scheme with revocation capability, which is optimal in terms of user memory storage and more efficient in terms of communication complexity than the previous results. We obtain a slightly improved result from [13] and [14] by using the new broadcasting method. In addition, we prove that our scheme has the properties of t-wise forward secrecy and t-wise backward secrecy, and extend this self-healing approach to the session key recovery scheme from a single broadcast message.

Key Words : Group Key Distribution, Self-healing Property, Revocation Capability

1. 서 론

안전한 그룹 통신을 실현하기 위해서 가장 중요한 문제는 그룹키를 안전하게 분배하고, 그룹키 관련 요소들을 관리하는 그룹키관리(group key management)라 할 수 있다. 그룹키관리 시스템은 그룹 멤버 간에 공유된 그룹키를 안전하게 설치 및 유지하는 것이다. 멤버의 교체가 빈번한 큰 그룹인 경우 멤버쉽의 변화에 따른 그룹키의 업데이트 및 안전한 재분배 기술은 필수적인 것이다. 그룹키의 재분배 방법 중 가장 단순하면서 안전성을 보장할 수 있는 것으로 그룹 매니저가 각 멤버들에게 업데이트된 그룹키를 암호화해서 송신하는 방법을 생각해볼 수 있다. 그러나 이 방법은 그룹 크기에 따라서 비용이 선형적으로 증가하기 때문에 효율적인 방법이라 할 수 없다. 멤버쉽의 변화에 따른 효율적인 그룹키 업데이트 및 재분배 방법은 최근에 많은 연구가 이루어졌으며[1, 2, 3, 4, 5], 멤버쉽의 변화 대신에 주기적으로 그룹키를 재분배하는 방식들도 제안되었다[6, 7]. 주기적으로 키를 재분배하는 방식은 그룹 매니저의 통신 오버헤드를 줄임으로써 트리 구조에 기반한 그룹키관리 프로토콜의 확장성과 효율성을 높이는 방식이다. 특권이 주어진 그룹으로부터 사용자 취소를 다룬 경우[4, 5, 8]도 있으며, 국내에서는 신분확인 프로토콜에 기반을 둔 그룹키 분배 및 갱신 프로토콜[15], 멀티캐스트 환

※ 제1저자는 2004년도 국민대학교 신진교수 연구지원금으로 본 연구를 수행하였음.
† 정 회 원 : 국민대학교 수학과 조교수
†† 정 회 원 : 한국전자통신연구원 선임연구원
논문접수 : 2005년 2월 11일, 심사완료 : 2005년 10월 26일

경에서 효율적인 그룹키관리 방식[16], 유료 방송 시스템을 위한 그룹키 동의 프로토콜[17] 등이 발표되는 등 그룹키관리 관련 연구 결과들은 꾸준히 발표되어 왔다. 그러나 이와 같은 모든 연구 결과들은 기본적으로 네트워크의 신뢰성(reliability)을 가정한 상태에서 출발하였다.

신뢰성을 가정할 수 없는 네트워크 환경에서의 그룹키 분배 방식은 그동안 상대적으로 많은 관심을 받지 않아서 활발히 연구되어 오지 못했다. 다만 비상호적인 수단을 통해서 패킷 손실을 만회할 수 있는 키 분배 기법으로 [9]와 [10]의 연구 결과를 주목해 볼 수 있다. [9]에서는 에러 정정 기술이 적용되었고, [10]에서는 짧은 힌트 메시지가 패킷에 추가되는 기술이 이용되었다.

한편, Staddon 등[11]은 최근 자가 치료(self-healing) 기능을 가진 그룹키 분배 기법으로 명명한 흥미로운 프로토콜을 제안하였다. 이 프로토콜은 신뢰성이 담보되지 않은 환경 속에서 주기적인 그룹키 재분배를 가능하게 해준다. 특정한 세션에서의 그룹키 정보를 받지 못한 사용자가 그 세션 이전과 이후의 세션들에서 정당한 멤버쉽을 소유하고 있을 경우, 그 사용자는 그룹 매니저와의 추가적인 통신이 없이 스스로 해당 세션의 그룹키를 복구할 수 있다. 또한, 이들이 제안한 방식은 취소 능력을 가짐으로써 가입과 탈퇴가 자유로운 동적인 그룹에서 공모 공격(collusion attack)에 대한 저항성을 갖는다.

자가 치료 기능을 가진 그룹키 분배 프로토콜은 그룹 멤버들이 패킷 손실을 경험하기 쉬운 환경에 적합한 새로운 방식이다. 이는 기본적으로 네트워크의 트래픽과 그룹 매니저의 작업 부담을 낮춘다는 장점과 함께 트래픽 분석을 통한 사용자 노출의 위험성을 줄여주는 방식이다. 무선(wireless), 이동(mobile), 임시 네트워크(ad hoc network)의 사용이 증가하는 현재의 상황에서 보안 문제가 가장 중요한 요소가 되는 경우에 자가 치료 기능을 가진 그룹키 분배 프로토콜은 매우 유용한 도구가 될 것이다. 특히, 군사적 임무 수행, 구출 작전, 과학적 연구 조사 등을 위한 응용 환경에서는 일반적으로 신뢰성 높은 네트워크 인프라가 존재한다고 볼 수 없다. 이러한 환경에서 공격자들은 통신 정보를 가로채거나 방해함으로써 그들의 목적을 달성하려고 노력할 것이다. 이 경우 보안 문제는 가장 먼저 고려해야할 항목이 된다. 이와 같은 제반 여건하에서 통신 보안을 보장할 수 있는 유용한 기술 중의 하나가 바로 자가 치료 기능을 가진 그룹키 분배 프로토콜인 것이다.

Staddon 등[11]에 의해서 제안된 방식에 대해서는 자가 치료 기능이라는 새로운 응용이 가능하게 되었다는 것에 큰 의미를 부여할 수 있지만, 이 방식에는 통신 오버헤드가 크고 유지 비용도 매우 비싸다는 단점도 내재되어 있다. 그래서 이에 대한 개선 방안으로 발표된 연구 결과들이 [12], [13], [14] 등이다. Blundo 등[13]은 [11]의 방식에서 발견된 이론적인 오류를 지적하면서 이들과는 약간 다른 모델 하에서 새로운 자가 치료 가능한 그룹키 분배 프로토콜을 제안하였다. 이들은 단일 브로드캐스트 메시지로부터 세션키 복구가 가능한 방식도 함께 제안하였다. Liu 등[14]은 브로드캐스트 채널을 통해서 효율적인 개인키(personal key) 분배를 가능케 하는 새로운 키 분배 방식을 제안하고, 이 방식에 Staddon 등[11]의 자가 치료 기능을 합성한 그룹키 분배 프로토콜을 제안하였다. Blundo 등과 Liu 등의 연구 결과들은 모두 메모리 저장소(memory storage)와 통신 복잡도 측면에서 원래 Staddon 등의 프로토콜 보다 개선된 방식들이다.

본 연구를 통해서 우리가 얻은 결과를 요약하면 다음과 같다. 첫째, Blundo 등[13]의 자가 치료 가능 그룹키 분배 모델을 기반으로 하여 [13]과 [14]에서 사용한 브로드캐스트 기법을 원용함으로써 이들에 비해서 저장 용량과 통신 오버헤드가 작은 효율적인 프로토콜을 새롭게 제안한다. 제안하는 방식과 기존 방식들 간의 효율성 비교표도 제공한다. 둘째, 제안한 프로토콜이 t-차 순방향 및 역방향 기밀성 성질을 만족한다는 사실을 증명한다. 마지막으로, 제안된 자가 치료 가능 그룹키 관리 방식을 기반으로 단일 브로드캐스트 메시지로부터 사용자가 정당한 멤버쉽을 소유하고 있는 동안의 모든 세션키를 복구할 수 있는 프로토콜을 제안한다. 우리가 제안하는 단일 브로드캐스트를 이용한 세션키 복구 방식도 기존 Blundo 등[13]의 방식 보다 효율적이다.

2. 자가 치료 기능을 가진 그룹키 분배 모델

여기에서 고려하는 자가 치료 기능을 가진 그룹키 분배 모델은 Blundo 등[13]이 제안한 것으로 최초에 Sttadon 등[11]이 제안한 것을 약간 개선한 것이다. 네트워크 내의 통신 개체들은 브로드캐스트 메시지 접근을 제어할 수 있는 그룹을 구성한다고 가정한다. 네트워크의 수명은 세션이라 불리는 시간 구간(time interval)들로 분할된다. 우리가 원하는 바는 취소 능력과 자가 치료 기능을 가진 효율적이고 무조건적으로 안전한(unconditionally secure) 세션키 분배 방식을 개발하는 것이다. 그룹 매니저는 다수의 인가받은 그룹 멤버들에게 그룹 세션키를 분배하는 책임을 진다. 세션키를 분배하는 과정에서 반드시 연속적일 필요는 없는 세 개의 세션열(sequence of sessions) 동안 정당한 멤버쉽을 가진 사용자가 첫 번째와 세 번째 세션으로부터 복구된 정보로부터 가운데 세션인 두 번째 세션의 세션키를 복구할 수 있는 경우 자가 치료 기능(self-healing property)을 갖는다고 말한다. 또한, t 명 이하의 멤버쉽 취소자들만의 공모로는 새로운 세션키를 알아내는 것이 불가능할 때, 그 세션키 분배 방식은 t-취소 능력(t-revocation capability)을 갖는다고 부른다.

이제 한명의 그룹 매니저가 있고, 유한한 수의 멤버들이 존재하는 경우를 고려하자. 그룹 매니저는 가입(join)과 탈퇴(revoke) 동작을 통해서 동적인 사용자 그룹인 $\mathbb{U}$를 만들고 관리한다. p가 안전성을 유지할 수 있는 충분히 큰 소수(prime number)일 때, 모든 연산은 유한체 $\mathbb{F}_p$에서 이루어진다. 즉, 그룹키, 브로드캐스트 메시지, 개인키 등이 모두 유한체 $\mathbb{F}_p$ 내의 원소이고, 이들 간의 모든 연산들이 $\mathbb{F}_p$ 내에서 이

루어진다. 유한체의 크기가 클수록 더 많은 멤버들을 수용할 수 있지만, p의 크기에 따라서 메모리 저장량과 통신 복잡도도 증가한다는 단점이 있다. 그룹의 수용 인원을 최대 δ라 하고, 안전성 문제로 세션키의 크기를 적어도 80-비트 길이로 할 경우 p는 $p > max\{2^{80}, \delta\}$를 만족하면 된다.

세션 j에서 그룹 매니저에 의해 구축된 통신 그룹을 $G_j \subseteq \mathbb{U}$라 하자. 사용자 $U_i \in G_j$는 U_i가 그룹 매니저에 의해서 그룹으로부터 제거되기 전까지는 세션키 복구를 위해서 사용되는 개인키 $S_i \in \mathbb{F}_p$를 그룹 G_j에 가입할 때에 그룹 매니저로부터 받는다. 세션의 전체 개수는 m이라 가정하고, 세션 j에서 멤버쉽이 취소된 사용자들의 집합을 R_j라 하며, 세션 j에서 새롭게 가입한 사용자들의 집합을 $Join_j$라 놓는다. 그러므로 $G_j = (G_{j-1} \cup Join_j) - R_j$가 된다. $j = 1, \cdots, m$에 대하여, 세션키 K_j는 그룹 매니저에 의해서 랜덤하게 선택되어 브로드캐스트 메시지 B_j를 통해서 그룹 멤버들에게 송신된다. 각 사용자 $U_i \in G_j$에 대해서 j번째 세션의 그룹 세션키 K_j는 B_j와 개인키 S_i에 의해서 결정된다.

정보 이론(information theory)을 이용한 표현법을 사용하기 위해서 S_i, B_j, K_j를 확률 변수(random variable)로 간주하자. 세션키 K_j들은 $\mathbb{F}_p$에 균등 분포(uniform distribution)가 주어졌다는 가정 하에 각각 독립적으로 $\mathbb{F}_p$에서 선택되어진다고 하자. 그리고 엔트로피 함수를 $H(\cdot)$로 나타내기로 하자. 그러면 취소 능력과 자가 치료 기능을 가진 그룹키 분배 방식에 대한 엄밀한 정의를 다음과 같이 기술할 수 있다.

[정의 1] [13] $\mathbb{U}$를 한 네트워크 내의 모든 사용자들의 집합이라 하고, m을 세션들의 최대 개수라 하자.

1. $\mathbb{D}$가 다음 두 가지 조건 (a)와 (b)를 만족할 때, $\mathbb{D}$를 세션키 분배 방식(session key distribution scheme)이라 한다.
   (a) 임의의 멤버 $U_i \in G_j$에 대하여 세션키 K_j는 B_j와 S_i에 의해서 결정된다. 즉, 다음을 만족한다.
   $$H(K_j | B_j, S_i) = 0.$$
   (b) 그룹 멤버들이 브로드캐스트 B_j와 그들의 개인키로부터 얻을 수 있는 정보는 브로드캐스트 또는 개인키 하나만으로는 결정되지 않는 것이다. 수식으로는 다음이 성립한다.
   $$\begin{aligned} &H(K_1, \cdots, K_m | B_1, \cdots, B_m) \\ &= H(K_1, \cdots, K_m | S_1, \cdots, S_n) \\ &= H(K_1, \cdots, K_m), \end{aligned}$$
   여기에서 $S_1, \cdots, S_n$은 $G_1 \cup \cdots \cup G_m$ 안에 있는 사용자들인 $U_1, \cdots, U_n$의 개인키들을 의미한다.
2. 각 세션 j에 대하여 $R = R_j \cup R_{j-1} \cup \cdots \cup R_1$으로 놓고, $|R| \le t$인 경우 그룹 매니저가 R 내에 있는 멤버쉽이 취소된 모든 사용자들이 K_j를 복구할 수 없는 브로드캐스트 B_j를 생성할 수 있을 때, $\mathbb{D}$는 t-취소 능력(t-revocation capability)을 갖는다고 말한다. 수식으로 표현하면, 다음이 성립한다.
   $$H(K_j | B_j, B_{j-1}, \cdots, B_1, S_R) = H(K_j),$$
   여기에서 S_R은 R에 있는 모든 사용자의 개인키를 나타낸다.
3. $\mathbb{D}$가 다음 두 가지 조건 (a)와 (b)를 만족할 때, $\mathbb{D}$는 자가 치료 기능(self-healing property)을 갖는다고 한다.
   (a) $1 \le r < s \le m$인 경우 $U_i \in G_r$인 사용자 U_i가 세션 s 이전에 취소되지 않는다면, $l = r, \cdots, s$에 대하여 U_i는 모든 세션키 K_l을 복구할 수 있다. 수식으로는 다음이 성립한다.
   $$H(K_r, \cdots, K_s | S_i, B_r, B_s) = 0.$$
   (b) $C \subseteq (R_r \cup R_{r-1} \cup \cdots \cup R_1)$을 세션 r 이전에 제거된 멤버들의 공모(coalition)라하고, $D \subseteq (Join_s \cup \cdots Join_m)$을 세션 s 이후에 가입한 멤버들의 공모라 하며, $|C \cup D| \le t$라 하자. 그러면, 임의의 $r \le j \le s$에 대하여 이러한 공모는 세션키 K_j에 대한 어떠한 정보도 얻을 수 없다. 수식으로는 다음이 성립한다.
   $$\begin{aligned} &H(K_r, \cdots, K_{s-1} | B_1, \cdots, B_m, S_C, S_D) \\ &= H(K_r, \cdots, K_{s-1}), \end{aligned}$$
   여기에서 S_C는 C에 있는 사용자들의 개인키를 나타내고, S_D는 D에 있는 사용자들의 개인키를 의미한다.

한편, Liu 등[14]은 세션키 분배 방식의 안전성 논의를 보다 명확히 하기 위해서 t-차 순방향 기밀성(t-wise forward secrecy)과 t-차 역방향 기밀성(t-wise backward secrecy)이라는 개념을 소개하였다. t-차 순방향과 역방향 기밀성은 본래의 순방향 및 역방향 기밀성 보다 강한 개념으로 키 독립성, 그룹키 기밀성 등을 보장한다. Liu 등[14]은 실제로 자신들이 제안한 방식 2(Scheme 2)가 t-차 순방향 및 역방향 기밀성을 만족한다는 사실을 증명하였다. 우리는 본 논문에서 제안하는 방식 역시 t-차 순방향 및 역방향 기밀성을 만족한다는 사실을 보일 것이다. 이를 위해서 이 개념들을 다음 정의에서와 같이 엄밀하게 인용하기로 한다.

[정의 2] [14] $t, i \in \{1, \cdots, n\}$이고, $j \in \{1, \cdots, m\}$이라 하자.

1. 집합 $R \subseteq \{U_1, \cdots, U_n\}$이 세션 j 이전에 취소된 $r \in R$들의 모임이고, $|R| \le t$를 만족할 때, R 내에 있는 멤버들만으로는 세션 j 이전의 그룹키를 알고 있다고 하여도 K_j에 대한 어떠한 정보도 얻을 수 없다면, 이 세션키 분배 방식은 t-차 순방향 기밀성(t-wise forward secrecy)을 보장한다고 말한다. 수식으로는 다음을 만족한다.
   $$\begin{aligned} &H(K_j | B_1, \cdots, B_m, \{S_i\}_{U_i \in R}, K_1, \cdots, K_{j-1}) \\ &= H(K_j). \end{aligned}$$
2. 집합 $R \subseteq \{U_1, \cdots, U_n\}$이 세션 j 이후에 가입한 $r \in R$들의 모임이고, $|R| \le t$를 만족할 때, R 내에 있는 멤버들만으로는 세션 j 이후의 그룹키를 알고 있다고 하여도 K_j

에 대한 어떠한 정보도 얻을 수 없다면, 이 세션키 분배 방식은 t-차 역방향 기밀성(t-wise backward secrecy)을 보장한다고 말한다. 수식으로는 다음을 만족한다.

$$H(K_j|B_1, \cdots, B_m, \{S_i\}_{U_i \in R}, K_{j+1}, \cdots, K_m) = H(K_j).$$

3. 기존의 자가 치료 가능 그룹키 분배 기법

자가 치료 기능을 가진 그룹키 분배 모델은 최초에 Sttadon 등[11]이 제안하였다. 그 이후의 주목할만한 성과로는 Blundo 등[13]의 결과와 Liu 등[14]이 제안한 것을 들 수 있다. 본 논문에서 새롭게 제안하는 방식과 비교 검토하기 위해서 이 소절에서는 이 세 가지 연구 결과에 나타나 있는 대표적인 방식들을 간단히 살펴보기로 한다.

• Staddon 등[11]의 방식 3 (Construction 3)

1. 장치(Setup) : t는 양의 정수이고, N은 사용자 인덱스와 다른 $\mathbb{F}_p$의 원소라 하자. 그룹매니저는 m개의 t차 다항식 $p_1(x), \cdots, p_m(x)$을 $\mathbb{F}_p[x]$에서 랜덤하게 선택하고, m개의 세션키 $K_1, \cdots, K_m$을 $\mathbb{F}_p$에서 랜덤하게 선택한다. 그리고 $j=1, \cdots, m$에 대해서 $q_j(x) = K_j - p_j(x)$로 정의한다. 각각의 $j \in \{1, \cdots, m\}$에 대해서 $\mathbb{F}_p[x, y]$ 내에 있는 랜덤한 m개의 다항식 $s_{1,j}, \cdots, s_{m,j}$를 선택한다. 여기에서 $s_{i,j}(x,y) = a_{0,0}^{i,j} + a_{1,0}^{i,j}x + a_{0,1}^{i,j}y + \cdots + a_{t,t}^{i,j}x^t y^t$이다. 각 사용자 U_i ($i \in \{1, \cdots, n\}$)는 개인키로 S_i를 다음과 같이 저장한다. $S_i = \{N, i, s_{1,1}(i,i), \cdots, s_{m,m}(i,i)\}$.
2. 브로드캐스트(Broadcast) : $A, R \subset \{U_1, \cdots, U_n\}$는 각각 세션 j에서 활성화된(active) 사용자와 취소된(revoked) 사용자를 나타내고, $|R| \le t$이라 한다. 그룹매니저는 R에 있는 사용자 인덱스를 포함하고, A의 사용자 인덱스는 포함되지 않으며, $N \notin W$인 집합 $W = \{w_1, \cdots, w_n\} \subset \mathbb{F}_p$를 선택한다. 그러면 세션 j에서의 브로드캐스트는 $B_j^1 \cup B_j^2$이다. 여기에서
$$B_j^1 = \{p_{j'}(x) + s_{j',j}(N,x)\}_{j'=1,\cdots,j-1} \cup \{K_j + s_{j,j}(N,x)\} \cup \{q_{j'}(x) + s_{j',j(N,x)}\}_{j'=j+1,\cdots,m}$$
$$B_j^2 = \{w_l, \{s_{j',j}(w_l,x)\}_{j'=1,\cdots,m}\}_{l=1,\cdots,t}$$
3. 세션키와 공유값(shares) 계산 : 사용자 U_i는 $\{s_{j,j}(w_l,x)\}_{l=1,\cdots,t}$를 이용하여 $x=i$일 때를 계산하고, $(i, s_{j,j(i,i)})$와 $\{(w_l, s_{j,j}(w_l,i))\}_{l=1,\cdots,t}$를 이용한 보간법(interpolation)에 의해서 $s_{j,j}(x,i)$를 복구할 수 있다. 그러면 $x=N$을 $s_{j,j}(x,i)$에 대입하고, 그 값을 $(K_j + s_{j,j}(N,x))|_{x=i}$에서 뺌으로써 세션키 K_j를 복구할 수 있다.

   추가적으로 U_i는 $\{s_{j',j}(x,i)\}_{j'=1,\cdots,j-1,j+1,\cdots,m}$을 결정하기 이해서 보간법을 사용할 수 있고, 이로부터 공유값인 $\{p_{j'}(i)\}_{j'=1,\cdots,j-1}$과 $\{q(i)\}_{j'=j+1,\cdots,m}$을 유사한 방법으로 복구할 수 있다.

• Blundo 등[13]의 방식 2 (Sheme 2)

1. 장치(Setup) : $G_1 = \{U_1, \cdots, U_n\}$이라 놓자. 그룹매니저는 균등하게(uniformly) m개의 t-차 다항식 $s_1(x), \cdots, s_m(x) \in \mathbb{F}_p[x]$를 선택하고, 이와는 독립적으로 m개의 세션키 $K_1, \cdots, K_m \in \mathbb{F}_p$를 균등하게 뽑는다. 그리고 각 $j=1, \cdots, m$에 대해서 $z_j = K_j + s_j(0)$으로 정의한다. 그룹매니저는 U_i ($i=1, \cdots, n$)에게 개인키 $S_i = \{s_1(i), \cdots, s_m(i)\}$를 안전한 통신 경로를 통해서 전달한다.
2. 브로드캐스트(Broadcast) : $R_j \subset G_{j-1}$은 세션 j에서 취소된 사용자들의 집합이고, $R = R_j \cup R_{j-1} \cup \cdots \cup R_2$이며, $|R| \le t$라 놓는다. 그룹매니저는 R에 속한 인덱스 집합 I_R을 포함하고, $W \cap I_{G_j} = \varnothing$을 만족하는 인덱스 집합 $W = \{w_1^j, \cdots, w_t^j\}$를 선택한다. 그리고 세션 j에 메시지 $B_j = B_j^1 \| B_j^2$를 다음과 같이 구성하여 전송한다.

   $j=1, 2$에 대해서

   $B_j = \{z_j \| w_1^j, \cdots, w_t^j, s_j(w_1^j), \cdots, s_j(w_t^j)\}$,

   $j=3, \cdots, m$에 대해서

   $B_j^1 = \{z_1 + z_2, \cdots, z_1 + z_{j-1}, z_j\}$,

   $B_j^2 = \{w_1^j, \cdots, w_t^j, s_j(w_1^j), \cdots, s_j(w_t^j)\} \| B_{j-1}^2$.

   여기에서 $B_0^2 = \varnothing$으로 놓는다.
3. 세션키 계산 : 사용자 U_i는 라그랑지의 보간법을 이용하여 $\{(w_l^j, s_j(w_l^j))\}_{l=1,\cdots,t}$와 $(i, s_j(i))$로부터 $s_j(0)$를 복구한다. 그리고 $z_j - s_j(0)$를 계산함으로써 세션키 K_j를 얻는다.

• Liu 등[14]의 방식 3 (Scheme 3)

1. 장치(Setup) : 그룹매니저는 m개의 마스킹을 위한 $2t$차 다항식 $\{h_i(x)\}_{i=1,\cdots,m}$과 m개의 t차 다항식 $\{f_i(x)\}_{i=1,\cdots,m}$을 $\mathbb{F}_p[x]$로부터 랜덤하게 선택한다. 각 사용자 U_v는 그룹매니저로부터 안전한 통신로를 통하여 개인비밀 정보인 $S_v = \{h_i(v), f_i(v)\}_{i=1,\cdots,m}$을 얻는다. 그룹 매니저는 균등하게(uniformly) m개의 t-차 다항식 $p_1(x), \cdots, p_m(x) \in \mathbb{F}_p[x]$를 선택하고, 이와는 독립적으로 m개의 세션키 $K_1, \cdots, K_m \in \mathbb{F}_p$를 균등하게 뽑는다. $j=1, \cdots, m$에 대하여, $q_j(x) = K_j - p_j(x)$로 놓는다.
2. 브로드캐스트(Broadcast) : j번째 세션에서 그 때까지 취소된 멤버들의 ID 집합이 주어지고, $R_i = \{r_1, \cdots, r_{w_i}\}_{i=1,\cdots,j}$이며, $|R_i| = w_i \le t$, $i=1, \cdots, j$라고 하자. 그룹매니저는 다음의 메시지를 브로드캐스트 한다.
$$B_j = \{R_i\}_{i=1,\cdots,j} \cup \{P_i(x) = g_i(x)p_i(x) + h_i(x)\}_{i=1,\cdots,j} \cup \{Q_i(x) = q_i(x) + f_i(x)\}_{i=j,\cdots,m}$$

여기에서 $g_i(x)=(x-r_1)(x-r_2)\cdots(x-r_{w_i})$이다.

3. 세션키와 공유값 계산: U_v는 수신한 메시지로부터 $\{P_i(x)\}_{i=1,\cdots,j}$ $\{P_i(x)\}_{i=1,\cdots,j}$와 $\{Q_i(x)\}_{i=j,\cdots,m}$의 $x=v$에서의 값을 계산하여 공유값 $\{p_1(v),\cdots,p_j(v)\}$와 $\{q_j(v),\cdots,q_m(v)\}$를 복구한다. 그리고 $K_j=p_j(v)+q_j(v)$로 세션키를 복구하고 자신에게 없는 정보들을 저장한다.

위에서 기술한 바를 바탕으로 살펴보면, Staddon 등[11]의 방식은 자가 치료 기능이라는 새로운 응용이 가능하게 되었다는 창조성에 큰 의미를 부여할 수 있지만, 통신 오버헤드가 크고 유지 비용도 매우 비싸다는 점을 느낄 수 있다. Blundo 등[13]의 방식은 [11]의 방식에 비해서 한층 간결해진 프로토콜임을 알 수 있다. 그리고 Liu 등[14]의 방식은 브로드캐스트 채널을 통해서 효율적인 개인키(personal key) 분배를 가능케 하는 새로운 키 분배 방식을 제안하고, 이 방식에 Staddon 등[11]의 자가 치료 기능을 합성한 것으로 볼 수 있다. Blundo 등과 Liu 등의 연구 결과들은 모두 메모리 저장소(memory storage)와 통신 복잡도 측면에서 원래 Staddon 등의 프로토콜 보다 개선된 방식들이다.

4. 새로운 자가 치료 가능 그룹키 분배 기법

4.1 효율적인 자가 치료 가능 키 분배 기법

본 소절에서는 새로운 자가 치료 가능 그룹키 분배 기법을 제안한다. 여기에서 제안하는 방식의 새로운 점으로는 기존 [11], [13], [14] 등에 제안된 방식들과는 다른 자가 치료 기술(self-healing technique)을 적용하였다는 점과 기존 방식들보다 개선된 효율성을 보인다는 점을 들 수 있다. 구체적으로는 [13]과 [14]의 방식에서 보여지는 브로드캐스트 방법을 적절히 원용함으로써 이 두 방식들 보다 메모리 저장소와 통신 복잡도 관점에서 약간씩 개선된 결과를 얻었다는 것이다. 또한, 제안한 프로토콜이 t-차 순방향 및 역방향 기밀성을 만족한다는 사실도 증명한다.

• 제안방식 1

1. 장치(Setup): $G_1=\{U_1,\cdots,U_n\}$이라 놓자. 그룹 매니저는 균등하게(uniformly) m개의 t-차 다항식 $s_1(x),\cdots,s_m(x)\in\mathbb{F}_p[x]$를 선택하고, 이와는 독립적으로 m개의 세션키 $K_1,\cdots,K_m\in\mathbb{F}_p$를 균등하게 뽑는다. $i=1,\cdots,n$에 대하여, 각 사용자 U_i는 자신의 개인키 $S_i=\{s_1(i),\cdots,s_m(i)\}$를 그룹 매니저로부터 안전한 통신 경로를 통해서 받는다.
2. 브로드캐스트(Broadcast): 임의의 $1\le j\le m$에 대하여, $W_j=\{r_1^j,r_2^j,\cdots,r_{w_j}^j\}$는 세션 j와 그 이전까지 취소된 사용자 ID들의 집합이고, $|W_j|=w_j\le t$라고 가정한다. 그리고 $r_j(x)=(x-r_1^j)\cdots(x-r_{w_j}^j)$로 놓는다. j번째 세션키 분배를 위해서 그룹 매니저는 다음과 같이 구성된 메시지 B_j를 브로드캐스트 한다.

   $j=1,2$일 때,

   $$B_j=P_j(x)\cup W_j,$$

   $3\le j\le m$일 때,

   $$B_j=\{P_1(x)+P_2(x),P_2(x)+P_3(x),\cdots,P_{j-2}(x)+P_{j-1}(x),P_j(x)\}\cup(\cup_{i=1}^{j}W_i),$$

   여기에서 $P_j(x)=r_j(x)K_j+s_j(x)$이다.
3. 세션키 계산: 멤버쉽이 취소되지 않은 사용자 U_i가 j번째 세션키 분배 메시지를 수신하였을 때, 먼저 $r_j(i)$를 계산하고, 이로부터 $K_j=(P_j(i)-s_j(i))/r_j(i)$를 계산함으로써 세션키를 얻을 수 있다.
4. 그룹 멤버의 추가: 그룹 매니저가 j' 세션부터 새로운 멤버를 추가하고자 할 때는 이전에 한번도 사용되지 않았던 ID인 $i'\in\mathbb{F}_p$을 새로운 멤버에게 배정하고, 현재 이후의 세션에 대한 개인키인 $\{s_k(i')\}_{k=j',\cdots,m}$을 안전한 통신 경로를 통해서 새로운 멤버에게 전달한다.

제안방식 1에서 묵시적으로 가정된 조건은 어떤 세션 j에서 멤버쉽이 취소된 사용자 U_i는 이후의 모든 세션에서 취소된 상태로 남아 있어야 한다는 것이다. 제안방식 1이 취소 능력과 자가 치료 기능을 가지고 있다는 사실을 우리는 다음 정리에서 보는 바와 같이 증명할 수 있다.

[정리 1] 제안방식 1은 t-취소 능력을 가진 자가 치료 가능 그룹키 분배 기법이다.

[증명] 제안방식 1이 정의 1의 모든 조건들을 만족한다는 사실을 밝히면 된다.

1. (a) 멤버 U_i에 의한 세션키 복구는 제안방식 1의 3단계에 나타나 있다.

   (b) 세션키들은 개인키들과는 독립적이고, 균등하게 선택되기 때문에 개인키들만으로는 세션키들에 대한 어떠한 정보도 얻지 못한다. 이제, 브로드캐스트만으로는 세션키에 대한 정보를 얻을 수 없음을 밝히도록 하자. 브로드캐스트 메시지 $B_1,\cdots,B_m$이 주어지면, $P_1(x),\cdots,P_m(x)$를 계산하는 것이 가능하다. 그러나 $\{s_j(x)\}_{i=1,\cdots,m}$은 모두 독립적이고 균등하게 선택되기 때문에 세션키들은 브로드캐스트 메시지만으로는 결정될 수 없다.
2. 세션 j에서 t명의 취소된 멤버들이 공모한 집합 R을 가정하고, $W_j=\{r_1^j,\cdots,r_t^j\}$라 놓자. 브로드캐스트 메시지로부터 세션키 K_j를 복구하기 위해서는 R 내부의 취소된 사용자들이 $i\notin W_j$인 i에 대해서 $s_j(i)$를 계산해야만 한다. 그러나 R 내부의 사용자들은 기껏해야 $s_j(x)$의 t개에 대한 값들만을 알 수 있을 뿐이다. t-차 다항식 $s_j(x)$는 $t+1$개의 계수를 갖기 때문에 $s_j(x)$의 t개에 대한 값들만으로는 보간법(interpolation)에 의한 $s_j(x)$의 결정이 불가능하다. 그러므로 K_j의 기밀성은 유지된다.

3. (a) $1 \le r < s \le m$이고, U_i가 r과 s 세션에서 정당한 멤버일 경우, $\{P_r(i), P_{r+1}(i), \cdots, P_s(i)\}$를 복구할 수 있다. 그러면 제안방식 1의 3단계에 의해서 U_i는 세션키 $K_r, \cdots, K_s$를 계산해낼 수 있다.
(b) 집합 $C \cup D$ 내부의 사용자들만으로는 기껏해야 $s_j(x)$의 t개에 대한 값들만을 알 수 있을 뿐이므로 임의의 $K_j (r \le j \le s)$의 기밀성은 유지됨을 알 수 있다. □

제안방식 1이 t-차 순방향 및 역방향 기밀성을 보장한다는 사실은 다음 정리에 의해서 알 수 있다.

[정리 2] 제안방식 1은 t-차 순방향 기밀성(t-wise forward secrecy) 및 t-차 역방향 기밀성(t-wise backward secrecy)을 보장한다.

[증명] 그룹 멤버 t명의 공모 집합 R이 있다고 가정하자. R 내의 모든 사용자들이 세션 j 이전에 취소되었다면, [정리 1]의 증명에 의해서 R 내부의 공모만으로는 t-차 다항식 $s_j(x)$의 기껏해야 t개 값만을 알 수 있다. 그리고 이후 세션의 브로드캐스트 메시지로부터는 모든 $r \in R$에 대해서 $r_j(r) = 0$만을 알 수 있을 뿐이다. 그러므로 공모자들에게는 세션키 $K_j = (P_j(x) - s_j(x)) / r_j(x)$가 여전히 랜덤하게 보일 뿐이다.

R 내의 모든 사용자들이 세션 j 이후에 가입되었다면, 제안방식 1의 4단계로부터 이들이 세션 j에 대한 개인키를 얻을 수 없음을 알 수 있다. 그러므로 R 내부 멤버들의 공모로는 $s_j(x)$에 대한 정보를 알 수 없어서 공모자들에게는 세션키 $K_j = (P_j(x) - s_j(x))/r_j(x)$가 여전히 랜덤한 형태로 남아있다. □

4.2 기존 방식들과의 효율성 비교

메모리 저장소(memory storage) 관점에서 제안방식 1은 각 그룹멤버들이 $(m-j+1)\log p$ 크기의 개인키 저장소를 요구한다. 이는 [11]의 보조정리 2에 의하면 최적(optimal)의 양이다. 세션 j에서의 브로드캐스트 메시지는 j개의 취소 집합 $\{W_i\}_{i=1,\cdots,j}$, 그리고 $j-1$개의 다항식들로 구성된다. $W_1 \subseteq W_2 \subseteq \cdots \subseteq W_m$이고 $|W_m| \le t$을 만족하므로 각 세션 j에서 취소된 멤버들을 관리하기 위해서 j개의 일차원 배열(array)을 이용할 수 있다. 다시 말해서 W_j를 나타내는 배열만으로 $\{W_i\}_{i=1,\cdots,j}$ 모두를 표현할 수 있다. 사용자 ID는 작은 크기의 유한체로 구성 가능하기 때문에 취소된 사용자 ID 목록을 브로드캐스트하는 통신 오버헤드는 여기에서 무시하기로 한다. 그러면, $j \ge 3$에 대해서 브로드캐스트 메시지의 크기는 $(t+1)(j-1)\log p$가 되고, 이 양은 가장 최근에 발표된 [13]에서의 크기 $(2tj+j)\log p$비트 보다 약 2배 정도 효율적인 것이다. 다음 <표 1>은 기존에 제안된 대표적 방식들과 본 논문의 제안방식 1에 요구되는 메모리 저장소와 통신 복잡도를 비교해 놓은 것이다.

<표 1> 효율성 비교

키 분배 방식	저장소	통신 복잡도
[11]의 방식 3	$(m-j+1)^2\log p$	$(mt^2+2mt+m+t)\log p$
[13]의 방식 2	$(m-j+1)\log p$	$(2tj+j)\log p$
[14]의 방식 3	$2(m-j+1)\log p$	$\{(m+j+1)t+(m+1)\}\log p$
제안방식 1	$(m-j+1)\log p$	$(tj+j-t-1)\log p$

실제로 80-비트의 그룹키를 사용한다고 가정할 때, $\log p$의 값이 80이므로 최대 세션 수 $m = 500$이라 하면, 각 멤버들에게 요구되는 최대 저장소는 본 제안방식 1의 경우 40K-비트 정도가 된다. 최대 세션 수 m이 각각 100, 300, 500인 경우에 최대 공모 수 t를 m의 10%로 가정하고 실제의 최대 통신 복잡도($j = m$인 경우)를 비교해 본 결과가 <표 2>에 나타나 있다. 이를 살펴보면 [13]과 [14]의 방식과 제안방식 1이 원래의 방식인 [11]의 방식 보다 월등히 효율적임을 수치적으로 확인할 수 있다. 또한, 제안방식 1이 최근의 [13]과 [14]에 제안된 방식에 비해서 약 2배 정도 개선된 결과임을 볼 수 있다. <표 2>에서도 $\log p = 80$으로 놓았다.

<표 2> 통신 복잡도의 수치적 비교

키 분배 방식	$m = 100$ $t = 10$	$m = 300$ $t = 30$	$m = 500$ $t = 50$
[11]의 방식 3	968,800	23,066,400	104,044,000
[13]의 방식 2	168,000	1,464,000	4,044,000
[14]의 방식 3	168,880	1,466,480	4,044,080
제안방식 1	80,000	741,520	2,035,920

5. 단일 브로드캐스트부터의 세션키 복구

제안방식 1에서는 사용자가 만일 첫 번째 브로드캐스트 메시지 B_1을 수신하지 못했다면, 그 이후에 B_j를 받았다고 할지라도 받지 못한 세션키 K_1을 복구할 수 없다. 이는 다른 대부분의 자가 치료 가능 그룹키 분배 기법도 마찬가지다. 그래서 Blundo 등[13]은 사용자가 정당한 멤버쉽을 소유한 기간 동안의 세션 내에서는 단일 브로드캐스트 메시지만으로 그 기간 동안의 모든 세션키를 복구할 수 있는 방식을 제안하였다. 여기에서는 [13]의 방식 3을 개선한 것으로 단일 브로드캐스트로 해당 세션키 복구가 가능한 프로토콜을 제안한다.

• 제안방식 2

1. 장치(Setup) : $G_1 = \{U_1, \cdots, U_n\}$이라 놓자. 그룹 매니저는 균등하게(uniformly) m개의 t-차 다항식 $s_1(x)$,

$\cdots$, $s_m(x) \in \mathbb{F}_p[x]$를 선택하고, 이와는 독립적으로 m개의 세션키 K_1, $\cdots$, $K_m \in \mathbb{F}_p$를 균등하게 뽑는다. $i=1, \cdots, n$에 대하여, 각 사용자 U_i는 자신의 개인키 $S_i = \{s_1(i), \cdots, s_m(i)\}$를 그룹 매니저로부터 안전한 통신 경로를 통해서 받는다.

2. 브로드캐스트(Broadcast) : 임의의 $1 \le j \le m$에 대하여, $W_j = \{r_1^j, r_2^j, \cdots, r_{w_j}^j\}$는 세션 j와 그 이전까지 취소된 사용자 ID들의 집합이고, $|W_j| = w_j \le t$라고 가정한다. 그리고 $r_j(x) = (x - r_1^j) \cdots (x - r_{w_j}^j)$로 놓는다. j번째 세션키 분배를 위해서 그룹 매니저는 다음과 같이 구성된 메시지 B_j를 브로드캐스트 한다.
   $1 \le j \le m$에 대하여,
   $B_j = \{P_1(x), P_2(x), \cdots, P_j(x)\} \cup (\cup_{i=1}^{j} W_i)$,
   여기에서 $P_j(x) = r_j(x)K_j + s_j(x)$이다.
3. 세션키 계산 : 멤버쉽이 취소되지 않은 사용자 U_i가 j번째 세션키 분배 메시지를 수신하였을 때, 먼저 $r_j(i)$를 계산하고, 이로부터 $K_j = (P_j(i) - s_j(i))/r_j(i)$를 계산함으로써 세션키를 얻을 수 있다.

제안방식 2에서 고려하는 세션키 복구 성질은 [정의 1]의 1.(a)와 3.(a)를 대체하는 다음과 같은 것이다.

$l \le j \le m$이고, 임의의 멤버 $U_i \in G_l$가 세션 j 이전에 취소되지 않는다면, 세션키 K_l은 B_j와 S_i에 의해서 결정된다. 즉, 다음을 만족한다.

$$H(K_l | B_j, S_i) = 0.$$

[정리 1]의 증명 과정과 매우 흡사한 방법에 의해서 제안방식 2도 안전하고 올바른 그룹 세션키 분배 방식임을 보일 수 있다. 특히, 임의의 브로드캐스트 B_j로부터 G_l에 속한 사용자 U_i는 $l \le j$인 경우 $K_l = (P_l(i) - s_l(i))/r_l(i)$를 계산함으로써 세션키 K_l을 얻을 수 있다. 제안방식 2에서 요구되는 브로드캐스트 크기는 $(t+1)j\log p$이고, 이 양은 유사한 방식인 [13]의 방식 3의 $(2tj+j)\log p$에 비해서 효율적인 것이다.

본 논문에서 제안한 방식은 유한한 세션 크기 m을 가정했다는 제한성을 갖는다. 그러나 제안방식 1과 2는 기존 결과들인 [11]과 [13]에 나타나 있는 수명 확장 방법을 그대로 적용하여 수명 연장이 가능하므로 이러한 제한성은 문제가 되지 않음을 밝혀둔다.

6. 결 론

자가 치료 기능을 가진 그룹키 분배 프로토콜은 그룹 멤버들이 패킷 손실을 경험하기 쉬운 환경에 적합한 새로운 세션키 분배 방식이다. 무선(wireless), 이동(mobile), 임시 네트워크(ad hoc network)의 사용이 증가하는 현재의 상황에서 보안 문제가 가장 중요한 요소가 되는 경우에 자가 치료 기능을 가진 그룹키 분배 프로토콜은 매우 유용한 도구가 될 것으로 보인다. 본 논문에서는 Blundo 등[13]의 자가 치료 가능 그룹키 분배 모델을 기반으로 하여 기존의 방식들에 비해서 저장 용량은 최적이고, 통신 오버헤드는 약 2배 정도 효율적인 프로토콜을 새롭게 제안하였다. 그리고 제안하는 방식의 안전성 증명을 하였으며, 기존 방식들과 효율성을 비교한 표도 제공하였다. 또한, 제안된 자가 치료 가능 그룹키 관리 방식을 기반으로 단일 브로드캐스트 메시지로부터 사용자가 정당한 멤버쉽을 소유하고 있는 동안의 모든 세션키를 복구할 수 있는 프로토콜을 제안하였다. 제안된 단일 브로드캐스트를 이용한 세션키 복구 방식 역시 기존 방식 보다 효율적임을 알 수 있었다.

참 고 문 헌

[1] D. McGrew and A. Sherman, Key Estabilishment in Large Dynamic Groups Using One-Way Function Trees, TIS Report No.0755, 1998.

[2] C. Wong, M. Gouda and S. Lam, Secure Group Communications Using Key Graphs, Proc. of the ACM SIGCOMM'98, pp.68~79, 1998.

[3] D. Wallner, E. Harder and R. Agee, Key Management for Multicast : Issues and Architectures, IETF Request For Comments, RFC 2627, June, 1999.

[4] D. Naor, M. Naor and J. Lotspiech, Revocation and Tracing Schemes for Stateless users, Advances in Cryptology-Crypto'01, LNCS 2139, pp.41~62, 2001.

[5] D. Halevy and A. Shamir, The LSD Broadcast Encryption Scheme, Advances in Cryptology-Crypto'02, LNCS 2442, pp.47~60, 2002.

[6] X. Li, Y. Yang, M. Gouda and S. Lam, Batch Rekeying for Secure Group Communications, Proc. of World Wide Web Conference 10 (WWW10), 2001.

[7] Y. Yang, X. Li, X. Zhang and S. Lam, Reliable group rekeying : Design and Performance Analysis, Proc. of ACM SIGCOMM 2001, pp.27~38, 2001.

[8] D. Naor and B. Pinkas, Efficient Trace and Revoke Schemes, Financial Cryptography 2000, LNCS 1962, pp.1~21, 2000.

[9] C. Wong and S. Lam, Keystone : A Group Key Management Service, International Conference on Telecommunications, ICT 2000, 2000.

[10] A. Perrig, D. Song and J. Tygar, ELK, a New Protocol for

Efficient Large-Group Key Distribution, Proc. of the IEEE Symposium on Security and Privacy, pp.247~262, 2001.

[11] J. Staddon, S. Miner, M. Franklin, D. Balfanz, M. Malkin, and D. Dean, Self-Healing Key Distribution with Revocation, Proc. of the IEEE Symposium on Security and Privacy, pp. 224~240, 2002.

[12] C. Blundo, P. D'Arco and M. Listo, A New Self-healing Key Distribution Scheme, Proceedings of the IEEE Symposium on Computers and Communications(ISCC 2003), pp.803~808, 2003.

[13] C. Blundo, P. D'Arco, A. Santis and M. Listo, Design of Self-healing Key Distribution Schemes, Design Codes and Cryptography, N.32, pp.15~44, 2004.

[14] D. Liu, P. Ning and Sun, Efficient Self-Healing Key Distribution with Revocation Capability, Proceedings of the 10-th ACM Conference on Computer and Communications Security, pp.231~240, 2003.

[15] 오명욱, 김성열, 배용근, 정일용, "효율적인 그룹키 분배 및 갱신을 위한 보안 프로토콜의 설계", 정보처리학회논문지C, Vol. 9C, No.3, 2002년 6월, pp.331~336.

[16] 한근희, "멀티캐스트 환경에서 효율적인 그룹키 관리를 위한 트리구조 및 알고리즘 개발", 정보처리학회논문지B, Vol. 9B, No.5, 2002년 10월, pp.587~598.

[17] 김현주, 남정현, 김승주, 원동호, "유료 방송 시스템에 적합한 ID 기반의 2 라운드 그룹키 동의 프로토콜", 한국정보보호학회 논문지, Vol.15, No.1, 2005년 2월, pp.41~55.

강 주 성

e-mail : jskang@kookmin.ac.kr

1989년 고려대학교 수학과(학사)

1991년 고려대학교 일반대학원 수학과(이학석사)

1996년 고려대학교 일반대학원 수학과(이학박사)

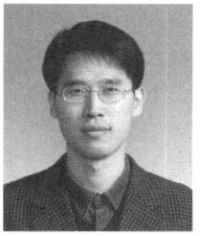
1996년~1997년 과학재단 박사후연구원

1997년~2004년 한국전자통신연구원 선임연구원, 팀장

2001년~2002년 벨기에 루벤대학 COSIC 방문연구원

2004년~현재 국민대학교 수학과 조교수

관심분야 : 암호 알고리즘, 정보보호 프로토콜, 응용확률론 등



홍 도 원

e-mail : dwhong@etri.re.kr

1994년 고려대학교 수학과(학사)

1996년 고려대학교 일반대학원 수학과(이학석사)

2000년 고려대학교 일반대학원 수학과(이학박사)

2000년~현재 한국전자통신연구원 선임연구원, 팀장

관심분야 : 암호 이론, 정보보호 이론, 이동통신 정보보호 등