논문 14-39B-09-01 The Journal of Korea Information and Communications Society '14-09 Vol.39B No.09
http://dx.doi.org/10.7840/kics.2014.39B.9.555

Shamir의 비밀 공유 방식의 그룹 키 전송 프로토콜

김 영 식◆

Group Key Transfer Protocol Based on Shamir's Secret Sharing

Young-Sik Kim◆

요 약

최근 그룹 내의 여러 멤버 사이에 하나의 그룹 세션키를 공유하는 연구가 활발히 진행되고 있다. 그 중에서 Harn과 Lin에 의해 Shamir의 비밀 공유 방식을 이용한 방식이 제안되었고, 이를 개선한 프로토콜이 Liu, Cheng, Cao, 그리고 Jiang에 의해서 다시 제안되었다. 특히 기존 방식들에서는 특정한 일부 비밀 정보를 알고 있는 그룹 멤버에 의해 다른 비밀 값이 알려지게 되는 '내부자 공격'에 대응하기 위해 유한한 원소를 갖는 유한 정수 환(finite integer ring)상에서 연산이 이루어지도록 프로토콜을 설계하였다. 이 논문에서는 기존 방식들이 기반을 둔 유한 정수 환 상의 그룹 세션키 분배 연산에서는 정당한 그룹 멤버들도 특정한 조건에서는 키 복구가 불가능한 상황이 발생하여 그룹 키 전송이 실패할 수 있음을 먼저 밝힐 것이다. 또한 이런 문제를 해결할 수 있는 새로운 프로토콜을 설계하여 제안한다.

Key Words : Secret sharing, Shamir's secret sharing, group session key, key agreement protocol

ABSTRACT

Recently, there are many researches on sharing group session key for members in a group. Among them, Harn and Lin proposed a scheme based on the Shamir's group session key and Liu, Cheng, Cao, and Jiang improved it to reduce the specific weakness. Especially, these schemes are based on the finite integer ring to protest the insider attack, in which a valid member can derived another member's secret using known information. In this paper, it is shown that the finite integer ring implies the failure of the reconstruction of group session key depending on the adopted parameters. We fix this problem and propose new group session key transfer scheme using the Shamir's secret sharing.

Ⅰ. 서 론

기밀성과 인증은 오늘날 암호 알고리즘을 통해서 제공이 가능한 가장 기본적인 보안 서비스로 많은 응용 분야에서 널리 활용되고 있다[1-3]. 안전한 보안 서비스 제공을 위해서, 사용되는 비밀키는 짧은 시간 동안만 사용되어야 하고 새로운 키로 수시로 업데이트 하는 것이 매우 중요하다. 이를 위해서는 새로운 세션키를 업데이트 할 수 있는 세션키 분배 프로토콜이 필요하다.

세션키를 분배하는 방식은 키 분배 센터(key distribution center)에서 생성한 후에 암호화하여 송신자와 수신자에게 전달하는 세션키 전송 방식과 특정한 값을 공개 채널로 교환함으로써 각 참가자가 동일한 키를 생성할 수 있는 키 교환(key agreement) 방식이 존재한다. 후자의 대표적인 프로토콜로 Diffie-Hellman

※ 이 논문은 2014년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(NRF-2014R1A2A2A01006870).
◆ First Author : Chosun University, Department of Information and Communication Engineering, iamyskim@chosun.ac.kr, 정회원
논문번호 : KICS2014-07-262, Received July 11, 2014; Revised August 13, 2014; Accepted September 1, 2014

방식이 가장 유명하지만 이 프로토콜은 두 개의 개체 사이에서의 키 교환만 가능한 단점을 가지고 있다[4].

최근에는 한 그룹 내의 멤버들에게 공통의 세션키를 분배하는 많은 연구들이 이루어졌다[5-10]. 그 중에서도 Harn과 Lin은 Shamir의 비밀 공유 방식을 기반으로 그룹 세션키를 분배하는 프로토콜을 제안하였다[11]. 그룹키 전송 프로토콜에 대한 공격은 크게 '외부자 공격'과 '내부자 공격'으로 구분 할 수 있다. 여기서 '외부자 공격'은 그룹에 속하지 않은 외부 공격자에 의해서 비밀 정보의 일부 또는 전체가 알려지게 되는 공격을 말하며, '내부자 공격'은 그룹 내부에 속하는 정당한 멤버가 허가된 정보 이외의 다른 멤버의 비밀 정보를 알게 되는 형태의 공격을 의미한다. 그러나 Harn-Lin이 제안한 방식에서는 원래 의도와 달리 내부자 공격을 완벽하게 차단하지 못하는 문제가 발견되어 Liu, Cheng, Cao, 그리고 Jiang은 이를 개선하는 방법을 새롭게 제안하였다[12].

이 두 가지 논문 모두 내부자 공격에 대한 대응을 위해서 유한한 원소를 갖는 유한 정수 환(finite integer ring)상에서 연산이 이루어지도록 설계하였다. 이 논문에서는 유한 정수 환(finite integer ring) 구조상에서 연산이 이루어질 경우 특정한 조건에서는 정당한 멤버가 키 복구를 할 수 없는 상황이 발생하는 문제가 있음을 보이고, 이 문제를 해결한 새로운 프로토콜을 설계하여 제안할 것이다.

Ⅱ. Shamir의 비밀 공유 방식

Shamir와 Blakley는 독립적으로 비밀 공유에 대한 개념을 처음으로 제안하였다[13]. 이 방식에서는 하나의 비밀 정보 K는 그림자(shadow)로 불리는 n개의 서로 다른 정보 조각으로 나누어진다. 이 때 미리 정해진 t개($t \le n$) 이상의 그림자를 갖고 있을 때에만 숨겨진 K를 복구할 수 있게 된다. 반면에 $t-1$개 이하의 그림자만을 가지고는 숨겨진 비밀 정보가 복구되지 않는다. 이것을 (t,n) 비밀 공유(secret sharing)이라 부른다.

이 중에서 Shamir가 제안한 비밀 정보 분배 방식에 대해서 살펴보도록 하자. 먼저 비밀 정보를 분배하는 신뢰성 있는 딜러(dealer)가 있다고 하자. 그러면 딜러는 먼저 차수가 $(t-1)$인 다항식을 랜덤하게 선택해서 다음과 같이 만든다.

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

이 때 상수 값을 숨기고자 하는 비밀 정보 $K = a_0 = f(0)$로 두고 모든 계수 a_0, a_1, $\cdots$, a_{t-1}은 소수 p개의 원소로 구성된 유한체(finite field) F_p상의 원소라 하자. 여기서 $f(x)$를 사용해서 n개의 그림자를 $s_i = f(i) \bmod p$를 통해 생성한다. (단, $0 \le i < n$) 그 후 딜러는 각 조각을 n명의 사용자 U_i에게 안전한 방식으로 분배한다.

비밀 정보를 다시 복구하기 위해서는 n개의 그림자 중에서 임의의 t개 이상의 그림자를 모아야 한다. 만일 임의의 t개의 조각을 $(s_{i_1}, s_{i_2}, \cdots, s_{i_t})$라 하면 다음과 같은 식을 통해서 비밀 정보를 다시 복구할 수 있다.

$$\begin{aligned} K = f(0) &= \sum_{i \in (i_1, i_2, \ldots, i_t)} s_i \beta_i \\ &= \sum_{i \in (i_1, \cdots, i_t)} s_i \left(\prod_{j \in (i_1, \cdots, i_t) - i} \frac{x_j}{x_j - x_i} \right) \bmod p \end{aligned} \quad (1)$$

여기서 β_i는 Lagrange 계수이다.

Ⅲ. Sharmir의 비밀 공유 기반의 그룹 세션키 분배 프로토콜

최근에 Shamir의 비밀 공유를 기반으로 한 그룹 키 전송 프로토콜에 대한 연구가 2010년에 Harn과 Lin에 의해서 제안되었고[11], 2013년에 Liu, Cheng, Cau와 Jiang에 의해서 개선되었다[12]. 먼저 전체 멤버가 t명이 있다고 가정하자. 이 때 그룹간 안전한 통신을 위해서 그룹 세션키 분배 프로토콜은 다음과 같은 조건을 만족해야 한다.

1) 분배된 키는 분배 후에 인증이 가능해야 함
2) 각 정보는 브로드캐스팅 방식으로 공개 채널을 통해서 분배
3) 허가 받은 각 멤버는 안전하게 그룹 세션키를 복원할 수 있어야 함
4) 인가되지 않은 공격자들은 세션 키를 복구할 수 없어야 함
5) 허가된 멤버가 가진 비밀 정보로 다른 멤버의 비밀 정보를 계산하는 것이 불가능해야 함

Harn-Lin 방식과 Liu-Cheng-Cau-Jiang의 방식에서는 전체 과정이 안전하게 동작하기 위해서 신뢰성을 갖춘 키 생성 센터(key generation center)의 도움이 필요하다고 가정하였다[11,12].

이 때 Harn-Lin 방식과 이를 개선한 Liu-

Cheng-Cau-Jiang 방식은 다음과 같이 거의 유사한 형태로 동작한다. 두 가지 방식이 유사하므로 이 논문에서는 Liu-Cheng-Cau-Jiang 방식을 기준으로 기존의 방식을 설명하고자 한다.

3.1 사전 분배 단계

먼저 p와 q가 암호학적으로 안전한 소수라 하자. 그러면 키 생성 센터(KGC)는 $N=pq$를 생성하여 공개한다. 또한 Z_N 상의 원소를 출력하는 두 개의 보안 해시 함수 $h_1(x)$와 $h_2(x)$를 생성하여 공개한다. 그리고 각 멤버 U_i는 KGC에 자신을 등록한다. 여기서 등록 과정에서 장기간 사용할 고유의 마스터키 (x_i, y_i)를 안전하게 KGC와 각 멤버 사이에 공유한다.

3.2 그룹 세션키 분배 프로토콜 단계

단계 1) 그룹 세션키 분배가 시작되기 위해서는 임의의 멤버가 KGC에게 멤버 목록 $(U_1, \cdots, U_t)$과 함께 키 분배 요청을 보낸다. 그러면 KGC는 키 분배 요청이 온 사실을 해당 멤버들에게 브로드캐스트한다.

단계 2) 키 분배 요청을 수신한 각 멤버 U_i는 Z_N 상에서 랜덤한 토큰 값 R_i를 생성하여 KGC로 전송한다.

단계 3) KGC는 그룹 세션키 값 K를 랜덤하게 생성한다. 그런 후 $(0, K)$ 점과 함께 멤버의 마스터키와 수신된 랜덤 토큰을 이용해서 t개의 점 $(x_i, y_i + h_1(x_i \| y_i \| R_i))$를 생성하고, 자신의 비밀정보를 포함한 $t+1$개의 점을 이용해서 $f(x)$를 생성한다. 이 때 Lagrange 보간 다항식 방식을 사용하여 다항식을 확보한다. 여기에서 모든 덧셈들은 Z_N 상에서 $\bmod N$으로 수행된다.

그리고 KGC는 추가로 t개의 점 $P_i = (i, f(i))$ (단, $1 \le i \le t$)와 인증 메시지 $Auth = h_2(K, U_1, \cdots U_t, R_1, \cdots, R_t, P_1, \cdots, P_t)$를 계산한다. 그리고 최종적으로 $Auth$값과 t개의 점 P_i $(1 \le i \le t)$를 모든 멤버에게 브로드캐스트한다.

단계 4) 각 멤버는 KGC와 비밀리에 공유한 마스터키 (x_i, y_i)를 이용해서 추가 비밀 포인트 $(x_i, y_i + h_1(x_i \| y_i \| R_i))$를 계산한다. 이 때 $h_1(\cdot)$와 R_i는 이미 모두 알고 있기 때문에 마스터키를 이용하면 추가 비밀 포인트는 쉽게 계산할 수 있다. 그런 후에 브로드캐스트된 t개의 포인트 P_i $(1 \le i \le t)$를 이용해서 비밀 정보 $K = f(0)$을 복구할 수 있다. 그런 후에 $Auth$를 사용해서 K값을 인증한다.

여기에서 Harn-Lin 방식을 Liu-Cheng-Cau-Jiang 방식과 비교할 때 유일한 차이점은 단계 3에서 $f(x)$를 생성할 때 $(x_i, y_i + h_1(x_i \| y_i \| R_i))$ 대신 $(x_i, y_i + R_i)$를 사용한다는 점뿐이다. 나머지는 두 가지 방식이 모두 동일한 절차를 따른다.

Ⅳ. 새로운 그룹 세션키 분배 프로토콜

이 장에서는 먼저 기존에 소개된 Harn-Lin 방식과 이를 개선한 Liu-Cheng-Cau-Jiang 방식에 모두 적용되는 문제점을 분석한다. 그리고 이를 해결할 수 있는 새로운 그룹 세션키 분배 프로토콜을 제안할 것이다.

4.1 기존 방식들의 문제점

Liu-Cheng-Cau-Jiang 방식과 그 이전의 Harn-Lin 방식은 내부자 공격에 대응하기 위해서 두 개의 소수 p와 q를 인수로 갖는 정수 N으로 구성된 정수 환 Z_N 상에서 성립하는 그룹 세션키 분배 방식을 설계하였다[12].

두 방식에서는 그룹 세션키 분배를 위해 Shamir의 비밀 공유 방식을 사용하였는데, 이 때 $f(x)$상에 존재하는 점은 $2t+1$개로 그 중에는 그룹 키 K, 각 사용자의 비밀키 $(x_i, y_i + h_1(x_i \| y_i \| R_i))$, 그리고 모두에게 공개되는 점 P_i가 포함된다. 여기서 $1 \le i \le t$이다. 다시 말해 Liu-Cheng-Cau-Jiang이 제안한 방식과 Harn-Lin이 제안한 방식은 모두 $2t+1$개의 그림자 중에서 $t+1$개의 그림자가 있어야 비밀 값을 계산할 수 있는 $(t+1, 2t+1)$ 비밀 공유 방식에 기반을 두고 있다고 말할 수 있다.

본래의 Shamir의 비밀 공유 방식에서는 각 사용자가 안전한 채널로 자신의 그림자를 딜러로부터 전달받지만 그룹 키 분배에서는 t개의 점 $P_i (1 \le i \le t)$는 딜러에 해당하는 키 생성 센터에 의해 그룹내 모든 멤버에게 공개 채널로 전송된다. 그러면 각 사용자는 자신만이 알고 있는 마스터키 (x_i, y_i)를 사용해서 추가되는 점 $(x_i, y_i + h_1(x_i \| y_i \| R_i))$를 생성하고 이 값은 t개의 전송받은 점 P_i와 함께 $t+1$개의 그림자를 구성하게 되어 (1) 식을 통해서 본래의 $f(x)$ 또는 비밀 값 K를 복구할 수 있게 된다.

그러나 문제는 Liu-Cheng-Cau-Jiang 방식과 그 이전의 Harn-Lin 방식이 모두 연산이 이루어지는 기본 집합이 유한체가 아닌 유한 정수 환(finite integer ring)인 Z_N상에서 수행된다는 데서 발생한다[8,9]. 다시

말해 $N=pq$이 합성수이기 때문에 Z_N상의 원소 중에는 곱의 역원이 존재하지 않는 점이 있다. 즉, p 또는 q의 배수인 점들은 모두 곱의 역원이 존재하지 않는다. 이 값은 총 pq개의 원소 중에서 $(p+q-1)$개에 해당되고 따라서 이런 값이 발생할 확률은 $(1/p+1/q-1/pq)$가 된다. 즉, 식 (1)에서 x_j-x_i의 역원이 p 또는 q의 배수가 되면 역원인 $1/(x_j-x_i)$가 존재하지 않게 되므로 (1)을 계산할 수가 없다. 식 (1)에서 서로 다른 x_j-x_i의 개수는 $1 \le i,j \le t$일 때 $t(t+1)/2$개 이므로 위의 연산에서 이런 문제가 발생할 확률은 다음과 같이 주어진다.

$$P_e = t(t+1)\left(\frac{1}{2p}+\frac{1}{2q}-\frac{1}{2pq}\right) \quad (2)$$

다시 말해 P_e의 확률로 정당한 사용자 U_i $(1 \le i \le t)$도 분배된 그룹 세션키 K를 계산을 통해 복구할 수가 없다. 이는 그룹 세션키 분배의 기본 요건을 충족하지 못한 것이 된다. 다음 예제에서는 실제 구체적인 숫자를 통해 문제가 생길 확률 P_e 값을 계산을 통해 보여준다.

예제 1. 그룹내 멤버 수가 $t=3$이고 $p=811$, $q=821$이라 하자. 그러면 $N=665{,}831$이 되고, 역원을 구하지 못할 확률은 식 (2)에 의해

$$P_e = 3\times 4\times \frac{(811+821-1)}{665831} = 0.0294$$

가 된다. 이 경우 100번 시도 중 3번 정도는 그룹 세션키 전송에 실패하게 된다. □

4.2 새로운 그룹 세션키 분배 방식

4.1절에서 논의한 문제점을 방지하기 위해서는 기존의 Liu-Cheng-Cau-Jiang 방식에 새로운 조건이 추가되어야 한다. 새로운 제안을 다음과 같이 나타낼 수 있다.

4.2.1 사전 분배 단계

먼저 p와 q가 암호학적으로 안전한 소수라 하자. 그러면 키 생성 센터(KGC)는 $N=pq$를 생성하여 공개한다. 또한 Z_N 상의 원소를 출력하는 두 개의 보안 해시 함수 $h_1(x)$와 $h_2(x)$를 생성하여 공개한다. 그리고 각 멤버 U_i는 KGC에 자신을 등록한다. 키 생성 센터는 등록과정에서 각 멤버들에게 장기간 사용할 수 있는 고유의 마스터키 (x_i,y_i)를 생성하여 분배하는데 다음과 같은 방식으로 생성한다.

단계 1) $i=1$일 때 x_1과 y_1를 랜덤하게 생성한다.

단계 2) $1<i\le t$일 때 x_i와 y_i를 랜덤하게 생성한다.

단계 3) $x_j(1 \le j < i)$에 대해서 $\gcd(x_j-x_i,N)$를 계산하여 이 값이 모두 1인지 검사한다. 만일 어느 하나라도 $\gcd(x_j-x_i,N)\ne 1$이라면 단계 2)로 돌아가서 x_i를 다시 생성한다.

위의 연산에서 gcd연산은 확장된 유클리드 호제법(extended Euclidean algorithm)을 통해 계산될 수 있고 계산 복잡도는 대략 $O((\log N)^2)$이 된다. gcd연산의 총 수행 회수는 $(t-1)!$번이다.

위와 같은 절차를 통해서 생성된 마스터키 (x_i,y_i) $(1 \le i \le t)$는 모든 가능한 x_j-x_i 값이 p또는 q의 배수가 되지 않도록 보장할 수 있고, 따라서 곱의 역원이 존재하는 경우를 완전히 없앨 수 있다. 그리고 그룹 세션키 분배 단계는 기존의 Liu-Cheng-Cau-Jiang 방식과 마찬가지로 다음과 같이 이루어진다.

4.2.2 그룹 세션키 분배 단계

그룹 세션키 분배 프로토콜은 다음과 같이 4단계로 구성된다.

단계 1) 그룹 세션키 분배가 시작되기 위해 임의의 멤버가 KGC에게 멤버 목록 $(U_1,\cdots,U_t)$과 함께 키 분배 요청을 보낸다. 그러면 KGC는 키 분배 요청이 온 사실을 해당 멤버들에게 브로드캐스트한다.

단계 2) 키 분배 요청을 수신한 각 멤버 U_i는 Z_N 상에서 랜덤한 토큰 값 R_i를 생성하여 KGC로 전송한다.

단계 3) KGC는 그룹 세션키 값 K를 랜덤하게 생성한다. 그런 후 $(0,K)$ 점과 함께 멤버의 마스터키와 수신된 랜덤 토큰을 이용해서 t개의 점 $(x_i,y_i+h_1(x_i\|y_i\|R_i))$를 생성하고, $t+1$개의 점을 이용해서 $f(x)$를 생성한다. 이 때 Lagrange 보간 다항식 방식을 사용하여 다항식을 확보한다. 여기에서 모든 덧셈들은 Z_N 상에서 $\bmod N$으로 수행된다.

그리고 KGC는 추가로 t개의 점 $P_i=(i,f(i))$ (단, $1 \le i \le t$)와 인증 메시지 $Auth=h_2(K,U_1,\cdots,U_t,R_1,\cdots,R_t,P_1,\cdots,P_t)$를 계산한다. 그리고 최종적으로 $Auth$값과 t개의 점 P_i $(1 \le i \le t)$를 모든 멤버에게 브로드캐스트한다.

단계 4) 각 멤버는 KGC와 비밀리에 공유한 마스

터키 (x_i, y_i)를 이용해서 추가 비밀 포인트 $(x_i, y_i + h_1(x_i \| y_i \| R_i))$를 계산한다. 이 때 $h_1(\cdot)$와 R_i는 이미 모두 알고 있기 때문에 마스터키를 이용하면 추가 비밀 포인트는 쉽게 계산할 수 있다. 그런 후에 브로드캐스트된 t개의 포인트 P_i $(1 \le i \le t)$를 이용해서 비밀 정보 $K = f(0)$을 복구할 수 있다. 그런 후에 $Auth$를 사용해서 K값을 인증한다.

본 논문에서 제안하는 그룹 세션키 분배 프로토콜에 대한 예시를 그림 1에 도시하였다. 그림 1에서는 그룹 멤버가 A, B, C, D 4명인 경우의 프로토콜의 동작 과정을 보여주고 있다. 키 생성 센터(KGC)는 그룹 멤버에게 마스터키를 사전에 분배하고 이후 멤버의 요청에 의해 모든 멤버들에게 프로토콜에 따라 세션키를 구성하는 t개의 점들을 브로드캐스트하며, 멤버들은 마스터키와 전달된 t개의 점들을 이용해서 세션키를 복구하게 된다.

본 논문에서 제안한 방식과 기존의 Liu-Cheng-Cao-Jiang이 제안한 방식[12]의 특징을 표 1에서 요약하여 보여주고 있다. 표 1에서 나타난 것처럼 새로운 방식에서는 대부분의 연산 특성은 Liu-Cheng-Cau-Jiang과 거의 유사하지만, 사전연산 단계에서 gcd 연산을 $(t-1)!$번 추가함으로써, 그룹키를 복원하는 과정에서 연산 오류가 일어날 확률을 0으로 만들 수 있었다.

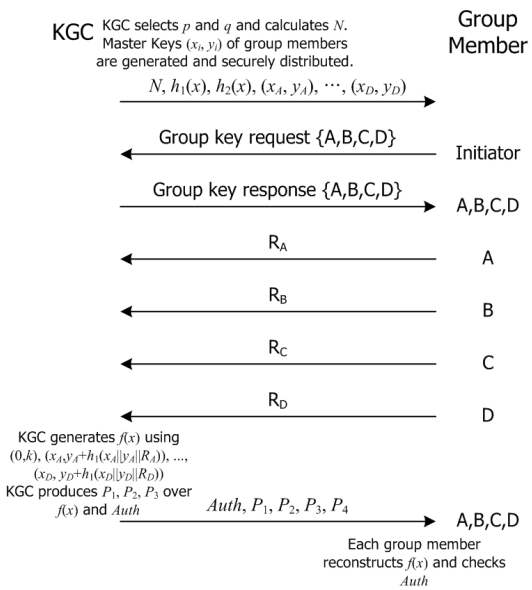

그림 1. 새로운 그룹 세션키 분배 프로토콜
Fig. 1. New group session key distribution protocol

표 1. 기존 방식[12]과 새로운 방식의 특성 비교
Table 1. Comparison of the previous scheme[12] and the proposed scheme.

Property	Previous Scheme[12]	Proposed Scheme
Number of Users	t	t
Number of Hash Functions	$3t+1$	$3t+1$
Number of GDC Operations	0	$(t-1)!$
Failure Probability of Group Key Sharing	P_e	0

V. 결 론

이 논문에서는 최근에 제안된 Liu-Cheng-Cau-Jiang의 그룹 세션키 전송 방식과 그 이전에 제안된 Harn-Lin의 그룹 세션키 전송 방식은 랜덤하게 생성된 파라미터에 따라 세션키 분배가 불가능할 수 있다는 점을 밝혔고, 이 문제를 해결한 새로운 그룹 세션키 전송 방식을 제안하였다. 향후에는 특정 그룹이 세션키를 공유하는데 필요한 데이터 교환을 최적화하는 방식에 대한 연구를 진행할 예정이다.

References

[1] H.-J. Seo and H.-W. Kim, “User authentication method on VANET environment,” *J. KICS*, vol. 37C, no. 7, pp. 576-583, Jul. 2012.

[2] Y.-S. Kim, “An efficient multi-signature scheme for shared data in a cloud storage,” *J. KICS*, vol. 38A, no. 11, pp. 967-969, Nov. 2013.

[3] S.-G. Min, Y.-H. Park, Y.-H. Park, and S.-J. Moon, “Secure routing protocol in cluster-based ad hoc networks,” *J. KICS*, vol. 37C, no. 12, pp. 1256-1262, Dec. 2012.

[4] E. Bresson, O. Chevassut, D. Pointcheval, and J.-J. Quisquater, “Provably authenticated group diffie-hellman key exchange,” in *Proc. ACM Conf. Comput. Commun. Security (CCS ’01)*, pp. 255-264, 2001.

[5] E. Bresson, O. Chevassut, and D. Pointcheval, “Provably-secure authenticated group diffie-hellman key exchange,” *ACM Trans. Inf. Syst. Security(TISSEC)*, vol. 10, no. 3, pp. 255-264,

Jul. 2007.

[6] J. M. Bohli, "A framework for robust group key agreement," in *Proc. Int. Conf. Comput. Sci. Appl. (ICCSA '06)*, pp. 355-364, 2006.

[7] M. Burmester and Y. Desmedt, "A secure and efficient conference key distribution system," in *Proc. Eurocrypt*, vol. 950, pp. 275-286, Italy, May 1994.

[8] B. Gopalakrishnan and A. Shanmugam, "An authenticated transitive-closure scheme for secure group communication in MANETS," in *Proc. Mining Intell. Knowledge Exploration*, vol. 8284 of LNCS, pp 362-369, Tamil Nadu, India, Dec. 2013.

[9] J. C. Cheng and C. S. Laih, "Conference key agreement protocol with non interactive fault-tolerance over broadcast network," *Int. J. Inf. Security*, vol. 8, no. 1, pp. 37-48, 2009.

[10] J. Wu, Q. Liu, and X. Liao, "A secure and efficient outsourceable group key transfer protocol in cloud computing," in *Proc. SCC'14*, pp. 43-50, Kyoto, Japan, Jun. 2014.

[11] L. Harn and C. Lin, "Authenticated group key transfer protocol based on secret sharing," *IEEE. Trans. Computers*, vol. 59, no. 6, pp. 842-846, Jun. 2010.

[12] Y. Liu, C. Cheng, J. Cao, and T. Jiang, "An improved authenticated group key transfer protocol based on secret sharing," *IEEE Trans. Computers*, vol. 62, no. 11, pp. 2335-2336, Nov. 2013.

[13] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612-613, 1979.

김 영 식 (Young-Sik Kim)

2001년 2월 : 서울대학교 전기공학부 졸업

2003년 2월 : 서울대학교 전기컴퓨터공학부 석사

2007년 2월 : 서울대학교 전기컴퓨터공학부 박사

2007년 3월~2010년 8월 : 삼성전자 책임연구원

2010년 9월~현재 : 조선대학교 정보통신공학과 조교수

<관심분야> 암호학, 정보보안, 정보이론, 오류정정부호, 하드웨어 보안