情報保護學會論文誌
第18卷 第3號, 2008. 6

세션상태 정보 노출 공격에 안전한 개선된 그룹 키 교환 프로토콜*

김 기 탁[1†], 권 정 옥[1], 홍 도 원[2], 이 동 훈[1‡]

[1]고려대학교 정보경영공학전문대학원, [2]한국전자통신연구원

Improved Group Key Exchange Scheme Secure Against Session-State Reveal Attacks*

Ki Tak Kim[1†], Jeong Ok Kwon[1], Dowon Hong[2], Dong Hoon Lee[1‡]

[1]Graduate School of Information Management and Security CIST, Korea University

[2]ETRI (Electronics and Telecommunications Research Institute)

요 약

세션상태 정보(session-state information)가 안전하지 않은 메모리에 저장되거나 또는 랜덤 난수 생성기 (random number generator)가 공격자에 의해 제어된다면 특정 세션에만 사용되는 난수 값과 같은 임시적인 데이터(ephemeral data)는 쉽게 노출될 수 있다. 본 논문에서는 Bresson과 그 외의 그룹 키 교환 스킴을 개선한 Nam과 그 외의 그룹 키 교환 스킴이 세션상태 정보노출 공격에 안전하지 않음을 보인다. 그리고 이러한 안전성의 결함을 보완한 개선된 스킴을 제안한다.

ABSTRACT

Ephemeral data are easily revealed if state specific information is stored in insecure memory or a random number generator is corrupted. In this letter, we show that Nam et al.'s group key agreement scheme, which is an improvement of Bresson et al.'s scheme, is not secure against session-state reveal attacks. We then propose an improvement to fix the security flaw.

Keywords : Group key agreement, session-state reveal attack, implicit key authentication, forward secrecy, known key security.

Ⅰ. 서 론

무선 네트워크 환경에서는 메시지의 도청, 삭제, 지연, 삽입, 재사용, 그리고 변경이 가능하기 때문에 이러한 안전하지 않은 무선 환경에서 안전한 통신을 위해서는 통신 개체들 간에 안전한 채널(secure channel)을 형성하는 것이 매우 중요하다. 이를 위한 한 가지 방안으로 WEP(Wired Equivalent Privacy) 프로토콜이 제안되었다. WEP는 IEEE 802.11 표준으로써, 모바일 기기

접수일 : 2007년 11월 21일; 채택일 : 2008년 03월 12일
* 본 연구는 정보통신부 및 정보통신연구진흥원의 IT신성장 동력핵심기술개발사업의 일환으로 수행하였음. [2005-Y001-04, 차세대 시큐리티 기술 개발], 이 연구에 참여한 연구자 중 일부는 '2단계 BK21사업'의 지원비를 받았음.
† 주저자, kitak@korea.ac.kr
‡ 교신저자, donghlee@korea.ac.kr

와 AP(access point) 즉, 게이트웨이 간에 트래픽을 사전에 공유한 세션키(session key)를 이용해서 어떻게 보호할 것인지에 대한 방법을 명기하고 있다. Bresson과 그 외는 저전력 모바일 기기들과 이에 상대적으로 컴퓨팅 능력이 좋은 게이트웨이가 존재하는 불균형적인 무선 네트워크 환경에서 WEP의 세션키 교환 프로토콜로 사용 가능한 효율적인 그룹키(세션키) 교환 스킴을 제안하였다[1]. Bresson과 그 외의 제안 프로토콜은 특정 그룹 내의 모바일 기기들과 게이트웨이가 공통된 그룹 키를 교환하기 위한 프로토콜로써 계산 부담을 게이트웨이에게 지움으로써 모바일 기기의 계산량을 낮추는 목적으로 제안되었다. 이 스킴은 랜덤 오라클 모델(random oracle model)에서 안전성이 증명되었다[1]. 이 프로토콜은 그룹의 구성원이 유동적인 경우를 고려한 스킴으로써, Setup, Remove와 Join의 세 가지 프로토콜로 구성되어 있다. 스킴의 중심이 되는 프로토콜인 Setup 프로토콜은 모바일 기기들로 구성된 그룹과 무선 게이트웨이가 그룹 키를 공유할 수 있도록 해 준다. Remove 프로토콜은 그룹의 일원으로 그룹 키를 맺었던 모바일 기기가 그룹을 효율적으로 탈퇴할 수 있도록 해 주고, Join 프로토콜은 새로운 모바일 기기가 그룹에 효율적으로 가입할 수 있도록 해 준다.

Nam과 그 외는 Bresson과 그 외의 Setup 프로토콜이 묵시적인 키 인증(implicit key authentication)과 전방향 안전성(forward secrecy), 그리고 기지 키 안전성(known key security)을 제공하지 못함을 보였다[7]. 또한 이러한 안전성의 결함을 보완하기 위해 Setup 프로토콜을 수정하였다.

서버의 개입이 필요하면서 구성원이 유동적인 경우를 고려한 스킴으로는 Bresson과 그 외의 프로토콜[1] 이외에 Lee와 그 외의 프로토콜[6]이 있다. [6]에서 제안된 프로토콜은 랜덤 오라클 모델(random oracle model)을 사용하지 않는 표준 모델(standard model)에서 전방향 안전성과 기지 키 안전성이 증명되었다.

세션상태 정보 노출(session-state revel) 공격은 특정 세션에만 사용되는 세션상태 정보에 접근할 수 있는 공격자를 모델링(modeling) 한다. 세션상태 정보는 보통 아직 완료되지 않은 세션에서 임시적으로 사용되는 난수와 같은 정보를 의미한다. 이러한 공격 시나리오는 특정 세션에서 사용되는 난수에 대한 정보가 롱-텀 (long-term) 비밀 키 보다 쉽게 노출될 수 있다는 사실에서 기인한다. 세션상태 정보 노출에 대한 안전성은 [2,5,3,4]에서 고려되었다. 만약 세션 키를 생성하는데 사용되는 임시적인 난수 값(ephemeral random number)이 노출된 경우에도 키 교환 프로토콜의 세션 키에 대한 기밀성(key secrecy)이 유지된다면, 그 키 교환 프로토콜은 세션상태 정보 노출 공격에 대한 안전성을 제공한다.

본 논문에서 Nam과 그 외의 개선된 키 교환 스킴[7]이 여러 가지 공격에 대하여 안전하더라도 세션상태 정보 노출 공격에는 안전하지 않음을 보인다. 그리고 Nam과 그 외의 개선된 스킴을 세션상태 정보 노출 공격에 안전하도록 제안한다.

Ⅱ. Nam과 그 외의 개선 스킴

Nam과 그 외는 Bresson과 그 외의 Setup 프로토콜이 묵시적인 키 인증, 전방향 안전성과 기지 키 안전성을 제공하지 못함을 인터리빙(interleaving) 공격을 통해 보였다[7]. 공격 시나리오에서 공격자는 이전에 종료된 세션에서 얻은 메시지(transcript)를 이용하여 묵시적인 키 인증과 전방향 안전성, 그리고 기지 키 안전성에 대한 공격을 수행한다. 실제로 Bresson과 그 외는 안전성 증명에서 여러 개체들의 인스턴스(instence)들이 공격자에 의해 동시에 수행될 수 있는 공격 환경을 고려하지 않았다.

다음에서 Bresson과 그 외의 Setup 프로토콜인 GKE.setup 프로토콜에 대한 Nam과 그 외가 개선한 스킴에 대하여 간략하게 설명한다.

ℓ은 안전성 파라미터 (security parameter)이고, $G=\langle g\rangle$는 ℓ-비트 소수인 q를 위수로 갖는 유한 순환 그룹이다. 세 가지 해쉬 함수인 H: $\{0,1\}^*\rightarrow\{0,1\}^{l}$, H_0: $\{0,1\}^*\rightarrow\{0,1\}^{l_0}$와 H_1: $\{0,1\}^{l_1}\times\mathbb{G}\rightarrow\{0,1\}^{l_0}$가 사용된다. 여기서 ℓ_1은 스킴에서 사용되는 카운터 c의 최대 비트 길이다. 그리고 안전한 서명 스킴인 $SIGN=(SIGN.KGen, SIGN.Sig, SIGN.Ver)$이 사용된다. $SIGN.KGen$은 키 생성 알고리즘(algorithm)이고, $SIGN.Sig$는 서명 생성 알고리즘, $SIGN.Ver$은 서명 검증 알고리즘이다.

초기 단계. C는 모바일 기기 또는 클라이언트(client)의 그룹이고, S는 서버(게이트웨이)를 나타낸다. 각 클라이언트 U_i와 서버 S는 자신의 롱-텀 키를 다음과 같이 생성한다.

(1) 각 클라이언트 $U_i\in C$는 $SIGN.KGen$을 사용하여 서명용 개인키/공개키 쌍 (SK_i, PK_i)를 생성한다.

(2) 서버 S는 임의의 난수 $x \in Z_q^*$를 선택하고, 자신의 개인키/공개키 쌍을 $(SK_S, PK_S)=(x, y)$로 설정한다. 이 때, $y=g^x$이다.

이 단계에서 서버 S와 C에 속하는 모든 클라이언트들은 자신의 카운터 c를 0으로 초기화 한다.

GKE.setup 프로토콜. $G_C \subseteq C$를 서버 S와 세션 키를 공유하고자 하는 클라이언트의 집합이라고 하자. I_C는 G_C에 속하는 클라이언트들의 ID 집합이라고 하자. 프로토콜은 다음과 같은 과정을 수행한다.

(1) 각 클라이언트 $U_i \in G_C$는 임의의 난수 $x_i \in Z_q^*$를 선택하고, $y_i = g^{x_i}$와 $\alpha_i = y^{x_i}$를 계산한다. 클라이언트 U_i는 *SIGN.Sig*를 사용하여 개인키 SK_i로 y_i의 서명 σ_i를 생성하고 (y_i, σ_i)를 서버 S에게 전송한다.

(2) 서버 S는 모든 $i \in I_C$에 대하여 *SIGN.Ver*을 사용하여 공개키 PK_i로 서명 σ_i를 검증한다. 만약 모든 서명이 올바르다면 S는 모든 $i \in I_C$의 $\alpha_i = y_i^x$를 계산한다. 서버 S는 프로토콜의 각 새로운 세션마다 카운터 c을 모노톤(monotone)하게 증가시키고 공유 비밀 값을 다음과 같이 계산한다.

$$K = H_0\left(c \| \{\alpha_i\}_{i \in I_C}\right).$$

그리고 서버 S는 모든 $i \in I_C$에 대하여 다음을 계산한다.

$$K_i = K \oplus H_1(c \| \alpha_i \| G_C \| S).$$

마지막으로 서버 S는 (c, K_i)를 각 클라이언트 U_i에게 전송한다.

(3) 각 클라이언트 $U_i \in G_C$는 (c, K_i)를 받고 난 뒤 새롭게 받은 카운터가 자신이 가지고 있던 카운터보다 큰 값인지 확인한다. 만약 새로운 카운터가 이전 카운터보다 크지 않다면 각 클라이언트 U_i는 프로토콜을 종료한다. 그렇지 않으면, 각 클라이언트 U_i는 다음과 같이 비밀 공유 값 K를 복원한다.

$$K = K_i \oplus H_1(c \| \alpha_i \| G_C \| S).$$

서버와 클라이언트는 다음과 같이 동일한 세션 키를 계산한다.

$$sk = H(K \| G_C \| S)$$

마지막으로 각 클라이언트 $U_i \in G_C$는 카운터를 전송받은 카운터로 갱신한다.

Ⅲ. Nam과 그 외의 개선 스킴의 세션상태 정보 노출 공격에 대한 안전성

본 장에서는 Nam과 그 외의 개선 스킴이 세션상태 정보 노출 공격에 대한 안전성을 제공하지 않음을 보인다.

A를 세션상태 정보인 임시적으로 사용하는 난수 값에 접근할 수 있는 공격자라고 하자. 자세한 공격 시나리오는 다음과 같다.

(1) A는 공격할 대상인 클라이언트의 ID, $j \in I_C$와 세션 t를 임의로 선택한다.

(2) A는 세션 t에서 클라이언트 U_j가 $\alpha_j = y^{x_j}$를 계산하기 위하여 사용한 난수인 x_j를 얻는다.

(3) GKE.setup 프로토콜에서 A는 서버 S로부터 클라이언트 U_j로 전송되는 메시지 (c, K_j)를 도청한다. 이 때, $K_j = K \oplus H_1(c \| \alpha_j \| G_C \| S)$이다.

(4) A는 난수 값 x_j을 이용하여 y^{x_j}를 계산하고, $h = H_1\left(c \| y^{x_j} \| G_C \| S\right)$을 계산한다.

(5) A는 공유 비밀 값 $K = K_j \oplus h$을 계산하고, 세션 t에 대한 세션 키 $sk = H(K \| G_C \| S)$를 계산한다.

위와 같이 일단 클라이언트의 특정 세션에 대한 임시적인 난수 값이 노출되면 이 난수 값을 가지고 있는 공격자는 공격 대상 세션에 대한 세션 키를 항상 계산할 수 있다. 따라서 Nam과 그 외의 개선 스킴은 세션상태 정보 노출공격에 안전하지 않다.

Ⅳ. 개선 스킴

본 장에서는 Nam과 그 외의 그룹 키 교환 스킴을 세션상태 노출 공격에 안전하도록 개선한다. 본래의 GKE.setup 프로토콜에서 세션 키 값은 각 클라이언트들의 임시적인 난수 값 x_i만으로 계산된다. 그러므로 이 프로토콜은 세션상태 정보 노출 공격으로부터 안전할 수 없다. 이러한 취약점을 고려해서, 세션상태 정보 노출 공격에 안전한 프로토콜을 설계하기 위해서 본 논문에서는 세션 키를 생성하는 과정에서 각 참여자의 롱

-텀 개인키를 적절하게 사용할 것이다. 즉, 개선 스킴에서 세션 키는 임시적인 디피-헬만(ephemeral Diffie-Hellman) 키 값과 고정적인 디피-헬만(static Diffie-Hellman) 키 값으로부터 계산된다. 임시적인 디피-헬만 키 값은 각 클라이언트의 임시적인 난수 값과 서버의 롱-텀 비밀키로부터 계산되고, 고정적인 디피-헬만 키 값은 각 클라이언트와 서버의 롱-텀 개인키 값들로부터 계산된다. 본 장에서는 제안하는 개선 스킴과 Nam과 그 외의 스킴의 차이점만 기술한다.

초기화 단계. 각 클리이언트 U_i는 두 개의 개인키/공개키 쌍을 다음과 같이 생성한다 : U_i는 본래의 프로토콜과 동일하게 자신의 서명용 개인키/공개키 쌍을 (SK_i, PK_i)로 설정한다. U_i는 보조적인(auxiliary) 개인키인 $u_i \in Z_q^*$를 랜덤하게 선택하고, 자신의 롱-텀 개인키/공개키 쌍을 (u_i, v_i)로 설정한다. 이 때, $v_i = g^{u_i}$이다.

GKE.setup 프로토콜.

(1) 서버 S는 모든 $i \in I_C$에 대하여 서명 σ_i의 모든 검증이 완료된 후, $\beta_i = v_i^x$를 계산한다. 그리고 공유 비밀 값을 다음과 같이 계산한다.

$$K = H_0\left(d \| \{\alpha_i\}_{i \in I_C} \| \{\beta_i\}_{i \in I_C}\right).$$

서버 S는 모든 $i \in I_C$에 대해 다음을 계산한다.

$$K_i = K \oplus H_1(d \| \alpha_i \| \beta_i \| G_C \| S).$$

(2) 클라이언트 U_i는 서버로부터 (c, K_i)를 전송 받은 뒤, 다음과 같이 공유 비밀 값을 복원한다.

$$K = K_i \oplus H_1(d \| \alpha_i \| \beta_i \| G_C \| S).$$

(3) 각 클라이언트 U_i는 세션 키를 다음과 같이 계산한다.

$$sk = H(K \| G_C \| S).$$

세션상태 정보 노출 공격에 대한 안전성. 본 논문에서 제안하는 프로토콜의 세션상태 정보 노출 공격에 대한 안전성은 공격자 A가 임의의 난수로부터 세션 키를 구분하는 확률로 측정된다. 이에 대한 A의 어드벤티지를 $Adv^{ake-ssr}(A) = 2\Pr[CG] - 1$라 놓는다. 여기서 $\Pr[CG]$는 주어진 값이 난수인지 실제 세션 키인지 A가 정확히 맞추는 확률이다. 제안 프로토콜의 안전성은 계산적인 디피-헬만 가정(CDH : computational Diffie- Hellman assumption)에 기반한다. CDH 문제는 그룹 G, 생성자 g, 그리고 G의 두 원소 g^a와 g^b가 주어졌을 때, g^{ab}를 계산하는 문제이다. 여기서 a와 b는 알려지지 않은 값이다. 만약 다음의 부등식을 만족한다면, 실행 시간이 t인 알고리즘 A는 ϵ의 어드벤티지(advantage) $Adv_G^{cdh}(t)$로 CDH 문제를 푼다고 한다.

$$\left|\Pr\left[a, b \leftarrow Z_q : A(g, g^a, g^b) = g^{ab}\right]\right| \geq \epsilon.$$

만약 무시할 수 없는(non-negligible) 어드벤티지로 CDH 문제를 풀 수 있는 확률적인 다항 함수 시간 알고리즘 A가 존재하지 않는다면 그룹 G에서 CDH 가정을 만족한다고 한다. $Adv_G^{cdh}(t)$는 그룹 G에서 CDH 공격자의 성공 확률을 나타낸다.

정리. A를 개선 프로토콜 P의 세션상태 정보 노출 공격에 대한 안전성을 깨는 공격자라 놓자. 여기서 A는 최대 N_s개의 세션을 만들고, 해쉬 오라클인 H_0와 H_1에 각각 최대 q_{H_0}와 q_{H_1}개의 쿼리를 요청한다. $q_H = q_{H_0} + q_{H_1}$으로 놓고, N을 전체 클라이언트들의 수로 놓자. 그러면 A의 어드벤티지는 다음과 같다.

$$Adv_P^{ake-ssr}(A) = 2q_H(N+1)N_s \cdot Adv_G^{cdh}(t).$$

증명. 공격자 A가 세션상태 정보 노출 공격에 대한 안전성을 무시할 수 없는 확률로 깬다고 가정하자. A는 아직 완료되지 않은 세션에서 모든 $i \in I_C$에 대한 난수 값 x_i를 얻는다고 가정하자. 그러면 A는 x_i를 사용해서 모든 클라이언트들의 $\alpha_i = g^{x_i x}$를 쉽게 계산할 수 있다. 세션 키에 대한 정보를 얻기 위해서 A는 $K = H_0\left(d \| \{\alpha_i\}_{i \in I_C} \| \{\beta_i\}_{i \in I_C}\right)$ 또는 $K_i = K \oplus H_1(d \| \alpha_i \| \beta_i \| G_C \| S)$에 대한 정보를 알아내려고 시도할 것이다.

다음에서 A를 하위 루틴으로 이용해서 CDH 문제를 무시할 수 없는 확률로 푸는 알고리즘 F를 만들 수 있음을 보인다. F에게 CDH 문제의 인스턴스 (instance)로 $(g, A = g^a, B = g^b)$가 주어졌다고 가정하자. 그러면 F는 CDH의 해를 구하기 위해서 주어진 인스턴스를 프로토콜 P에 다음과 같이 심는다 : 먼저 F는 $[1, ..., N_s]$에서 공격 대상인 세션 t와 클라이언트 $U_i \in G_C$를 랜덤하게 선택한다. 그리고 F는 U_i의 보조 공개키를 $v_i \leftarrow g^a$로

설정하고, 서버 S의 공개키를 $y \leftarrow g^b$로 설정한다. F는 랜덤 오라클인 H_0와 H_1를 공격자 A에게 시뮬레이션(simulation) 해준다. 그리고 A가 요청하는 q_H개의 해쉬 쿼리 중에서 g^{ab} 값이 있는지 찾는다.

랜덤 오라클 모델에서 $\{\alpha_i = g^{x_i x}\}_{i \in I_C}$를 얻은 A가 sk에 대한 정보를 얻기 위해서, A는 반드시 해쉬 오라클인 H_0 또는 H_1에 $\beta_i = g^{ab}$를 요청해야 한다. $AskH = AskH0 \vee AskH1$를 A가 그러한 해쉬 쿼리를 요청하는 사건으로 놓자. 여기서 $AskH0$와 $AskH1$은 다음과 같다.

- $AskH0$: A가 H_0에 $(d \| \{\alpha_i\}_{i \in I_C} \| \{\beta_i\}_{i \in I_C})$를 요청하는 사건.
- $AskH1$: A가 H_1에 $(d \| \alpha_i \| \beta_i \| G_C \| S)$를 요청하는 사건.

그러면 A가 세션 키를 올바르게 추측할 확률은 다음과 같다.

$$\begin{aligned}\Pr[CG] &= \Pr[CG \wedge AskH] + \Pr[CG \wedge \overline{AskH}] \\ &= \Pr[CG|AskH] \cdot \Pr[AskH] \\ &\quad + \Pr[CG|\overline{AskH}] \cdot \Pr[\overline{AskH}] \\ &\le \Pr[AskH] + \frac{1}{2} Pr[\overline{AskH}] \\ &\le \Pr[AskH] + \frac{1}{2}.\end{aligned}$$

만약 $AskH$가 발생한다면, $\beta_i = g^{ab}$이다. 여기서 $a = \log_g v_i = \log_g A$이고, $b = \log_g y = \log_g B$이다. 따라서 F는 주어진 CDH 문제의 올바른 해를 얻을 수 있다. 만약 $AskH0$가 확률 $\frac{1}{q_{H_0}}$로 발생한다면, $\Pr[AskH0] \le q_{H_0} \cdot Adv_G^{cdh}(t)$이다. 만약 $AskH1$이 확률 $\frac{1}{q_{H_1}}$로 발생한다면, $|G_C| = N$중에서 공격 대상을 올바르게 추측해야 하기 때문에 $\Pr[AskH1] \le q_{H_1} N \cdot Adv_G^{cdh}(t)$이다. 결과적으로 N_s개의 세션에서 세션 t를 올바르게 추측할 확률이 $\frac{1}{N_s}$이고, $q_H = q_{H_0} + q_{H_1}$이므로 $\Pr[AskH] \le q_H(N+1)N_s \cdot Adv_G^{cdh}(t)$이다.

그룹 키 교환 스킴이 만족해야 하는 일반적인 안전성. 제안 프로토콜에서는 세션상태 정보 노출 공격에 대한 안전성 위해서 기존 Nam과 그 외의 스킴에 각 클라이언트와 서버의 롱-텀 개인키 값들로부터 계산된 고정적인 디피-헬만 키 값을 추가적으로 사용하였다. 고정적인 디피-헬만 키 값을 계산하는 것은 계산적 디피-헬만 문제이므로 추가된 디피-헬만 키 값은 기존의 Nam과 그 외의 스킴이 일반적으로 만족하고 있는 그룹 키 교환 스킴의 안전성(예를 들면 전방향 안전성(forward secrecy), 기지-키 공격(known-key attack), 등)에 영향을 주지 않는다. 따라서 제안 프로토콜이 만족해야 하는 일반적인 그룹 키 교환 스킴의 안전성은 Nam과 그 외의 스킴의 안전성에 귀속된다. 즉, 제안 프로토콜은 Nam과 그 외의 스킴이 만족하는 안전성을 모두 만족하며, 세션상태 정보 노출 공격에 대한 안전성도 만족한다. 본 논문에서는 제안 프로토콜의 세션상태 정보 노출 공격에 대한 안전성만을 증명하였다.

V. 결 론

본 논문에서는 Bresson과 그 외의 그룹 키 교환 스킴을 개선한 Nam과 그 외의 스킴이 세션상태 정보 노출 공격에 안전하지 않음을 보였다. 또한 이러한 안전성 취약점을 개선한 스킴을 제안하고, 제안 스킴이 세션상태 정보 노출 공격에 안전함을 랜덤 오라클 모델에서 증명하였다.

참고문헌

[1] E. Bresson, O. Chevassut, A. Essiari, and D. Pointcheval, "Mutual authentication and group key agreement for lowpower mobile devices," Proc. of the 5th IFIP-TC6 International Conference on Mobile and Wireless Communication Networks (MWCN'03), pp.59-62, October 2003. The full version appears in Journal of Computer Communications, vol. 27, no. 17, pp.1730-1737, July 2004.

[2] R. Canetti and H. Krawczyk. "Analysis of Key-xchange Protocols and Their Use for Building Secure Channels," Proc. of EURO CRYPT 2001, Lecture Notes in Computer Science 2045, pp.453-474, May 2001.

[3] I. R. Jeong, J. O. Kwon, D. H. Lee. "A Diffie-Hellman Key Exchange Protocol Without Random Oracles," Proc. of CANS 2006,

Lecture Notes in Computer Science 4301, pp. 37-54, Nov. 2006.

[4] I. R. Jeong, J. O. Kwon, D. H. Lee. Strong Diffie-Hellman-DSA Key Exchange. IEEE Commun. Lett., vol. 11, no. 5, pp.432-433, May 2007.

[5] H. Krawczyk. "HMQV : A High-Performance Secure Diffie-Hellman Protocol," Proc. of CRYPTO 2005, Lecture Notes in Computer Science 3621, pp.546-566, August 2005.

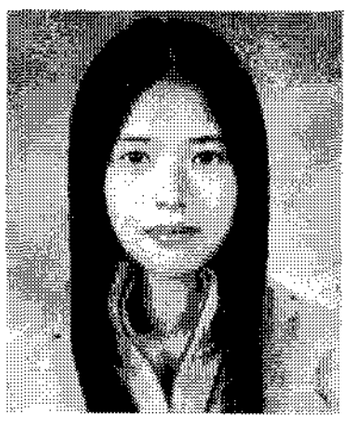
[6] S. M. Lee, S. Y. Lee, D. H. Lee. "Efficient Group Key Agreement for Dynamic TETRA Networks," Proc. of SOFSEM 2007, Lecture Notes in Computer Science 4362, pp.400- 409, July 2007.

[7] J. Nam, S. Kim, and D. Won. A Weakness in the Bresson-Chevassut-Essiari-Pointcheval's Group Key Agreement Scheme for Low-Power Mobile Devices. IEEE Commun. Lett., vol. 9, no. 5, pp. 429-431, May 2005.

〈著者紹介〉

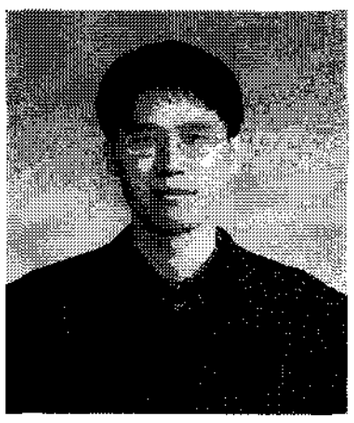
김 기 탁 (Ki Tak Kim) 학생회원

2006년 8월 : 고려대학교 수학과 학사 졸업
2006년 9월~현재 : 고려대학교 정보경영공학전문대학원 석사 과정
<관심분야> 암호프로토콜, 암호이론



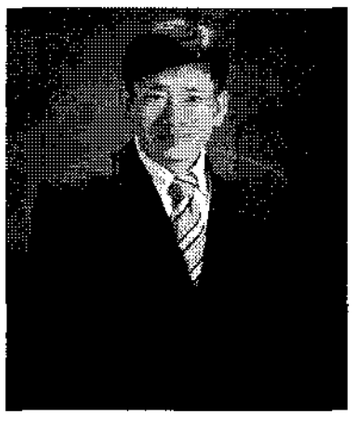
권 정 옥 (Jeong Ok Kwon) 정회원

2000년 8월 : 동덕여자대학교 전자계산학과 졸업
2003년 2월 : 고려대학교 정보보호기술협동과정 석사 졸업
2007년 2월 : 고려대학교 정보경영공학전문대학원 박사 졸업
2007년 3월~2007년 8월 : 고려대학교 정보보호기술연구센터 박사후연구원
2007년 9월~현재 : 고려대학교 BK21 유비쿼터스 정보보호 사업단 연구교수
<관심분야> 암호프로토콜, 암호이론



홍 도 원 (Dowon Hong) 정회원

1994년 2월 : 고려대학교 수학과 학사 졸업
1996년 2월 : 고려대학교 수학과 석사 졸업
2000년 2월 : 고려대학교 수학과 박사 졸업
2000년 4월~현재 : 한국전자통신연구원 암호기술연구팀 팀장
<관심분야> 암호프로토콜, 암호이론, 프라이버시 보호기술



이 동 훈 (Dong Hoon Lee) 종신회원

1983년 8월 : 고려대학교 경제학과 학사 졸업
1987년 12월 : Oklahoma University 전산학과 석사 졸업
1992년 5월 : Oklahoma University 전산학과 박사 졸업
1993년 3월~1997년 2월 : 고려대학교 전산학과 조교수
1997년 3월~2001년 2월 : 고려대학교 전산학과 부교수
2001년 2월~현재 : 고려대학교 정보경영공학전문대학원 교수
<관심분야> 암호프로토콜, RFID/USN 보안, 프라이버시 보호기술