특집논문-08-13-1-09

그룹 사용자간 안전한 콘텐츠 전송을 위한 Zhou의 ID-기반의 인증된 그룹 키 교환 프로토콜 분석

최 재 탁[a], 권 정 옥[a], 윤 석 구[a]‡

Analysis on Zhou et al.'s ID-Based Authenticated Group Key Agreement To Exchange Secure Contents among Group Users

Jae Tark Choi[a], Jeong Ok Kwon[a], and Seok Koo Yoon[a]‡

요 약

유료 콘텐츠를 정당한 서비스 수신자에게 안전하게 제공하기 위해서는 서비스 제공자와 수신자 사이에 안전한 키 교환이 필요하다. 그룹 키 교환 프로토콜은 이러한 그룹에 속한 멤버들이 공개된 통신망을 이용하여 안전하고 효율적인 방법으로 그룹의 세션키를 설정할 수 있게 한다. 최근에 L. Zhou는 효율적인 인증된 그룹 키 교환 프로토콜을 설계하였다. 본 논문에서 우리는 Zhou의 기법이 전방향 안전성을 제공하지 않음을 보인다.

ABSTRACT

An authenticated group key agreement protocol allows a group of parties communicating over an insecure network to share a common secret key. In this paper, we show that Zhou et al.'s ID-based authenticated group key agreement schemes do not provide forward secrecy.

Keywords : ID-based cryptosystem, group key agreement, bilinear pairing

Ⅰ. 서 론

인증된 그룹 키 교환(authenticated group key agreement) 프로토콜을 이용하여 그룹에 속하는 사용자들은 안전하지 않는 공개된 통신망을 이용하여 안전하고 효율적인 방법으로 그룹 세션 키를 교환할 수 있다. 이러한 세션 키는 암호화/복호화, MAC, 인증과 디지털 서명 등에 사용되어 진다.

a) 고려대학교 정보경영공학전문대학원
Graduate School of Information Security CIST, Korea University
‡ 교신저자 : 윤석구(yun1015@korea.ac.kr)
※ 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원 사업의 연구결과로 수행되었음" (IITA-2008-(C1090-0801-0025))

ID 기반의 공개키 방식의 기본 개념은 Adi Shamir[1]가 처음으로 제안하였다. ID 기반의 암호 시스템에서 공개키로 비밀 키를 가지고 있는 사용자를 쉽게 확인할 수 있는 이메일 주소와 같은 공개 정보로 구성된 공개 확인자(identity ,ID)를 사용하고 있다. Bilinear pairing을 이용한 Boneh 와 Franklin[2]의 ID 기반의 암호 시스템에 관한 연구 이래로 ID 기반의 그룹 키 교환에 관한 연구가 진행되어 왔다. ID 기반의 인증된 그룹 키 교환 프로토콜은 K. C. Reddy[3]가 N. P. Smart[4]의 양자간 키 교환 방식을 이용하여 트리 기반의 그룹 키 교환 기법을 제안하였다. 그 후, R. Barua[5]는 A. Joax[6]의 3자간 키 교환 방식을 이용한 트리 기반의 그룹 키

교환 기법을 제안하였다. 하지만 위의 두 가지 방식은 트리의 깊이의 수만큼 키 교환이 필요하다는 단점이 있다. 그래서 Reddy와 Barua의 기법은 많은 사용자를 가지는 그룹 키 교환 방식에는 적용하기에는 비효율적이다. 고정된 라운드를 가지는 ID 기반의 인증된 그룹 키 교환 프로토콜이 Choi et al.[7]와 Du et al.[8]에 의해서 제안 되었다. Choi와 Du의 기법은 2 라운드를 필요로 한다. 그러나 Zhang과 Chen[9]은 이 두 기법에 대한 위장공격의 취약점을 발견하였다. 그 후, Du et al.[10]는 자신의 기법에 대한 위장공격에 안전하게 보완한 그룹 키 교환 기법을 제안하였다.

[11]에서 Y. Shi는 1라운드를 가지는 ID 기반의 인증된 그룹 키 교환 기법을 제안하였다. 최근에 L. Zhou[12]는 두 개의 그룹 키 교환 기법을 제시하였는데, 하나는 1라운드가 필요하고 다른 하나는 2라운드가 필요하다. 2라운드가 필요한 기법은 1라운드가 필요한 기법보다는 전송 효율이 더 좋은 기법이다.

본 논문에서, 우리는 Zhou et al.[12]의 두 개의 ID 기반의 인증된 그룹 키 교환 프로토콜이 전방향 안전성을 만족하지 못함을 발견하고 이를 증명하였다.

II. 정 의

1. The Bilinear Map

G_1을 위수가 q인 덧셈 연산군이라 하고, G_2를 위수 q를 갖는 곱셈 연산군이라 하자. 이때 G_1, G_2에서의 이산 대수 문제(discrete logarithm problem)는 어렵다고 가정한다.

Bilinear Diffie-Hellman(BDH) 파라미터 생성자를 확률적 다항식 시간(PPT) 연산 알고리즘이라고 하자. 다항식 시간 안에 BDH 파라미터 생성자는 위수가 소수 q를 가지는 두 그룹 G_1, G_2와 다음 성질을 만족하는 a bilinear map $e: G_1 \times G_1 \rightarrow G_2$를 생성한다.

- Bilinear : 모든 $P, Q \in G_1$와 $a, b \in Z_q^*$에 대해서 $e(aP, bQ) = e(P, Q)^{ab}$
- Non-degenerate : 모든 $Q \in G_1$에 대하여 $e(P, Q) = 1$을 만족하면, $P = O$이다.
- Computable : 모든 $P, Q \in G_1$에 대하여 다항식 시간 안에 $e(P, Q)$를 계산할 수 있는 효율적인 알고리즘이 존재한다.

2. 안전성 성질들

본 절에서는 키 교환에 관한 기본적인 안전성 성질들에 관해서 알아본다.

키 교환 프로토콜의 가장 기본적인 안전성 요구사항은 키 기밀성 (key secrecy)이다. 유한한 계산 능력을 지닌 공격자는 정직한 사용자 간의 통신을 도청하거나, 공격자가 프로토콜에 참여함으로써 정직한 사용자에게 메시지를 전송 할 수 있다. 키 기밀성은 이러한 공격자가 세션 키에 대한 어떠한 정보도 얻을 수 없어야 한다는 것이다. 키 교환 프로토콜에 요구되는 다른 안전성은 전방향 안전성 (forward secrecy)과 기지 키 공격에 대한 안정성 (known-key secrecy)이다.

전방향 안전성은 사용자의 롱텀 비밀 키(long-term key)를 알고 있는 어떠한 공격자라도 정직한 구성원 간에 성공적으로 확립된 이전의 세션 키에 대한 어떠한 정보도 없을 수 없어야 함을 의미한다.

III. Zhou의 그룹 키 교환 기법

본장에서, 우리는 Zhou et al. 의 1라운드를 가지는 ID 기반의 인증된 그룹 키 교환 프로토콜(O-AGKA)와 2라운드를 가지는 ID 기반의 인증된 그룹 키 교환 프로토콜(T-AGKA)에 대해서 살펴본다.

1. Zhou의 1라운드를 가지는 ID 기반의 인증되 그룹 키 교환 프로토콜(O-AGKA)

본 절에서, 우리는 Zhou의 1라운드를 가지는 ID 기반의

인증된 그룹 키 교환 프로토콜(O-AGKA)을 살펴본다.

먼저 그룹 관리자(Group Administrator : GA)는 암호학적 일방향 해쉬 함수 $H_1 = \{0,1\}^* \rightarrow G_1$, $H_2 = G_2 \rightarrow \{0,1\}^n$ 그리고 $H_3 = \{0,1\}^n \rightarrow \{0,1\}^n$를 생성한다. H_1, H_2와 H_3는 안전성 분석에서 랜덤 오라클(random oracle)로 간주된다.

Setup. GA는 BDH 파라미터 생성자를 이용하여 위수가 소수 q인 두 그룹 G_1과 G_2, bilinear map $e : G_1 \times G_1 \rightarrow G_2$를 생성한다. 그리고 임의의 생성자 $P \in G_1$과 난수 $s \in Z_q^*$를 선택한 후 $P_{pub} = sP$를 계산한다. GA는 s를 마스터 비밀 키로 하고 공개 시스템 파라미터 $\text{parms} = \{e, G_1, G_2, q, P, P_{pub}, H_1, H_2, H_3\}$를 공개한다.

Extract. 확인자(identity)가 ID_i인 사용자 U_i의 비밀 키를 생성하기 위해서, GA는 $Q_i = H_1(ID_i)$를 계산하여 비밀 키 $S_i = sQ_i$를 계산한 후 S_i를 안전한 채널로 사용자 U_i에게 전송한다.

$U_1, \cdots, U_n$을 그룹 세션 키를 생성하기를 원하는 사용자들이라고 하자. 그룹 키 교환 프로토콜은 다음과 같다.

Round 1. 각 사용자 U_i는 먼저 임의의 난수 $\delta_i \in_R G_2$, $r_i, k_i \in_R \{0,1\}^n$를 선택한 후 $P_i^j = H_2(e(S_i, Q_j) \cdot \delta_j) \oplus r_i$, $1 \le j \le n, j \ne i$를 계산한다. 그런 후에, U_i는 D_i를 다음과 같이 계산하여 다른 사용자들에게 브로드캐스트 한다.

$D_i = \langle \delta_i, P_i^1, \cdots, P_i^{i-1}, P_i^{i+1}, \cdots, P_i^n, H_3(r_i) \oplus k_i, \mathcal{L} \rangle$

단, $\mathcal{L}$은 P_i^j가 어느 사용자와 연관되어 있는지에 관한 정보를 포함하는 분류 표시이다.

Key Computation. $D_j = \langle R_j, P_j^1, \cdots, P_j^n, V_j, \mathcal{L} \rangle$라 하자. 사용자 U_i는 다른 사용자로부터 D_j를 전송 받은 후에 $\mathcal{L}$을 이용하여 P_j^i를 찾는다. 그리고 다음을 계산한다.

$$k_j' = H_3(H_2(e(Q_j, S_i) \cdot R_j) \oplus P_j^i) \oplus V_j$$

각 사용자 U_i는 공통된 세션 키를 다음과 같이 계산할 수 있다.

$$K = K_i = k_1' \oplus \cdots \oplus k_{i-1}' \oplus k_i \oplus k_{i+1}' \oplus \cdots \oplus k_n'$$

2. Zhou의 2라운드를 가지는 ID 기반의 인증되 그룹 키 교환 프로토콜(T-AGKA)

본 절에서, 우리는 Zhou의 2라운드를 가지는 ID 기반의 인증된 그룹 키 교환 프로토콜(T-AGKA)을 살펴본다. T-AGKA 프로토콜은 위에서 제시한 O-AGKA를 변형한 것이다.

Setup. O-AGKA 기법과 동일하다. 추가적으로, T-AGKA는 새로운 세 개의 해쉬 함수 $H_4 : G_2 \rightarrow \{0,1\}^n$, $H_5 : \{0,1\}^n \rightarrow Z_q^*$와 $H_6 : G_1 \rightarrow \{0,1\}^n$을 생성한다.

Extract. O-AGKA 기법과 동일하다.

$U_1, \cdots, U_n$을 그룹 세션 키를 생성하기를 원하는 사용자들이라고 하면, 그룹 키 교환 프로토콜은 다음과 같다.

Round 1. 개시자(initiator) U_1은 먼저 임의의 난수 $\delta \in_R G_2$, $r \in_R \{0,1\}^n$과 $k_1 \in_R Z_P^*$을 선택한다. 그런 후에, U_1은 $D_1 = \langle R, P_2, \cdots, P_n, V, W, \mathcal{L} \rangle$을 다음과 같이 계산하여 다른 사용자들에게 브로드캐스트 한다.

$$D_1 = < \delta, r \oplus H_4(e(S_1, Q_2) \cdot \delta), \cdots, r \oplus H_4(e(S_1, Q_n) \cdot \delta), H_5(r) \cdot k_1 P, k_1 P_{pub}, \mathcal{L} >$$

단, $\mathcal{L}$은 P_i가 어느 사용자와 연관되어 있는지에 관한 정보를 포함하는 분류 표시이다.

Round 2. 각 응답자 $U_i (2 \le i \le n)$가 U_1으로부터 D_1을 받으면, $\mathcal{L}$의 정보를 이용하여 자신의 P_i를 찾은 후에, $r' = H_4(e(Q_1, S_i) \cdot R) \oplus P_i$를 계산한다. 만약에 메시지 D_1이 정당하다면, $r' = r$임을 알 수 있다. 그리고 U_i는 임의의

난수 $k_i \leftarrow Z_P^*$를 선택한 후 $D_i\langle H_5(r)\cdot k_iP, k_iP_{pub}\rangle$를 계산하여 다른 모든 사용자에게 브로드캐스트 한다.

Key Computation. $D_j=\langle X_j, Y_j\rangle$라 하자. 다른 사용자로부터 D_j를 전송 받은 후에, 개시자 U_1과 사용자 U_i는 $z_1=H_5(r)^{-1}\cdot V$과 $z_j=H_5(r)^{-1}\cdot X_j (2\le j\le n)$를 계산한다. 그런 후에, 각 사용자 U_i는 계산된 z_j들을 저장하고 z_j가 올바른 값인지를 다음의 식을 이용하여 확인한다.

$$e\left(P,\sum_{j=1}^{n}Y_j\right)\stackrel{?}{=}e\left(P_{pub},\sum_{j=1}^{n}z_j\right)$$

위의 식을 이용하여 모든 z_j가 올바른 값으로 확인되면, U_i는 다른 그룹 사용자들이 정당한 사용자라는 것을 확인할 수 있게 된다. 따라서 모든 사용자 U_i는 공통된 세션 키를 다음과 같이 계산할 수 있다.

$$K=K_i=H_6(z_1)\oplus\cdots\oplus H_6(z_n)$$

Ⅳ. 안전성 분석

본 장에서, 우리는 3장에서 소개한 Zhou et al.의 그룹 키 교환 프로토콜에 대한 안전성을 분석한다. 먼저, O-AKGA 기법이 한명의 사용자의 롱텀 비밀 키(long-term private key)가 알려졌을 경우에는 전방향 안전성(forward secrecy)를 만족함을 보이고, 두 명 이상의 사용자의 비밀 키가 알려졌을 경우에는 전방향 안전성을 제공하지 않음을 보인다. 그리고 우리는 한명의 사용자의 비밀 키를 알고 있는 공격자는 이전 세션에 대한 세션 키(session keys)를 계산할 수 있음을 보임으로써 T-AKGA 기법이 전방향 안전성이 만족하지 않다는 것을 보이기로 한다.

먼저, 공격자가 한명의 사용자 U_i의 롱텀 비밀 키(long-term private key) $S_i (1\le i\le n)$를 알고 있다고 하자. 그러면 공격자는 다른 그룹 사용자들이 U_i에게 전송한 메시지 $D_j=\langle R_j, P_j^1,\cdots,P_j^n, V_j, \mathcal{L}\rangle$와 U_i의 롱텀 비밀 키 S_i를 이용하여 $k_j'=H_3(H_2(e(Q_j,S_i)\cdot R_j)\oplus P_j^i)\oplus V_j$ $(1\le j\le n, j\ne i)$를 계산할 수 있다. 만약에 공격자가 메시지 $D_i=<R_i, P_i^1,\cdots,P_i^n, V_i, \mathcal{L}>$를 이용하여 k_i를 계산할 수 있다면, 공격자는 모든 $k_l (1\le l\le n)$를 알게 되므로 세션 키 K를 계산할 수 있게 된다. 하지만 아래의 각 경우에서, 우리는 공격자가 D_i로부터 k_i를 계산할 수 없음을 보인다.

CASE 1. 공격자가 H_3 해쉬 쿼리를 이용하여 $H_3(r_i)$를 얻으면, $V_i=H_3(r_i)\oplus k_i$로부터 k_i를 얻을 수 있게 된다. 하지만 랜덤 오라클 모델에서 공격자가 $H_3(r_i)$를 얻을 수 있는 확률은 무시해도 좋을 정도이다. 랜덤 오라클 모델에서 해쉬 함수는 실제 랜덤 함수로 여겨진다. 따라서 공격자가 k_i를 얻을 확률은 매우 낮다.

CASE 2. 만약에 공격자가 H_2해쉬 쿼리를 이용하여 $P_i^j=H_2(e(S_i,Q_j)\cdot\delta_i)\oplus r_i$로부터 r_i을 계산할 수 있다면, 공격자는 $k_i=H_3(r_i)\oplus V_i$를 알 수 있게 되므로 세션 키 K를 계산할 수 있게 된다. 하지만 CASE 1과 동일하게 공격자가 랜덤 오라클 모델 하에서 $H_3(r_i)$를 얻을 수 있는 확률은 무시해도 좋을 정도이다.

CASE 3. 마지막으로, 공격자가 GA의 마스터 비밀 키(master secrete key) s를 얻게 되면, 공격자는 $e(S_i,Q_j)=e(sQ_i,Q_j)=e(Q_i,Q_j)^s$를 계산할 수 있게 된다. 그러므로 공격자는 k_i를 다음과 같이 계산할 수 있다.

$$k_i=H_3\left(H_2\left(e(Q_i,Q_j)^s\cdot R_i\right)\oplus P_i^j\right)\oplus V_i$$

하지만 공격자가 GA의 마스터 비밀 키 s를 얻기 위해서는 $P_{pub}=sP$로부터 s를 계산해 낼 수밖에 없다. $P_{pub}=sP$로부터 s를 계산하는 것은 이산 대수 문제(discrete logarithm problem)을 계산하는 것과 동일하다.

위에서 설명한 바와 같이 어떠한 경우에도 공격자는 k_i를 구할 수 없다. 따라서 공격자는 세션 키 K에 대한 어떠한 정보도 얻을 수 없다.

1. O-AGKA 기법에 대한 분석

위에서 설명한 바와 같이 O-AGKA 기법은 두 명 이상의 사용자의 롱텀 비밀 키가 드러나지 않을 경우에는 전방향 안전성을 제공한다. 하지만 이러한 가정은 실제 공격 환경을 제대로 모델링하지 못하고 있다. 즉, 실제 공격 환경에서는 여러 명의 사용자에 대한 비밀 키를 얻을 수 있다.

만약 두 명 이상 사용자의 롱텀 비밀 키가 공격자에게 알려졌을 경우, 공격자는 이전의 세션 키를 다음과 같이 계산할 수 있게 된다. 먼저, 공격자가 두 명의 사용자 U_i, U_j의 롱텀 비밀 키 S_i, $S_j(1 \le i,j \le n, i \ne j)$를 알고 있다고 하자. 공격자는 다른 그룹 사용자들이 U_i에게 전송한 메시지 $D_l = \langle R_l, P_l^1, \cdots, P_l^n, V_l, \pounds \rangle (1 \le l \le n, l \ne i)$와 U_i의 비밀 키 S_i를 이용하여 다음을 계산할 수 있다.

$$k_l = H_3(H_2(e(Q_l, S_i) \cdot R_l) \oplus P_l^i) \oplus V_l$$

따라서 공격자는 $k_1 \oplus \cdots \oplus k_{i-1} \oplus k_{i+1} \oplus \cdots \oplus k_n$을 계산할 수 있게 된다. 그리고 공격자는 U_i가 브로드캐스트한 메시지 $D_i = \langle R_i, P_i^1, \cdots, P_i^n, V_i, \pounds \rangle$에서 U_j에 대응하는 P_i^j를 찾고, U_j의 비밀 키 S_j를 이용하여 $k_i = H_3(H_2(e(Q_i, S_j) \cdot R_i) \oplus P_i^j) \oplus V_i$를 계산할 수 있다. 따라서 공격자는 모든 $k_l(1 \le l \le n)$를 알게 되므로, 세션 키 $K = k_1 \oplus \cdots \oplus k_{i-1} \oplus k_i \oplus k_{i+1} \oplus \cdots \oplus k_n$를 계산할 수 있다. 결국 공격자는 둘 이상의 사용자의 비밀 키를 알게 되면 이전의 세션 키에 대한 정보를 얻을 수 있게 된다.

2. T-AGKA 기법에 대한 분석

본 절에서, 우리는 다음의 두 가지 경우에서 공격자가 알려진 한 사용자의 비밀 키를 이용하여 세션 키를 얻을 수 있음을 보인다.

CASE 1. 먼저 공격자는 개시자(initiator) U_1의 롱텀 비밀 키(long-term private key) S_1을 알고 있다고 하자. 그러면 공격자는 $e(S_1, Q_i)$을 계산할 수 있고, Round 1에서 개시자(initiator)가 다른 그룹 사용자에게 전송한 메시지 $D_1 = \langle R, P_2, \cdots, P_n, V, W, \pounds \rangle$에서 $P_i = r \oplus H_4(e(S_1, Q_i) \cdot R)$를 이용하여 r을 구할 수 있다. 따라서 공격자는 $V_1 = H_5(r) \cdot k_1 P$에서 $z_1 = k_1 P$를 계산할 수 있다. Round 2에서 사용자들이 전송한 메시지 $D_i = \langle X_i, Y_i \rangle (1 \le i \le n)$로부터 공격자는 $z_i = H_5(r)^{-1} \cdot X_i$를 계산할 수 있다. 그러므로 공격자는 모든 z_i를 알 수 있게 되고, 세션 키 $K = H_6(z_1) \oplus \cdots \oplus H_6(z_n)$를 계산할 수 있다.

CASE 2. 공격자가 개시자 U_1이외의 사용자 $U_i(2 \le i \le n)$의 롱텀 비밀 키 S_i를 알고 있다고 하자. Round 1에서 U_1이 다른 사용자에게 전송한 메시지 D_1으로부터, 공격자는 S_i를 이용하여 $r = H_4(e(Q_1, S_i) \cdot R) \oplus P_i$를 계산할 수 있으므로, $z_1 = H_5(r)^{-1} \cdot V$임을 확인할 수 있다. 또한 공격자는 Round 2에서 $U_j(2 \le j \le n)$이 브로드캐스트한 메시지 D_j로부터 $z_j = H_5(r)^{-1} \cdot X_j (2 \le j \le n)$을 계산할 수 있다. 따라서 공격자는 세션 키 $K = H_6(z_1) \oplus \cdots \oplus H_6(z_n)$를 계산할 수 있게 된다.

T-AGKA 기법은 공격자가 그룹 사용자 중에서 한명의 사용자의 비밀 키를 알고 있으면 이전 세션 키의 정보를 알 수 있게 된다.

V. 결 론

L. Zhou의 인증된 그룹 키 교환 프로토콜은 공격자가 한 명의 사용자의 비밀 키만을 알고 있을 경우에는 전방향 안전성을 제공한다. 하지만 이러한 가정은 실제 공격 환경에서는 일어나지 않는다. 그래서 본 논문에서 우리는 L. Zhou의 기법이 두 명 이상의 사용자의 비밀 키가 알려졌을 경우에는 이전의 세션 키를 알 수 있기 때문에 전방향 안전성을 제공하지 않음을 증명하였다.

참 고 문 헌

[1] A. Shamir, "Identity Based Cryptosystems and Signature Schemes", Advances in Cryptology - CRYPTO'84, Springer-Verlag, LNCS 196, pages 47 - 53, 1985

[2] D. Boneh and M. Franklin, "Identity Based Encryption from the Weil Pairing", Advances in Cryptology - CRYPTO 2001, Springer-Verlg, LNCS 2139, pages 213 - 229, 2001

[3] K. C. Reddy, and D. Nalla. "Identity Based Authenticated Group Key Agreement Protocol", In Proceeding of INDOCRYPT 2002, LNCS 2551, pages 215 - 233, 2002.

[4] N. P. Smart, "An Identity Baed Authenticated Key Agreement Protocol Based on the Weil Pairing", Cryptology ePrint Archive, Report 2001/111, 2001, http://eprint.iacr.org/

[5] R. Barua, R. Dutta, and P. Sarkar. "Extending Joux's Protocol to Multi Party Key Agreement", In Proceeding of INDOCRYPT 2003, LNCS 2904, pages 205 - 217, 2003.

[6] A. Joux. "A One Round Protocol for Tripartite Diffie-Hellman", In Proceeding of ANTS IV, LNCS 1838, pages 385 - 394, 2000.

[7] K. Y. Choi, J. Y. Hwang and D. H. Lee. "Efficient ID-Based Group Key Agreement with Bilinear Maps", 2004 International Workshop on Practice and Theory in Public Key Cryptography (PKC '04), LNCS 2947, pages 130 - 144. 2004.

[8] X. Du. Y. Wang, J. Ge, and Y. Wang. "ID-Based Authenticated Two Round Multi-Party Key Agreement", Cryptology ePrint Archive, Report 2003/247, 2003.

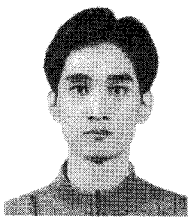
[9] F. Zhang, and X. Chen. "Attack on an ID-based AuthenticatedGroup Key Agreement Scheme from PKC 2004", Information Processing Letters, Vol. 91, pages 191 - 193, 2004.

[10] X. Du. Y. Wang, J. Ge, and Y. Wang. "An Improved ID-Based Authenticated Group Key Agreement Scheme", Cryptology ePrint Archive, Report 2003/260, 2003.

[11] Y. Shi, G. Chen, and J. Li. "Id-Based One Round Authenticated Group Key Agreement Protocol with Bilinear Pairing", International Conference on Information Technology: Coding and Computing (ITCC '05), Vol. I, pages 757 - 761, 2005.

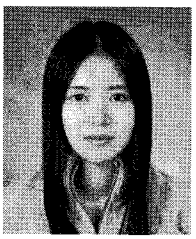
[12] L. Zhou, W. Susilo, and Y. Mu. "Efficient ID-Based Authenticated Group Key Agreement from Bilinear Pairing", In Proceeding of MSN '06, LNCS 4325, pages 521 - 532, 2006.

저 자 소 개



최 재 탁

- 2002년 : 충북대학교 수학과 학사
- 2005년 : KAIST 수학과 석사
- 2005년 ~ 현재 : 고려대학교 정보경영공학전문대학원 박사과정
- 주관심분야 : 암호이론, 암호프로토콜



권 정 옥

- 2000년 : 동덕여자대학교 전자계산학과 학사 졸업.
- 2003년 : 고려대학교 정보보호기술 학과 석사 졸업.
- 2007년 : 고려대학교 정보보호대학원 정보보호학과 박사학위.
- 주관심분야 : 암호이론, 암호프로토콜

저 자 소 개

윤 석 구

- 1979년 2월 : 건국대학교 수학과 (학사)
- 1981년 2월 : 건국대학교 수학과 대학원 (석사)
- 1981년 ~ 2001년 : 국가정보원 정보보안단장
- 2002년 ~ 2004년 : 국가사이버안전센터장
- 2005년 2월 : 고려대학교 정보보호대학원 정보보호학과 (박사)
- 2005년 ~ 현재 : 고려대학교 정보경영공학전문대학원 BK21 연구교수
- 주관심분야 : 정보보호정책, 사이버 포렌식, 암호알고리즘 분석 등