Journal of Korea Multimedia Society Vol. 8, No. 4, April 2005(pp. 525-535)

패스워드 기반 인증된 3자 키 교환 프로토콜

이상곤[†], 이훈재[††], 박종욱[†††], 윤장홍[††††]

요 약

A. Joux의 프로토콜을 기반으로 패스워드 기반 인증된 3자 키 교환 프로토콜을 제안하였다. 공유 패스워드를 이용한 대칭 키 암호를 사용하여 A. Joux의 프로토콜이 갖는 인증과 man-in-the-middle attack 문제를 해결하였다. 또한 패스워드를 사용한 대칭 키 암호의 취약점인 오프라인 사전공격에 대한 대책도 제시하였다. 제안된 프로토콜은 인증서 기반 인증과 ID 기반 인증에서 요구되는 신뢰 기관이 필요 없으므로 ad hoc 네트워크와 같이 네트워크 인프라 구축이 어려운 환경에서 유용하게 사용될 수 있다. 제안된 프로토콜은 기존에 발표된 패스워드 인증된 키 교환 프로토콜보다 통신적인 면에서 더 효율적이며 트리기반 그룹 키 프로토콜에 적용될 경우 계산상의 약점을 보상받을 수 있다.

Password-Based Authenticated Tripartite Key Exchange Protocol

SangGon Lee[†], HoonJae Lee[††], JongWook Park[†††], JangHong Yoon[††††]

ABSTRACT

A password-based authenticated tripartite key exchange protocol based on A. Joux's protocol was proposed. By using encryption scheme with shared password, we can resolve man-in-the-middle attack and lack of authentication problems. We also suggested a scheme to avoid the offline dictionary attack to which symmetric encryption schemes are vulnerable. The proposed protocol does not require a trusted party which is required in certificate or identity based authentication schemes. Therefore in a ad hoc network which is difficult to install network infrastructure, the proposed protocol would be very useful. The proposed protocol is more efficient in computation aspect than any existing password-based authenticated tripartite key exchange protocols. When it is used as a base line protocol of tree based group key exchange protocol, the computational weak points of the proposed protocol are compensated.

Key words: Key Exchange Protocol(키 교환 프로토콜), Password(패스워드), Group Key Exchange(그룹 키 교환), TGDH, Pairing(페어링)

1. 서 론

어떤 회의에서 소규모 그룹의 사람들이 특별회의(ad hoc meeting)를 위하여 회의실에 모였고, 회의 동안 그들의 랩톱 컴퓨터들 간에 무선 네트워크를 구성하려고 한다. 그리고 회의실 밖에서는 회의 내용을 엿들을 수 없도록 정보를 안전하게 공유하고자 한다. 회의에 참석한 사람들은 서로 잘 알고 신뢰하고 있지만, 공개키 인증서나 신뢰된 키 분배 센터 등을 접근 할 수 없는 상황이다. 문제는 "이러한 상황에서 어떻게 비밀 채널을 만들 것인가?"이다[1].

위에서 언급한 시나리오처럼 ad hoc 네트워크에

※ 교신저자(Corresponding Author) : 이상곤, 주소 : 부산시 사상구 주례2동 산 69-1(671-761), 전화 : 051)320-1760, FAX : 051)327-8955, E-mail : nok60@dongseo.ac.kr
접수일 : 2005년 1월 10일, 완료일 : 2005년 4월 14일
[†] 정회원, 동서대학교 인터넷공학부 조교수
[††] 정회원, 동서대학교 인터넷공학부 조교수
(E-mail : hjlee@dongseo.ac.kr)
[†††] 정회원, 국가보안기술연구소 책임연구원
(E-mail : khspjw@etri.re.kr)
[††††] 국가보안기술연구소 팀장
(E-mail : jhyoon@etri.re.kr)
※ 본 연구는 2003년 동서대학교 교내특별연구과제비와 정보통신부지정 ITRC 연구비 지원에 의한 결과임.

서는 기반자원이 충분하지 않은 환경에서 운영되어지는 경우가 많다. 이런 경우에는 비용이 적게 들면서 효율적인 인증 메커니즘이 요구되어 지는 반면 안전한 멀티 캐스트 세션이 요구된다. 패스워드 기반 인증된 키 교환 프로토콜은 인간이 기억할 수 있는 간단한 패스워드를 사용하여 키 교환 프로토콜에 참여하는 개체를 인증하고 이와 동시에 세션을 위한 강력한 키를 참여 각 개체들이 공유할 수 있도록 해준다. 이 프로토콜은 참여 개체가 소지하고 있는 공유 패스워드를 사용하여 인증하므로 공개 키 기반 인증에서 요구되는 공개 키 인증기관(CA)이나 ID 기반 인증에서 요구되는 비밀 키 생성자(private key generator)가 필요 없으므로, 신뢰센터를 두기 어려운 ad hoc 네트워크 환경에서 유용하게 사용될 수 있다.

패스워드 기반 인증된 키 교환 프로토콜에서는 키 교환에 참여하는 개체들이 외부에 노출되지 않은 신규 패스워드를 선택하고 공유한다. 만일 이 패스워드가 충분히 긴 랜덤 문자열이면 바로 세션 키로 사용될 수 있다. 그러나 실제에 있어서 긴 랜덤 문자열을 찾고 기억한다는 것은 어렵다. 인간이 기억 가능한 패스워드는 엔트로피가 낮으므로 사전공격(dictionary attack)에 취약하다. 그러므로 취약한 공유 패스워드로부터 강력한 세션 키를 유도해 내는 프로토콜 설계가 패스워드 기반 인증된 키 교환 프로토콜의 주요 관건이다.

1.1 관련된 연구들

Bellovin과 Merritt[2]는 공개 키 방식을 이용한 키 교환 프로토콜에 공유 패스워드를 이용한 대칭 키 암호 인증을 결합한 암호화된 키 교환(encrypted key exchange: EKE) 프로토콜을 처음으로 제안하였다. Bellovin 과 Merritt의 발표 이후 이것으로부터 변형된 여러 알고리듬들이 발표되었다[3]. EKE 프로토콜을 공개 키 기반 및 ID 기반 인증된 키 교환 프로토콜과 대비하여 패스워드 기반 인증된 키 교환 프로토콜이라 부른다.

그룹 구성원 간에 비밀 통신을 위한 키 교환을 그룹 키 교환이라 한다. Y. Kim 등[4]은 트리 기반 그룹 DH 프로토콜(tree-based group Diffie-Hellman : TGDH)을 제안하였다. TGDH 방식은 그룹 구성원을 모듈화할 수 있고 그룹별 키를 설정할 수 있으며 그룹 구성원 가입 및 탈퇴에 따른 키 갱신이 효율적이다[4,5]. 트리 기반 그룹 키 교환 프로토콜의 계산량은 키 트리의 높이에 비례한다. S. Lee 등[6]은 2진 트리 대신 3진 트리를 사용하여 키 트리 레벨을 낮춤으로써 계산량을 $O(\log_2^n)$에서 $O(\log_3^n)$로 줄일 수 있었다. Y. Kim 등은 프로토콜 설계에서 인증에 대한 부분은 고려를 하지 않았다. S. Lee 등은 F. Zhang 등[7]이 제안한 ID 기반 인증된 3자 키 교환 프로토콜을 3진 트리에 적용하여 타원곡선 pairing을 사용한 인증된 TGDH를 제안하였다.

1.2 연구동기 및 연구내용

본 논문에서는 3진 트리를 사용한 그룹 키 교환 프로토콜에 적용할 목적으로 A. Joux[8]가 제안한 3자 키 교환 프로토콜의 패스워드 기반 인증에 대하여 연구한다. A. Joux는 타원곡선 상에서 pairing을 사용하여 1 라운드 3자 키 교환 프로토콜을 제안하였으나 인증기능이 없어 man-in-the-middle attack에 취약하다. S. S. Al-Riyami 등[9]은 공개 키 인증서를 사용하여 인증 기능을 부여하였으며, F. Zhang 등은 ID를 사용하여 이 문제를 해결하였다. 하지만 공개 키 기반 인증과 ID 기반 인증을 위해서는 신뢰된 기관이 필요하다. 본 논문에서는 전술한 것처럼 ad hoc 네트워크에서 신뢰기관을 구축하기 어려운 상황에서의 응용을 위하여 공유 패스워드를 사용하여 A. Joux 프로토콜의 인증문제를 해결하고자 한다. 본 연구에서 제안하는 프로토콜은 대칭 키 암호알고리듬을 사용하여 A. Joux 프로토콜의 메시지를 암호화하여 전송하게 된다. 프로토콜 메시지를 단순히 대칭 키 암호화 할 경우 오프라인 사전공격(dictionary attack)을 당하게 되므로[10] 이를 해결하기 위하여 C. Boyd 등[11]이 제안한 사전공격 회피 기법을 적용한다.

제안하는 3자 키 교환 프로토콜과 기존의 패스워드 기반 인증된 프로토콜을 비교 검토한다. 비교대상을 설정하기 위하여 기존에 발표된 대표적인 패스워드 기반 인증된 그룹 키 교환 프로토콜[1,12,13]을 프로토콜 참여자가 3명인 경우로 한정하여 기술한다. 그리고 계산량 및 통신량 면에서 비교 검토하며, 여러 가지 공격에 대하여 제안된 프로토콜의 안전성도 검토한다.

2. 기존의 패스워드 기반 인증된 3자 키 교환 프로토콜

본 장에서는 본 논문에서 제안한 프로토콜의 비교를 위하여 기존에 발표된 패스워드 기반 인증된 키 교환 프로토콜을 소개한다. 기존에 발표된 패스워드 인증 키 교환 프로토콜 가운데 3자 키 교환을 목표로 개발된 것은 아직 발표된 바 없다. 모두가 그룹 키 교환 프로토콜이거나 2자 키 교환 프로토콜이다. 그래서 제안된 프로토콜과의 비교를 위하여 대표적으로 N. Asokan 등[1], E. Bresson 등[12], 그리고 황정연 등[13]의 그룹 키 교환 프로토콜을 그룹 크기가 3인 경우로 한정하여 기술한다.

2.1 N. Asokan 등의 3자 키 교환 프로토콜

프로토콜 절차는 다음과 같다. 위수가 p인 곱셈군 Z_P^*의 생성자를 g라 둔다. 그리고 프로토콜 참여자 A, B, C는 패스워드 pw를 공유하고 있다.

(1) $A \rightarrow B : g^a$

(2) $B \rightarrow A, C : \pi = g^{ab}$

(3) $A \rightarrow C : E_{pw}(c_A)$, 여기서 $c_A = \pi^{\hat{a}/a}$

$B \rightarrow C : E_{pw}(c_B)$, 여기서 $c_B = \pi^{\hat{b}/b}$

(4) $C \rightarrow A : c_A^c$

$C \rightarrow B : c_B^c$

프로토콜에서 $A \rightarrow B$는 참여자 A로부터 참여자 B로의 단일 전송(unicasting)을 의미한다. 그리고 E_{pw}는 대칭 키 알고리듬 E에 공유 패스워드 pw를 적용한 암호화를 의미한다. 4 라운드의 메시지 교환단계가 완료되면 각 개체는 아래와 같이 공유 비밀 키를 계산한다.

A : $K_A = (c_A{}^c)^{a/\hat{a}} = g^{abc}$

B : $K_B = (c_B{}^c)^{b/\hat{b}} = g^{abc}$

C : $K_C = \pi^c = g^{abc}$.

공유 비밀 키를 이용하여 적절한 방법에 따라 세션 키를 생성 할 수 있다.

2.2 E. Bresson 등의 3자 키 교환 프로토콜

$G = < g >$, 즉 G를 생성자가 g이고 위수가 q인 순환군이라 정의한다. $\overline{G} = G \backslash \{1\}$으로 표기한다. $h \in \overline{G}, \overline{G} = \{h^r | r \in \{1, \cdots, q-1\}\}$로 표현할 수 있다. 키 교환 프로토콜에 사용될 공유 패스워드는 pw이다. 블록의 크기에 따라 여러 개의 블록암호 알고리듬들을 정의한다. 두 그룹의 대칭 키 암호화 및 복호화 알고리듬을 각각 E, E' 과 D, D'로 표기한다. 프로토콜 절차는 다음과 같다

(1)
$x_1 \xleftarrow{R} [1, q-1]$
$v_1 \xleftarrow{R} [1, q-1]$
$g_1 = g_0^{v_1}$
$X_1 = \{g_1, g_1^{x_1}\}$
$A \rightarrow B : Fl_1 = E_{pw}(X_1)$

(2)
$x_2 \xleftarrow{R} [1, q-1]$
$X_1 = D_{pw}(Fl_1)$
$v_2 \xleftarrow{R} [1, q-1]$
$g_2 = g_1^{v_2}$
$X_2 = \{g_2, g_2^{x_2}, g_2^{x_1}, g_2^{x_1 x_2}\}$
$B \rightarrow C : Fl_2 = E_{pw}(X_2)$

(3)
$x_3 \xleftarrow{R} [1, q-1]$
$X_2 = D_{pw}(Fl_2)$
$v_3 \xleftarrow{R} [1, q-1]$
$g_3 = g_2^{v_3}$
$X_3 = \{g_3^{x_2 x_3}, g_3^{x_1 x_3}, g_3^{x_1 x_2}\} = \{\alpha_1, \alpha_2, \alpha_3\}$
$C \rightarrow A, B : Fl_3 = E'_{pw}(X_3)$

메시지 전송형태가 유니 캐스트인 단계 1, 2와 멀티 캐스트인 단계 3에서 서로 다른 형식의 대칭 키 암호 알고리듬을 사용하였다. 위의 각 단계는 선행단계가 완료되어야 다음 단계의 메시지가 처리되므로 각각의 단계는 1 라운드를 이룬다. 따라서 3 라운드의 메시지 교환이 요구된다. 메시지 교환이 끝나면 A, B는 Fl_3를 복호한다. 참여자들은 다음과 같이 공유 비밀 키를 계산한다.

$A: K_A = (\alpha_1)^{x_1} = g_3^{x_1 x_2 x_3}$

$B: K_B = (\alpha_2)^{x_2} = g_3^{x_1 x_2 x_3}$

$C: K_C = (\alpha_3)^{x_3} = g_3^{x_1 x_2 x_3}$

공유 비밀 키를 이용하여 세션 키 $sk = H(A \mid B \mid C \mid Fl_3 \mid K)$를 생성한다.

2.3 황정연 등의 3자 키 교환 프로토콜

다음과 같이 프로토콜 설명에 필요한 기호를 정의한다.

- g : 위수가 q인 곱셈 연산군 G의 생성자.
- pw : 프로토콜 참여자들이 소유한 패스워드.
- $E_{pw}()$: 패스워드 pw를 사용한 대칭 키 암호화.
- $D_{pw}()$: 패스워드 pw를 사용한 대칭 키 복호화.
- h : $\{0,1\}^* \rightarrow \{0,1\}^\ell$인 해쉬함수.
- r_i : 프로토콜 참여자 i 가 선택한 랜덤한 값.
- K : 공유 비밀 키.

라운드 1 : $A \rightarrow B, C : E_{pw}(g^{r_A})$

$B \rightarrow A, C : E_{pw}(g^{r_B})$

$C \rightarrow A, B : E_{pw}(g^{r_C})$

라운드 2 : $A \rightarrow B, C : Z_A = h(g^{r_A r_C}) \oplus h(g^{r_A r_B})$

$B \rightarrow A, C : Z_B = h(g^{r_A r_B}) \oplus h(g^{r_B r_C})$

$C \rightarrow A, B : Z_C = h(g^{r_A r_C}) \oplus h(g^{r_B r_C})$

위의 프로토콜은 2라운드의 메시지 전송이 요구된다. 메시지 전송이 완료되면 각 참여자들은 $h(g^{r_A r_B}), h(g^{r_B r_C})$ 그리고 $h(g^{r_C r_A})$ 값 중에서 자신이 모르는 항목을 수신된 Z_i 값과 알고 있는 해쉬 값으로부터 구할 수 있다. 예를 들어 A는 $h(g^{r_B r_C}) = Z_B \oplus h(g^{r_A r_B})$와 같이 구할 수 있다. 각 참여자는 동일하게 아래와 같이 공유 비밀 키를 계산한다.

$K = h(h(g^{r_A r_B}) \mid h(g^{r_B r_C}) \mid h(g^{r_C r_A}))$

3. 제안된 패스워드 기반 인증된 3자 키 교환 프로토콜

본 장에서는 A. Joux가 제안한 3자 키 교환 프로토콜의 문제점을 기술하고 해결방안을 제시한다. 우선 프로토콜의 기반이 되는 타원곡선 상의 pairing과 BDHP 가정을 기술한다.

3.1 타원곡선 pairing과 BDHP 가정

여기서 사용되는 기호는 Boneh와 Franklin[14]의 것을 따른다. G_1을 위수가 소수 q인 생성자 P에 의해서 만들어진 순환 덧셈 군(cyclic additive group)이고, G_2 또한 같은 위수 q의 순환 곱셈 군(cyclic productive group)이라 정의한다. G_1과 G_2에서 이산대수문제(the discrete logarithm problems : DLP)가 어렵다고 가정한다. $e: G_1 \times G_1 \rightarrow G_2$를 다음과 같은 조건을 만족하는 pairing 이라 두자.

1. Bilinear :
   $e(P_1 + P_2, Q) = e(P_1, Q)e(P_2, Q)$
   $e(P, Q_1 + Q_2) = e(P, Q_1)e(P, Q_2)$
2. Non-degenerate :
   $e(P, Q) \neq 1$인 $P \in G_1$과 $Q \in G_1$가 존재 한다.
3. Computability :
   모든 $P, Q \in G_1$에 대하여 $e(P, Q)$를 연산하는 효율적인 알고리듬이 존재한다.

pairing은 G_1상에서 정의된 타원곡선 상의 두 점을 G_2 상의 한 원소로 사상하는 것이다. Weil 또는 Tate pairing이 pairing 연산에 사용될 수 있다.

정리 1: Bilinear Diffie-Hellman problem(BDHP)
주어진 $P, aP, bP, cP \in G_1$에 대하여 $e(P,P)^{abc}$를 계산한다. 여기서 a, b, c는 Z_q^*로부터 임의로 선택된 랜덤변수이다. 어떤 알고리듬이

$Pr[A(P, aP, bP, cP) = e(P,P)^{abc}] \geq \epsilon$

을 만족하면 ϵ의 이점으로 BDHP를 푼다고 말하여진다.

BDHP 가정 : BDHP가 어렵다고 가정한다. 즉, 이것은 주목할 만한 확률(non-negligible probability)로 BDHP를 풀 다항식 시간(polynomial time) 알고리듬이 없음을 의미한다. 공격자가 P, aP, bP, cP를 알지라도 $e(P,P)^{abc}$ 값을 계산하기가 어렵다는 의미이다.

3.2 A. Joux 프로토콜의 문제점

A. Joux는 pairing을 사용하여 1 라운드에 실행되는 3자 키 교환 프로토콜을 제안하였다. 프로토콜 참여자 A, B, C는 각각 랜덤변수 a, b, c를 생성하고 생성자 P에 스칼라 곱셈을 취한 값을 멀티 캐스팅 한다.

(1) $A \rightarrow B, C : aP$
(2) $B \rightarrow C, A : bP$
(3) $C \rightarrow A, B : cP$

이어서 각 참여자는 아래와 같이 공유 비밀 키를 계산한다.

$A : K_A = e(bP, cP)^a = e(P, P)^{abc}$
$B : K_B = e(aP, cP)^b = e(P, P)^{abc}$
$C : K_C = e(aP, bP)^c = e(P, P)^{abc}$

각 참여자가 보내는 메시지에는 송신자를 인증할 어떠한 정보도 포함되어 있지 않으므로, 악의적인 다른 개체 D가 A의 통신 메시지 aP를 제거하고 대신 aP를 전송하면 D는 B, C와 키 공유에 성공할 수 있다. 따라서 인증 기능이 없으며 결과적으로 man-in-the-middle attack에 취약하다. 이 문제를 해결하기 위하여 S. S. Al-Riyami 등은 공개 키 인증서를 사용하는 방법을, F. Zhang 등은 ID를 사용한 방법을 제시하였다. 다음 절에서는 이 문제를 해결하는 다른 방법을 제시 한다.

3.3 제안된 프로토콜

다음과 같이 프로토콜 설명에 필요한 기호를 정의한다.

- P : 위수가 q인 덧셈 연산군 G_1의 생성자.
- A, B, C : 프로토콜 참여자.
- pw : 크기가 N인 패스워드 집합에서 균일하게 선택한 모든 프로토콜 참여자가 공유한 패스워드.
- $E_{pw}()$: 패스워드 pw를 사용한 대칭 키 암호화.
- $D_{pw}()$: 패스워드 pw를 사용한 대칭 키 복호화.
- $H_1(), H_2(), H_3()$: 서로 다른 해쉬함수.
- r_i : 프로토콜 참여자 i가 선택한 랜덤한 값.
- K : 공유 비밀 키.

사전에 프로토콜 참여자 A, B, C는 아래와 같이 3개의 프로토콜 메시지 교환용 암호 키를 계산한다.

$P_A = H_1(A, B, C, pw)$
$P_B = H_2(A, B, C, pw)$
$P_C = H_3(A, B, C, pw)$

3.3.1. 단순 대칭 키 암호화의 문제점

3.2절에서 서술한 A. Joux 프로토콜에 묵시적 인증(implicit authentication) 기능 추가와 man-in-the-middle attack을 해결하기 위해 단순히 대칭 키 암호화만을 적용할 경우 오프라인 사전공격의 일종인 분할공격(partition attack)을 당하게 된다.

단순 패스워드 암호화 $E_{pw}(G_A)$를 생각해 보자. 여기서 $G_A = (X_A, Y_A)$이다. 공격자는 가능한 모든 패스워드를 pw_i를 사용하여 $E_{pw}(G_A)$를 복호한다. 만약 pw_i가 올바르지 않으면 복호된 결과는 랜덤 쌍 (X_i, Y_i)이 될 것이다. 만약 (X_i, Y_i)가 타원곡선상의 점이라면

$$Y_i^2 = g(X_i) \bmod p$$

를 만족한다. 여기서 $g(X)$는 타원곡선 다항식이다. 즉 pw_i가 올바르면 $g(X_i)$는 2차 잉여류이다. Hasse[15]의 이론에 의하면 타원곡선이 정의된 유한체내의 임의 원소 X_i가 타원곡선 x 축의 좌표가 될 확률은 거의 1/2이다. 따라서 공격자가 한 개의 유효한 $E_{pw}(G_A)$를 획득하면 가능한 패스워드 공간을 반으로 줄일 수 있다. 이것은 패스워드 공간 크기의 log 값 규모의 유효한 세션 값들만 있으면 패스워드를 추출할 수 있음을 의미한다. C. Boyd는 untwisted 타원곡선과 twisted 타원곡선을 랜덤하게 선택하여 암호화함으로써 복호되는 모든 X_i의 $g(X_i)$가 2차 잉여류가 되게 하여 패스워드 추측이 불가능하게 하였다.

3.3.2 분할공격에 강인한 패스워드 기반 인증된 3자 키 교환 프로토콜

본 절에서는 A. Joux의 프로토콜에 C. Boyd의 기법을 적용하여 분할공격에 강인한 패스워드 기반 인증된 3자 키 교환 프로토콜을 제시한다.

$\Gamma = GF(q)$라 두자. 여기서 $q = p^m, p > 3$ 이다. 타원곡선 $E_{a,b} : Y^2 = X^3 + aX + b$을 정의한다. 타원곡선 $E_{a,b}$의 생성점(generating point)를 G로 표기한다.

타원곡선의 오른쪽 다항식을 $g(X)$라 둔다. 어떤 $\nu \in \Gamma^*$에 대하여 $a' = \nu^2 a, b' = \nu^3 b$라 둔다. 그리고 $g_\nu(X) = \nu^3 g(X/\nu)$라 정의한다. 그러면 $E_{a,b}$의 twisted 타원곡선 $E_{a',b'}$은 $Y^2 = g_\nu(X)$이다. $E_{a',b'}$의 생성점을 H로 표기한다. 아래 정리 2는 본 논문에서 다루는 분할 공격의 방어기법을 위한 기본 이론을 제공한다.

[정리 2][15]
C={$X \in \Gamma \mid g(X)$는 Γ에서 2차 잉여류}
T={$X \in \Gamma \mid g_\nu(\nu X)$는 Γ에서 2차 잉여류}라 두자.

그러면 다음이 성립한다.

1. $C \cap T = \varnothing$. 만일 $g(X) \neq 0$이면 $X \in C \cup T$이다.
2. $X \in C \leftrightarrow g(X) \neq 0$이고 $(X, Y) \in E_{a,b}$인 Y가 존재한다.
3. $X/\nu \in T \leftrightarrow g(X/\nu) \neq 0$이고 $(X, Y) \in E_{a',b'}$인 Y가 존재한다.

위의 정리는 타원곡선이 정의되는 유한체 Γ의 임의 원소는 반드시 $E_{a,b}$ 또는 $E_{a',b'}$의 x 좌표점이 됨을 의미한다. 이 정리는 untwisted 타원곡선과 twisted 타원곡선을 사용하여 분할공격을 방어하는 기본 아이디어를 제공한다.

이제 분할 공격에 대응하는 패스워드 기반 인증된 Joux 프로토콜에 대하여 설명한다. 본 논문에서 제시하는 자세한 프로토콜 절차는 다음과 같다. 참여자 A를 3자 키 교환 프로토콜의 그룹리더(group leader)로 선정한다.

1. A는 프로토콜 실행을 위하여 $E_{a,b}$ 혹은 $E_{a',b'}$를 랜덤하게 선택한다.
2. A는 랜덤값 r_A를 선택한다. 그리고 선택된 타원곡선이 $E_{a,b}$이면 $G_A = r_A G$를 그렇지 않으면 $H_A = r_A H$를 계산한다.
3. A는 $G_A = (X_A, Y_A)$(혹은 $H_A = (X_A, Y_A)$)를 (X_A, y_A)로 압축한다. 여기서 y_A는 압축된 형식에서 Y_A를 나타내는 단일 비트이다.
4. A는 압축된 점을 공유 패스워드로 암호화하여 B, C에게 멀티 캐스팅 한다. 이때 단계 1에서 선택된 타원곡선이 $E_{a,b}$이면 $E_{p_A}(X_A \mid y_A)$를, 그렇지 않으면 $E_{p_A}(X_A/\nu \mid y_A)$를 전송한다.
5. B와 C는 수신된 메시지를 복호하여 $(X \mid y_A)$를 얻는다. 만일 $g(X)$이 2차 잉여류이면 A가 선택한 타원곡선은 untwisted 타원곡선이고 $X_A' = X'$이다. 그렇지 않으면 A가 선택한 타원곡선은 twisted 타원곡선이고 $X_A' = \nu X'$이다.
6. B와 C는 결정한 x축 좌표 점 X_A'과 y_A로부터 점 G_A' 혹은 H_A'을 복구한다. 그리고 B와 C는 A가 선택한 것으로 판단한 곡선에 따라 각각 $G_B = r_B G$ (혹은 $H_B = r_B H$)와 $G_C = r_C G$ (혹은 $H_C = r_C H$)를 계산한다.
7. B와 C는 $G_B = (X_B, Y_B)$ (혹은 $H_B = (X_B, Y_B)$)와 $G_C = (X_C, Y_C)$ (혹은 $H_C = (X_C, Y_C)$)를 $(X_B \mid y_B)$와 $(X_C \mid y_C)$로 압축한다. 여기서 y_B와 y_C는 각각 압축된 형식에서 Y_B와 Y_C를 나타내는 단일 비트이다.
8. B와 C는 $E_{p_B}(X_B \mid y_B)$(혹은 $E_{p_B}(X_B/\nu \mid y_B)$)와 $E_{p_C}(X_C \mid y_C)$(혹은 $E_{p_C}(X_C/\nu \mid y_C)$)를 각각 멀티 캐스팅 한다.
9. A, B, C는 각각 프로토콜 참여 상대들로부터 수신한 정보를 복호한 후, 압축된 점을 복원한다. 선택된 타원곡선에 따라 A는 B, C로부터 G_B' (혹은 H_B') 와 G_C' (혹은 H_C')을 얻게 되고, B는 C로부터 G_C' (혹은 H_C')를 얻게 되며, C는 B로부터 G_B' (혹은 H_B')를 얻게 된다.

그림 1은 선택된 타원곡선이 untwisted 타원곡선 $E_{a,b}$일 때의 절차는 나타낸다. 그림에서 프로토콜 절차를 전송단계와 각 주체의 계산단계로 구분하여 표기하였다. 전송단계 (1)은 A가 계산단계 (A.1)을 처리 후 메시지를 멀티 캐스팅, 전송단계 (2-B)는 B가 계산단계 (B.1)에서 A로부터 수신한 메시지를 처리한 후 자신의 메시지를 멀티 캐스팅, 그리고 전송단계 (2-C)는 C가 (C.1)에서 A로부터 수신한 메시지를 처리한 후 자신의 메시지를 멀티 캐스팅하는 과정을 나타낸다. 계산단계 (A.2), (B.2), 그리고 (C.2)는 각 개체가 상대방으로부터 수신한 메시지를 복호한 후 공유 비밀 키를 계산하는 과정을 나타낸다. 이상과 같은 절차를 통하여 제안된 프로토콜은 2라운드에 종료된다.

개체 A, B, C는 선택된 타원곡선에 따라 아래와 같이 공유 비밀 키를 계산한다.

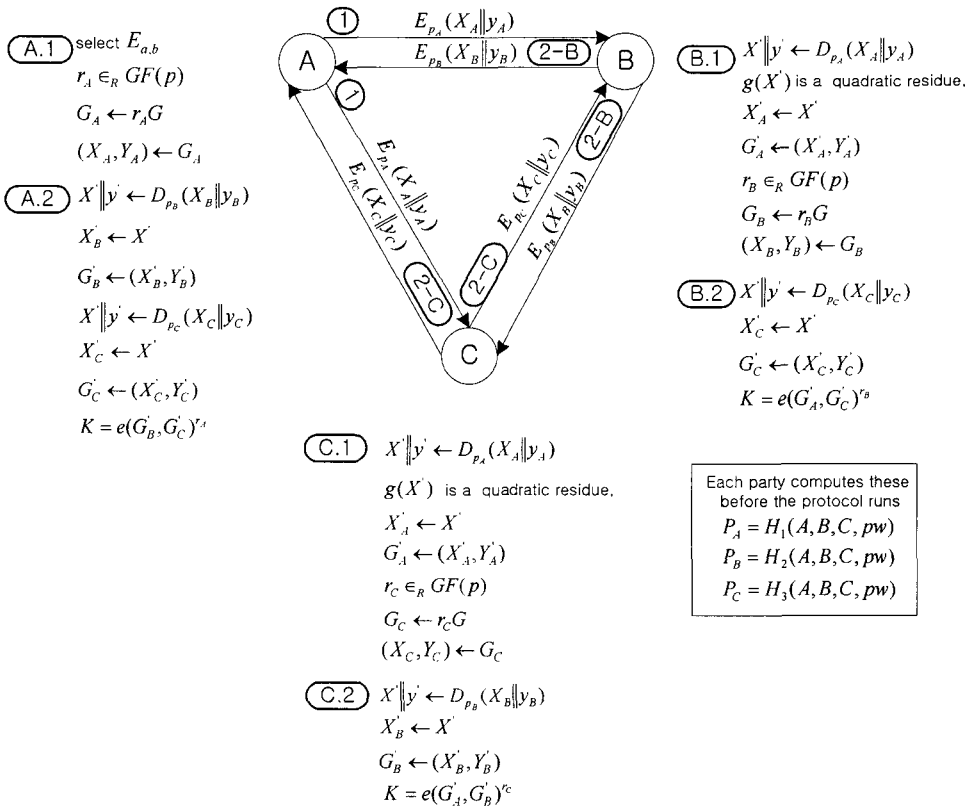


그림 1. 제안한 패스워드 기반 인증된 3자 키 교환 프로토콜 : 선택된 타원곡선이 untwisted 타원곡선 $E_{a,b}$일 때.

$A: K_A = e(G'_B, G'_C)^{r_A} = e(G, G)^{r_A r_B r_C}$ 혹은
$K_A = e(H'_B, H'_C)^{r_A} = e(H, H)^{r_A r_B r_C}$
$B: K_B = e(G'_A, G'_C)^{r_B} = e(G, G)^{r_A r_B r_C}$ 혹은
$K_B = e(H'_A, H'_C)^{r_B} = e(H, H)^{r_A r_B r_C}$
$C: K_C = e(G'_A, G_B)^{r_C} = e(G, G)^{r_A r_B r_C}$ 혹은
$K_C = e(H'_A, H'_B)^{r_C} = e(H, H)^{r_A r_B r_C}$

계산된 공유 비밀 키를 이용하여 다른 적절한 방법으로 새로운 세션 키를 계산할 수 있다. 세션 키 계산에 관한 토의는 본 논문의 범위에서 제외한다.

4. 안전성 검토 및 타 프로토콜과의 비교

4.1 안전성 검토

키 교환 프로토콜의 안전성 검토 시 고려되어야 할 안전성의 종류와 정의는[16,17]을 참고하였다.

1) 알려진 세션 키 안전성(known session key security)

공격자(adversary)가 이전의 세션 키를 알았더라도 현재 수행 중인 프로토콜의 세션 키를 얻을 수 없어야 한다. 세션 키를 알아내는 것은, 예를 들어 P, aP, bP, cP로부터 $K_A = e(bP, cP)^a$를 구하는 것은, BDHP를 푸는 것과 동일하다. 그리고 세션 마다 다른 랜덤 값을 선택하므로 이전의 세션 키로부터 현재의 세션 키를 알 수 없다. 따라서 본 프로토콜은 *알려진 세션 키 안전성*을 제공한다.

2) 전방향 안전성(forward secrecy)

프로토콜에 참여한 한 개체 이상의 장기 개인 키(long-term key)가 노출되더라도 이전의 세션 키의 기밀성에 영향을 미치지 않아야 한다. 공격자가 패스워드 pw를 안다고 가정하자. 이전의 동일 세션에서 획득한 메시지 $G'_A(=r'_A G)$, $G'_B(=r'_B G)$, 그리고 $G'_C(=r'_C G)$로부터 세션 키 $SK = e(G, G)^{r'_A r'_B r'_C}$ 를 구하는 것은 BDHP를 푸는 것과 동일하다. 따라서 제안된 프로토콜에서 세션 키는 BDHP의 어려움에 기초하고 있으므로 장기간 사용되는 패스워드가 노출 되더라도 이전의 세션 키는 노출되지 않으므로

*전방향 안전성*을 제공한다.

3) 알려지지 않는 키 공유 불가성(No unknown key-share)

개체 A가 개체 B와 키를 공유하고 있을 때 공격자 C가 A를 강요하여 키를 공유할 수 있으면 프로토콜은 *알려지지 않는 키 공유 공격*을 당하고 있다고 한다. C가 합법적인 메시지를 보내고 그 응답을 얻어서 패스워드를 추출 할 수 있으면 원하는 대로 A, B 와 세션 키를 공유할 수 있다.

공격자가 A로 위장하여 이전의 세션 메시지 $E_{P_A}(X_A \| y_A)$를 프로토콜 참여자 B와 C에게 보냈다고 가정하자. A는 B, C로부터 $E_{P_B}(X_B' \| y_B)$와 $E_{P_C}(X_C' \| y_C)$를 받지만 이들 메시지로부터 패스워드를 추출하기는 불가능하다. 그러므로 제안된 프로토콜은 *알려지지 않는 키 공유 불가성*을 만족한다고 할 수 있다.

4) 키 제어 불가성(No key control)

프로토콜 참여자 중에서 특정 참여자 또는 공격자가 미리 선택된 값이나 예측할 수 있는 값으로 세션 키를 생성하도록 강요할 수 없어야 한다. 제안된 프로토콜의 세션 키는 $SK = e(G, G)^{r_A r_B r_C}$ 혹은 $SK = e(H, H)^{r_A r_B r_C}$로 주어지므로 특정 참여자의 임시 키 ($r_A$, r_B 혹은 r_C) 에 의하여 세션 키가 원하는 값으로 제어되지 않으므로 *키 제어 불가성*을 만족한다.

5) 키 탈취 위장 불가성(No key-compromise impersonate)

프로토콜 한 참여자 A의 장기 개인 키를 탈취였더라도 공격자가 다른 참여자에 대하여 참여자 A로 위장 할 수 없어야 한다. 패스워드 기반 인증 키 교환 프로토콜은 오직 패스워드에 의존하여 개체 인증을 하고 인증을 위하여 제 3의 신뢰 기관을 두지 않으므로 근본적으로 *키 탈취 위장*에 취약하다. 따라서 제안된 프로토콜도 *키 탈취 위장*에 취약하다. 암호 시스템의 응용 환경에 따라서 시스템의 복잡성과 안전성 간의 타협이 요구되는 부분이다.

6) Man-in-the-middle attack

공격자가 원래 메시지를 제거하고 다른 것으로 대체 전송하여 프로토콜 실행에 성공하면 man-in-the-middle attack에 취약하다. A를 위장한 공격자 D가 패스워드 pw'를, 세션 참여자 B와 C는 패스워드 pw를 가자고 있다고 자정하자. A는 B, C와 서로 다르게 $P_A' = (A, B, C, pw')$, $P_B' = (A, B, C, pw')$, 그리고 $P_C' = (A, B, C, pw')$를 계산하게 되므로 세션은 실행될 수 있을 지라도 B, C와 동일한 세션 키를 공유할 수는 없게 된다. 그러므로 제안된 프로토콜에 대하여 공격자는 공유 패스워드를 모르는 한 다른 메시지를 주입하여 키 교환에 성공할 수 없으므로 man-in-the-middle attack에 강인하다.

4.2 타 프로토콜과의 비교

표 1은 본 논문에서 제안한 프로토콜과 2장에서 소개한 3개의 프로토콜의 계산량과 통신량을 비교한 것이다. 연산 비용면에서 타원곡선 상에서 pairing 연산이 가장 복잡하고, 타원곡선 스칼라 곱셈이 이에 대응되는 곱셈 군에서의 지수 연산에 비하여 빠르다고 알려져 있다[18]. Pairing 연산은 대략적으로 지수 연산의 3배 정도 된다고 가정한다[12,19,20]. 공식적인 발표는 없었으나 최근에는 지수연산과 동일하게 보는 경우도 있다.

알고리듬의 비교는 그것이 사용되는 환경에 따라서 기준이 바뀔 수 있다. 예를 들어 무선 데이터 통신 환경에서는 근본적으로 브로드캐스팅의 특성을 지니고 있으며, 유선을 사용한 인터넷에서는 근본적으로 단일 메시지 전송의 특성을 지닌다. 본 논문에서는 무선 ad hoc 네트워크 환경에서 프로토콜 사용을 가정한다. 따라서 단일 전송과 브로드 캐스팅을 동일한 비용으로 가정한다.

표 1. 계산량과 통신량의 비교

Protocols	computation				communication	
	P	SM	QR	E	Round/ Pass	Msg Length
N. Asokan 등	-	-	-	9	4/6	6|g|
E. Bresson 등	-	-	-	13	3/3	9|g|
황정연 등	-	-	-	9	2/6	6|g|
Proposed	3	5	2	3	2/3	3|p|

P : no. of pairing, SM : no. of scalar multiplication over elliptic curve, QR : no. of quadratic residue, E : no. of exponentiation, Round : no. of rounds, Pass : no. of message passes, Msg Length : message length.

표에서 연산횟수는 프로토콜 1회 실행에 소요되는 전체 연산량을 나타내고, 메시지 길이는 전송되는 전체 메시지 길이를 의미한다. 타원곡선의 경우 점의 압축을 고려하여 1개의 점은 1개의 유한요소로 취급하였다. Hashing, 암호화/복호화, 모듈러 역수 연산, 모듈러 곱셈 연산은 다른 연산에 비하여 계산량이 적으므로 비교 기준에서 제외한다.

제안된 프로토콜의 단일 메시지 길이($|P| \approx 250$|)가 나머지 프로토콜의 단일 메시지 길이($|g| \approx 1024$|)보다 훨씬 짧다[20]. 그리고 라운드 수 및 통신 횟수에 있어서도 가장 우수하다. 따라서 통신량 면에서는 제안된 프로토콜이 가장 우수하다.

Pairing 연산 3회는 지수 연산 9회와 대략적 대등하게 볼 수 있으므로, 기존의 프로토콜 가운데 최저 계산량인 지수 연산 9회에 비하여 제안된 프로토콜은 지수 연산 3회, 스칼라 연산 5회, 그리고 2차 잉여류 연산 2회가 추가적으로 요구된다. 하지만 pairing 연산의 효율성이 증가하고 있고 스칼라 연산과 2차 잉여류 연산은 타원곡선의 기저체에서 이루어지므로, 전체 연산 중에 추가 연산이 차지하는 비중은 첨자 줄어 들 수 있을 것으로 기대된다.

트리기반 그룹 키 설정 프로토콜에서 가입이나 탈퇴 이벤트가 발생하면 이벤트가 발생한 최하위 서브 그룹 키가 갱신되고, 이것이 상위 레벨로 보내어져 상위 레벨 서브 그룹 키 갱신이 이루어지고 최종적으로 최 상위 레벨에 도달하면 전역 그룹 키 갱신이 이루어진다[21]. Pairing 기반 키 일치 프로토콜을 사용하면 이벤트가 발생한 최하위 서브 트리에서만 참여 개체가 협력하여 서브 그룹 키를 만든다. 그리고 이것을 상위 트리로 보내면, 상위 레벨에서는 나머지 그룹 멤버들에게 키 갱신용 데이터(blinded subgroup key)만 전송해 주면 지역에서 각각 그룹 키 갱신 계산이 가능한 장점을 누릴 수 있다. 예를 들어 개체 A, B, C가 그룹 멤버이고 현재 각각 aP, bP, cP 값을 이용하여 서브 그룹 키 $e(P,P)^{abc}$를 가지고 있다. A가 하위 레벨로부터 새운 키 a'을 받아 블라인드된 키 $a'P$을 B와 C에게 전해주면 이들은 각각 $e(a'P,cP)^b$, $e(a'P,bP)^c$를 계산하여 서브 그룹 키를 갱신할 수 있다. 따라서 최하위 레벨을 제외한 상위 레벨에서는 서버 그룹 키 일치 프로토콜을 실행 하지 않고도 서버 그룹 키를 갱신할 수 있다. 하지만 paring을 사용하지 않는 기존의 패스워드 인증된 3자 키 교환 프로토콜에서는 이 장점을 누릴 수 없다. 따라서 트리기반 그룹 키 일치 프로토콜에 본 논문에서 제안한 프로토콜을 사용하면, 처음에 그룹 키가 설정된 이후에는 그룹 키 갱신 시 이벤트가 발생한 최하위 서버 그룹을 제외한 나머지 멤버들은 지역에서 1회의 pairing 및 지수 연산만으로 그룹 키 갱신이 가능하므로, 앞서 설명한 계산상의 열세를 극복할 수 있다.

5. 결 론

본 논문은 A. Joux 프로토콜의 패스워드 인증을 처음으로 제안하였으며, 트리 기반 그룹 키 일치 프로토콜의 기반 프로토콜로의 사용을 검토하였다. 논문에서 제안한 프로토콜은 기존의 패스워드 인증된 3자 키 일치 프로토콜보다 통신적 측면에서 우수하다. 반면에 pairing 연산의 사용에 따른 비용증가로 계산적 측면에서는 열세이다. 하지만 트리기반 그룹 키 일치 프로토콜에서 제안된 프로토콜을 사용하면, 그룹 키 갱신 시 이벤트가 발생한 최하위 서버 그룹에서만 3자 키 일치 프로토콜을 실행하고 나머지 멤버들은 지역에서 1회의 pairing 및 지수 연산만으로 그룹 키 갱신이 가능하므로 계산상의 열세를 극복할 수 있다.

참 고 문 헌

[1] N. Asokan and Philip Ginzboorg, "Key Agreement in Ad-Hoc Networks," *Computer Communications*, Vol.23, pp. 1627-1637, 2000.

[2] S. M. Bellovin and M. Merritt, "Encrypted Key Exchange : Password-Based Protocols Secure Against Dictionary Attacks." In *Proceeding of IEEE Symposium on Research in Security and Privacy*, IEEE Computer Society Press, pp. 72-84, 1992.

[3] C. Boyd and A. Mathuria, *Protocols for Authentication and Key Establishment*, Springer-Verlag, Berline, 2003.

[4] Y. Kim, A. Perrig, and G. Tsudik. "Simple and Fault-Tolerant Key Agreement for Dynamic Collaborative Groups." S. Jajodia, editor, In *Proceeding of 7th ACM Conference on Computer and Communications Security*, ACM

Press, Athens, Greece, pp. 235-244, 2000.

[5] R. Barua, R. Dutta and P. Sarkar, " Provably Secure Authenticated Tree Based Group Key Agreement Protocol using Pairing," *Cryptology ePrint Archive,* Report 2004/122, 2002.

[6] S. Lee, Y. Kim, K. Kim, and D. Ryu, "An Efficient Tree Based Group Key Agreement Using Bilinear Map," *ACSN2003*, China, LNCS Vol.2846, Springer-Verlag, pp. 357-371, 2003.

[7] F. Zhang, S. Liu, and K. Kim, "ID-based One Round Authenticated Tripartite Key Agreement Protocol with Pairings," *Cryptology ePrint Archive*, Report 2002/122, 2002.

[8] A. Joux, "A One Round Protocol for Tripartite Diffie-Hellman," In W. Bosman, editor, *Proceedings of Algorithmic Number Theory Symposium-ANTS IV*, LNCS Vol.1838, Springer-Verlag, pp. 385-394, 2000.

[9] S. S. Al-Riyami and K.G. Paterson, "Tripartite Authenticated Key Agreement Protocols from Pairings", In *Proceeding of IMA Conference on Cryptography and Coding*, LNCS Vol.2898, pp. 332-359, 2003.

[10] S. Patel, "Number Theoretic Attacks on Secure Password Schemes," in *Proceedings of the Symposium on Security and Privacy*, IEEE, pp. 236-247, 1997.

[11] C. Boyd, P. Montague and K. Nguyen, "Elliptic Curve Based Password Authenticated Key Exchange Protocols", In *Proceedings of the Information Security and Privacy (ACISP 2001)*, LNCS Vol.2119, Springer-Verlag, pp. 487-501, 2001.

[12] E. Bresson, O. Chevassut and D. Pointcheval, "Group Diffie-Hellman Key Exchange Secure Against Dictionary Attacks," In *Proceedings of Asiacrypt '02*, LNCS Vol.2501, Springer-Verlag, pp. 497-514, 2002.

[13] 황정연, 최규영, 이동훈, 백종명, "효율적인 패스워드 기반 그룹 키 교환 프로토콜", 정보보호학회 논문지, 제 14권 제 1호, pp. 47-58, 2004.

[14] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," in J. Kilian, editor, *advances in Cryptology-CRYPTO 2001*, LNCS Vol.2139, Springer-Verlag, pp. 213-229, 2001.

[15] I. F. Blake, G. Seroussi, and N. P. *Smart, Elliptic Curves in Cryptography*, LMS Lecture Notes Series 265, CUP, 1999.

[16] S.Blake-Wilson, D. Jonson, and A. Menzes, "Key Agreement Protocols and Their Security Analysis," In *Proceedings of the sixth IMA International Conferences on Cryptography and Coding*, LNCS Vol.1355, Springer-Verlag, pp. 30-45, 1997.

[17] S. Blake-Wilson and A. Menezes. "Authenticated Diffie-Hellman Key Agreement Protocols." In S. Tacares and H. Meijer, editors, 5th *Annual Workshop on Selected Areas in Cryptography (SAC'98), LNCS* Vol.1556, Springer-Verlag, pp. 339-361, 1998.

[18] Z. Cheng, L. Vasiu and R. Comely, "Pairing-Based One-Round Tripartite Key Agreement Protocols," *Cryptology ePrint Archive*, Report 2004/79, 2004

[19] R. Barua, R. Dutta and P. Sarkar, "Extending Joux's Protocol to Multi Party Key Agreement," *Cryptology ePrint Archive*, Report 2003/62, 2003.

[20] P. Barreto and H.Y Kim and M Scott, "Efficient Algorithms for Pairing-Based Cryptosystems," *Advances in Crytology-Crypto' 2002*, LNCS Vol.2442, Springer-Verlag, pp. 354-386, 2002.

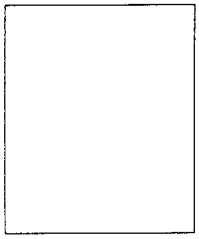
[21] 박명호, 이경현, "피어그룹을 위한 ID 기반의 그룹 키 관리 프로토콜," 멀티미디어학회논문지, 제 7권 7호, pp. 922-933, 2004.

이 상 곤

1986년 2월 경북대학교 전자공학과 졸업(학사)
1988년 2월 경북대학교 대학원 전자공학과 졸업(석사)
1993년 2월 경북대학교 대학원 전자공학과 졸업(박사)
1991년 3월~1997년 2월 창신대학 정보통신과 조교수
1997년 3월~현재 동서대학교 인터넷공학부 조교수
관심분야 : 암호 프로토콜, 네트워크 보안, 자바기술

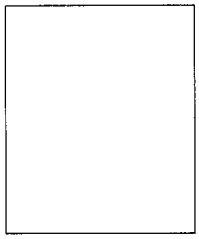
이 훈 재

1985년 경북대학교 전자공학과 졸업(학사)
1987년 경북대학교 대학원 전자공학과 졸업(석사)
1998년 경북대학교 대학원 전자공학과 졸업(박사)
1987년 2월~1998년 1월 국방과학연구소 선임연구원
1998년 3월~2002년 2월 경운대학교 컴퓨터공학과 조교수
2002년 3월~현재 동서대학교 인터넷공학부 조교수
관심분야 : 정보보안, 네트워크 보안, 스마트카드 보안, etc.



박 종 욱

1986년 경북대학교 전자공학과 졸업(학사)
1988년 경북대학교 대학원 전자공학과 졸업(석사)
2002년 경북대학교 대학원 전자공학과 졸업(박사)
2000년 2월~현재 국가보안기술연구소 책임연구원
관심분야 : 정보통신보안 etc.



윤 장 홍

1982년 경북대학교 전자공학과 졸업(학사)
1984년 경북대학교 대학원 전자공학과 졸업(석사)
1997년 경북대학교 대학원 전자공학과 졸업(박사)
1987년~2000년 1월 31일 국방과학연구소 팀장
2000년 2월 1일~현재 국가보안기술연구소 팀장
관심분야 : 정보보호시스템, 센서네트워크