情報保護學會論文誌
第16卷 第1號, 2006. 2

비대칭 컴퓨팅 환경을 위한 ID-기반의 인증된 키 동의 프로토콜*

최 규 영,[1†] 황 정 연,[1] 이 동 훈,[1‡] 홍 도 원[2]
[1]고려대학교, [2]한국전자통신연구원

ID-based Authenticated Key Agreement for Unbalanced Computing Environment*

Kyu-young Choi,[1†] Jung-yeon Hwang,[1] Dong-hoon Lee,[1‡] Do-won Hong[2]
[1]Center for Information Security Technology(CIST), Korea University
[2]Electronics and Telecommunications Research Institute(ETRI)

요 약

키 동의 프로토콜은 가장 기본적이고 널리 사용되는 암호 프로토콜 중 하나이다. 본 논문에서는 bilinear map을 이용한 효율적인 키 동의, 즉 서버와 저 전력 클라이언트를 위한 ID-기반의 인증된 키 동의 프로토콜을 제안한다. 특히 본 논문에서는 저 전력 클라이언트를 고려하여 클라이언트 측의 pairing 연산과 같은 복잡한 연산을 사용하지 않았다. 제안한 키 동의 프로토콜은 signcryption을 이용하며 랜덤 오라클 모델에서 그 안전성을 제공한다.

ABSTRACT

Key Agreement protocols are among the most basic and widely used cryptographic protocols. In this paper we present an efficient ID-based authenticated key agreement (AKA) protocol by using bilinear maps, especially well suited to unbalanced computing environments : an ID-based AKA protocol for Server and Client. Particularly, considering low-power clients' devices, we remove expensive operations such as bilinear maps from a client side. Our protocol uses signcryption and provide security in random oracle model.

Keywords : *Key Agreement, ID-based Cryptosystem, Signcryption*

Ⅰ. 서 론

1. 배경

현대의 많은 협업과 분산 환경에서 인증된 키 동의는 매우 중요한 문제 가운데 하나이다. 키 동의 프로토콜은 분배된 키를 소유한 사용자들과의 비밀 통신을 목적으로 한다. 그리고 이러한 키 동의 프로토콜에 어떤 의도된 사용자들에 대한 상호 인증을 제공하는 키 동의 프로토콜을 인증된 키 동의(AKA) 프로토콜이라 한다. 다양한 인증 기법들 중 전형적인 인증서 기반의 공개키 기반 구조(Public Key Infrastructure, PKI)는 인증하고자 하는 상대방의 공개키에 대하여 신뢰 기관으로부터 발급된 인증서가 필요하다. 반면에 ID-기반 시스템은 단지 사용자의 메일 주소와 같은 평이한 공개 정보로 구성된 공개 확인자(Identity, ID)만을 사용하므로 공개키

접수일 : 2005년 9월 7일 ; 채택일 : 2005년 12월 23일
* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음.
† 주저자 : young@cist.korea.ac.kr
‡ 교신저자 : donghlee@korea.ac.kr

에 대한 인증서가 필요하지 않기 때문에 공개키에 대한 인증절차가 간단하다.

최근 무선 환경이 급속도로 발달함에 따라 이에 적당한 키 동의 프로토콜이 요구되고 있다. 특히 서버와 저 전력 모바일과 같은 비대칭 컴퓨팅 환경에서의 안전한 채널의 형성은 안전한 통신을 위하여 꼭 필요하다. 그러나 불행하게도 기존의 ID-기반의 AKA 프로토콜은 연산 속도와 계산량의 복잡함 때문에 이러한 비대칭 환경에 적용하기엔 적절하지 않다.

2. 논문의 결과 및 구성

본 논문에서는 Bilinear Map을 이용한 비대칭 환경을 위한 ID-기반의 AKA 프로토콜, 즉 무선 환경과 같은 저 전력 클라이언트와 서버를 위한 ID-기반의 키 동의 프로토콜을 설명한다.

Bilinear map을 이용한 ID-기반 시스템은 Weil/Tate pairing 연산과 ID를 표현한 수를 타원곡선(elliptic) 위의 한 점으로 변환시키는 Map-To-Point 연산과 같은 계산량이 많은 복잡한 연산을 필요로 한다. 따라서 이러한 복잡한 연산 특히 pairing 연산을 줄이기 위하여 많은 연구[3,4,10]가 되어 왔음에도 불구하고 여전히 pairing 연산은 타원곡선에서의 스칼라 곱에 비하여 계산량이 훨씬 많기 때문에 기존에 제안된 ID-기반의 키 동의 기법은 저 전력 모바일 장치에 사용하기엔 적합하지 않았다. 이렇게 기존에 제안된 ID-기반의 AKA은 클라이언트 측의 무거운 계산량을 수행할 수 있는 유선 네트워크 환경에 기반하여 제안되었다.

제안하는 ID-기반 AKA 역시 bilinear map을 사용하여 설계하였다. 첫 번째, 우리는 클라이언트 측에서의 복잡한 pairing 연산과 Map-To-Point 연산을 사용하지 않았다. 두 번째, 오프라인 사전 계산을 사용하면 온 라인 상에서 클라이언트는 단지 타원곡선에서 두 번의 스칼라 곱과 한 번의 덧셈만 수행하면 된다. 제안한 프로토콜은 메시지 암호화와 서명을 함께 수행하는 signcryption의 개념을 이용한다.

제안한 ID-기반의 AKA의 안전성은 랜덤 오라클 모델에서 k-CAA (collusion attack algorithm with k traitors) 문제와 k-mBIDH (modified Bilinear Inverse DH with k values) 문제의 어려움에 기반한다. 제안한 프로토콜은 서버의 고정된 비밀키가 노출되면 이전의 세션키가 폭로되지만, 클라이언트의 고정된 비밀키가 노출되어도 이전의 세션키가 안전한 부분 전방향 안전성 (partial forward secrecy)을 제공한다.

3. 관련 연구

최초의 양자간 Diffie-Hellman 키 동의 프로토콜은 [9]에 제안되었으며, 그 후 인증된 키 동의 기법은 많은 연구가 되어왔다. 특히 Bellare와 Rogaway는 증명가능한 안전성(provable security)을 제공하는 키 동의 기법과 최초로 일반화된 모델을 제안하였다[5,6]. Huang 등은 센서 네트워크 사이에서 인증서 기반의 키 동의를 타원곡선 암호를 이용하여 제안하였다[11]. Bresson 등은 저 전력 모바일 장치를 위한 인증서 기반의 인증된 그룹 키 동의[1]을 제안하였으나 parallel session 공격에 취약함이 밝혀졌다[18]. 근래에 Katz 등은 양자간에서 다자간으로 확장하는 컴파일러[14]를 그리고 Hwang 등은 키 동의를 인증된 키 동의로 변환하는 컴파일러[12]를 제안하였다. 최근에 Kim 등은 저 전력 모바일 장치를 위한 효율적인 인증된 그룹 키 동의를 제안하였다[13]. 그러나 제안된 모든 AKA 프로토콜은 ID-기반이 아닌 인증서에 기반한 것이다.

II. 모 델

본 장에서는 Bellare 외 저자들[5,6,7]에 의해 제안된 외부 공격 환경하의 양자간 키 동의에 대한 안전성 모델과 정의에 대한 개념을 토대로 ID-기반의 양자간 키 동의 모델에 대해서 살펴본다. 모델과 안전성에 대한 좀 더 구체적인 내용들은 [5,6,7]을 참조한다.

1. 안전성 모델

모바일 클라이언트 U와 서버 V의 유일한 확인자를 각각 ID_U와 ID_V라 가정한다. 클라이언트 U는 서버 V와 계속적인 실행을 수행하며, 프로토콜은 서로 구별되고 병렬적인 실행에 관여되는 오라클이라고 하는 많은 인스턴스들을 갖는다. 여기서는 참가자 $U(V)$의 s-번째 인스턴스를 $\Pi_U^s(\Pi_V^s)$로 나타내기로 한다. 클라이언트와 서버 그리고 공격자는 공개된 파라미터 params와 확인자 ID = $\{ID_U, ID_V\}$를 알고 있다고 가정한다.

공격 모델(Adversarial model). 안전성의 개념을 정의하기 위해 공격자의 능력에 대한 모델을 설명한다. 공격자는 아래에 설명될 오라클들에 대한 접근을 통하여 네트워크상의 모든 통신에 접근하여 도청이나 조작이 가능하다. 공격자는 오라클에 질의를 하여 그에 대한 응답을 얻을 수 있으며, 이와 같은 공격 모델은 실제 시스템에서 공격자가 이용할 수 있다. 우리는 ID-기반의 AKA를 위한 공격자의 질의 종류를 다음과 같이 고려한다. 여기서 $id \in \{U,V\}$라 하자.

- **추출** $Extract(ID)$: 이 질의는 공격자가 선택한 확인자 $ID \in$ ID에 대한 고정된 비밀키를 얻는다.
- **전송** $Send(\Pi_{id}^s, M)$: 이 질의는 공격자가 사용자 오라클 Π_{id}^s에게 메시지 M을 보내는 상황을 모델링 한다. 사용자 오라클 Π_{id}^s는 공격자에 의해서 조작된 통신 메시지를 받고 프로토콜에 의해 기술된 방식으로 반응한다. 가장 공격이나 중간자 공격 (man-in-the-middle)이 전송 질의를 사용하여 수행할 수 있다.
- **실행** $Execute(U, V)$: 이 질의는 공격자가 단순한 도청에 의해 정직한 실행에 대한 접근을 얻는 수동적인 공격을 모델링 한다. 이 경우 공격자는 클라이언트와 서버 사이의 정직한 프로토콜 실행에 의해 얻어지는 전달 메시지들을 얻는다.
- **유출** $Reveal(\Pi_{id}^s)$: 이 질의는 한 세션에 대한 키의 손실로부터 다른 세션키의 노출로 연결되는 알려진 키 공격(known key attack) 개념을 모델링 한다. 공격자에게 Π_{id}^s에 대한 세션키가 주어지게 된다.
- **손상** $Corrupt(ID)$: 이 질의는 상대적으로 고정된 비밀키의 노출로부터 다른 세션들을 보호하고자 하는 전방향 안전성(forward secrecy)의 개념을 모델링 한다. 제안한 ID-기반의 AKA는 부분 전방향 안전성을 제공한다. 따라서 공격자는 $Corrupt(\Pi_U^s)$ 질의를 할 수 있지만, $Corrupt(\Pi_V^t)$ 질의는 할 수 없다.
- **테스트** $Test(\Pi_{id}^s)$: 이 질의는 기법의 의미론적 (semantic) 안전성에 대해 공격자의 성공 능력을 측정하기 위해 이용된다. 사용자 인스턴스 Π_{id}^s가 세션키 SK_{id}^s를 가지고 승인했을 ($acc_{id}^s = TRUE$) 경우 다음을 실행한다. 임의의 비트 b가 선택되어 만일 b=1이면 정당한 세션키 SK_{id}^s가, b=0이면 임의의 난수가 되돌려진다. 이 질의는 한번만 이용될 수 있고, 새로운($fresh$) 사용자 인스턴스 Π_{id}^s에 대해서만 가능하다.

위 공격의 형태에 따라서 우리는 공격자의 두 유형을 고려한다. 우선 수동적인(passive) 공격자는 실행, 유출, 손상 그리고 테스트 질의를 할 수 있으며 반면에 능동적인(active) 공격자는 여기에 전송과 추출 질의가 더해진다. 추출 질의는 [5,6,7]에서의 양자간 키 동의 안전성 모델에 없는 새로이 추가된 질의이다. 이는 ID-AKA 공격자가 공격 대상 ID를 선택하여 그에 대한 비밀키를 키 생성기관으로부터 획득할 수 있기 때문이다.

파트너링(Partnering). 다음은 세션 아이디와 파트너 아이디에 의하여 정의되는 파트너링을 정의한다. Π_{id}^s의 세션 아이디 sid_{id}^s는 프로토콜의 한 실행에 참가한 Π_{id}^s에 의해 보내고 받은 모든 메시지들을 참가자 아이디의 순서로 연접한 문자열이라고 하자. 그리고 Π_{id}^s의 파트너 아이디 πd_{id}^s는 Π_{id}^s가 세션키를 교환하기 원하는 참가자들의 아이디들을 사전식 순서로 연접한 문자열이라고 하자. 만일 $\pi d_U^s = \pi d_V^t$이고 $sid_U^s = sid_V^t$라면 참가자 인스턴스 Π_U^s와 Π_V^s는 '파트너 되어졌다'라고 불리어진다.

정확성(Correctness). 정확성은 프로토콜에 참가한 정당한 사용자들은 모두 동일한 세션키를 계산함을 보장한다. 즉, 만약 U와 V가 $\pi d_U^s = \pi d_V^t$, $sid_U^s = sid_V^t$파트너 되어졌고 $acc_U^s = acc_V^t = TRUE$이 성립하면 세션키 $SK_U^s = SK_V^t$이 성립한다.

Freshness. 여기서는 전방향 안전성이 고려된 개념을 정의한다. 만약 공격자가, (1) 사용자 인스턴스 Π_U^s 또는 이의 파트너 Π_V^s에게 전송 질의를 하기 전에 손상 질의를 하지 않았고, (2) Π_U^s가 세션키 $SK_U^s (\neq NULL)$를 계산한 후 Π_U^s 또는 이의 파트너에게 유출 질의를 하지 않았다면 사용자 인스턴스 Π_U^s는 '새롭다(fresh)'라고 정의된다.

2. 안전성 개념

안전성(Security) 정의. 키 비밀성에 관한 안전성의 개념은 공격자의 존재 하에서 프로토콜을 실행하는

환경에서 발생한다. 다음과 같은 게임을 통해 고려해 보자. 게임은 키 생성 알고리즘, 공격자(알고리즘), 모든 오라클 Π_{id}^{s}에게 확률분포에 관련된 동전을 제공함으로써 초기화되며 아래와 같이 진행된다.

- 보안 상수 (security parameter)와 연계된 초기화 (initialization) 과정을 거쳐 각 사용자의 공개키와 비밀키를 할당한다.
- 공격자를 초기화하고 오라클에 대한 접근과 질의들을 허용한다. 그리고 생성된 질의에 대해 적절한 응답을 돌려준다.
- 게임이 끝나는 시점에서, 공격자는 테스트 질의에 관련된 비트 b의 추측 값 b'을 출력한다.

위와 같은 게임에서 공격자 A가 새로운(fresh) 사용자 인스턴스 Π_{U}^{s}에 테스트 질의를 한 후 되돌려 받은 키 값의 Real 또는 Random의 패리티 정보 b를 올바르게 추측하는 사건을 Succ로 나타낸다. 이때 키 동의 프로토콜 P을 공격하는 공격자 A의 이점은 다음과 같이 정의한다.

$$Adv_{A,P}(k) = |2 \cdot \Pr[\mathrm{Succ}] - 1|.$$

만약 임의의 수동적인 확률적 다항식 시간(probabilistic polynomial-time, PPT) 공격자에 대하여 그 공격자의 이점 $Adv_{A,P}(k)$이 무시할만하다(negligible)면 P를 안전한 키 동의 프로토콜이라고 한다. 또한 임의의 능동적인 PPT 공격자에 대하여 그 공격자의 이점 $Adv_{A,P}(k)$가 무시할만하다면 P를 안전한 인증된 키 동의 프로토콜이라고 한다.

전방향 안전성(Forward Secrecy). 전방향 안전성은 참가자의 고정된 비밀키의 노출이 이전 세션에 구성된 세션키를 손상시키지 않는다는 안전성 개념이다. 만약 전방향 안전성이 고려되지 않는다면 손상(Corrupt) 오라클에 대한 공격자의 접근이 제한된다.

인증(Authentication). 본 논문에서 인증은 AKA 프로토콜에서 비밀키를 알고 있는 정당한 사용자만이 올바른 세션키를 생성 할 수 있다는 암시적인 (implicit) 인증에 초점을 맞춘다.

Ⅲ. Bilinear Map과 암호학적 가정들

본 장에서는 이 후 제안할 프로토콜과 관련된 몇 가지 정의와 가정들에 대해서 살펴본다. 본 논문에서 우리는 G_1을 위수가 q인 덧셈 연산 군이라 하고, G_2를 같은 위수 q를 갖는 곱셈 연산 군이라 하자. 그리고 P는 G_1의 생성자이다. 이 때 G_1, G_2에서의 이산 대수 문제(DLP)는 어렵다고 가정한다. 임의의 $P, Q \in G_1$와 $a,b \in Z_q^*$에 대하여 아래와 같은 조건을 만족하는 함수 $e: G_1 \times G_1 \rightarrow G_2$를 우리는 admissible bilinear map 이라 한다.

- Bilinear: $e(aP,bQ) = e(P,Q)^{ab}$
- Non-degenerate : $e(P,Q) \neq 1$을 만족하는 $P, Q \in G_1$가 존재한다.
- Computable : $e(P,Q)$을 계산할 수 있는 효율적인 알고리즘이 존재한다.

Computational Diffie-Hellman (CDH) problem: CDH 문제는 $a,b \in Z_q^*$인 P, aP, bP가 주어지면 abP를 계산하는 문제이다.

Inverse Computational Diffie-Hellman (ICDH) problem: ICDH 문제는 $a \in Z_q^*$인 P, aP가 주어지면 $a^{-1}P$를 계산하는 문제이다.

Modified Inverse Computational Diffie- Hellman (mICDH) problem: mICDH 문제는 $a,b \in Z_q^*$인 b, P, aP 그리고 $(a+b)P$가 주어지면 $(a+b)^{-1}P$를 계산하는 문제이다.

Bilinear Diffie-Hellman (BDH) problem: BDH 문제는 $a,b,c \in Z_q^*$인 P, aP, bP 그리고 cP가 주어지면 $e(P,P)^{abc}$를 계산하는 문제이다.

Bilinear Inverse Diffie-Hellman (BIDH) problem: BIDH 문제는 $a,c \in Z_q^*$인 P, aP, cP가 주어지면 $e(P,P)^{a^{-1}c}$를 계산하는 문제이다.

Modified Bilinear Inverse Diffie- Hellman (mBIDH) problem: mBIDH 문제는 $a,b,c \in Z_q^*$인 b, P, aP 그리고 cP가 주어지면 $e(P,P)^{(a+b)^{-1}c}$를 계산하는 문제이다.

위 문제 중 CDH와 ICDH 그리고 mICDH 문

제는 서로 다항식 시간(polynomial time) 동치임을 쉽게 알 수 있다.

정리 1. BDH와 BIDH 그리고 mBIDH 문제는 서로 다항식 시간 동치이다.

(증명) BDH와 BIDH 문제는 다항식 시간 동치이다[23]. 그러므로 우리는 단지 BIDH와 mBIDH가 서로 다항식 시간 동치임을 증명한다.

- [BIDH ⇒ mBIDH] b, P, aP 그리고 cP가 mBIDH에 주어지면 $a'P = aP + bP$를 계산하여 $P, a'P, cP$를 BIDH에 입력한다. BIDH가 $e(P,P)^{a'^{-1}c} = e(P,P)^{(a+b)^{-1}c}$를 출력하면 mBIDH 역시 같은 값을 출력한다.
- [mBIDH ⇒ BIDH] P, aP, cP가 BIDH에 주어지면 $a'P = aP - bP$를 계산하여 $b, P, a'P$ 그리고 cP를 mBIDH에 입력한다. mBIDH가 $e(P,P)^{(a'+b)^{-1}c} = e(P,P)^{a^{-1}c}$를 출력하면 BIDH 역시 같은 값을 출력한다.

우리는 CDH, BDH 그리고 BIDH 문제가 어렵다고 가정한다. 이것은 CDH, BDH 그리고 BIDH 문제를 다항식 시간 안에 의미있는 확률을 가지고 계산하는 알고리즘이 존재하지 않음을 의미한다. [2]에서 나타난 것과 같이 gap Diffie-Hellman (GDH) 가정을 만족하는 GDH 파라미터 생성기는 타원곡선 상에서의 Weil/Tate pairing으로 구성할 수 있다.

제안하는 프로토콜의 안전성을 증명하기 위하여 우리는 k-CAA (Collusion Attack Algorithm with k traitor) 문제와 k-mBIDH (modified BIDH with k values) 문제를 정의한다. 사실 k-mBIDH는 k-CAA 문제를 bilinear 형태로 변환한 문제이다.

정의 1. k-CAA[17] 문제는 아래와 같이 주어졌을 때 $h \in Z_q^*$에 대하여 $(s+h)^{-1}P$를 계산하는 문제이다.

$$P, sP, \ h_1, h_2, ..., h_k \in Z_q^*, .$$
$$(s+h_1)^{-1}P, (s+h_2)^{-1}P, ..., (s+h_k)^{-1}P.$$

정의 2. k-mBIDH 문제는 아래와 같이 주어졌을 때 $e(P,P)^{(s+h)^{-1}t}$를 계산하는 문제이다.

$$P, sP, tP, \ h, h_1, h_2, ..., h_k \in Z_q^*, .$$
$$(s+h_1)^{-1}P, (s+h_2)^{-1}P, ..., (s+h_k)^{-1}P.$$

알고리즘 A에 대한 좀 더 일반적인 이점은 다음과 같이 정의된다.

$$\left| \Pr\left[A\left(\begin{array}{c} P, sP, tP, h, h_1, ..., h_k, \\ (s+h_1)^{-1}P, (s+h_2)^{-1}P, ..., (s+h_k)^{-1}P \end{array} \right) = e(P,P)^{(s+h)^{-1}t} \;\middle|\; \begin{array}{l} s,t,h,h_1,...,h_k \leftarrow Z_q^*; \\ R \leftarrow G_1; \ h \neq h_i \end{array} \right] \right|$$

Ⅳ. 제안한 프로토콜과 안전성 분석

이 장에서는 [15]에 제시된 signcryption 기법을 이용하여 모바일 클라이언트 U와 서버 V 사이의 ID-기반의 인증된 키 동의 프로토콜을 제안하고 랜덤 오라클 모델에서의 안전성을 증명한다. 우리는 제안한 프로토콜을 ID-AKA라 명한다.

1. ID-기반의 인증된 키 동의 프로토콜

먼저 두 그룹 G_1, G_2와 bilinear map e를 GDH 생성기를 사용하여 생성한다. 우리는 G_1에서 mICDH 문제는 어렵다고 가정한다. 제안하는 ID-AKA 프로토콜은 주어진 공개 확인자에 대응되는 비밀키를 생성하는 신뢰기관인 키 생성 기관 (KGC)을 이용하며, 이때 생성된 비밀키에 대한 안전성은 mICDH 문제의 어려움에 기반하게 된다.

Setup. KGC는 난수 $s \in Z_q^*$와 G_1의 생성자 P를 선택하고 $P_{pub} = sP$를 계산한다. 또한 암호학적 일방향 해쉬 함수 $H: \{0,1\}^* \rightarrow Z_q^*$, $H_1 : G_2 \rightarrow Z_q^*$, $H_2 : \{0,1\}^* \rightarrow \{0,1\}^t$ 그리고 $H_3 : \{0,1\}^* \rightarrow \{0,1\}^k$를 선택한다. 여기서 t는 보안 상수 (security parameter)이며 k는 세션키의 비트 길이이다. 또한 KGC는 마스터 비밀키인 s를 비밀로 하고 공개 시스템 파라미터 $params = \{e, G_1, G_2, q, P, P_{pub}, H, H_1, H_2, H_3\}$를 공개한다.

Extract. 확인자가 ID_U인 클라이언트 U가 비밀키를 얻기를 원할 때, KGC는 $q_u = H(ID_U)$와 $g = e(P,P)$를 계산하여 비밀키 $S_U = (s+q_U)^{-1}P$를 계산한 후, (g, S_U)를 안전한 채널로 U에게 전송한다. 동일한 방법으로, 확인자가 ID_V인 서버 V도

$q_v = H(ID_V)$를 계산한 후, 비밀키 $S_V = (s+q_V)^{-1}P$를 계산하여 안전한 채널로 V에게 전송한다.

U와 V가 세션키를 생성하기 위해서 다음과 같이 프로토콜을 수행한다.(그림 1. 참조)

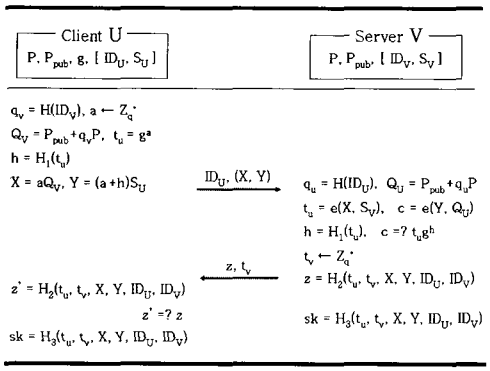


그림 1. ID-AKA 프로토콜

1. 클라이언트 U는 $q_v = H(ID_V)$를 계산하고 난수 $a \in Z_q^*$를 선택하여 $t_u = g^a$와 $Q_V = P_{pub} + q_v P$를 계산한다. 그 다음으로 U는 $h = H_1(t_u), X = aQ_V$ 그리고 $Y = (a+h)S_U$를 계산하여 $\langle ID_U, (X,Y)\rangle$를 V에게 전송한다.

2. 서버 V는 $q_u = H(ID_U)$와 $Q_U = P_{pub} + q_u P$를 계산한 후, $t_u = g^a$와 $c = e(Y, Q_U)$를 전송받은 메시지와 자신의 비밀키 S_V를 이용하여 계산한다. 또한 $h = H_1(t_u)$를 계산하여 $c = t_u g^h$임을 확인한다. 만약 식이 성립하지 않으면 V는 실패를 출력하고, 식이 성립하면 난수 $t_v \in Z_q^*$를 선택하여 인증 메시지 $z = H_2(t_u, t_v, X, Y, ID_U, ID_V)$를 계산한 후, z와 t_v를 U에게 전송한다. 결국 서버 V는 세션키로 $sk = H_3(t_u, t_v, X, Y, ID_U, ID_V)$를 계산한다.

3. 클라이언트 U는 $z' = H_2(t_u, t_v, X, Y, ID_U, ID_V)$을 t_u와 t_v를 이용하여 계산한 후, $z' = z$임을 확인한다. 만약 식이 성립하지 않으면 U는 실패를 출력하고, 식이 성립하면 세션키 $sk = H_3(t_u, t_v, X, Y, ID_U, ID_V)$를 계산한다.

정확성과 인증. 클라이언트의 메시지 (X,Y)를 받은 서버는 X와 자신의 비밀키인 S_V를 이용하여 다음과 같이 클라이언트의 비밀 정보인 t_u값을 계산할 수 있다.

$$e(X, S_V) = e(aQ_V, S_V)$$
$$= e(a(s+q_v)P, (s+q_v)^{-1}P) = e(P,P)^a = t_u.$$

위의 식처럼 $X = a(s+q_v)P$로부터 t_u값을 계산하기 위해서는 $S_V = (s+q_v)^{-1}P$값을 알고 있는 서버만이 계산할 수 있다. 서버는 또한 $h = H_1(t_u)$와 $c = e(Y, Q_U)$값을 계산하여 $c = t_u g^h$가 성립하는지 확인한다. 여기서 c값은 누구나 계산할 수 있으나 t_u와 h값은 정당한 서버만이 알 수 있다. 만약 정당한 서버라면 다음과 같이 $c = t_u g^h$이 성립함을 알 수 있다.

$$t_u g^h = e(P,P)^a e(P,P)^h = e(P,P)^{a+h}$$
$$= e((a+h)P, P)$$
$$= e((a+h)(s+q_u)^{-1}P, (s+q_u)P)$$
$$= e((a+h)S_U, Q_U) = e(Y, Q_U) = c$$

위의 식에서 c값은 클라이언트의 공개 정보인 Q_U값이 사용되기 때문에 메시지 Y에 클라이언트의 비밀키 정보가 들어있지 않으면 위의 식이 성립할 수 없다. 따라서 위의 식이 성립하면 서버는 전송받은 메시지 (X,Y)가 정당한 클라이언트 ID_U로부터 전송되었음을 확인할 수 있다.

메시지 z는 클라이언트의 비밀정보 t_u와 서버의 난수 t_v값 등이 함께 해쉬되어 있으며 이 t_u값은 정당한 서버만이 계산할 수 있기 때문에 클라이언트는 $z = z'$이 성립하면 메시지 z, t_v가 정당한 서버가 전송한 메시지임을 확인할 수 있다.

제안한 ID-AKA 첫 번째 라운드의 (X,Y)는 클라이언트의 메시지 t_u에 대한 signcryption 메시지이다. 따라서 정당한 서버만이 메시지의 복호화와 서명 검증을 할 수가 있다. 또한 ID-AKA에서 클라이언트 U는 t_u와 Y를 사전에 계산할 수 있다. 그러면 온-라인 상에서 U는 한번의 포인트 덧셈과 두 번의 스칼라 곱셈만을 계산하면 된다. 더구나 해쉬 함수 H는 계산량이 많은 Map-To-Point 연산이 아니라 일반적인 해쉬 함수이기 때문에 U의 계산량은 매우 적다고 할 수 있다.

또한, 제안한 ID-AKA 프로토콜은 부분 전방향 안전성을 제공한다. 만약 서버의 비밀키가 유출되면

공격자는 전송 메시지로부터 모든 세션키를 계산할 수 있지만, 클라이언트의 비밀키가 유출되면 이를 이용하는 공격자는 이전 세션키들에 관한 어떠한 정보도 얻을 수 없게 된다. 일반적으로 모바일 클라이언트는 낮은 파워를 가진 장치이기 때문에 서버에 비하여 공격에 취약하게 된다. 따라서 서버보다 클라이언트에서의 전방향 안전성의 제공이 더욱 효과적이라 할 수 있을 것이다. 제안한 기법에 완전한 전방향 안전성(perfect forward secrecy)를 제공하기 위해서는 클라이언트 측에서 pairing연산이 필요하게 된다. 그러나 이는 비대칭 컴퓨팅 환경에 적합하지 못하다. 결국 제안한 기법은 클라이언트 측에서의 계산량이 매우 적어 저 전력 모바일 장치에 적합하지만 서버 측에서의 부분 전방향 안전성을 제공하지 못하는 trade-off가 발생하게 된다.

2. 안전성 분석

제안한 프로토콜의 안전성 분석을 위해 ID-AKA에서 클라이언트의 전송 메시지를 위조하는 공격자를 *Forger*라 하자. 먼저 주어진 ID_U와 ID_V로부터 클라이언트의 전송 메시지의 위조가 불가능함을 보인다.

보조정리 1. 해쉬 함수 H와 H_1을 랜덤 오라클이라 하고 *Forger* A를 ID_U와 ID_V가 주어지고 러닝(running) 타임 t_0와 ϵ_0의 성공확률을 가진 위조자라 가정하자. A는 각각 q_H, q_{H_1}, q_S 그리고 q_E개의 H, H_1, 전송 그리고 추출 질의를 한다고 하자. 만약 $\epsilon_0 \geq 10q_{H_1}^2(q_S+1)(q_S+q_H)/q$라 하면 러닝 타임이 $t_1 \leq 120686q_{H_1}t_0/\epsilon_0$인 k-CAA문제를 계산하는 공격자 B가 존재한다.

(증명) 먼저 B에게 $k \geq q_H, q_S$인 k-CAA 문제의 입력값 $P, sP, q_1, q_2, \ldots, q_k, (s+q_1)^{-1}P, (s+q_2)^{-1}P, \ldots, (s+q_k)^{-1}P$이 주어진다. B의 목적은 임의의 q_0에 대하여 $(s+q_0)^{-1}P$를 계산하는 것이다. B는 A를 이용하기 위해 A의 공격 환경을 시뮬레이션 해 준다. 먼저 B는 GDH 파라미터 $\langle e, G_1, G_2\rangle$를 생성하고 $P_{pub}=sP$와 $g=e(P,P)$를 계산하여 시스템 파라미터 $\langle e, G_1, G_2, P, P_{pub}, g\rangle$를 A에게 입력한다.

일반성을 잃지 않고, 주어진 ID에 대하여 A는 H, H_1, 전송 그리고 추출 질의를 한번만 하며, 전송과 추출 질의 사전에 H질의를 수행한다고 가정하자. 충돌을 방지하고 질의에 대한 일관성 있는 응답을 위해 B는 목록 L_H과 L_{H_1}을 유지한다. 이 목록들은 초기에 비어있다. B는 A의 질의에 대하여 다음과 같이 응답한다.

- **H-질의.** A가 ID_i에 대한 H-질의를 했을 때, 만약 $ID_i = ID_U$이면 B는 q_0를 전송하고, 그 외의 경우에는 $\langle ID_i, q_i\rangle$를 목록 L_H에 추가하고 q_i를 전송한다.
- **H_1-질의.** A가 m에 대한 H_1-질의를 했을 때, B는 난수 h를 전송하고 이를 목록 L_{H_1}에 추가한다.
- **전송-질의.** A가 전송(Π_i) 질의를 했을 때, 만약 $ID_i = ID_U$이면 B는 난수 a와 h를 선택하여 $X=a(sP+q_0P)$와 $Y=hP$를 계산한 후, ID_U, (X,Y)를 A에게 전송한다. 그 외의 경우 B는 목록 L_H에서 $\langle ID_i, q_i\rangle$를 찾은 후, 난수 a와 h를 선택하고 $X=a(sP+q_iP)$ 와 $Y=(a+h)(q_i+s)^{-1}P$ 를 계산하여 $ID_U, (X,Y)$ 를 A에게 전송한다. 만약 A의 전송 질의가 $ID_i = ID_U$이면 B는 정당한 Y값을 생성할 수 없기 때문에 임의의 Y값을 전송하게 된다. 그러나 A는 서버의 비밀키 S_V를 알지 못하기 때문에 전송받은 (X,Y)에 대한 정당성을 확인할 수 없다. 따라서 전송 질의에 대한 B의 시뮬레이션은 타당하다.
- **추출-질의.** A가 $ID_i \notin \mathrm{ID_U}, \mathrm{ID_V}$에 대한 추출 질의를 했을 때, B는 목록 L_H에서 $\langle ID_i, q_i\rangle$를 찾은 후, $(s+q_i)^{-1}P$를 전송한다.

마침내 A는 새로운 정당한 메시지 $ID_U, (X,Y)$를 출력하게 된다. B는 forking lemma [20]과 같이 위의 H_1과 다른 해쉬 함수 H_1'를 사용하여 동일하게 시뮬레이션 하면 결국 A는 $h \neq h'$인 서로 다른 정당한 두 메시지 쌍 $\langle ID_U, (X=aQ_V, Y=(a+h)(q_0+s)^{-1}P)\rangle$, $\langle ID_U, (X=aQ_V, Y'=(a+h')(q_0+s)^{-1}P)\rangle$ 을 출력하게 된다. 그러면 B는 $(Y-Y')/(h-h') = (q_0+s)^{-1}P$를 계산한 후 이를 k-CAA 문제의 결과로 출력한다.

B가 h와 h'을 정확히 추측할 확률은 $1/q_{H_1}^2$이며, 전체 러닝 타임 t_1은 forking lemma에 요구된 러닝 타임과 동일한 $120686q_{H_1}t_0/\epsilon_0$에 유계하게 된다.

정리 2. 제안된 ID-AKA에 사용된 해쉬 함수를 랜덤 오라클이라 하고 ID_U와 ID_V가 주어지고 러닝(running) 타임 t인 ID-AKA 공격자 A가 존재한다고 가정하자. 그러면 ID-AKA는 k-mBIDH 문제의 어려움에 기반하여 부분 전방향 안전성을 제공하는 안전한 AKA 프로토콜이다. 즉,

$$Adv^{AKA-hfs}_{ID\_AKA,A}(t) \le \frac{1}{2} q_S q_{H_i} Adv^{k-mBIDH}_{G_1,G_2,e}(t) + Adv^{Forge}(t).$$

여기서 $Adv^{Forge}(t)$는 러닝 타임이 t인 임의의 $Forger$의 최대 이점이며, q_S, q_C그리고 q_{H_i}는 공격자 A가 생성하는 전송, 손상 그리고 해쉬 H_i 질의의 개수를 나타낸다.

(증명) A를 ID-AKA를 공격하는 능동적인(active) 공격자라 하자. 그러면 A는 두 가지 경우에 의한 공격을 시도할 수 있다. 첫 번째는 인증 메시지들의 위조. 즉, 클라이언트로의 가장 공격을 시도하거나. 두 번째는 전송 메시지의 위조나 변조하지 않고 도청만 하여 공격하는 경우이다. 공격자가 서버의 전송 메시지를 위조하는 것, 즉, 서버로 가장하는 공격은 결국 z값을 위조해야만 하고 이는 클라이언트의 비밀 정보인 t_u값을 모르고서는 성공할 수 없다. 그러나 해쉬 함수 H_2의 일방향성에 의해 z값의 위조는 불가능하다. 따라서 공격자 A의 공격은 위의 두 가지 경우로 제한된다.

먼저 A가 첫 번째 경우의 공격을 시도한다면 A를 이용하여 정당한 메시지 쌍 $ID_U(X,Y)$을 위조하는 $Forger$ F를 구성할 수 있다. 이는 F가 시스템에 필요한 모든 공개키와 비밀키를 올바르게 생성한 후, A의 질의에 대해 시뮬레이션 해줌으로써 쉽게 구성할 수 있다. $Forge$를 A가 새로운 정당한 메시지 쌍을 생성하는 사건이라 하면 F가 성공할 확률은 $\Pr_A[Forge] \le Adv^{Forge}_F(t) \le Adv^{Forge}(t)$가 된다. 보조정리 1.에 의하여 확률 $\Pr_A[Forge]$은 무시할 만한 값이다.

다음으로 A가 두 번째 경우의 공격을 시도할 때를 고려해보자. 세션키 sk의 정보를 얻기 위해서 A는 해쉬 오라클 H_3에 $\langle t_u, t_v, X, Y, ID_U, ID_V \rangle$를 질의해야만 한다. 따라서 A는 비밀 정보인 t_u를 계산해야만 한다. 그러므로 우리는 A를 이용하여 k-mBIDH 문제를 계산하는 공격자 B를 다음과 같이 구성할 수 있다. 먼저 B에게 $k \ge q_H, q_S$인 k-mBIDH 문제의 입력값 $e, G_1, G_2, P, sP, tP, q_0, q_1, q_2, ..., q_k, (s+q_1)^{-1}P, (s+q_2)^{-1}P, ..., (s+q_k)^{-1}P$이 주어진다. B의 목적은 $e(P,P)^{(s+q_0)^{-1}t}$를 계산하는 것이다. B는 A를 이용하기 위해 A의 공격 환경을 시뮬레이션 해 준다. 먼저 B는 GDH 파라미터 $\langle e, G_1, G_2 \rangle$를 생성하고 $P_{pub} = sP$와 $g = e(P,P)$를 계산하여 시스템 파라미터 $\langle e, G_1, G_2, P, P_{pub}, g \rangle$를 A에게 입력한다. A의 이점을 활용하기 위해 B는 임의의 α를 선택한다. α는 A가 α번째 세션에 테스트 질의를 하는 것을 추측하기 위한 값이다.

일반성을 잃지 않고, A는 동일한 메시지에 대해서는 한번만 질의 하며, 전송과 추출 질의 사전에 H질의를 수행한다고 가정하자. 충돌을 방지하고 질의에 대한 일관성 있는 응답을 위해 B는 목록 L_H, L_{H_1}와 L_{H_2}을 유지한다. 이 목록들은 초기에 비어있다. B는 A의 질의에 대하여 다음과 같이 응답한다.

- **H-질의.** A가 ID_i에 대한 H-질의를 했을 때, 만약 $ID_i = ID_U$이면 B는 q_0를 전송하고, 그 외의 경우에는 $\langle ID_i, q_i \rangle$를 목록 L_H에 추가하고 q_i를 전송한다.
- **H_1-질의.** A가 임의의 메시지 m에 대한 H_1-질의를 하면 B는 h를 전송한다. 그 외의 경우에 B는 난수 h를 전송하고 (m,h)을 L_{H_1}에 추가한다.
- **H_2-질의.** A가 H_2-질의 $\langle t_u, t_v, X, Y, ID_U, ID_V \rangle$를 했을 때, B는 L_{H_2}목록에서 $(\langle t_u, t_v, X, Y, ID_U, ID_V \rangle, z)$를 찾아서 z를 A에게 전송한다.
- **H_3-질의.** A가 임의의 메시지 m'에 대한 H_3-질의를 하면 B는 임의의 난수를 A에게 전송한다.
- **전송-질의.** 전송 질의는 다음과 같은 두 가지 전송질의에 대하여 고려한다.
  - A가 전송$(\Pi^s_U, Start)$ 질의를 했을 때, 만약 이 질의가 α번째 세션에 대한 요청이면, B는 난수 r을 선택하고, $X = tP$와 $Y = rP$를 계산한 후, $ID_U(X,Y)$를 A에게 전송한다. 그 외의 경우 B는 목록 L_H에서 $\langle ID_i, q_i \rangle$를 찾은 후, 난수 a와 h를 선택하고 $Q_V = sP + q_0 P$, $X = aQ_V$, $Y = (a+h)(q_u + s)^{-1}P$ 그리고 $t_u = e(P,P)^a$를 계산하여 t_u와 h는 목록 L_{H_1}에 추가하고 $ID_U(X,Y)$를 A에게 전송한다.
  - A가 전송$(\Pi^t_V, (ID_U, X, Y))$ 질의를 했을 때, B는

난수 z와 t_v를 선택하고 이를 A에게 전송한 후 $\langle (t_u, X, Y, ID_U, ID_V), z \rangle$ 를 목록 L_{H_2}에 추가한다.

- **실행-질의**. A가 실행(U, V) 질의를 했을 때, B는 전송 질의의 시뮬레이션을 이용하여 메시지 $\langle (ID_U, X, Y), (z, t_v) \rangle$ 를 A에게 전송한다.
- **추출-질의**. A가 $ID_i \notin ID_U, ID_V$ 에 대한 추출 질의를 했을 때, B는 목록 L_H에서 $\langle ID_i, q_i \rangle$ 를 찾은 후, $(s+q_i)^{-1}P$ 를 전송한다.
- **손상-질의**. A가 ID_U에 대한 손상 질의를 했을 때, B는 목록 L_H에서 $\langle ID_U, q_u \rangle$ 를 찾은 후, $(s+q_u)^{-1}P$ 를 전송한다.
- **유출-질의**. A가 유출 질의를 했을 때, B는 난수를 A에게 전송한다.
- **테스트-질의**. A가 테스트 질의를 했을 때, 만약 그 질의가 α번째 세션에 대한 질의이면 B는 실패를 출력하고, 그 외의 경우에는 임의의 비트 b를 선택한다. 만약 b=1이면 세션키를 아니면 난수를 A에게 전송한다.

B의 성공 확률은 B가 α를 정확히 추측한 사건과 A가 비밀 값 $t_u = e(P,P)^{(s+q_u)^{-1}t}$ 를 H_1 해쉬 오라클에 질의한 사건에 의존한다. 위의 시뮬레이션에서 B가 α를 정확히 추측할 확률은 $1/q_S$이고, A의 이점이 ϵ 이라면 A가 비밀 값 t_u를 H_1 해쉬 오라클에 질의할 확률은 2ϵ이 된다. (2ϵ되는 결과에 대한 증명은 [2]의 Lemma 4.3의 결과와 동일하므로 참조한다.) 따라서 B가 α를 정확히 추측하였다면 t_u는 2ϵ의 확률로 목록 L_{H_1}에 존재하게 된다. 그러므로 B는 k-mBIDH 문제를 적어도 확률 $2\epsilon/q_S q_{H_1}$로 계산할 수 있게 된다. 결국 증명의 처음부분에서 언급한 두 번째 사건에 대한 A의 이점은 최대 $\frac{1}{2} q_S q_{H_1} Adv^{k-mBIDH}_{G_1, G_2 e}(t)$ 만큼의 이점을 가지게 된다. 마침내 우리는 위의 증명의 결과로 아래와 같은 식을 얻을 수 있다.

$$Adv^{AKA-hfs}_{ID\_AKA\cdot A}(t) \leq \frac{1}{2} q_S q_{H_1} Adv^{k-mBIDH}_{G_1, G_2 e}(t) + Adv^{Forge}(t) \quad .$$

V. 결 론

본 논문에서 우리는 컴퓨팅 파워가 다른 두 사용자(서버, 클라이언트) 사이의 효율적인 ID-기반의 인증된 키 동의 프로토콜은 제안하였다. 특히 클라이언트 측의 계산량을 줄임으로써 낮은 파워를 가진 모바일 장치에 알맞게 설계하였다. 제안한 프로토콜의 안전성은 랜덤 오라클 모델에서의 k-CAA와 k-mBIDH 문제의 어려움에 기반한다.

참 고 문 헌

[1] E. Bresson, O. Chevassut, A. Essiari and D. Pointcheval, "Mutual Athentication and Group Key Agreement for Low-Power Mobile Devices", *In the 5th IEEE International Conference on Mobile and Wireless Communications Networks, 2003.*

[2] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing", *Proc. of Crypto '01*, LNCS 2139, pp.213-229, Springer- Verlag, 2001.

[3] P. S. L. M. Barreto, H. Y. Kim, B. Lynn and M. Scott, "Efficient algorithms for pairing-based cryptosystems", *Proc. of Crypto '02*, LNCS 2442, pp. 354-368, Springer-Verlag, 2002.

[4] P. S. L. M. Barreto, B. Lynn and M. Scott, "Efficient implementation of pairing-based cryptosystems.", *Journal of Cryptology*, pp. 321-334, 2004.

[5] M. Bellare, P. Pointcheaval and P. Rogaway, "Authenticated key exchange secure against dictionary attacks", *Proc. of Eurocrypt' 00*, LNCS 1807, pp.139-155, Springer-Verlag, 2000.

[6] M. Bellare and P. Rogaway, "Entity authentication and key distribution", *Proc. of Crypto '93*, pp.232-249.

[7] M. Bellare and P. Rogaway, "Provably-Secure Session Key Distribution : The Three Party Case", *Proc. of STOC '95*, pp. 57-66.

[8] K. Y. Choi, J. Y. Hwang and D. H. Lee, "Efficient ID-based Group Key

Agreement with Bilinear Maps", *Proc. of PKC '04*, LNCS 2947, pp. 130-144, Springer-Verlag, 2004.

[9] W. Diffie and M. Hellman, "New Directions in Cryptography", *IEEE Transactions on Information Theory 22(6)*, pp.644-654, 1976.

[10] S. D. Galbraith, K. Harrison and D. Soldera, "Implementing the Tate pairing", *Proc. of ANTS'02*, LNCS 2369, pp.324-337, Springer- Verlag, 2002.

[11] Q. Huang, J. Cukier, H. Kobayashi, B. Liu and J. Zhang, "Fast Authenticated Key Establishment Protocols for Self-Organizing Sensor Networks", *In Proc. of WSNA'03*, Copyright 2003 ACM.

[12] J. Y. Hwang, S. M. Lee and D. H. Lee, "Scalable key exchange transformation : from two-party to group", *Electronics Letters*, Vol. 40, No. 12, Jun. 2004.

[13] H. J. Kim, S. M. Lee and D. H. Lee, "Constant-Round Authenticated Gourp Key Exchange for Dynamic Groups", *Proc. of Asiacrypt 2004*, LNCS 3329, pp.245-259, Springer-Verlag, 2004.

[14] J. Katz and M. Yung, "Scalable Protocols for Authenticated Group Key Exchange", *Proc. of Crypto 2003*, LNCS 2729, pp.110-125, Springer-Verlag, 2003.

[15] N. McCullagh and P. S. L. M. Barreto, "Effcient and Foward-Secure Identity-Based Signcryption", *Cryptology ePrint Archive*, Report 2004/117.

[16] N. McCullagh and P. S. L. M. Barreto, "A New Two-Party Identity-Based Authenticated Key Agreement", *Proc. of CT-RSA'05*, LNCS 3376, pp.262-274, Springer-Verlag, 2005.

[17] S. Mitsunari, R. Sakai and M. Kasahara, "A new traitor tracing", *Proc. of IEICE Trans.* Vol. E85-A, No.2, pp.481-484, 2002.

[18] J. Nam, S. Kim and D. Won, "Attacks on Bresson-Chevassut-Essiari-Pointcheval's Group Key Agreement Scheme for Low-Power Mobile Devices", *Proc. of IEEE Communications Letters, 2005.*

[19] D. Nalla and K. C. Reddy, "ID-based tripartite Authenticated Key Agreement Protocols from pairings", *Cryptology ePrint Archive*, Report 2003/004.

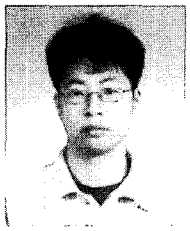
[20] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures", *Journal. of Cryptology*, Vol. 13, pp.361-396, 2000.

[21] N.P.Smart, "An Identity based authenticated Key Agreement protocol based on the Weil pairing", *Electronics Letters*, vol. 38 (13): 630--632, June 2002.

[22] A. Shamir, "Identity Based Cryptosystems and Signature Schemes", *Proc. of Crypto 1984*, LNCS 0196, Springer-Verlag, 1984.

[23] F. Zhang, R. Safavi-Naini and W. Susilo, "An Efficient Signature Scheme from Bilinear Pairings and Its Applications", *Proc. of PKC '04*, LNCS 2947, pp.277-290, Springer- Verlag, 2004.

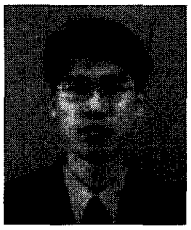
〈著者紹介〉



최 규 영 (Kyu-young Choi) 학생회원
2002년 2월 : 고려대학교 수학과 학사
2004년 8월 : 고려대학교 정보보호대학원 석사
2004년 8월~현재 : 고려대학교 정보보호대학원 (박사과정)
〈관심분야〉 암호 프로토콜, 암호이론

황 정 연 (Jung-yeon Hwang) 학생회원
1999년 2월 : 고려대학교 수학과 학사
2003년 2월 : 고려대학교 정보보호대학원 석사
2003년 3월~현재 : 고려대학교 정보보호대학원 (박사수료)
〈관심분야〉 암호 프로토콜, 암호이론, 공개키 암호

이 동 훈 (Dong-hoon Lee) 정회원
1984년 2월 : 고려대학교 경제학과 학사
1987년 2월 : Oklahoma Univ. 전산학 석사
1992년 2월 : Oklahoma Univ. 전산학 박사
1993년 3월~현재 : 고려대학교 전산학과 정교수
2000년 3월~현재 : 고려대학교 정보보호대학원 교수
〈관심분야〉 암호 프로토콜, 암호이론, 정보이론



홍 도 원 (Do-won Hong)
1994년 2월 : 고려대학교 이과대학 수학과(학사)
1996년 2월 : 고려대학교 수학과(석사)
2000년 2월 : 고려대학교 수학과(박사)
2000년 4월~현재 : 한국전자통신연구원 팀장
〈관심분야〉 암호이론, 정보보호 이론, 이동통신 정보보호