情報保護學會論文誌
第12券 第1號, 2002. 2

ECDSA를 적용한 ID 기반의 사용자 인증 및 키 교환 프로토콜*

박 영 호**, 박 호 상***, 정 수 환***

An ID-based entity-authentication and authenicated key exchange protocol with ECDSA

Young-Ho Park**, Ho-Sang Park***, Souhwan Jung***

요 약

본 논문은 제3자 신뢰기관인 키 인증센터(KAC)로부터 미리 등록된 두 사용자간에 2회의 통신으로 KAC의 참여없이 사용자 인증과 키 교환이 가능한 ID 기반의 프로토콜을 제안한다. 제안된 프로토콜은 ECDSA의 서명기법과 Diffie-Hellman 키교환 방식을 H. Sakazaki, E. Okamoto 그리고 M. Mambo[9]에 의해서 제안된 타원곡선상의 ID-기반 키 분배 프로토콜(SOM 프로토콜)에 적용하여 개발되었다. 제안된 프로토콜의 안전성은 타원곡선 이산대수 문제(ECDLP)와 Diffie-Hellman 문제(ECDHP)의 어려움에 기반을 두며, unknown key share attack 방지, perfect forward secrecy를 제공함으로써 SOM 프로토콜의 취약점을 보완하였다.

ABSTRACT

This paper proposes an ID-based entity-aunthentication and authenticated key exchange protocol with ECC via two-pass communications between two parties who are registered to the trusted third-party KC in advance. The proposed protocol is developed by applying ECDSA and Diffie-Hellman key exchange scheme to the ID-based key distribution scheme over ECC proposed by H. Sakazaki, E. Okamoto and M. Mambo(SOM scheme). The security of this protocol is based on the Elliptic Curve Discrete Logarithm Problem(ECDLP) and the Elliptic Curve Diffie-Hellman Problem(ECDHP). It is strong against the unknown key share attack and it provides the perfect forward secrecy, which makes up for the weakness in SOM scheme.

keyword : *ECDSA, ECDLP, ECDH, ID-based Key Agreement, Mutual Authentication*

Ⅰ. 서 론

인터넷을 통한 전자상거래의 활성화를 위해 무엇보다 상호간의 인증과 안전한 정보교환을 위한 키 분배가 선행되어야 한다. 기존의 인증서(certificate) 기반의 공개키 기반구조(PKI : Public Key Infra-structure)에서는 공개키와 그 소유자를 대응시켜주는 문서인 인증서를 공인인증기관(CA)으로부터 받아 상호간의 인증에 사용한다. 그러나 매번 인증서 발급으로 통화량의 증가와 비용 및 시간의 소모가 있으며 인증서 검증, 키 관리등 복잡한 문제를 안고 있다. 따라서 제 삼자의 신뢰기관인 키 인증센터(KAC)

* 본 연구는 정보통신부에서 지원하는 대학기초연구지원 사업으로 수행하였습니다.
** 고려대학교 정보보호기술연구센터(youngho@cist.korea.ac.kr)
*** 숭실대학교 정보통신전자공학부(hosang@cnslsvr.ssu.ac.kr, souhwanj@saint.ssu.ac.kr)

(등록기관 또는 키 관리 기관)를 두되 PKI 기반의 인증기관과 달리, 그 역할을 가입자의 공개키에 대한 공증, 키 관리에 두고 가입한 사용자간의 실제적인 통신 및 전자상거래 시, 신뢰기관과의 접촉 없이 독립적으로 안전한 사용자 인증 및 키 분배가 가능한 시스템에 대한 연구가 필요하게 되었다.

이러한 목적으로 가입자의 개인 신분정보를 일방향 함수(one-way function)로 하여 공개키를 형성하는 ID 기반 시스템 개념이 1984년 Shamir[8]에 의해 처음 제안되었다. ID 기반 시스템은 거래를 원하는 상대방의 인터넷 도메인(Domain)의 주소(IP), 주민등록번호, 전화번호, 카드번호 등 사용자의 신분을 유일하게 확인할 수 있는 신분정보(ID) 만으로도 쉽게 상대방을 인증할 수 있고 이것을 바탕으로 공개키 기반의 전자서명과 키 분배를 사용자간에 독립적으로 할 수 있는 장점이 있다.

Shamir[8]에 의해 ID 기반의 서명기술이 제안된 이후 많은 연구가 진행되었다. 지금까지 제안된 ID 기반 프로토콜들은 대부분 인수분해문제(FP)를 기반으로 하는 것이 많았다. Okamoto와 Tanaka[6]는 Shamir의 생각을 확장하여 RSA 기술[7]에 기반을 두고 키 분배와 디지털 서명을 조합하였다. 이 시스템은 공통 키 교환을 위해 오직 2회 Pass 통신을 사용하므로 통신상 낮은 복잡도 때문에 매우 흥미를 끌었다. 그러나, 많은 대역폭 사용과 많은 계산량 부담, 그리고 위장공격등 안전성에 문제점을 안고있다. 최근에 Shieh, Yang과 Sun[10]은 적은 계산량과 Okamoto와 Tanaka 기술[6]에서 나타나는 안전성 문제를 해결한 인증 프로토콜을 제안하였다. 그러나, 이 기술은 메시지의 반복 공격과 알려지지 않은 키 공유 공격(unknown key share attack)에 약하다는 Yen[12]의 분석이 있었다. 위 프로토콜들의 안전성은 RSA 공개키 암호 시스템과 같이 두 개의 큰 소수의 곱인 합성수의 인수분해문제(FP)에 기반한다. 때문에 이들 기술들은 타원곡선 암호법(ECC)를 사용하는 알고리즘들과 비교할 때 많은 대역폭의 사용과 많은 계산량이 요구된다.

한편 이산대수문제(DLP)에 안전성을 기반으로 하는 기술은 Tsujii[11]에 의해 처음 제안되었다. 그는 ElGamal의 공개키 시스템[2]을 이용하여 ID 기반의 암호 시스템을 제안하였는데, 이 기술은 많은 계산량 뿐만 아니라 공모 문제와 같은 보안의 취약성을 갖고 있다. Günther[3]는 유한 체의 곱셈 군에 기반을 둔 ID 기반의 키 교환 프로토콜을 제안하였는데, 이 프로토콜은 perfect forward secrecy를 제공할 뿐만 아니라 KAC의 비밀키가 노출된다 하더라도 perfect forward secrecy를 제공하는 장점을 지닌다. 그러나, 이 프로토콜은 공통 세션 키를 위해서 4회의 통신이 필요하므로 많은 통신량이 요구된다.

최근, Sakazaki, Okamoto와 Mambo[9]은 타원곡선 상에서 Nyberg와 Rueppel 기법[5]을 적용한 ID 기반의 키 분배 시스템(SOM)을 제안하였다. 이 기법은 2회의 통신이 요구되며, 공통 키 생성을 위한 데이터 전송을 Nyberg-Rueppel의 것의 반으로 줄였다.

본 논문에서는 SOM 프로토콜이 비록 효율적이나, 공통키 생성과정에서 난수를 사용하지 않고 사용자의 비밀정보만이 사용되었기 때문에 "알려지지 않은 키 공유 공격"과 "perfect forward secrecy"와 같은 안전성에 취약성이 있음을 보일 것이다. 또한 이들의 취약점을 보완한 사용자 인증과 인증된 키 교환이 가능한 새로운 ID 기반의 프로토콜을 제안한다. 이 프로토콜은 ECC를 사용하여 구축하였고, ECDSA 기술을 변형하여 구체적인(explicit)사용자 인증을 행할 수 있게 하고 perfect forward secrecy를 제공하는 키교환을 가능하게 하였다. 또한 제안된 프로토콜은 상대방 인증과 키 교환을 동시에 수행하는데 오직 2회의 통신만이 요구되는 장점을 지닌다. 이 제안 프로토콜의 안전성은 타원곡선 이산대수 문제(ECDLP)와 Diffie-Hellman 문제(ECDHP)의 어려움에 기반을 두고 있다.

II. Sakazaki-Okamoto-Mambo 기법

2.1 SOM 기법 소개

Sakazaki-Okamoto-Mambo의 프로토콜을 간략하게 살펴보면 다음과 같다. 이 스킴은 3가지 단계로 나누어져 있다. 설정단계(Set up phase), 등록단계(Registration phase), 키교환단계(Key exchange phase).

- **설정단계(Set-up phase)** : 시스템을 설정하기 위해 키 인증센터(KAC)는 다음의 단계를 실행한다: p는 160 비트 이상의 크기를 갖는 큰 소수 그리고 F_p는 p개의 원소를 갖는 유한체라 하자. 원소 $a, b \in F_p$는 $4a^3+27b^2 \neq 0 \bmod p$를 만

족하는 파라미터로 놓는다. 타원곡선 $E_p(a, b)$는 $y^2 = x^3 + ax + b$의 방정식을 만족하는 F_p 상의 점들과 무한점으로 이루어진 집합을 의미한다.

① 타원곡선 군(group)의 위수가 160비트 이상의 크기를 갖는 소수 q를 갖는 암호학적으로 적당한 타원곡선 $E_p(a, b)$를 선택한다.
② 위수가 q인 basepoint $G \in E_p(a, b)$를 선택한다.
③ KAC의 비밀키인 난수 $a_C \in [1, q-1]$를 선택 하며, 비밀을 유지한다.
④ 점 $Q = a_C \cdot G$를 계산한다.
⑤ 암호학적으로 안전한 일방향 해쉬함수(one-way hash function) H를 선택한다.

따라서, KAC는 보안 네트워크에 참여하는 모든 사용자에게 공개 정보인 ($E_p(a, b), p, q, G, Q, H$)를 분배한다.

- **등록단계(Registration)** : 네트워크에 등록을 요청한 사용자 A와 KAC 사이에 다음의 4단계를 실행한다. 본 논문에서 ID_A는 사용자 A의 신분정보 ID를 나타낸다.

① 사용자 A는 비밀정보 $a_A \in [1, q-1]$를 택하고 $a_A G = (x_A, y_A)$ 계산하여 KAC로 보낸다. KAC는 사용자 A가 a_A를 알고있는지 여부를 확인한다. 이때 KC는 사용자의 비밀정보 a_A를 알 수 없다.
② KAC는 난수 $k_A \in [1, q-1]$를 선택하고 다음을 계산한다: $R_A = a_A G + k_A G$와 $r_A \equiv x(R_A) H(ID_A)^{-1} \bmod p$를 계산한다. 여기서, $x(R_A)$는 점 R_A의 x-좌표로 정의한다.
③ KAC는 $s_A \equiv k_A + r_A a_C \bmod q$를 만족하는 s_A를 계산하고, 사용자 A에게 비밀 채널을 통해 (r_A, s_A)를 전달한다.
④ 사용자 A는 KAC로부터 받은 r_A로부터 $x(R_A) = r_A H(ID_A) \bmod p$를 얻고 R_A를 복원하여 $(a_A + s_A)G = r_A Q + R_A$를 확인한 후 s_A를 또 하나의 비밀정보로 취급한다.

(사실 r_A로부터 정당한 R_A를 복원하기 위해서는 1비트의 부가적인 정보가 필요하다. 왜냐하면 R_A의 x-좌표 $x = x(R_A)$가 주어졌을 때 R_A의 y-좌표는 $\pm\sqrt{x^3 + ax + b}$ 이므로 유일한 y좌표를 구하기 위해서는 1 bit의 부가정보가 첨가되어야 한다. 따라서 본 논문에서 전달정보는 특별한 언급이 없어도 1 bit의 부가정보가 첨가된 것으로 본다.)

- **키교환단계(Key exchange)** : 사용자 A와 B가 통신을 원할 때, 다음과 같은 방법으로 키 교환을 행한다.

① 사용자 A는 사용자 B에게 r_A를 보낸다. 사용자 B는 $x(R_A) \equiv r_A H(ID_A) \bmod p$를 계산하고 R_A를 구성한다. 마지막으로, B는
$K_{BA} = (a_B + s_B)(r_A Q + R_A)$
$= (a_B + s_B)(a_A + s_A) \cdot G$
를 계산한다.
② 사용자 B는 사용자 A에게 r_B를 보낸다. 같은 방법으로 사용자 A는 공동 세션 키인
$K_{AB} = (a_A + s_A)(r_B Q + R_B)$
$= (a_A + s_A)(a_B + s_B) \cdot G$
를 얻는다.

2.2 SOM 스킴의 암호분석

비록 SOM 기법이 공통키 생성을 위해 2회 통신과 적은 데이터 전송을 요구하지만, 사용자의 long-term 비밀키가 난수의 사용 없이 세션 키 공유에 사용됨으로서 "알려지지 않은 키 공유 공격(unknown key share attack)과 "perfect forward secrecy"와 같은 안전성에 취약성이 있다.

- **알려지지 않은 키 공유 공격(Unknownkey Share Attack)** : SOM스킴에서 키의 무결성을 확인하는 것은 쌍방간에 키 교환이 행해진 후, 실제 암호문 전송과 복호가 실행되기 전에는 불가능하다는 것을 다음의 공격에 의해 보여줄 것이다.
공격자는 사용자 A가 보낸 r_A를 가로챈 후,

$$(c \cdot r_A \cdot H(ID_A))^3 + a(c \cdot r_A \cdot H(ID_A)) + b \quad (1)$$

가 $\bmod p$에서 quadratic residue가 되도록 임의의 $c \in [1, p-1]$를 선택한다. 이 후, 공격자는 사용자 B에게 r_A대신에 $c \cdot r_A$를 보낸다. 사용자 B는 이전에 설명한 것과 같은 프로토콜의 단계를 수행하여, $c \cdot r_A \cdot H(ID_A) \bmod p$ 를 x-좌표

로 갖는 타원곡선 $E_p(a,b)$ 위의 점 R_c를 얻는다. (만일 식 (1)이 quadratic residue가 아니라면 사용자 B는 $c \cdot r_A \cdot H(ID_A) \bmod p$ 를 x-좌표로 갖는 타원곡선 $E_p(a,b)$ 위의 점 R_c를 잡을 수 없다.) 따라서 사용자 B는 세션키로 $K_{BA}=(a_B+s_B)(c \cdot r_A \cdot Q+R_C)$를 얻을 것이다. 그러나, 다른 한편으로는, 사용자 A는 세션키로 $K_{AB}=(a_A+s_A)(a_B+s_B) \cdot G$를 구성할 것이다. 명백히, $K_{AB} \neq K_{BA}$ 이며 두 사용자 A와 B는 그들이 통신을 시작하기 전까지 분배된 키의 무결성을 확인할 수 없을 것이다.

- **Perfect Forward Secrecy** : SOM 스킴의 세션키 생성 과정에서 난수를 사용하지 않고 사용자의 long-term 비밀정보를 사용하므로, 만약 공격자가 사용자 A의 long-term 비밀정보인 a_A, s_A 또는 a_A+s_A를 알 수 있다면 공격자는 이전에 A가 사용했던 모든 세션 키들을 알아낼 수 있다. 왜냐하면, 공격자가 A와 키 교환을 위해 온 모든 정보들 r_B, ID_B를 저장해 놓았다가 a_A+s_A를 이용하여

$$K_{AB}=(a_A+s_A)(r_BQ+R_B)$$

을 계산할 수 있고 세션 키 K_{AB}를 알아 낼 수 있다. 따라서 perfect forward secrecy를 만족하는 키 분배 프로토콜의 구축을 위해서는 반드시 사용자의 비밀 정보가 아니라 난수의 사용이 필요함을 알 수 있다.

Ⅲ. 제안 프로토콜

본 장에서는 SOM 스킴에 나타난 안전성의 취약점을 보완하고 사용자 인증과 키 교환이 가능한 ID 기반의 프로토콜을 제안한다. 이 제안 프로토콜은 난수의 사용과 ECDSA 기법을 사용하여 안전성을 강화하고 상대방 인증과 키 교환을 동시에 수행하는데 오직 2회의 통신만이 요구되는 장점을 지닌다. 제안된 스킴은 SOM 스킴과 설정단계와 등록단계가 동일하고 SOM 스킴에서 안전성이 취약한 부분인 키 교환 프로토콜을 변형하였다. 따라서 SOM 스킴과 같이 본 제안 프로토콜은 3단계로 구성되어 진다: 설정단계, 등록단계 그리고 사용자 인증 및 키 교환 단계. 앞의 두 단계는 SOM 스킴과 동일하고 마지막 단계만을 수정 보완하였다.

- **설정단계(Set-up phase)** : SOM 스킴의 설정단계와 동일함.

- **등록단계(Registration)** : SOM 스킴의 등록단계와 동일하며 사용자 A는 a_A+s_A를 사용자 인증 및 키 교환을 위한 long-term 비밀키로 사용한다. 이 비밀키 a_A+s_A는 사용자만이 알고 있으며 신뢰기관인 KAC도 s_A만을 알고 있을 뿐이다.

- **사용자 인증 및 키 교환 단계(Entity authentication and authenticated key exchange)** : 네트워크에 등록된 사용자 A와 B가 통신을 원할 때, 제 삼자인 KAC와의 접촉없이 오직 통신에 관계하는 사용자 A와 B 사이에 2회의 통신만으로 사용자 인증과 키 교환을 완료할 수 있다.

① 사용자 A는 다음을 실행한다.

1) 난수 $k_1, k_2 \in [1, q-1]$를 택하여 $P_A=k_1G$, $T_A=k_2G$를 계산한다.
2) $\rho_A=x(P_A)$, $\tau_A=x(T_A)$로 놓고, 다음식 $H(ID_A \| ID_B \| Time \| \rho)=(a_A+s_A) \cdot \rho_A+k_1\sigma_A \bmod q$를 만족하는 σ_A를 구한다. 여기서 $Time$은 반복공격(replay attack)을 방지하는 시간(time), counter 같은 정보를 의미한다. (만약 $\sigma_A=0$ 이면 난수 k_1를 다시 잡고 반복 시행한다.)
3) 사용자 A는 사용자 B에게 세션키 교환을 위해 $(r_A, \rho_A, \sigma_A, \tau_A)$를 보낸다.

② 사용자 B는 사용자 A에게서 받은 정보 $(r_A, \rho_A, \sigma_A, \tau_A)$를 가지고 다음을 계산한다.

1) $0<r_A, \rho_A, \tau_A<p$ 와 $0<\sigma_A<q$ 임을 확인한다.
2) $(r_A, \rho_A, \sigma_A, \tau_A)$와 1 비트의 추가정보들로부터 $r_AH(ID_A)$를 x-좌표로 갖는 R_A와 ρ_A, τ_A를 각각 x-좌표로 갖는 P_A, T_A를 구성한다.
3) $V=r_AQ+R_A$를 계산한 후 $H(ID_A \| ID_B \| Time \| \tau_A)G = \rho_AV+\sigma_AP_A$ 임을 검증한다.
4) 만약 검증결과가 사실로 판명되면 사용자 B는 상대방이 A임을 신뢰한다. A가 생성한 것과 동일한 방법으로 B도 난수 k'_1, k'_2를 생성하여 자

신의 ID_B와 비밀키를 사용하여 $(r_B, \rho_B, \sigma_B, \tau_B)$를 생성한 후 공유키 분배를 통하여 사용자 A에게 전달한다.

위의 2회 통신 후에 각 사용자에 의해 공통 세션 키가 다음과 같이 계산된다.

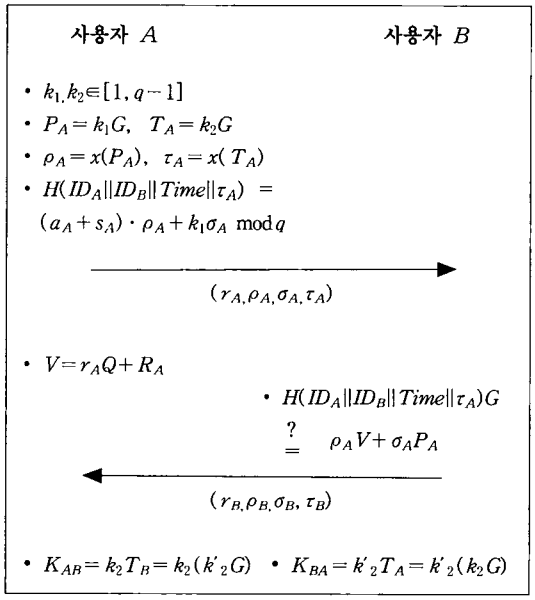
- **사용자** A : ① 단계에서 생성된 난수 k_2와 ②단계에서 받은 τ_B를 이용하여
  $K_{AB} = k_2 T_B = k_2(k'_2 G)$
  를 계산한다.

- **사용자** B : 위와 마찬가지로,
  $K_{BA} = k'_2 T_A = k'_2(k_2 G)$
  를 계산한다.

따라서, $K = K_{AB} = K_{BA}$ 임이 명백하고, 공동된 K를 사용하여 A와 B의 동일한 세션 키를 공유한다.

다음은 표는 제안된 프로토콜을 도식으로 표현한 것이다.

〔표 1〕 제안 프로토콜



다음은 ②단계의 3)의 검증과정을 자세히 증명하자: 만일 사용자 A가 보낸 정보 $(r_A, \rho_A, \sigma_A, \tau_A)$가 공격자나 제 3의 원인에 의해 변조되지 않았다고 가정하자. 그러면 0

$$V = r_A Q + R_A = r_A a_C G + (a_A + k_A)G$$
$$= (r_A a_C + a_A + k_A)G = (a_A + s_A)G$$

을 만족한다.(SOM 스킴의 등록단계 ②와 ③ 과정에 의함). 또한

$$\rho_A V + \sigma_A P_A = [\rho_A(a_A + k_A)]G + \sigma_A k_1 G$$
$$= (\rho_A(a_A + k_A) + \sigma_A k_1)G \quad (①의2)에 의해)$$
$$= H(ID_A||ID_B||Time||\tau_A)G$$

를 만족한다.

Ⅳ. 제안된 프로토콜의 안전성

본 논문에서 제안된 프로토콜은 타원곡선 암호법(ECC)를 사용하고 있으며 ECDSA와 ECDH 키 교환 방식을 사용하고 있다. 타원곡선의 사용은 대역폭의 효과적인 사용과 적은 계산량을 요구할 뿐만 아니라 유한체의 곱셈군 기반의 알고리즘들을 무력하게 만드는데 유용한 homomorphism 공격과 방정식공격(equation attack)을 방어하는데도 유용하다.[4] 제안된 알고리즘의 안전성은 암호학적으로 안전한 타원곡선에서의 이산대수문제(ECDLP)와 Diffie-Hellman 문제(ECDHP)의 어려움에 기반을 두고 있다. 또한 본 알고리즘은 크게 SOM 스킴의 등록단계에서의 안전성[9]과 ECDSA의 안전성[1]에 기반하여 안전성을 보장한다. SOM 스킴의 등록단계의 안전성은 KC로부터 사용자 A에게 전달하는 정보 (r_A, s_A)를 공격자가 위조(forgery)할 확률은 무시할(negligible) 만하다[9]는 것에 근거한다. 또한 최근 D. Brown에 의해 타원곡선이 generic 군으로 설계되고(model) 해쉬함수의 충돌회피(collision-resistant)성을 기반으로 ECDSA의 안전성을 증명하였다.[1]

[가정]

ECDSA에서 비밀정보를 모르는 공격자가 유효한 서명쌍 (ρ, σ)를 위조(forgery)할 확률은 무시할(negligible) 만하다.

위 가정을 기반으로 제안된 프로토콜의 안전성을 살펴보자.

- **반복공격(Replay Attack)** : 공격자가 사용했던 정보들을 다시 사용한다면 검증단계인 ②의 3)에서

해쉬함수 $H(..\|time\|..)$ 내부의 $Time$이 변경되어 검증과정을 통과할 수 없다.

- **공모공격(Conspiracy Attack)** : n명의 사용자 A_i들이 공모하여 KAC의 비밀키인 a_C를 알아내기 위해서 그들은 n개의 (r_{A_i}, s_{A_i}) 정보를 가지고 연립방정식

$$s_{A_i} = k_{a_i} + r_{A_i} a_C \mod q \quad (1 \le i \le n)$$

을 풀어야 한다. 그러나 모든 사용자에게 k_{A_i}는 비밀정보이고 서로 다르게 주어진다면 이 문제를 푸는 것은 불가능하다.

- **위장공격(IA:Impersonation Attack)** : 공격자가 사용자 A로 위장하여 사용자 B를 속이려한다고 가정하자. 먼저 공격자가 r_A를 변조하지 않았을 경우 ②의 3) 검증과정을 통과하기 위해서는 $a_A + s_A$을 알아내거나 $a_A + s_A$를 모르고 $ID_A\|ID_B\|Time\|\tau'$에 대한 정당한 서명 값 ρ', σ'을 얻어야한다. 전자는 ECDLP에 의해 후자는 ECDSA의 안전성 가정에 의해 공격이 성공할 확률은 아주 적다(negligible). 이제 공격자가 r_A를 변조하여 $r'_A \neq r_A$로 하여 정보 $(r'_A, \rho'_A, \sigma'_A, \tau'_A)$을 만들어 검증과정을 통과했다고 가정하자. 가정에 의해 공격자는 비밀정보 $(a'_A + s'_A)$를 알고 있으며 이를 사용하여 $ID_A\|ID_B\|Time\|\tau'_A$에 대한 정당한 서명 값 ρ'_A, σ'_A를 얻었다. (비밀 정보 $(a'_A + s'_A)$를 알지 못하고 정당한 서명을 위조할 확률이 아주 적기 때문). ②의 3) 검증과정에서 알 수 있듯이

$$(a'_A + s'_A)G = r'_A Q + R'_A \qquad (2)$$

를 만족해야 한다. 여기서 R'_A는 $r'_A H(ID_A) \mod p$를 x-좌표로 갖는 타원곡선상의 한 점이다. 따라서 공격자는 식 (2)를 만족하는 $r'_A, a'_A + s'_A$를 만들 수 있어야 한다. 그러나 비밀정보 a_C를 알지 못하고 메시지 ID_A를 복원하는 서명 값 (r'_A, s'_A)를 얻는 것은 확률적으로 불가능하다.[9] 그러므로 본 프로토콜은 위장공격을 방어할 수 있다.

- **알려지지 않은 키 공유 공격(USA:Unknownkey Share Attack)** : SOM 스킴에서와 달리 제안된 프로토콜은 키 교환 스킴이 실행된 후에 공유된 세션 키는 변조되지 않았다는 것을 사용자에게 확신시켜준다. 왜냐하면 만일 공격자가 사용자 A로부터 사용자 B로 전송되는 정보 중 τ_A를 $\tau'_A \neq \tau_A$로 변조하여 사용자 B의 ②의 3) 검증과정을 통과하기 위해서는 해쉬함수 $H(ID_A\|ID_B\|Time\|\tau'_A)$ $H(ID_A\|ID_B\|Time\|\tau_A)$를 만족하는 τ'_A를 택해야 한다. 하지만 이것이 성공할 확률은 해쉬함수의 충돌회피 성질에 의해 무시할(negligible) 만하다.

- **Perfect Forward Secrecy(PFS)** : 제안된 스킴은 세션 키 생성과정에서 사용자의 long-term 비밀정보와 상관없는 난수 k_2)를 사용하여 Diffie-Hellman 키 교환 방식을 사용하므로 perfect forward secrecy하다. 만일 공격자가 사용자 A의 $a_A + s_A$를 알았다고 가정하자. 사용자 B와 이미 사용했던 세션 키 $K_{AB} = k_2 T_B$를 아는 것은, k_2를 알지 못할 경우에, ECDHP를 푸는 것과 동치이다. 또한 난수 k_2를 알기 위해서는 $T_A = k_2 G$의 ECDLP를 풀어야 한다. 따라서 본 키 교환 스킴은 perfect forward secrecy하다.

- **KAC의 비밀키 노출 경우** : 제안된 프로토콜은, 비록 KAC의 비밀키가 노출된다고 해도 사용자의 비밀은 직접 드러나지 않는다는 특성을 가지고 있다. 뿐만 아니라 KAC의 비밀키 노출은 악의의 사용자를 만들 수 있지만 기존의 등록된 사용자간의 공유 세션 키들을 알아낼 수 는 없다. 다라서 기존의 인수분해문제를 기반으로 하는 키분배 프로토콜[6,10]과는 달리 KAC의 비밀키가 노출되더라도 perfect forward secrecy하다.

〔표 2〕 기존의 프로토콜과의 비교

		제안 프로토콜	SOM [9]	Günther [8]	Okamoto -Tanaka [6]
기반		ECDLP ECDH	ECDLP ECDH	DLP DH	FP DH
통신회수		2	2	4	2
안전성	IA	o	o	o	x
	USA	o	x	o	o
	PFS	o	x	o	o

* o와 x는 각 공격에 대하여 강함과 약함을 나타낸다.

V. 결 론

본 논문에서는 SOM 프로토콜 안전성의 취약점을 분석하였고 이들의 취약점을 보완한 사용자 인증과 인증된 키 교환이 가능한 ID 기반의 프로토콜을 제안하였다. 이 제안 프로토콜은 또한 메시지 복원 서명기법과 ECDSA 기법을 적용하였다. 또한 무선 환경에 적합한 ECC를 사용하여 계산량과 통신량의 효율성을 높였고 상대방 인증과 키 교환을 동시에 수행하는데 오직 2회의 통신만이 요구되는 장점을 지닌다. 또한 제안 프로토콜은 사용자들이 KAC에 초기 등록을 위한 단계를 제외하고는 사용자와 KAC 간에는 추가의 상호작용이 요구되지 않으며 상대방과의 상호 인증과 인증된 세션 키 분배가 가능하다. 이 제안된 프로토콜의 안전성은 타원곡선 이산대수 문제(ECDLP)와 Diffie-Hellman 문제(ECDHP)의 어려움에 기반을 두며 반복공격, 공모공격, 위장공격, 알려지지 않은 키 공유공격에 강하며 또한 perfect forward secrecy를 보장한다.

제안된 ID 기반의 인증 및 키분배 프로토콜은 사용자의 신분을 유일하게 확인할 수 있는 신분정보(ID)를 기반으로 하는 모든 시스템(E-mail, 신용카드, 이동전화등)에 적용가능하다. 하지만 ID 기반의 시스템을 현실적으로 사용하기 위해서는 "키 분실로 인한 키 관리 문제"등 해결해야할 문제점들이 존재한다. 따라서 ID 기반 시스템의 현실적 사용에 있어 발생하는 문제점들과 이들에 대한 해결책 연구가 향후 연구되어져야 한다.

참 고 문 헌

[1] Daniel R.L. Brown, IEEE P1363: Research Contributions, January 16, 2001.

[2] T. El-Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Trans. Inform. Theory, Vol. IT-31, pp. 469~472,1985.

[3] G. Günther, "An Identity-based key exchange protocol," in EUROCRYPT' 89, Lec. Notes in Comp. Sci. Vol. 434, Springer Verlag, pp. 29~37, 1990.

[4] A. Miyaji, "Strengthened message recovery signature scheme," Proc. Sym. on Crypto. and Infor. Secu., SCIS'96-2C,1996.

[5] K. Nyberg and R.A. Rueppel, "A new segnature scheme based on the DSA giving message recovery," Proc. ACM Conference on Compu. and Commun. Sec., ACM, 1993.

[6] E. Okamoto, K. Tanaka, "Identity-based Information Security Management System for Personal Computer Networks," IEEE J. Select. Areas Commun., Vol. SAC-7, pp. 290~294, 1989.

[7] R.L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystem," Commun. ACM, Vol. 21, pp. 120~126, 1978.

[8] A. Shamir, "Identity-based cryptosystems and signature schemes," in CRYPTO'84, Santa Barbara, CA, 1984, pp. 47~53.

[9] H.Sakazaki, E.Okamoto, M.Mambo, "Constructing identiy-based key distribution systems over elliptic curves," IEICE TRANS. Fundamentals, Vol. E81-A, pp. 2138~2143, 1998.

[10] S.P. Shieh, W.H. Yang, and H.M. Sun, "An authentication protocol without trusted third party," IEEE Commun. Lett., Vol. 1, pp. 87~89, May 1997.

[11] S. Tsujii, T. Itho, and K. Kurosawa, "ID-based cryptosystem using discrete logarithm problem," Electron. Lett. Vol. 23, pp. 1318~1320, 1987.

[12] S-M Yen, "Cryptanalysis of an Authentication and Key Distribution Protocol," IEEE Commun. Lett., Vol. 3, pp. 7~8, Jan 1999.

〈著者紹介〉

박 영 호 (Young-Ho Park) 정회원
1990년 2월 : 고려대학교 수학과 학사
1993년 2월 : 고려대학교 수학과 석사
1997년 2월 : 고려대학교 수학과 박사
2001년~현재 : 고려대 정보보호기술연구센터 객원조교수
〈관심분야〉 정수론, 공개키 암호, 암호 프로토콜

박 호 상 (Ho-Sang Park) 정회원
1997년 2월 : 시립인천대학교 물리학과 학사
2000년~현재 : 숭실대학교 대학원 정보통신공학과 석사과정
〈관심분야〉 사용자 인증, Key Management, PKI

정 수 환 (Souhwan Jung) 정회원
1985년 2월 : 서울대학교 전자공학과 학사
1987년 2월 : 서울대학교 전자공학과 석사
1988년~1991년 : 한국통신 전임연구원
1996년 : 미 워싱턴 주립대(시애틀) 박사
1996년~1997년 : Stellar One SW Engineer
1998년~현재 : 숭실대학교 정보통신전자공학부 조교수
〈관심분야〉 VoIP security, 사용자 인증, Cryptography, PKI