# 개인정보에 기초한 인증, 서명 및 키 분배 통합 시스템

°이 형철, 하 재철, 문 상재

경북대학교 전자공학과

# ID-based integrated cryptosystem for authentication, digital signature, and key distribution

°Hyung-Chul Lee, Jae-Cheol Ha, Sang-Jae Moon

Dept. of Electronics, Kyungpook National University

요 약 문

개인정보에 기초한 암호법은 통신자간 인증문제를 극복하고 공개 키 화일을 제거할 수 있는 방안으로 많이 연구되고 있다. Harn-Yang은 AMV 서명 기법에 기반하여 사용자 인증, 디지탈 서명과 키 분배가 가능한 개인정보에 기초한 암호법을 제시하였다. 본 논문에서는 이를 분석하고 Moon의 서명 기법을 사용하여 개인정보에 기초한 사용자 인증, 디지탈 서명과 키 분배 시스템을 제안한다. 이 시스템의 안전성은 이산대수에 근거하며, 연산량과 시스템 구현 측면에서 효율적이다. 대화형 간접 인증 키 분배 방식을 개선하였고 E-mail 등의 일방향 통신에 적합한 키 분배 방안을 제시한다

## 1. 서 론

1984년 Shamir[1]는 개인정보(identity, ID)에 기초한 암호법의 개념을 처음으로 도입하였고, 이후 인증, 디지탈 서명, 키 분배 등에 관한 연구들이 있다[2,3]. 이 암호법은 일종의 비대칭 키 암호법으로 유일한 개인의 성명, 주민등록번호, 주소 혹은 전화번호등 개인정보를 공개 키로 사용하는 것이다. 일반에게 공인된 신상의 정보를 사용하므로, Diffie-Hellman 혹은 RSA(Rivest, Shamir, Adleman) 공개 키 방법에서 개인정보와 관련이 없는 랜덤수 형태의 공개 키 화일을 인증하는 문제를 쉽게 해결하는 것이다.

개인정보에 기초한 암호 시스템은 키 관리 센타(key management center, KMC)의 신뢰가 절대적인 가정이다. 왜냐하면 키 관리 센타가 시스템을 구성하는 기본 파라미터를 설정하고 비밀 키를 생성하기 때문이다. 개인정보를 기초로 생성된 비밀 키와 시스템 관련 정보등은 IC 카드와 같은 물리적으로 보호된 매체를 통해 발급된다. 특히 한 사용자의 암호 시스템에 사용하는 개인정보는 다른 사람의 개인정보와 무관하므로 새로운 가입자가 등록시에도 다시 갱신할 필요가 없다. 카드 발급후에는 센타와의 별도의 통신이 없어도 통신을 원하는 상대방의 ID를 이용하여 직접 암호 프로토콜을 구현할 수 있다. 키 관리 센타의 설립이 용이하고 신뢰가 보장되기 용이한 여건하에서 즉, 일반 공중망이나 대형 통신망보다는 기업체, 은행 혹은 개인 통신망 등 사용자가 제한된 그룹에서 사용하기가 좋다. 이 암호법은 통신자간 인증문제를 극복하고 공개 키 디렉토리를 제거할 수 있는 장점에도 불구하고 시스템 구현에 어려움이 있다.

D-H 혹은 RSA 암호법에서는 공개 키가 서로 같은 구조로 되어 있어 다양한 형태의 키 분배 방

식을 구현하기가 용이하다. 개인정보를 공개 키 자체로 사용하는 것은 공개 키의 인증문제를 해결하는데 가장 효과적이다. 그러나 공개 키가 서로 상관이 없는 개인정보 자체이므로 서로 다른 구조를 갖고 있다. 그러므로 다양한 형태의 키 분배 방식을 구현하기가 쉽지 않다 것이 단점이 되기도 한다.

이러한 문제점을 극복하기 위해서 개인정보와 이를 간접적으로 관련시킨 공개 키를 사용하는 키 분배 방법이 연구발표되었다[4,5]. 이 방법으로는 one-pass 키 분배 및 대화형 키 분배 시스템 등을 비교적 다양하게 구현할 수 있고 인증 및 디지탈 서명과 같은 보호 서비스도 제공할 수 있다. 반면에 개인정보를 공개 키 자체로 하는 방법에 비해서는 계산량이 비교적 많다.

Harn-Yang은 AMV(Agnew, Mullin, and Vanstone)의 서명 기법[6]을 이용하여 개인정보에 기초한 사용자 인증, 디지탈 서명 그리고 키 분배를 할 수 있는 효율적인 방안을 제시하였다[7]. 본 논문에서는 Harn-Yang의 암호 시스템을 분석하고 계산량을 줄일 수 있고 구현 측면에서 효율적인 방법을 제시한다. 이를 바탕으로 사용자 인증, 디지탈 서명 및 키 분배를 통합할 수 있는 방안을 제시하고, E-mail 등의 일방향 통신에 적합한 키 분배 방안도 제시한다

## 2. 개인정보에 기초한 Harn-Yang의 암호 시스템

1984년 Shamir에 의하여 개인을 식별하는 유일한 개인정보를 공개 키로 하는 비대칭 키 암호법을 발표하였다. 이 암호법의 특징은 개인정보를 공개 키 자체 혹은 연관하여 사용하므로 공개 키 화일의 인증문제를 쉽게 해결하는 것이다. 키관리 센터의 설치와 신뢰의 보장이 쉬운 여건에서는 개인정보에 기초한 암호법이 공개 키 화일의 관리가 간단한 장점을 지닌다. 그러나 개인정보를 공개 키 자체로 사용하는 제한조건이 사용자 인증, 디지탈 서명 및 키 분배 서비스간의 통합성과 다양한 활용에는 제한적인 요소가 된다. 이러한 제한성을 벗어나기 위해서 개인정보를 공개 키 자체로 사용하는 대신, 개인정보와 이에 기초한 공개 키를 사용하는 암호법들이 연구되었다.

각 가입자는 개인정보를 센타에 등록하며, 센타는 이에 상응하는 비밀 키를 IC카드에 저장하여 해당 가입자에게 배부한다. 송신자 A는 상대방의 개인정보에 기초하여 세션 키를 만들고 이를 사용하여 메세지를 암호화하여 전송한다. 수신자 B는 자기 개인정보에 연관된 비밀 키에 기초하여 동일한 세션 키를 만들어 메세지를 복호한다. 이 과정에서 사용되는 개인정보는 해당 통신자를 유일하게 식별하는 정보인 공개 키이므로 이를 인증할 필요가 없어진다. 특히 한 사용자의 암호 시스템에 사용하는 개인정보는 다른 사람의 개인정보와 무관하므로 새로운 가입자가 등록시에도 다시 갱신할 필요가 없다. IC 카드 발급후에는 센타와의 별도의 통신 없이 통신을 원하는 상대방의 개인정보를 이용하여 직접 암호 프로토콜을 구현할 수 있다.

Harn-Yang은 AMV의 디지탈 서명 방식에 기초하여 사용자 인증, 디지탈 서명과 키 분배가 가능한 개인정보에 기초한 암호법을 제시하였다. 일반적으로 ID에 기초한 암호 시스템은 시스템 구성 단계, 사용자 등록 단계 그리고 응용 단계로 나누어진다. 시스템 구성 단계와 사용자 등록 단계는 키 관리 센타에서 수행하며 응용 단계는 가입된 통신자간에 이루어진다.

### 2.1 시스템 구성 및 사용자 등록

키 관리 센타는 다음 절차에 의해 시스템을 구성한다. (1) 센타는 소수를 모듈라 p로 선택한다. (2) 유한체 GF(p)상의 원시원 g를 선택한다. (3) 일방향 함수 f를 선택한다. (4) 센타는 $\gcd(X, p-1) = 1$을 만족하는 비밀 키 $X \in (1, p-1)$를 선택한다. (5) 센타는 공개 키 $Y = g^X \bmod p$ 를 계산한다. 여기서 일방향 함수 f와 p, g, Y는 사용자에게 공개하고 비밀 키 X는 비밀로 간직한다.

사용자가 처음 자신의 ID를 센타에 등록하면 센타는 그에 대응하는 비밀 키를 계산하여 IC카드와 같이 물리적으로 안전한 매체를 통해 사용자에게 발급한다. 즉, AMV의 디지탈 서명 방식에서 메세지 m에 대한 디지탈 서명을 ID에 대한 디지탈 서명으로 대치하여 생성한 s와 r을 센타가 사용자에게 발급한다. s는 사용자의 비밀 키에 해당하는 비밀 정보이며 r는 공개할 수 있는 정보이다. 구체적인 과정은 다음과 같다.

(1) 센타는 $0<k<p$를 만족하는 랜덤수 k를 선택한다.

(2) 센타는 $r = g^k \bmod p$를 계산한다.

(3) 센타는 가입자의 ID를 일방향 함수 f를 사용하여 확장한다. 즉, $EID = f(ID)$이다.

(4) 센타는 다음 식을 만족하는 s를 구한다.

$$s = (EID - k \cdot r) \cdot X^{-1} \bmod p-1$$

(5) 센타는 사용자에게 (s, r)을 발급한다.

### 2.2 사용자 인증

시도 응답형(challenge-response type)으로 사용자 A가 확인자 B에게 자신의 신분을 증명하는 과정을 기술하면 다음과 같다.

(1) 사용자 A가 확인자인 B에게 자신의 $(ID_A, r_A)$ 정보를 전송한다.

(2) 확인자 B는 랜덤 홀수 $v_B$를 선택하여 $W = Y^{v_B} \bmod p$를 계산해서 A에게 보낸다. 여기서, $v_B \in (1, p-1)$이고, $\gcd(v_B, p-1) = 1$을 만족해야 하며, Y는 센타의 공개 키이다.

(3) A는 $Z = W^{s_A} \bmod p$를 계산하고 Z를 B에게 보낸다.

(4) B는 $EID_A = f(ID_A)$를 구한 후, 다음 방정식을 확인하여 등식이 성립하면 B는 A를 인증한다. 즉 $g^{EID_A} = r_A^{r_A} \cdot Z^{V_B^{-1}} \bmod p$ 이다.

### 2.3 디지탈 서명

서명자가 메세지 m에 서명을 하고자 함을 가정할 때 센타가 발급한 비밀 키 s는 $\gcd(s, p-1) = 1$를 만족하는 홀수여야 한다. 서명 방식은 원래의 AMV 서명을 이용한다. 구체적인 과정을 기술하면 다음과 같다.

< 서명 생성 과정 >

(1) 랜덤수 $\sigma$, $0<\sigma<p-1$, 를 발생한다.

(2) $\delta = Y^{\sigma} \bmod p$ 를 계산한다.

(3) $m' = f(m)$를 구한다.

(4) $\eta = (m' - \sigma \cdot \delta) \cdot s^{-1} \bmod p-1$ 를 계산한다.

(5) 서명 쌍 $(\delta, \eta)$에 메세지 m과 r을 추가한 $(m, r, \delta, \eta)$를 검증자에게 전송한다.

< 서명 확인 과정>

(1) $m' = f(m)$를 구한다.

(2) 확인자는 서명자의 ID를 이용하여 $EID = f(ID)$를 구한 후, 다음 등식을 만족하면 메세지 m에대한 서명을 검증한다. 즉, $Y^{m'} = \delta^{\delta} \{ g^{EID} r^{-r} \}^{\eta} \bmod p$ 이다.

### 2.4 키 분배

공개 키 인증 문제를 해결하는 방법의 하나로써 Shamir의 개인정보를 공개 키로 사용하는 개념을 키 분배 방식에 적용한 것이 개인정보에 기초한 키 분배 시스템(ID-based key distribution system, IDKDS)이다. 이를 사용자간의 사전 통신을 통해 세션 키를 공유하는 대화형(interactive)방식과 사전 통신 없이도 공개 자료만을 사용하여 공통의 세션 키를 계산할 수 있는 비대화형(noninteractive) 방식으로 대별할 수 있다.

대화형은 동시에 쌍방간에 통신이 가능해야 하므로 일방적으로 암호화하여 보내는 전자메일의 전송이나 암호화된 화일을 저장해 두는 등의 환경하에서는 실용화되기가 어렵다. 이런 환경하에서는 비대화형이 적합하다. 사전통신없이 공개된 자료만으로 키를 생성하는 비대화형은 변화가 없는 공개된 자료만을 사용하므로 근본적으로는 매번 동일한 세션 키를 만들게 된다. 만약 한번 키가 제 3자에게 노출되면 이전의 모든 암호화된 내용이 복호되므로 그대로는 실용될 수 없는 문제점이 있다.

Harn-Yang은 간접 인증만 제공하고 통신하고자 하는 두사용자가 같을 경우는 공유하는 비밀 세션 키가 항상 일정한 키 분배 방식과 직접 인증을 제공하면서 두사용자가 같아도 매 키 분배마다 공유하는 비밀 세션 키가 다른 키 분배 방식을 제안하였다. 간접인증 방식에서는 상대 통신자의 ID에 기초하여 공개 키를 구성하는 방법에 D-H의 키 분배 방식[8]을 적용한 것이다. 사용자 A와 사용자 B가 간접인증 기능을 제공하면서 비밀 세션 키를 공유하는 구체적인 과정은 다음과 같다.

(1) 사용자 A는 자신의 $(ID_A, r_A)$를 사용자 B에게 전송하고 사용자 B도 $(ID_B, r_B)$를 A에게 전송한다.

(2) A는 비밀 공유 세션 키인 $K_{AB}=(g^{EID_B}r_A^{-r_B})^{s_A}=(Y^{s_B})^{s_A} \mod p$를 계산하며, 또한 B도 비밀 공유 세션 키인 $K_{BA}=(g^{EID_A}r_A^{-r_A})^{s_B}=(Y^{s_A})^{s_B} \mod p$를 계산할 수 있다.

위와 같이 A와 B가 공유하는 비밀 세션 키는 $Y^{s_A s_B}$로 항상 일정하다. 이 방식의 공유 비밀 세션 키가 D-H 원형의 키 분배[8]와 같이 두 사용자의 비밀 키의 멱승 형태이므로 비밀 키를 모르는 비인가자는 비밀 세션 키를 생성할 수 없으므로 간접 인증만 제공한다. 그리고 매번 동일한 세션 키를 만들게 되므로 실제 사용하기에는 문제점이 있다.

반면 두번째로 제안한 키 분배 방식은 비밀 세션 키를 공유하는 과정에서 상대의 공개 키를 인증하기 때문에 직접 인증 기능을 제공한다. 즉 세션 키를 만드는 과정에 필요한 정보를 디지탈 서명기법을 이용하여 인증한다. 사용자 A와 사용자 B가 비밀 세션 키를 공유하는 구체적인 과정은 다음과 같다.

(1) 사용자 A와 B는 각각 랜덤수 $v_A, v_B$를 선택한다.

(2) A는 $W_A = Y^{v_A} \mod p$를 계산하고, B는 $W_B = Y^{v_B} \mod p$를 계산한다.

(3) 일방향 함수 f를 이용하여 A는 $E_A = f(W_A)$를 구하고, B는 $E_B = f(W_B)$를 구한다.

(4) A는 $\eta_A=(E_A-v_AW_A)s_A^{-1} \mod p-1$를 계산하고
B는 $\eta_B=(E_B-v_BW_B)s_B^{-1} \mod p-1$를 계산한다.

(5) A는 B에게 $(ID_A, r_A, W_A, \eta_A)$를 전송하고, B는 A에게 $(ID_B, r_B, W_B, \eta_B)$를 전송한다.

(6) A는 $W_B$에대한 서명을 다음 식으로 검증하여 등식이 성립하면 $K_{AB} = W_B^{v_A}$를 계산하여 공유 비밀 세션 키를 생성한다. 즉 검증식은 $Y^{E_B} = W_B^{W_B}\{g^{EID_B}(r_B^{-r_B})\}^{\eta_B} \mod p$ 이다.
B도 위와 동일하게 $W_A$에대한 서명을 검증하고 다음 등식이 성립하면 비밀 세션 키인

$K_{BA} = W_A{}^{V_B}$를 계산한다. 즉 검증식은 $Y^{E_A} = W_A^{W_A}\{g^{EID_A}(r_A^{-r_A})\}^{r_A} \bmod p$ 이다.

Harn-Yang이 제시한 개인정보에 기초한 암호법은 다음의 몇가지 특징을 가지고 있다. 첫째, 키 관리 센타가 사용자에게 비밀 정보를 발급하는 단계에서 AMV의 디지탈 서명을 사용하고 있다. 이 서명 방식은 서명 생성시 통신자마다 역수 계산을 하는 ElGamal 서명 방식[9]을 개선한 것으로 센타의 비밀 키에 대한 역수 계산을 1회만 하도록 하였다. 그러나 카드 발급후 각 사용자가 자신의 서명을 생성할 때는 자신의 비밀 키에 대한 역수 계산이 필요하다. 그러므로 비밀 키 s의 역수 계산 결과를 저장해야 하거나 통신시마다 매번 계산해야 한다. 또한 센타에서 비밀 키 s가 p-1과 서로 소(relatively prime)인지의 확인과정이 필요하다. 둘째, 통신자간 응용단계에서 공개 키 $Y^s$는 $g^{EID} \cdot r^{-r} \bmod p$ 로 계산된다. 이 계산은 2회의 멱승연산이 필요하다. 또한 서명 검증시에는 공개 키 계산과정을 제외하고 3회의 멱승이 필요하다. 셋째, 간접 인증 대화형 키 분배 방식에서 통신시마다 매번 동일한 세션 키가 생성되므로 실제 사용할 경우 문제점이 있고 일방향 통신을 위한 키 분배 방식은 제시되지 않았다.

## 3. 개인정보에 기초한 암호 시스템의 제안

개인정보를 공개 키 생성에 이용하는 암호 시스템을 설계하는 방법은 크게 RSA서명을 이용하는 경우[4]와 ElGamal 형태의 서명 기법을 이용하는 경우[5]로 크게 구분할 수 있다. Harn-Xu는 기존의 발표된 서명 기법을 포함하여 ElGamal 형태의 디지탈 서명을 일반화 하였다[10]. 일반화된 ElGamal 형태의 서명 방정식은 다음과 같다.

$$ax = bk + c \bmod \phi(p)$$

여기서 계수 (a, b, c)는 (m, r, s) 자체 혹은 그것의 수학적인 조합으로 이루어진다. 단, m은 서명할 메세지이고 r과 s는 메세지에 대한 서명이며 x는 사용자의 비밀 키 이며 k는 불규칙 정수이다. 그리고 $\phi(p)$는 p에 대한 Euler 함수값이다. Harn-Xu는 일반식 중에서 안전성이 고려된 서명방법을 18가지로 구분하였다.

ElGamal 형태의 서명 방식을 사용하여 키 관리 센타에서 개인정보에 기초한 서명 쌍을 생성한 후 통신자간 응용 단계에 사용하기 위해서는 가급적 다음 성질을 만족하는 서명 방식이 적합하다. 첫째, 공개하는 r과 ID만으로 공개 키인 $g^s$나 $Y^s$를 계산할 수 있어야 한다. 둘째, 공개 키를 생성하는 계산량이 상대적으로 적은 서명방법을 이용하는 것이 효율적이다. 셋째, 서명과 검증 계산량이 적고 메세지 해쉉이 효율적이어야 한다. Harn-Xu가 구분한 ElGamal 형태의 서명 방식 중 Moon이 제시한 서명 방식이 위의 성질들을 만족한다. 그러므로 이 서명 방식을 사용하여 개인정보에 기초한 암호 시스템을 구성하는 방안을 제시한다.

### 3. 1 시스템 구성 및 사용자 등록

키 관리 센타는 다음 절차에 의해 시스템을 구성한다. (1) 센타는 소수를 모듈라 p로 선택한다. (2) $q \mid p-1$인 소수를 모듈라 q로 선택한다. (3) $g = h^{(p-1)/q} \pmod p$인 g를 선택한다. 여기서, $g > 1$이고, h는 $0 < h < p$인 임의의 정수이다. (4) 일방향 해쉬함수 H를 선택한다. (5) 센타는 비밀 키 $X$ ( $0 < X < q$)를 선택한다. (6) 센타는 공개 키 $Y = g^X \bmod p$를 계산한다. 여기서 H, p, q, g, Y는 각 사용자에게 공개하고 비밀 키 X는 비밀로 간직한다.

사용자가 처음 자신의 ID를 센타에 등록하여 센타가 서명 s와 r을 생성하는 구체적인 과정은 다음과 같으며 그림 1에 나타내었다.

(1) 센타는 0<k<q 를 만족하는 랜덤수 k를 선택한다.

(2) 센타는 $r = g^k \pmod p$로 계산한다.

(3) 센타는 $EID = r \cdot H(ID)$를 구하고 $s = k - X \cdot EID \pmod q$를 계산한다.

(4) 센타는 사용자에게 (s, r)을 발급한다.

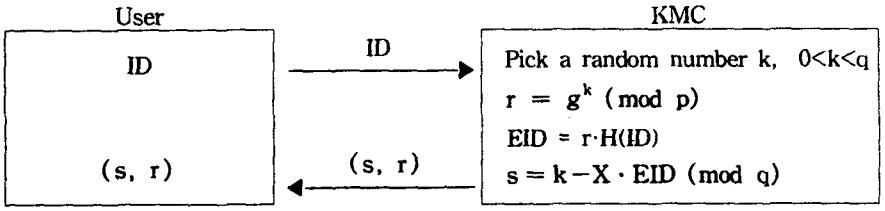


Fig. 1. User registration phase.

### 3. 2 사용자 인증

시도 응답형으로 사용자 A가 확인자 B에게 자신의 신분을 증명하는 과정을 기술하면 다음과 같고 그림 2에 나타내었다.

(1) 사용자 A가 확인자인 B에게 자신의 $(ID_A, r_A)$ 정보를 전송한다.

(2) 확인자 B는 랜덤수 $v_B$ ( $1 < v_B < q$)를 선택하여 $W = g^{v_B} \bmod p$를 계산 후 A에게 전송한다.

(3) A는 $Z = W^{s_A} \bmod p$를 계산하고 Z를 B에게 전송한다.

(4) B는 $EID_A = r_A \cdot H(ID_A) \bmod q$를 구한 후, 다음 방정식을 확인하여 등식이 성립하면 B는 A를 인증한다. 즉 $(r_A \cdot Y^{-EID_A})^{v_B} = Z \bmod p$ 이다.

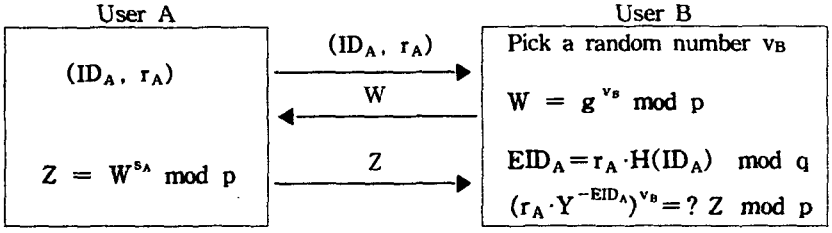


Fig. 2. User authentication scheme.

### 3.3 디지탈 서명

다음은 Moon 서명 방식을 사용한 메세지 m에 대한 서명 생성 및 검증과정이다.

< 서명 생성 과정 >

(1) 랜덤변수 $\sigma$, $0 < \sigma < q$, 를 발생한다.

(2) $\delta = g^{\sigma} \bmod p$를 계산한다.

(3) 메세지 m에대한 $m' = H(m)$를 구한다.

(4) $\eta = \sigma - s\delta m' \bmod q$를 계산한다.

(5) 서명쌍 $(\delta, \eta)$을 포함한 $(m, r, \delta, \eta)$을 검증자에게 전송한다.

<서명 확인 과정>

(1) $m' = f(m)$를 구한다.

(2) $EID = r \cdot H(ID) \mod q$를 계산한다.

(3) $\delta = g^{\eta} \cdot (r \cdot Y^{-EID})^{\delta m'} \mod p$를 검증한다

### 3.4 키 분배

제안한 시스템에서도 Harn-Yang이 제시한 바와 같이 D-H의 키 분배 방식을 그대로 적용할 수 있으며 두 통신자간에 교환하는 ID와 r로써 공개 키를 생성하는 과정과 인증을 위한 서명과정만이 다르다. 즉 사용자의 공개 키는 $g^s = r \cdot Y^{-EID} \mod p$ 이다. 다음은 직접인증 기능을 제공하면서 통신시마다 사용자 A와 B가 다른 키를 공유하는 과정을 기술한 것이며 그림 3에 나타내었다.

(1) 사용자 A와 B는 각각 랜덤수 $v_A$, $v_B$를 선택한다. 단, $0 < v_A, v_B < q$ 이다

(2) A는 $W_A = g^{v_A} \mod p$를 계산하고, B는 $W_B = g^{v_B} \mod p$를 계산한다.

(3) A는 $E_A = W_A \cdot H(W_A) \mod q$를 구하고, B는 $E_B = W_B \cdot H(W_B) \mod p$를 구한다.

(4) A는 $\eta_A = v_A - s_A \cdot E_A \mod q$를 계산하고 B는 $\eta_B = v_B - s_B \cdot E_B \mod q$를 계산한다.

(5) A는 B에게 $(ID_A, r_A, W_A, \eta_A)$를 전송하고, B는 A에게 $(ID_B, r_B, W_B, \eta_B)$를 전송한다.

(6) A는 $W_B$에대한 서명을 다음 식으로 검증하여 등식이 성립하면 $K_{AB} = W_B^{v_A}$를 계산하여 공유 비밀 세션 키를 생성한다. 즉 검증식은 $W_B = g^{\eta_B}(r_B \cdot Y^{-EID_B})^{W_B \cdot H(W_B)} \mod p$ 이다. B도 위와 동일하게 $W_A$에 대한 다음 검증식이 성립하면 비밀 세션 키인 $K_{BA} = W_A^{v_B}$를 계산한다. 즉 검증식은 $W_A = g^{\eta_A}(r_A \cdot Y^{-EID_A})^{W_A \cdot H(W_A)} \mod p$ 이다.

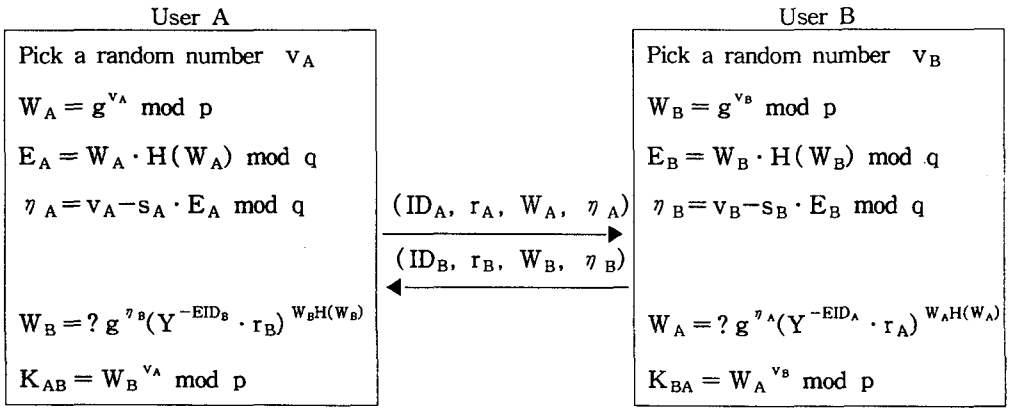


Fig. 3. Key distribution with direct authentication.

간접인증을 제공하는 대화형 키 분배 방식에서 Harn-Yang의 방식을 적용하면 매번 동일한 세션 키가 생성되는 문제점이 있다. 이를 개선하여 매 통신시마다 다른 키를 공유할수 있는 방법을 제시한

다. 사용자 A와 B가 다른 키를 공유하는 과정은 다음과 같으며 그림 4에 나타내었다.

(1) 사용자 A와 B는 각각 랜덤수 $t_A, t_B$를 선택한다. 단, $0 < t_A, t_B < q$ 이다

(2) A는 $T_A = g^{t_A} \bmod p$를 계산하고, B는 $T_B = g^{t_B} \bmod p$를 계산한다.

(3) A는 B에게 $(ID_A, r_A, T_A)$를 전송하고, B는 A에게 $(ID_B, r_B, T_B)$를 전송한다.

(4) A는 $EID_B = r_B \cdot H(ID_B) \bmod q$를 계산하고 세션 키를 다음과 같이 생성한다.

$$K_{AB} = (T_B \cdot r_B \cdot Y^{-EID_B})^{(s_A + t_A)} = g^{(s_B + t_B)(s_A + t_A)} \bmod p$$

B는 $EID_A = r_A \cdot H(ID_A) \bmod q$를 계산하고 세션 키를 다음과 같이 생성한다.

$$K_{BA} = (T_A \cdot r_A \cdot Y^{-EID_A})^{(s_B + t_B)} = g^{(s_A + t_A)(s_B + t_B)} \bmod p$$

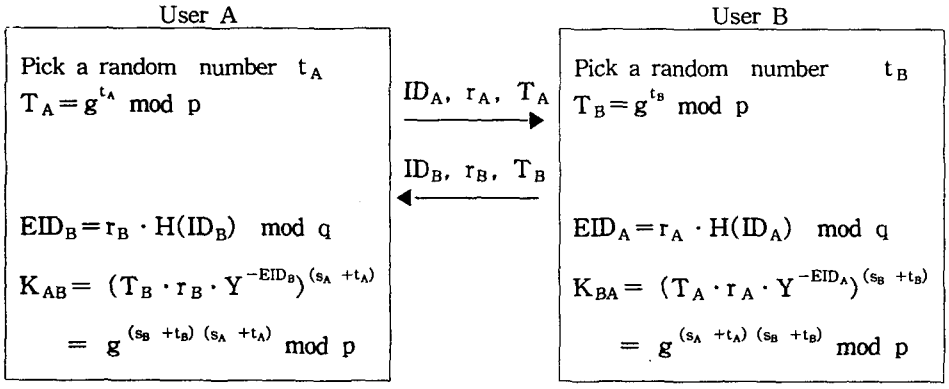


Fig. 4. Key distribution with indirect authentication.

이 키 분배 방식에서 전송정보 T나 r로부터 비밀정보 t나 s를 알수 없으며 세션 키를 계산하는 것은 이산 대수 문제와 같다. 즉, $g^{(s_A + t_A)}$와 $g^{(s_B + t_B)}$를 계산할 수 있으나 $g^{(s_B + t_B)(s_A + t_A)}$를 계산할 수 없다. 또한 통신 후에 s가 노출되었고 전송정보 T를 알고 있는 공격자라도 이전에 암호에 사용되었던 세션 키를 계산할 수 없어 비밀이 유지된다.

제안한 암호 시스템으로 one-pass로 인증된 세션 키를 공유하는 방법이 필요하다. 즉, 통신자 A는 B에게 자신의 불규칙 정수를 서명해서 r과 함께 전송하면 B는 서명 검증 후 D-H의 키 분배 방식에 적용하여 세션 키를 계산할 수 있다. 그러나 A가 공유 세션 키를 생성하기 위해서는 B의 공개 키가 필요하다. 즉, A는 B의 개인정보와 개인정보 관련 정보 r을 이용해야만 B의 실제 공개 키를 구할 수 있다. One-pass 키 분배 시스템의 경우에는 개인정보만이 공개 키가 아니므로 개인정보와 관련 정보 r를 함께 관리하는 공개 키 디렉토리가 있어야 한다. 공개 키 관련 정보 r는 센타에서 생성하므로 확인서는 필요하지 않으므로 검증과정도 필요하지 않다. 이러한 조건하에서 one-pass 메카니즘을 실현하는 과정을 기술하면 다음과 같다. 이를 나타낸 것이 그림 5이다.

(1) 사용자 A는 랜덤수 $v_A$( $0 < v_A < q$ )를 선택한다.

(2) A는 $W_A = g^{v_A} \bmod p$를 계산한다.

(3) A는 $E_A = W_A \cdot H(W_A) \bmod q$를 구한다.

(4) A는 $\eta_A = v_A - s_A \cdot E_A \bmod q$를 계산한다.

(5) A는 B에게 $(ID_A, r_A, W_A, \eta_A)$를 전송한다 .

(6) A는 세션 키를 다음과 같이 생성한다.

$EID_B = r_B \cdot H(ID_B) \bmod q$

$K_{AB} = (r_B \cdot Y^{-EID_B})^{v_A} \bmod p = g^{S_B \cdot v_A} \bmod p$

(7) B는 $W_A$에 대한 다음 검증식이 성립하면 비밀 세션 키인 $K_{BA} = W_A{}^{S_B} = g^{S_B \cdot v_A} \bmod p$를 계산한다. 즉 검증식은 $W_A = g^{\eta_A}(r_A \cdot Y^{-EID_A})^{W_A \cdot H(W_A)} \bmod p$ 이다.

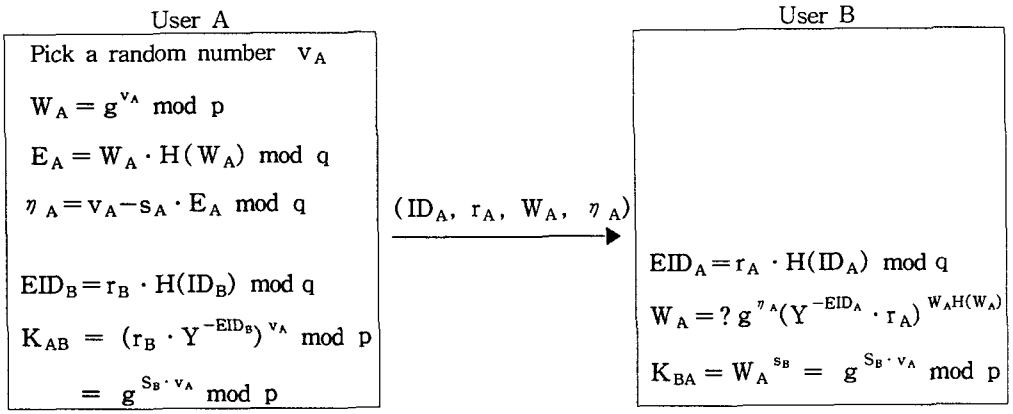


Fig. 5. One-pass key distribution with unilateral authentication.

## 4. 분석 및 시뮬레이션

### 4.1 비교 분석

Harn-Yang이 제시한 개인정보에 기초한 암호 방식은 3장에서 언급한 몇가지 단점이 있다. 이러한 문제를 해결하기 위해 키 관리 센타에서 효율적으로 비밀 키를 분배하고 연산량을 줄이는 서명 방식으로 Moon이 제안한 서명 방식을 사용하였다. 센타에서 구성한 시스템의 안전도는 디지탈 서명 원래의 안전도와 동일하며 이는 이산 대수 문제에 근거한다. 사용자 인증과 간접인증 및 직접인증의 키 분배 방식의 안전도 역시 이산 대수 문제로 귀착된다.

연산량을 비교해 볼 때 근본적으로 Harn-Yang은 모듈라 p상에서의 연산이며 제안한 방식은 Schnorr의 서명[11]에서와 같이 계산량을 줄일 수 있도록 모듈라 q를 도입하여 사용하였다. 실제 구현시 p를 512비트 그리고 q를 160비트로 할 경우 제안 방식의 계산 속도가 향상된다. 제안한 방식을 모듈라 p상에서 구현한다고 가정할 때에도 공개 키를 구하는 과정에서 Harn-Yang 방식은 2회의 멱승이 필요하며 제안한 방식은 1회의 멱승 정도로 볼 수 있다. 또한 디지탈 서명의 확인 과정에서도 Harn-Yang 방식은 4회의 멱승이 필요한 반면 제안한 방식은 3회의 멱승이므로 보다 효율적이다. 이에 Schnorr가 제안한 계산 방법[11]을 적용한다면 $X^a \cdot Y^b \bmod p$의 계산은 (1.75n+1)번 그리고 $X^a \cdot Y^b \cdot Z^c \bmod p$는 (1.875n+4)번의 곱셈으로 줄일 수 있다. 여기서 n는 a, b 및 c의 비트 수를 나타낸다. 예를들어 두 방식 모두 모듈라 p상에서만 디지탈 서명을 구현 하였을때 서명 확인 과정에서 Schnorr의 계산식을 적용한 곱셈은 Harn-Yang방식이 1.5n+1.875n번의 곱셈이 필요하고 제안한 방식은 1.875n번의 곱셈이 필요하다.

AMV의 디지탈 서명을 사용할 경우 서명 생성 과정에서 역수 계산이 필요하다. 그러므로 비밀 키 s의 역수 계산 결과를 저장해야 하거나 통신시마다 매번 계산해야 한다. 또한 센타에서 비밀 키 s가

p-1과 서로 소(relatively prime)인지의 확인과정이 필요하다. 그러나 제안 방식은 서명 생성시 역수 계산이 없어 효율적이며 비밀 키의 선택이 용이하다.

One-pass로 키를 공유하는 방식에서 ID와 공개 키 관련 정보 r을 관리해야 하지만 센타에서 생성하므로 확인서는 필요하지 않으므로 확인서에 기반(certificate-based)한 방식보다 통신량이 줄어든다. D-H의 키 분배 방식에서는 임의의 불법자가 공개 키 디렉토리의 공개 키를 자신의 것으로 대체하고 자신이 정당한 통신자로 위장(impersonation)할 수 있다. 그러나 제안된 방식에서 불법자가 ID와 r이 있는 공개 키 디렉토리에 접근하여 r을 자신의 것으로 대치하더라도 그에 상응하는 비밀 키를 생성할 수 없으므로 위장공격이 불가능하다.

### 4. 2 시뮬레이션

본 절에서는 제안한 개인정보에 기초한 암호 시스템을 소프트웨어적으로 구현하여 시뮬레이션 하였다. 구현 환경은 IBM-PC 486 50MHz 에서 Borland C 컴파일러를 사용하였다. 시스템 구성 및 사용자 인증, 디지탈 서명, 키 분배를 구현 알고리듬으로 개발하였고 해쉬 알고리듬은 SHA(Secure Hash Algorithm)[12]을 사용하였다. 한 예로 사용자 A(갑돌이)와 B(을순이)간 one-pass 키 분배 시스템의 구현 과정과 그 결과를 나타내었다. 여기에 표시된 데이타는 16진수로 최상위 비트부터 표시하였다.

[시스템 구성 단계]

512 비트의 소수 p와 p-1의 약수인 160 비트의 q를 선정한다. p보다 작은수 g′를 선택하고 원시원 g를 계산한다. 센타는 q보다 작은 비밀 키 X를 선택하고 공개 키를 계산한다.

- 소수 p : 9505 e383 51fc 6769 8fcb e0a8 da98 95b2 e74f c59e ce12 6073 8e49 b2da 49b2 32cc f8f dc9e 9769 21da 2947 f4ef f5b4 ba61 33d7 34d7 6689 3bd0 801b 1643 4df4 2465
- 소수 q : 945b 19e4 5104 3c10 9119 ca44 5d26 5f72 a938 3e93
- 원시원 g : 17e4 a2d6 f551 6389 c514 5639 96f dd5c c928 2097 ad21 1a5b ea56 4bab 28c0 6bba a00 81f7 a58b 42cf d959 2d72 e001 c34 bb17 35e6 72cf bf47 d247 ca13 6297 6549
- 센타 비밀 키 X : 8cca f7b0 c604 44dd 4161 992b f4f5 46b7 8c29 4d31
- 센타 공개 키 Y : 4bf0 24b5 c5ee b37 b6ec 2f1d 3440 1a49 504f f8ae 31f9 1068 6f34 6225 6b69 1fac 7554 eafc af2f 976b 4a2a 8182 9577 28cb b4e9 f3ee 4296 3346 fa74 c7ce 3c17 4695

[사용자 등록 단계( A)]

센타는 사용자의 $ID_A$를 등록하고 불규칙 정수 $k_A$를 발생하며, $\{r_A, s_A\}$를 계산한다.

- 불규칙 정수 $k_A$ : 8945 8282 5172 2828 9832 9ba4 5826 9222 8323 8989
- $r_A$ : ( $g^{k_A} \bmod p$) : 10ca a0c0 2abe 8a5e 884c ad9 5a99 9bb2 6600 d39b fcb9 11b9 788f f9ab 23fb f0b3 7fb9 a365 507e 26db dbbd 4cfa a2cb 5b3e 6fb5 5df1 5fee 599d f867 a2ec a991 3dc7
- $ID_A$ : ( kapdolee ) : 6565 6c6f 6470 616b
- $H(ID_A)$ : 163e f971 3bf2 ab3e cdab 49a 7d08 6ca0 2118 13ab

• $EID_A$ : ( $r_A \cdot H(ID_A)$ mod q) : 7a9d eaf7 d15d f190 2852 73fc f1fe 3ab7 238a d7d2

• $s_A$ : ( $k_A - X \cdot EID_A$ mod q) : 6af 8a4c 84b8 1469 ea24 878d 8ee6 9ba0 86f7 296e

[사용자 등록 단계( B)]

센타는 사용자의 $ID_B$를 등록하고 불규칙 정수 $k_B$를 발생하며, 서명쌍 $\{r_B, s_B\}$를 계산한다.

• 불규칙 정수 $k_B$ : 6288 9438 b334 64ca bc42 4923 a6e6 7763 8333 ca7e

• $r_B$ : ( $g^{k_B}$ mod p) : 43f4 a5ee 4354 2b4b dfe0 8cb9 c5d8 fce2 c6db 2b89 5b7f ab10 d719 1f70 6c1e c650 650f 8d9d 343d 8f62 9795 b7ad 585c b773 50ac 33b8 ec52 97f2 9f69 3cb4 cb4 db35

• $ID_B$ : ( yulsoonee ) : 65 656e 6f6f 736c 7579

• $H(ID_B)$ : d914 10e0 8992 f8b0 6dee 2d98 f402 298b bbc6 5f4e

• $EID_B$ : ( $r_B \cdot H(ID_B)$ mod q) : 5658 eea f05 9a8c 4b9a 9279 7a12 7d5c 87b7 34de

• $s_B$ : ( $k_B - X \cdot EID_B$ mod q) : 17c5 69ad 1ea7 6673 dbd4 7589 fe57 a601 c25c 572f

[ 키 분배 단계]

(1) 사용자 A는 랜덤수 $v_A$( $0 < v_A < q$ )를 선택한다.

• $v_A$ : 8288 baa6 5829 2921 c8ac 9882 818a 9922 4129 bc51

(2) A는 $W_A = g^{v_A}$ mod p를 계산한다.

• $W_A$ : 2e1b c7a8 95e 7d23 7a73 f302 207d 9738 4539 7ca4 9722 f9c5 4218 5660 6234 b8de 6926 925c 967d c0ff 7b49 6b74 8b43 3fc7 4a2b 2e5b cb31 af23 694f 5939 e618 7d1d

(3) A는 $E_A = W_A \cdot H(W_A)$ mod q를 구한다.

• $H(W_A)$ : 82bd bba3 58ae beea 1da4 4986 1a4e cddb e7fe c34c

• $E_A$ : ( $W_A \cdot H(W_A)$ mod q) 45ff 54f0 929b 9cc3 dbfb 9ec6 bbc1 8486 597d 3074

(4) A는 $\eta_A = v_A - s_A \cdot E_A$ mod q를 계산한다.

• $\eta_A$ : 2a36 825c bce1 6ed3 1ac6 fc17 a15d 1386 8252 668

(5) A는 B에게 ($ID_A$, $r_A$, $W_A$, $\eta_A$)를 전송한다 .

(6) A는 세션 키를 다음과 같이 생성한다.

• $EID_B$ : ( $r_B \cdot H(ID_B)$ mod q) : 5658 eea f05 9a8c 4b9a 9279 7a12 7d5c 87b7 34de

• $g^{s_B}$ : ( $r_B \cdot (Y^{-EID_B})$ mod p) : 4e3b 189d 8235 5cda 51d3 a484 1cd2 7894 2f10 9407 5f90 3ee2 98ff ad07 6c33 5e38 45fa a657 4bf9 e3d0 ada4 654a ef4a 5447 b6c3 8f3e 2dfa d22b d6c5 5402 3888 d145

• $K_{AB}$ : ( $g^{S_B \cdot v_A}$ mod p ) : 8c89 9841 50a7 48bd e241 56dd ecbc c143 8811 fbf6 7414 83dc f3d3 19c9 132d 572f 7746 4c8f 1409 9029 f24b f26f e198 f3d4 ff59 8bc6 c131 372b 8471 2a42 7cae 2c80

(7) B는 $W_A$에 대한 다음 검증식이 성립하면 비밀 세션 키인 $K_{BA} = W_A^{s_B} = g^{S_B \cdot v_A} \bmod p$를 계산한다. 즉 검증식은 $W_A = g^{\eta_A}(r_A \cdot Y^{-EID_A})^{W_A \cdot H(W_A)} \bmod p$ 이다

- $EID_A$ : ( $r_A \cdot H(ID_A) \bmod q$) : 7a9d eaf7 d15d f190 2852 73fc f1fe 3ab7 238a d7d2
- $E_A$ : ( $r_A \cdot H(W_A) \bmod q$) : 45ff 54f0 929b 9cc3 dbfb 9ec6 bbc1 8486 597d 3074
- $g^{s_A}$ : ( $r_A \cdot (Y^{-EID_A}) \bmod p$) : b43 a631 802d 5365 9e5a 3af 1443 7849 2cad 2e5 a969 1369 5110 237c 89a4 b4d8 df14 5efb d46a 602d 62f8 cd25 263a 46b9 fb59 7e99 24c 6a05 f3d fcfd 186d daa8
- $g^{\eta_A}(r_A \cdot Y^{-EID_A})^{W_A \cdot H(W_A)}$ : 2e1b c7a8 95e 7d23 7a73 f302 207d 9738 4539 7ca4 9722 f9c5 4218 5660 6234 b8de 6926 925c 967d c0ff 7b49 6b74 8b43 3fc7 4a2b 2e5b cb31 af23 694f 5939 e618 7d1d
- $K_{BA}$ : ( $W_A^{s_B} = g^{t_A \cdot s_B} \bmod p$) : 8c89 9841 50a7 48bd e241 56dd ecbc c143 8811 fbf6 7414 83dc f3d3 19c9 132d 572f 7746 4c8f 1409 9029 f24b f26f e198 f3d4 ff59 8bc6 c131 372b 8471 2a42 7cae 2c80

## 5. 결 론

본 논문에서는 개인정보에 기초한 Harn-Yang의 암호 시스템을 분석하여 계산량을 줄일 수 있고 구현 측면에서 효율적인 방법을 연구하였다. ElGamal 형태의 서명방식 중 Moon의 서명 기법을 이용하여 개인정보에 기초한 인증, 디지탈 서명 그리고 키 분배를 할 수 있는 효율적인 방안을 제시하였다. 이를 바탕으로 인증, 디지탈 서명 및 키 분배를 통합할 수 있는 방안을 제시하고, E-mail 등의 일방향 통신에 적합한 키 분배 방안을 제시하였다.

제안된 방식의 안전성은 이산 대수 문제에 근거하며 계산량을 효과적으로 줄일 수 있다. 또한 제안 방식은 서명 생성시 역수 계산이 없어 효율적이며 Harn-Yang 방식보다 비밀 키의 선택이 용이하다. 간접인증을 제공하는 키 분배 방식에서 통신시마다 매번 다른 세션 키를 생성하는 방안을 제안하였으며 E-mail과 같은 일방향 통신에 적합한 one-pass 키 분배 방안도 제시하였다.

상기한 개인정보에 기초한 암호 시스템을 구현하기 위해 키 관리 센타에서의 시스템 계수 설정 단계, 사용자 등록 단계에 필요한 프로그램을 구현하였다. 응용 단계의 하나인 one-pass 키 분배 방식을 프로그램으로 구현하여 그 결과를 제시하였고 제안한 방식의 타당성을 검증하였다.

## 참고 문헌

[1] A. Shamir, "Identity-based cryptosystems and signature scheme." *Proc. of Crpyto'84,* pp. 47-53, 1985.

[2] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," *Proc. Crypto'86,* pp. 186-194, S-V, 1987.

[3] U. M. Maurer and Y. Yacobi, "Non-interactive public key cryptography," *Eurocrypt'91,*

pp. 498-507, 1991.

[4] E. Okamoto and K. Tanaka, "Key distribution system based on identification information," *IEEE J. Selected Areas in comm.*, vol. 7, no. 4, May 1989.

[5] C. G. Günther, "An identity_based key-exchange protocol," *Eurocrypt'89,* pp. 29-37, 1989.

[6] G. B. Agnew, R. C. Mullin, and S. A. Vanstone, "Improved digital signature scheme based on discrete exponentiation," *Elect. Lett.*, vol. 26, no. 14, pp. 1024-1025, July 1990.

[7] L. Harn and S. Yang, "ID-based cryptographic scheme for user identification, digital signature, and key distribution," *IEEE Journal on Selected Area in Comm.*, vol. 11, no. 5, June 1993.

[8] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. on Inform. Theory,* vol. IT-22, pp. 644-654, Nov. 1976.

[9] T. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithm," *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 469-472, July 1985.

[10] L. Harn and Y. Xu, "Design of generalized ElGamal type digital signature schemes based on discrete logarithm," *Elect. Lett.*, vol. 30, no. 24, pp. 2025-2026, Nov. 1994.

[11] C. P. Schnorr, "Efficient identification and signature for smart cards," *Advances in Cryptology-Crypto'89,* pp. 239-252, 1990.

[12] National Institute Standard Technology, *Specifications for a Secure Hash Standard(SHS)*, FIPS YY Draft, Jan. 1992.