通信情報保護學會論文誌
第 1 卷, 第 1 號, 1991. 12

이산대수 문제를 이용한 ID 기본 암호시스팀과 디지틀 서명방식에 관한 연구

염흥열* · 이만영**

ID-Based Cryptosystem and Digital Signature Scheme Using Discrete Logarithm Complexity

Heung-Youl Youm and Man-Young Rhee

요 약

Shamir는 공개키 저장을 위한 키 디렉토리(key directory)의 유지가 요구되지 않는 ID(identity) 기본 암호시스팀 및 디지틀 서명방식의 개념을 1984년 제안하였다. 본 논문에서는 지금까지 발표된 대표적인 공개키 암호알고리즘(RSA, Merkle-Hellman, El-Gamal 암호알고리즘) 등을 바탕으로 이산대수문제에 기반을 둔 ID 기본 암호시스팀의 개념과 실현방안을 분석 및 제시하며, 또 새로운 ID 기본 디지틀 서명방식을 제안하고 이에 대한 가능한 여러 공격 형태들을 분석함으로서 안전성(security)을 입증한다. 그리고 ID 기본 암호시스팀과 디지틀 서명방식의 특징을 제시한다.

Abstract

In 1984 Shamir proposed the concept of ID(identity)-based cryptosystem and digital signature scheme which does not require any public file for storing the user's public keys. In this paper, the concept of the ID-based cryptosystem based on discrete logarithm problem using the conventional public-key cryptosystems is described, and the implementation method of the ID-based cryptosystem is also presented. The new digital signature scheme based on the ID-based cryptosystem is proposed and possible attacks are considered and analyzed for the security of digital signature scheme. The proposed ID-based schemes are particularly useful for smart card and personal identification card application.

* 순천향대학교 공과대학 전자공학과
** 한양대학교 공과대학 전자통신공학과

1. 서 론

Diffie와 Hellman에 의한 공개키 암호시스템의 개념[1]이 1976년 도입된 이래 수많은 공개키 암호 알고리즘들이 연구되어져 왔다[2,3,4]. 그 대표적인 경우가 큰 정수를 인수분해하는 것이 계산적으로 어렵다는 이론에 기반을 둔 RSA 암호알고리즘[2]. trapdoor knapsack 문제에 기반을 둔 Merkle-Hellman 암호알고리즘[3]. 유한체상의 이산대수 (discrete logarithm)를 구하는 것이 매우 어렵다는 사실에 기초를 둔 El-Gamal의 공개키 암호시스템[4] 등을 들 수 있다. 한편 Shamir가 1984년 특정 소그룹간의 비밀통신(secure communication) 및 서명방식(digital signature)에 적합한 ID 기본 암호시스템 및 서명시스템의 개념[5]을 도입한 이래, ID (identity) 기본 암호시스템의 구체적인 실현 방법들이 몇가지 제안되었다[6,7]. ID 기본 암호시스템은 지금까지 공개키 저장을 위한 키 디렉토리(key directory)를 유지함으로서 통신개시시 키 센타와의 과도한 트래픽과 메모리가 요구되는 단점을 보완하여 통신 상대의 공개키를 상대방의 이름, 망 주소, 또는 전화번호 등의 조합으로 구성된 함수로부터 도출하므로서 망 내의 별도의 키 센타의 지속적인 유지를 요구하지 않는 것을 특징으로 하는 암호시스템이다. 그러므로 ID 암호시스템에서의 키 센타는 새로운 사용자가 처음으로 망에 가입할때만 동작하여 사용자의 비밀키 및 망 관련 공개 정보를 부여하는 기능만을 수행한다. 이의 전형적인 응용분야는 스마트카드(smart card)와 개인카드(personal identification card)를 이용하여 보안 통신 및 서명 통신을 수행하려는 통신 주체들로 구성되는 통신망이 될 것이다. 따라서 위의 특징을 갖는 ID 기본 암호시스템은 통신망에서의 응용영역이 점차 확대될 것으로 예측된다.

본 논문에서는 ID 기본 암호시스템 및 서명시스템을 정의 및 분석하고, 이를 바탕으로 간단하고 쉽게 실현될 수 있어서 스마트카드 등에 직접적으로 적용될 수 있는 실현 방법을 제시하고, El-Gamal의 디지틀 서명방식을 이용한 새로운 ID 기본 디지틀 서명시스템을 제안하고, 이에 대한 가능한 공격 형태를 분석함으로서 ID 기본 서명시스템의 타당성 및 안전성을 입증한다. 또한 ID 기본 암호시스템 및 디지틀 서명시스템의 특징을 분석한다. 본 논문에서 제시한 ID 기본 암호시스템 및 서명시스템은 스마트카드 및 개인 신용카드에 직접적으로 응용될 수 있을 것으로 기대된다.

2. ID 기본 암호시스템

2.1 El-Gamal의 공개키 암호시스템[4]

이산대수문제(discrete logarithm problem)에 기초한 공개키 암호시스템을 실현하기 위해서는 먼저 공개키와 비밀키를 생성해야 한다. 암호키 생성 절차는 다음과 같다. (1) 매우 큰 소수 p를 선택하고, (2) Zp^*(법 p에 대한 그룹)의 원시원(primitive element) g를 구하고, (3) $0 \le k \le p-2$ 조건을 만족하는 비밀키 k를 선택한 후, (4) 공개키 $y(\equiv g^k \bmod p)$를 계산한다. 이후 공개철에 공개키 y, p, g를 보관하고, 비밀키 k는 각 사용자가 보관한다.

사용자 A가 사용자 B에게 메세지 $m(0 \le m \le p-1)$를 전달하고 싶을 경우, 암호화는 다음과 같은 과정을 통해 수행된다. (1) 사용자 A는 임의의 난수(random number) $r(0 \le r \le p-2)$를 선택한다. (2) 사용자 A는 사용자 B의 공개키 y_B를 이용하여 암호문 (C_1, C_2)를 계산한다.

$$C_1 \equiv g^r \bmod p \qquad (1)$$
$$C_2 \equiv m \cdot y_B^r \bmod p$$

(3) 사용자 A는 사용자 B에 암호문 (C_1, C_2)를 전송한다.

(C_1, C_2)를 수신한 사용자 B는 자신의 비밀키 k_B와 p를 이용하여 다음과 같은 절차로 복호화를 수행한다. (1) 다음 식을 이용하여 C_1'를 계산한다.

$$C_1' \equiv (C_1)^{k_B} \equiv (g^r)^{k_B} \equiv (y_B)^r \quad \text{mod } p \quad (2)$$

(2) 사용자는 B는 C_1', C_2를 이용하여 메시지 m를 복구한다.

$$(C_1')^{-1} \cdot C_2 \equiv (y_B{}^r)^{-1} \cdot m \cdot y_B{}^r \equiv m \quad \text{mod } p \quad (3)$$

따라서 위의 과정을 통해 사용자 B는 사용자 A가 송신한 메세지 m를 복구할 수 있다.

한편 메세지가 m_1, m_2이고 암호화 과정에서 각각의 메세지에 대응하여 선택된 난수 r이 같다고 가정하면, m_1에 대한 암호문 (C_{11}, C_{21})과 m_2에 대한 암호문 (C_{12}, C_{22})는 다음과 같이 표현된다.

$$C_{11} \equiv g^r \quad \text{mod } p$$
$$C_{21} \equiv m_1 \cdot (y_B)^r \quad \text{mod } p \quad (4)$$

$$C_{12} \equiv g^r \quad \text{mod } p$$
$$C_{22} \equiv m_2 \cdot (y_B)^r \quad \text{mod } p \quad (5)$$

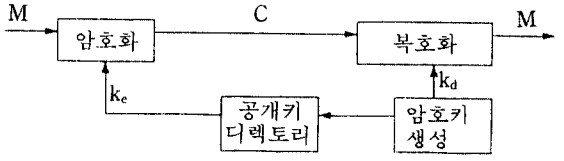
C_{21}를 C_{22}를 나누면,

$$C_{21}/C_{22} \equiv (m_1 \cdot (y_B)^r)/(m_2 \cdot (y_B)^r) \equiv m_1/m_2 \quad \text{mod } p \quad (6)$$

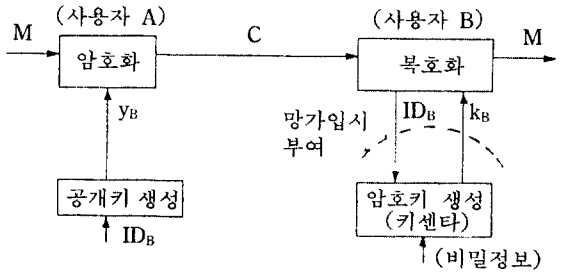
그러므로 m_1이 알려질 경우 m_2도 알려질 수 있다. 따라서 m_1, m_2에 대한 난수 r_1, r_2는 반드시 다르게 선택되어야 한다. El-Gamal의 공개키 암호시스템의 안전성은 다음 사실에 기초한다. C_1, C_2, y_B로부터 m를 구하기 위해서는 $C_1 \equiv g^r$ mod p에서 r이 먼저 구해져야 한다. 이는 $r \equiv \log_g C_1$ mod p가 되어 이산대수문제를 푸는 문제로 귀착된다.

2.2 ID 기본 암호시스템의 정의 및 개요

ID 기본 암호시스템은 1984년 Shamir가 처음



(a) 공개키 암호시스템



(b) ID 기본 암호시스템

그림 1. 공개키 암호시스템과 ID 기본 암호시스템의 비교

제안한 방식으로서, 공개키를 저장하기 위한 공개키 디렉토리의 유지가 필요없고, 통신중 제삼자의 개입이 요구되지 않으며, 통신 주체간의 공개키 또는 비밀키의 상호 교환이 요구됨이 없이 임의의 두 사용자의 서명문 인증(verification) 및 비밀통신을 가능케 하는 새로운 암호 통신방식이다[5].

ID 기본 암호시스템은 주로 공개키 암호시스템에 기반을 두고 설계되며, 각 사용자의 ID가 공개키로 이용되며 이는 상대방의 이름, 주소등록 번호, 망주소, 또는 성별 등의 조합으로 생성될 수 있다. 각 사용자의 비밀키는 믿을 수 있는 키 생성센터(trusted center)에서만 생성될 수 있으며, 이는 대회사 암호통신망의 경우 회사 본부가 될 것이다. 일반적으로 공개키 암호시스팀과 ID 기본 암호시스팀의 블럭도는 그림 1과 같다. 그림 1에서 알 수 있듯이 공개키 암호시스팀은 수신자가 암호키를 생성하여 비밀키 k_d를 자신이 간직하고, 공개키를 키 디렉토리에 공표함으로서 비밀통신이 수행되도록 구성되어 있다. 한편, ID 기본 암호시스팀에서는 수신자의 ID로 부터 암호화 키 $k_e(y)$를 구하여 암호화를 수행하고, 수신단에서는 망가입시 암호키 생성 센터에서 받은 자신의 비밀키 $k_d(k)$를 이용하여 복호를 수행한다. 따라서 공개키 암호시스팀에서와 같이 별도의 키 디렉토리가 요구되지 않는다. ID 기본 암호시스팀 설계시 고려해야 할 요구조건은 첫째로 암호키 센터의 공개키와 ID로 부터 각 사용자의 비밀키를 쉽게 구할 수 있어야 하며, 암호키 센터의 공개키와 각 사용자의 비밀키를 이용하여 사용자의 비밀키 생성을 위한 키 센터의 비밀 정보를 구하는 것이 계산적으로 불가능해야 한다는 것이다. ID 기본 암호시스팀의 안전성은 기반이 되는 암호알고리즘의 안전성, 키 생성 센터에 저장되어 있는 비밀정보의 보안성, 카드 발행전에 센터에 의해 수행되는 사용자에 대한 신분확인의 철저 정도, 그리고 사용자의 주의 등에 크게 영향을 받는다. ID 기본 암호시스팀의 주요 응응분야는 대회사의 집행 간부 등으로 구성된 소 그룹에서의 비밀통신 및 서명통신 분야와 개인 신분카드를 이용하여 수표나 전자메일에 전자적으로 서명하는 통신 분야 등을 들 수 있다.

2.3 ID 기본 암호시스팀의 실현

가. 키 센터에서의 시스팀 파라메타 생성

키 센터는 다음의 과정을 통해 암호시스팀의 시스팀 파라메타와 사용자 A의 비밀키를 생성한다.

(1) 각각의 사용자는 k차 2원 벡터(k-dimensional binary vector)를 이름, 또는 망주소 등으로 부터 결정하여 자신의 ID로 간주한다. 예를 들어 사용자 A의 경우,

$$\begin{aligned} ID_A &= f(\text{이름, 주소, } \cdots) \\ &= (ID_{A1}, \cdots, ID_{AK}) \qquad (7) \\ &\text{여기서, } ID_{Ai} \quad \{0, 1\}, \quad 1 \le i \le k \end{aligned}$$

그리고 각 사용자는 키 센터에 자신의 ID를 접수한 후, 키 센터는 ID와 키 센타의 비밀 정보를 이용하여 각 사용자의 비밀키를 생성한다.

(2) 키 센터는 두개의 임의의 큰 소수(prime) q_1, q_2를 선택한 후 $N(=q_1 \cdot q_2)$를 계산한다. 그리고 $GCD(e, \phi(N))=1$ (여기서 $\phi(N)=(q_1-1)\cdot(q_2-1)$)를 만족하는 임의의 수 e를 선택한다. 키 센터는 (e, N)를 공개한다. 이후 키 센터는 각 사용자의 확장 ID, EID(Extended ID)를 계산한다. 예를 들어 사용자 A의 EID는 다음과 같다.

$$\begin{aligned} EID_A &\equiv (ID_A)^e \quad \bmod N \qquad (8) \\ &= (EID_{A1}, \cdots, EID_{An}) \\ &\text{여기서, n : N을 2진수로 표시했을 경우의 비트수} \end{aligned}$$

(3) 키 센타는 다음식을 만족하는 초증가성계열(superincreasing sequence) $\mathbf{a}'$를 구한다.

$$\mathbf{a}' = (a_1', a_2', \cdots, a_n')$$

$$a_i' \ge t \cdot \sum_{j=1}^{i-1} a_j'$$

$$\sum_{i=1}^{n} a_i' < p-1$$

여기서, t : 임의의 정수 (9)

그리고 GCD(w, p−1)=1을 만족하는 w를 선택한 후 센터의 비밀정보 $\mathbf{a}(=(a_1, \cdots, a_n))$를 다음식을 이용하여 구한다.

$$a_i \equiv a_i' \cdot w \mod p-1, \text{ for } 1 \le i \le n \quad (10)$$

(4) Z_p^*에서 임의의 원시원 g를 선택한 후 키 센터의 공개키 $y(=(y_1, y_2, \cdots, y_n))$을 계산한다.

$$\mathbf{y}=(y_1, y_2, \cdots, y_n)$$
단, $y_i \equiv g^{a_i} \mod p$, for $1 \le i \le n$ (11)

(5) 센터의 비밀정보 **a**와 사용자의 EID를 이용하여 사용자의 비밀키 k를 계산한다. 예를 들어 사용자 A의 경우,

$$k_A \equiv \sum_{i=1}^{n} a_i \cdot EID_{Ai} \mod p-1 \quad (12)$$

키 센터는 고도의 보안채널(highly secure channel)을 통해 사용자 A의 비밀키 k_A를 보낸다. 이는 스마트카드의 경우 비밀 메모리에 저장함을 의미한다. 위와 같은 과정을 통해 생성되는 키 생성 센터와 각 사용자에서의 공개키 및 비밀키는 그림 2와 같이 구성된다.

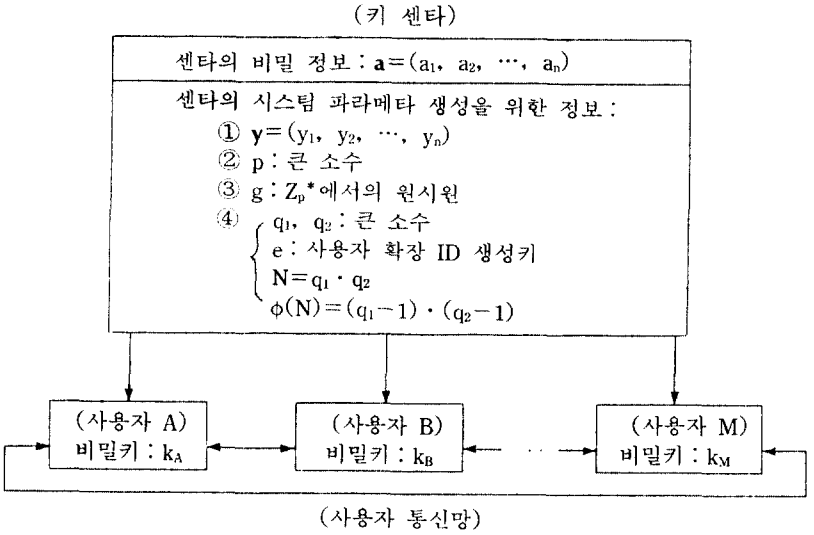


그림 2. ID 기본 암호시스템의 공개키와 비밀키

그림 2에서 보듯이 센타의 비밀 정보는 n차 2원 벡타인 a이고 센타의 공개키는 y, p, g, e, N 등이며 사용자의 공개키는 ID들이다. 각 사용자는 자신의 비밀키 k와 센타의 공개키들을 스마트카드에 소유하고 있다.

나. ID 기본 암호시스템에서의 암호화

만약 사용자 A가 사용자 B에 메세지 m을 전송하고자 할 때 다음과 같은 절차로 암호문(C_1, C_2)가 형성된다.

(1) 사용자 A는 사용자 B의 ID_B를 기초로 하여

EID_B를 계산한다.

$$EID_B \equiv (ID_B)^e \quad \text{mod } N \qquad (13)$$
$$= (EID_{B1}, \cdots, EID_{Bn})$$
여기서, $EID_{Bi} \in \{0, 1\}$ for $i=1, 2, \cdots, n$

(2) 사용자 A는 센타의 공개키 **y**를 이용하여 사용자 B의 공개키 y_B를 계산한다.

$$y_B \equiv \prod_{i=1}^{n} y_i^{EID_{Bi}} \quad \text{mod } p \qquad (14)$$
$$\equiv \prod_{i=1}^{n} \{g^{a_i}\}^{EID_{Bi}} \quad \text{mod } p$$
$$\equiv g^{\{\sum_{i=1}^{n} a_i \cdot EID_{Bi}\}} \quad \text{mod } p$$
$$\equiv g^{K_B} \quad \text{mod } p$$

(3) 사용자 A의 메세지를 $m(0 \le m \le p-1)$이라 가정하자. 사용자 A는 임의의 난수 r $(0 \le r \le p-2)$를 선택한다.
(4) 사용자 A는 m의 암호문 (C_1, C_2)를 다음식을 이용하여 구한다.

$$C_1 \equiv g^r \quad \text{mod } p \qquad (15)$$
$$C_2 \equiv m \cdot (y_B)^r \quad \text{mod } p$$

(5) 사용자 A는 (C_1, C_2)를 사용자 B에게 전달한다.

한편 메세지 m에 대한 암호문이 (C_1, C_2)이므로 암호문의 크기는 메세지 크기의 2배가 된다. 따라서 암호문의 크기 대 메세지 크기 비(ratio)를 줄이기 위해 다음과 같은 방법이 이용될 수 있다. m_1, m_2를 두 블럭의 메세지라 가정하면 이에 대응되는 암호문 (C_1, C_2, C_3)를 다음과 같이 정의하자.

$$C_1 \equiv g^r \quad \text{mod } p$$
$$C_2 \equiv m_1 \cdot (y_B)^r \quad \text{mod } p \qquad (16)$$
$$C_3 \equiv m_1 + m_2 \quad \text{mod } p$$

이에 대한 복호는 C_1, C_2로 부터 위의 과정을 따라 m_1를 구한후, $m_2 \equiv C_3 - m_1 \bmod p$로 부터 m_2를 구함으로서 완료된다. 이와 같은 방법을 이용하여 암호문의 크기 대 메세지 크기의 비를 1.5로 낮출 수 있다.

다. ID 기본 암호시스팀에서의 복호화

암호문 (C_1, C_2)를 수신한 사용자 B는 다음과 같은 절차로 메세지 m을 복구한다.
(1) 사용자는 B는 자신의 비밀키 k_B를 이용하여 C_1'를 계산한다.

$$C_1' \equiv (C_1)^{k_B} \quad \text{mod } p \qquad (17)$$
$$\equiv (g^r)^{k_B} \quad \text{mod } p$$

(2) C_1'과 C_2를 이용하여 사용자 B는 메세지 m를 복구한다.

$$(C_1')^{-1} \cdot C_2 \quad \text{mod } p \qquad (18)$$
$$\equiv \{(g^r)^{k_B}\}^{-1} \cdot m \cdot (y_B)^r \quad \text{mod } p$$
$$\equiv \{(g^r)^{k_B}\}^{-1} \cdot m \cdot (g^{k_B})^r \quad \text{mod } p$$
$$\equiv m \quad \text{mod } p$$

2.4 ID 기본 암호시스팀의 제약

ID 기본 암호시스팀의 제약은 정리 1에서 보는 바와 같이 n개의 사용자가 자신의 비밀키 k와 EID를 공표하고 이를 이용하여 센타의 비밀정보 $\mathbf{a}(=(a_1, a_2, \cdots, a_n))$를 구할 수 있으므로 사용자의 수 M을 n보다 훨씬 낮게 설정해야 한다는 것이다.

[정리 1] ID 기본 암호시스팀에서 n개의 사용자가 자신의 비밀키를 공표하고 공모하면 센타의 비밀정보는 완전히 결정될 수 있다.

(증명) (12) 식으로 부터,

$$k_A \equiv \sum_{i=1}^{n} a_i \cdot EID_{Ai} \bmod p-1 \qquad (19)$$

이를 n개의 사용자의 비밀키로 표현하면,

$$\begin{aligned} k_1 &= \sum_{i=1}^{n} a_i \cdot EID_{1i} - q1 \cdot (p-1) \\ &\cdots \\ k_n &= \sum_{i=1}^{n} a_i \cdot EID_{ni} - qn \cdot (p-1) \end{aligned} \qquad (20)$$

$$\begin{aligned} \sum_{i=1}^{n} a_i \cdot EID_{1i} - k_1 &= q_1 \cdot (p-1) \\ &\cdots \\ \sum_{i=1}^{n} a_i \cdot EID_{ni} - k_n &= q_n \cdot (p-1) \end{aligned} \qquad (21)$$

(20) 식은 (21)식과 같이 변형 될 수 있다. (21)식을 행렬로 표시하면 다음과 같다.

$$\begin{bmatrix} EID_{11} & EID_{12} & \cdots & EID_{1n} & -k_1 \\ & & \cdots & & \\ EID_{n1} & EID_{n2} & \cdots & EID_{nn} & -k_n \end{bmatrix} \cdot \begin{bmatrix} a_1 \\ a_2 \\ \cdot \\ a_n \\ 1 \end{bmatrix} = (p-1) \cdot \begin{bmatrix} q_1 \\ \cdot \\ \cdot \\ \cdot \\ q_n \end{bmatrix}$$

$$\mathbf{B} \cdot \mathbf{A} = (p-1) \cdot \mathbf{q} \qquad (22)$$

여기서,

$$\mathbf{B} = \begin{bmatrix} EID_{11} & EID_{12} & \cdots & EID_{1n} & -k_1 \\ & & \cdots & & \\ EID_{n1} & EID_{n2} & \cdots & EID_{nn} & -k_n \end{bmatrix} \qquad (23)$$

$$\mathbf{A} = \begin{bmatrix} a_1 \\ a_2 \\ \cdot \\ a_n \\ 1 \end{bmatrix} \quad \mathbf{q} = \begin{bmatrix} q_1 \\ q_2 \\ \cdot \\ \cdot \\ q_n \end{bmatrix} \qquad (24)$$

행렬 **B**의 첫 n개의 열은 선형독립이므로 **B**는 대부분 비특이(nonsingular)이다. 그러므로 det(**B**)는 0이 아니고 센타의 공개키 중의 하나인 p가 공표되어 있으므로,

$$\mathbf{B} \cdot \mathbf{A} \equiv 0 \mod p-1 \qquad (25)$$

Gauss-Jordan 방법에 의해 (25) 식을 풀면 센타의 비밀정보 **a**(=(a_1, a_2 ⋯, a_n))를 완전히 결정할 수 있다. Q.E.D.

따라서 센타의 비밀정보 **a**(=(a_1, ⋯, a_n))가 n개의 사용자의 공모에 의해 알려지면 모든 사용자의 비밀키는 (12)식을 이용하여 매우 쉽게 구해 질 수 있으므로 ID 기본 암호시스팀의 안전성은 침해당한다. 그러므로 사용자의 수 M은 n 보다 일반적으로 작게 설정해야 한다.

2.5 ID 기본 암호시스팀의 특징

ID 기본 암호시스팀의 특징은 (1) 상대방의 공개키는 상대방의 이름과 망주소를 바탕으로 생성되는 EID와 망의 공개키 **y**로부터 계산되고, (2) p값의 크기가 RSA의 N(=q_1, q_2)의 크기와 같다면 ID 기본 암호시스팀의 암호문의 크기는 RSA의 그것보다 2배가 되며, (3) 상대방 공개키 생성시 하

나의 모듈러 지수(modular exponentiation) 연산과 최대 n개의 곱(multiplication) 연산, 암호문 생성시 2개의 모듈러 지수 연산과 하나의 곱연산이 요구되며, (4) 복호화시 하나의 모듈러 지수 연산과 하나의 나누기(division) 연산이 요구된다는 것이다.

2.6 ID 기본 암호시스템의 수치예

가. 시스템 파라메타 생성

키 센타는 다음과 같은 과정을 통해 키센타의 비밀정보와 공개키 그리고 사용자의 비밀키를 생성한다.

(1) 사용자 A의 ID_A(k=3)를 다음과 같이 결정한다.

$$ID_A=(1,\ 0,\ 1)=(ID_{A1},\ ID_{A2},\ ID_{A3})=5$$

(2) $q_1=3$, $q_2=5$으로 정하면, $N=3\cdot 5=15$가 되고 $\Phi(N)=8$이 된다. e=7로 설정하면 사용자 A의 확장 EID_A(n=4)는 다음과 같다.

$$EID_A\equiv (ID_A)^7 \bmod N\equiv 5^7 \bmod 15\equiv 5 \bmod 15=(0,\ 1,\ 0,\ 1)$$

(3) 센타는 p=23, t=1로 정하고, 이를 이용하여 초증가성계열 $\mathbf{a}'(=(a_1', a_2', a_3', a_4')=(1, 2, 4, 8))$를 계산하고, w=7이라 설정하면 센타의 비밀정보 $\mathbf{a}=(7, 14, 6, 12)$이 된다.

(4) Z_{23}^*의 원시원 g를 7로 정하면 센터의 공개키 $\mathbf{y}=(5, 2, 4, 16)$가 된다.

(5) 사용자 A의 비밀키는 $k_A=\mathbf{a}\cdot EID_A \bmod p-1\equiv 4$가 된다.

나. 암호화 과정

사용자 B가 사용자 A에 메세지 m를 송신한다고 가정하자. 암호화 과정은 다음과 같다.

(1) 사용자 B는 ID_A로 부터 EID_A(n≡4)를 결정한다.

$$EID_A\equiv (ID_A)^3 \bmod N\equiv 5^7 \bmod 15\equiv 5 \bmod 15=(0101)$$

(2) 사용자 A의 공개키 y_A를 EID_A와 센타의 공개키를 이용하여 결정한다.

$$y_A\equiv \prod_{i=1}^{n} y_i^{EID_{Ai}} \bmod p\equiv 2\cdot 16 \bmod 23\equiv 9$$

(3) 메세지 m=7이라 하면, 사용자는 B는 임의의 난수 r=8를 선택한다.

(4) 암호문 (C_1, C_2)를 계산한다.

$$C_1\equiv 7^8 \bmod 23\equiv 12$$
$$C_2\equiv 7\cdot (9)^8 \bmod 23\equiv 22$$

사용자 B는 암호문 (12, 22)를 사용자 A에 보낸다.

다. 복호화 과정

사용자 A는 다음과 같은 과정을 통해 메세지 m를 복구한다.

(1) 사용자 A는 자신의 비밀키 k_A를 이용하여 C_1'을 계산한다.

$$C_1'\equiv (C_1)^{k_A} \bmod p\equiv (12)^4 \bmod 23\equiv 13$$

(2) 다음식을 이용하여 메세지 m을 계산한다.

$$(C_1')^{-1}\cdot C_2 \bmod p\equiv (13^{-1})\cdot 22\equiv 16\cdot 22 \bmod 23\equiv 7$$

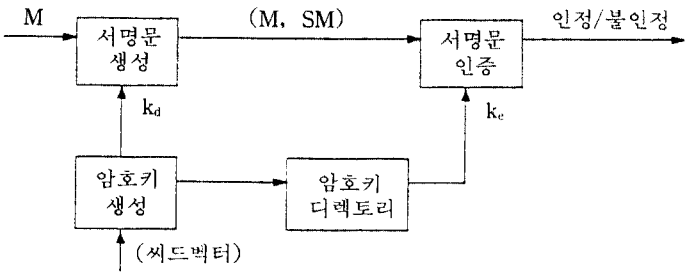
3. ID 기본 디지틀 서명방식

3.1 디지틀 서명방식의 개요

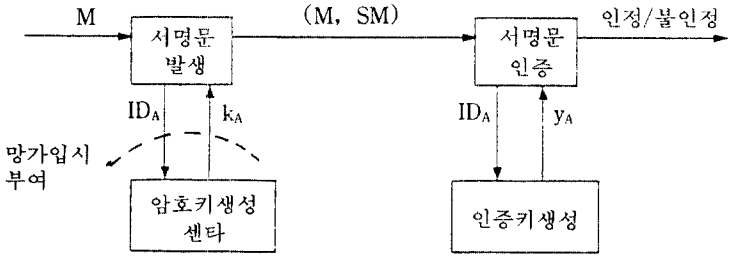
디지틀 서명방식은 서명의 주체가 쉽게 인증될 수

있고 제삼자가 위조하기 어려운 메세지 M과 관련된 서명문 SM(signed message)를 수신자에게 보냄으로서 수기 서명의 효과를 전자적으로 수행하는 암호통신 응용분야 중 하나이다. 디지틀 서명은 오직 한 사람만이 적법한 서명문을 생성할 수 있는 유일성, 제삼자에 의해 위조가 불가능한 위조 불가능성, 수신자 및 심판자가 서명문의 진위를 쉽게 확인할 수 있는 진위 확인의 용이성, 서명자가 자신의 서명문을 위조된 것이라고 거부하는 것이 불가능한 거부의 불가능성, 그리고 생성의 용이와 경제성을 보장하는 등의 요구사항들을 만족해야 한다. 그림 3은 공개키 암호시스템의 서명방식과 ID 기본 서명방식을 보이고 있다.

그림 3에서 알 수 있듯이 공개키 암호시스템을 이용한 서명방식에서는 자신의 비밀키 k_d를 이용하여 서명문을 생성하고, 수신단에서는 송신자의 공개키 k_e를 이용하여 서명문의 유효 여부를 결정하는 반면, ID 기본 방식에서는 망가입시 암호키 생성 센터로 받은 비밀키를 이용하여 서명문을 생성하고, 수신단에서는 송신자의 ID로 부터 상대방의 공개키를 계산하여 서명문의 유효 여부를 결정한다. 따라서 ID 기본 서명방식에서는 별도의 암호키 디렉토리가 요구되지 않는 특징이 있다.



(a) 공개키 암호시스템의 서명방식



(b) ID 기본 서명방식

그림 3. 디지틀 서명방식 비교

3.2 ID 기본 서명방식의 실현

ID 기본 서명방식의 키 센터의 공개키 및 사용자의 비밀키 생성 절차는 2.3절의 가. 항과 동일하다. ID 기본 서명방식은 그림 2에서와 같은 ID 기본 암호시스템에 기반을 두고 있으면서 동시에 디지틀 서명까지를 수행할 수 있는 새로운 서명방식이다. ID 기본 서명방식은 각 사용자가 센타의

공개키 **y**, p, g, e, N을 유지하고, 각 사용자의 EID를 쉽게 계산할 수 있다는 가정하에서, 사용자 A가 사용자 B에 서명문을 전송하려고 할 때, 사용자 A는 망가입시 암호키 센터로 부터 받은 비밀키 k_A를 이용하여 서명문을 발생하고, 수신자 B는 송신자 A의 ID로 부터 공개키 y_A를 계산하여 서명문의 진위 여부를 판단하는 개념을 바탕으로 실현된다. 사용자 A의 메세지를 $m(0\leq m\leq p-1)$이라 하고 m에 대응되는 서명문을 (r, s) $(0\leq r,\ s\leq p-1)$라 정의한다.

가. 디지틀 서명 과정

디지틀 서명은 다음과 같은 과정을 통해 수행된다.

(1) $GCD(a_0,\ p-1)=1$을 만족하는 임의의 난수 a_0 $(0\leq a_0\leq p-2)$와 Z_p^*의 임의의 원시원 g를 선택한다.

(2) 다음식을 이용하여 첫번째 서명문을 r를 계산한다.

$$r\equiv g^{a_0} \bmod p \tag{26}$$

(3) 다음 식을 만족하는 두번째 서명문 s를 계산한다.

$$m\equiv k_A\cdot r+a_0\cdot s \quad \bmod p-1 \tag{27}$$

만약 $GCD(a_0,\ p-1)=1$을 만족하면, $a_0\cdot s \bmod p-1\equiv m'$를 만족하는 유일한 s가 반드시 존재하므로 (28)식의 근 s는 반드시 유일하게 존재한다.

(4) 사용자 A는 메세지와 서명문 (m, r, s)를 사용자 B에게 전송한다.

나. 서명문 인증 과정

사용자 A가 전송한 (m, r, s)를 수신한 사용자 B는 다음의 과정을 통해 서명을 인증한다.

(1) 메세지 m를 이용하여 $g^m \bmod p$를 계산한다.

(2) 사용자 B는 사용자 A의 ID_A를 이용하여 EID_A를 계산한다.

$$\begin{aligned} EID_A &\equiv (ID_A)^e \bmod N \\ &=(EID_{A1},\ \cdots,\ EID_{An}) \end{aligned} \tag{28}$$

여기서, $EID_{Ai}\in\{0,\ 1\}$, for $i=1,\ 2,\cdots,\ n$

(3) 사용자 B는 센터의 공개키 **y**와 EID_A를 이용하여 사용자 A의 공개키 y_A를 계산한다.

$$\begin{aligned} y_A &\equiv \prod_{i=1}^{n} y_i^{EID_{Ai}} && \bmod p \\ &\equiv \prod_{i=1}^{n} (g^{a_i})^{EID_{Ai}} && \bmod p \\ &\equiv g^{\{\sum_{i=1}^{n} a_i\cdot EID_{Ai}\}} && \bmod p \\ &\equiv g^{k_A} && \bmod p \end{aligned} \tag{29}$$

(4) 사용자 B는 $(y_A)^r\cdot r^s \bmod p$를 계산한다.

[보조정리 1] ID 기본 디지틀 서명시스템에서 메세지 m과 서명문 (r, s)는 (30)식의 관계를 반드시 만족한다.

$$g^m\equiv y_A^r\cdot r^s \quad \bmod p \tag{30}$$

(증명) (28)식으로 부터 다음의 관계를 유도할 수 있다.

$$\begin{aligned} g^m &\equiv g^{(k_A\cdot r+a_0\cdot s)} && \bmod p \\ &\equiv (g^{k_A})^{r}\cdot g^{a_0\cdot s} && \bmod p \\ &\equiv (y_A)^r\cdot r^s && \bmod p \end{aligned}$$

Q.E.D.

(5) 사용자 B는 g^m과 $(y_A)^r\cdot r^s$가 같으면 정당한 서명문으로 간주하고, 같지 않으면 정당하지 않은 서명문으로 간주한다.

3.3 ID 기본 디지틀 서명방식에 대한 공격

ID 기본 디지틀 서명방식도 ID 기본 암호시스템과 시스템 파라메타 생성절차가 동일하므로 사용자수 M은 ID 기본 암호시스템과 동일한 제약을 받는다. ID 기본 디지틀 서명방식에 대한 공격은 메세지 m_i와 서명문(r_i, s_i)로 부터 송신자의 비밀키 k를 구하려는 방법과 비밀키 k의 복원없이 m에 대한 위조 서명문 (r, s)를 구하려는 방법으로 구분될 수 있다.

가. 송신자의 비밀키 k를 알아내는 방법

첫번째 가능한 공격은 주어진 $\{m_1, m_2, \cdots, m_l\}$과 $\{(r_1, r_2, \cdots, r_l), (s_1, s_2, \cdots, s_l)\}$로 부터 k를 구하는 것이다. 위의 가정으로 부터 $m_i \equiv k \cdot r_i + a_{0i} \cdot s_i$, for $i=1, 2, \cdots, l$를 구하면, 미지수가 $(k, a_{01}, \cdots, a_{0l})$이 되어 l+1개가 되므로 이 방정식을 푸는 것이 계산적으로 불가능하다. 만약 2개의 메세지 (m_i, m_j)에 대한 난수 (a_{0i}, a_{0j})가 같다면 방정식의 갯수가 l이 되어 k를 결정할 수 있으므로 반드시 서로 다른 메세지 (m_i, m_j)에 대한 난수 a_{0i}, a_{0j}를 다르게 설정해야 안전성을 보장받는다.

두번째 공격은 $g^m \equiv y^r \cdot r^s \bmod p$에서 $g^m \equiv g^{k \cdot r + a_0 \cdot s} \bmod p$로 부터 수행될 수 있다. $g^m \bmod p \equiv a$는 쉽게 구할 수 있으므로 앞의 방정식이 $a \equiv g^{k \cdot r + a_0 \cdot s} \bmod p$가 되어, 이것 또한 이산대수문제로 귀착된다.

나. 위조 서명문 (r, s)를 생성하는 방법

첫번째 공격은 m이 주어졌을 때 위조자는 $g^m \equiv y^r \cdot r^s$를 만족하는 서명문 (r, s)를 계산할려는 것이 될 것이다. 위조자가 GCD(j, p−1)=1를 만족하는 임의의 난수 j를 선택한 후 $r \equiv g^j \bmod p$를 계산하여 $m \equiv k \cdot r + j \cdot s \bmod p-1$를 만족하는 s를 구하기 위해서는 k가 먼저 결정되어야 한다. 위조자는 y_A $(\equiv g^k \bmod p)$와 p, g값을 알지만 y_A와 p, g값으로 부터 k값을 구하는 것이 이산대수문제로 귀착된다. 만약 위조자가 s를 먼저 결정한 후 $m \equiv k \cdot r + j \cdot s \bmod p-1$을 만족하는 r을 구하는 방법을 이용한다면 $g^m \pmod p \equiv A$라면 $r^s y^r \equiv A \bmod p$가 되어 이를 계산하는 것이 계산적으로 매우 어렵다.

두번째 공격은 하나의 메세지 및 서명문으로 부터 다른 메세지 및 서명문을 구하는 것이다. 먼저 m에 대한 (r, s)가 주어졌을 경우 이는 $g^m \equiv y^r r^s \bmod p$를 만족한다.

[정리 2] m에 대한 서명문이 (r, s)일 때, (m, r, s)의 함수인 (31)식의 (m_1, r_1, s_1)는 (30)식의 관계를 만족한다.

$$\begin{aligned} r_1 &\equiv r^A \cdot g^B \cdot y^C && \bmod p \\ s_1 &\equiv s \cdot r_1/(Ar - Cs) && \bmod p-1 \quad (31) \\ m_1 &\equiv r_1 \cdot (Am + Bs)/(Ar - Cs) && \bmod p-1 \end{aligned}$$

여기서, A, B, C는 GCD(Ar−Cs, p−1)=1를 만족하도록 설정되어야 한다.

(증명) (30), (31) 식을 이용하여,

$$\begin{aligned} y^{r_1} \cdot r_1^{s_1} &\equiv y^{r_1}(r^A \cdot g^B \cdot y^C)^{s_1} \\ &\equiv y^{r_1}(r^A \cdot g^B \cdot y^C)^{sr_1/(Ar-Cs)} \\ &\equiv (y^{r_1(Ar-Cs)})^{1/(Ar-Cs)} (r^{Asr_1} \cdot g^{Bsr_1} \cdot y^{Csr_1})^{1/(Ar-Cs)} \\ &\equiv (y^{Arr_1 - Csr_1 + Csr_1} \cdot g^{Bsr_1} \cdot r^{Asr_1})^{1/(Ar-Cs)} \\ &\equiv (y^{Arr_1} \cdot r^{Asr_1} \cdot g^{Bsr_1})^{1/(Ar-Cs)} \\ &\equiv (y^r \cdot r^s)^{Ar_1} \cdot g^{Bsr_1})^{1/(Ar-Cs)} \\ &\equiv (g^{mAr_1} \cdot g^{Bsr_1})^{1/(Ar-Cs)} \\ &\equiv g^{(mAr_1 + Bsr_1)/(Ar-Cs)} \\ &\equiv g^{m_1} \end{aligned}$$

여기서, $m_1 = \dfrac{mAr_1 + Bsr_1}{Ar - Cs}$

Q.E.D.

따라서 정리 2에 의해 (m, r, s)에 대응되는 위조 (m_1, r_1, s_1)을 생성할 수 있다. 그러나 정리 2에서와 같은 공격은 메세지 m이 랜덤하므로 임의의 메세

지에 대해서는 성공할 수 없으므로 본 서명시스팀을 깰 수 없음을 쉽게 알 수 있다.

3.4 ID 기본 디지틀 방식의 특징

ID 기본 디지틀 방식의 특징은 (1) 서명문의 크기가 메세지의 2배이고, (2) 서명과정에서 하나의 모듈러 지수 연산과 수 개의 곱셈연산이 요구되며, (3) 인증과정에서 상대방 EID 계산을 위한 하나의 모듈러 지수 연산과 n개의 곱셈 연산, 그리고 서명문 인증을 위한 3개의 모듈러 지수 연산과 하나의 곱 연산이 요구된다.

3.5 ID 기본 디지틀 방식의 수치예

사용자 A가 사용자 B에 메세지 m에 대한 서명문을 전송하고자 할 때, 키 생성절차는 2.6절의 가. 항과 동일하다는 가정하에서 다음과 같은 절차로 수행된다.

(1) 사용자 A는 $\gcd(a_0, 22)=1$를 만족하는 임의의 난수 $a_0=7$을 선택하고 원시원 g를 7로 결정한다.

(2) 사용자 A는 첫번째 서명문 r을 a_0을 이용하여 생성한다.

$$r \equiv g^{a_0} \mod p \equiv 7^7 \mod 23 \equiv 5$$

(3) 메세지 m=7이라 하면 다음 합동을 만족하는 두번째 서명문 s를 계산한다.

$$\begin{aligned} m &\equiv k_A \cdot r + a_0 \cdot s && \mod (p-1) \\ 7 &\equiv 4 \cdot 5 + 7 \cdot s && \mod 22 \\ s &\equiv 17 \end{aligned}$$

그러므로 메세지와 서명문은 (7, 5, 17)가 된다.

(4) (m, r, s)=(7, 5, 17)를 수신한 사용자 B는 먼저 ($g^m \mod p \equiv 7^7 \mod 23 \equiv 5$)를 계산한다.

(5) 사용자 B는 사용자 A의 ID_A로 부터 EID_A를 계산한다.

$$EID_A \equiv (5)^7 \mod 15 \equiv 5 \mod 15$$
$$\equiv (0101)$$

(6) 사용자 B는 센터의 공개키 y와 EID_A를 이용하여 y_A를 계산한다.

$$y_A \equiv \prod_{i=1}^{n} y_i^{EID_{Ai}} \mod p \equiv 2 \cdot 16 \mod 23 \equiv 9$$

(7) 사용자 B는 $(y_A)^r \cdot r^s \mod p$를 계산한다.

$$(y_A)^r \cdot r^s \mod p \equiv 9^5 \cdot 5^{17} \mod 23 \equiv 5$$

(8) 사용자 B는 $g^m \equiv (y_A)^{r \cdot r^s} \mod p$이므로 수신된 메세지와 서명문이 정당한 것으로 판단한다.

4. 결 론

본 논문에서는 유한체에서의 이산대수문제에 기초를 둔 ID 기본 암호시스팀과 디지틀 서명시스팀을 정의하고 쉽고 간단한 실현방법에 대해 기술하였으며, ID 기본 암호시스팀의 제약점을 이론적으로 도출하여 n개의 사용자가 공모하여 키센터의 비밀정보를 계산할 수 있음을 보였다. 그리고 ID 기본 암호시스팀에 바탕을 두고 El-Gamal의 디지틀 서명방식을 이용한 새로운 서명방식을 제안하였고, 이에 대해 구체적으로 예상되는 공격의 형태를 도출하여 각각에 대해 안전성을 입증하였다. ID 기본 디지틀 서명방식도 ID 기본 암호시스팀에 바탕을 두고 설계되었으므로, 사용자의 수 M을 n 이하로 설정하는 것이 바람직함을 알 수 있었다. 또한 ID 기본 암호시스팀과 디지틀 서명시스팀의 특징을 분석하였다. 한편, ID 기본 암호시스팀에서 비화강도에 크게 영향을 주지 않으면서 암호문대 메세지의 크기 비를 줄일 수 있는 한가지 방법을 제시하였다.

참 고 문 헌

1. W. Diffie and M.E. Hellman, "New Directions in Cryptography," IEEE Trans. on Inform. Theory, Vol. IT-22, pp.644-654, Nov. 1976.

2. R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystem," Comm. ACM, Vol. 21 (2), pp.120-126, Feb. 1987.

3. R.C. Merkle, and M.E. Hellman, "Hiding Information and Signatures in Trapdoor knapsacks," IEEE Trans. on Inform. Theory, Vol. IT-24, pp.525-530, 1987.

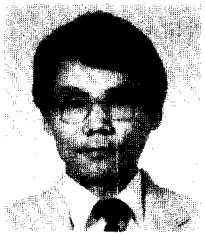
4. T. El-Gamal, "A Public-key Cryptosystem and Signature Scheme Based on Discrete Logarithm," IEEE Trans. on Inform. Theory, Vol. IT-31, pp.469-472, 1985.

5. A. Shamir, "Identity-based Cryptosystem and Signature Scheme," Lect. Notes Compu. Sci. 196, (Advances in Cryptology : Crypto'84) (Springer-Verlag, Berlin, 1985) pp.47-53.

6. S. Tsujii, T. Itoh, and K. Kurosawa, "ID-based Cryptosystem Using Discrete Logarithm Problem," Electronic Lett., 1987, 23, pp.1318-1320.

7. C.S. Laih, J.Y. Lee, "Modified ID-based Cryptosystem Using Discrete Logarithm Problem," Electronic Lett., 1988, 23, pp.858-859.

□ 著者紹介



廉 興 烈(正會員)

1981년 漢陽大學校 電子工學科(學士)
1983년 漢陽大學校 大學院 電子工學科(工學碩士)
1990년 漢陽大學校 大學院 電子工學科(工學博士)
韓國電子通信研究所 先任研究員
現 : 順天鄕大學校 工科大學 電子工學科 助教授

李 晩 榮(正會員)

1924년 11월 30日生
서울大學校 電氣工學科 工學士(BSEE)
美國 Colorado 大學校 工學碩士(MSEE) 및 工學博士(Ph. D.)
美國 Virginia 州立大 工科大學教授
美國 California Institute of Technology, JPL 研究員
國防科學研究所 第1副所長/韓國電子通信 社長/三星半導體通信 社長/漢陽大副總長/現 : 漢陽大 名譽教授/韓國通信情報保護學會 會長
著書 : Error Correcting Coding Theory, McGraw-Hill, New York, 1989.