通信情報保護學會誌
第4卷 第1號, 1994. 3

ID를 이용한 암호시스템에 관한 고찰

A Study on Identity-Based Cryptosystems

권 창영*, 김 경신**, 원 동호***

요 약

Shamir가 1984년 개인정보(ID)를 이용한 암호시스템의 개념을 제안한 이래 Fiat-Shamir 방식을 필두로 하여 Ohta, Guillou 등이 개인정보에 기반을 둔 서명법과 영지식 대화형 증명방식을 조합한 각종 개인식별 방식 및 디지탈 서명 방식들이 제안되어 왔다. 또한, Okamoto 등이 개인 정보를 이용한 키 분배 방식을 제안하였다. 본고에서는 지금까지 제안된 개인정보를 이용한 암호시스템의 대표적인 방식들에 대해 그들의 특징과 장단점을 비교 분석하였다.

1. 서 론

Diffie, Hellman이 1976년 공개키 분배방식[1]을 발표한 이래로 많은 공개키 방식이 제안되었다. 이러한 공개키 암호방식은 키 관리가 용이하지 않은 비밀키 암호방식의 문제점을 해결하였지만, 송신자와 메시지의 합법성을 확인해야 하는 인증에 관한 문제와 대규모 컴퓨터 네트워크상에서 공개키 암호방식을 이용한 각종 통신 서비스 제공시 대규모의 공개키 디렉토리가 필요하다는 문제점이 새롭게 대두된다.

인증에 관한 문제점은 몇 가지 방법으로 극복 가능하며 그 중 한가지 방법이 디지탈 서명 방식을 이용하는 것이다. 공개키 디렉토리의 필요성 및 공개키 디렉토리의 관리상의 문제점 때문에 합법적인 공개키(true public key)를 비합법적인 공개키(false public key)로 악의적으로 변경하는 등의 능동적인 공격에 부분적으로 공격당할 수 있다. 그러므로 본고에서는 전형적인 공개키 방식에서 공개키 디렉토리를 제거하는 방법인 certificated 방식과 identity-based 방식을 비교 설명하고, 1984년 Shamir가 *ID*를 이용한 암호시스템의 개념을 제안한 이래 Fiat-Shamir 방식을 필두로 하여 Ohta, Guillou 등의 개인정보에 기반을 둔 서명법과 영지식 대화형 증명방식을 조합한 각종 개인식별 방식과 디지탈 서명 방식, 그리고 Okamoto 등의 개인정보를 이용한 키 분배 방식 등 지금까지 제안된 *ID*를 이용한 암호시스템의 대표적인 방식들에 대해 그들의 특징과 장단점을 비교 분석하였다.

* 정회원, 대유공업전문대학 사무자동화과 전임강사
** 정회원, 연암공업전문대학 전산과 조교수
*** 종신회원, 성균관대학교 정보공학과 교수

2. Certificated 방식과 Identity-based 방식

전형적인 공개키 방식에서 공개키 디렉토리를 제거하는 데에는 2가지 방법이 있다. 그 중 하나

는 certificated 방식으로 변형하는 것이고, 또 하나는 identity-based 방식으로 변형하는 것이다. 임의의 공개키 방식은 앞에서 언급한 일반적인 방법으로 certificated 방식으로 변형되는데 반하여, 공개키 방식이 identity-based 방식으로 변형되려면 해당 공개키 방식에 적합한 독특한 방법이 필요하다[2].

2.1 Kohnfelder의 공개키 증명 분배방식

Certificated 방식은 신뢰 센터가 자신의 공개키를 공개하고, 가입자의 identity ID와 공개키 P에 대한 서명 즉, 공개키 증명 G를 가입자에게 분배하는 것이다. 시스템은 (ID, S, P, G)로 구성되며 (ID, P, G)는 공개된다. 가입자 ID를 확인하려면, 공개정보 (ID, P, G) 및 모든 가입자가 알고 있는 센터의 공개키를 이용하여 G를 검증할 수 있다.

대규모 컴퓨터 네트워크에서 공개키 암호 시스템을 이용하여 각종 통신 서비스를 제공하려면 대규모의 공개키 디렉토리를 필요로 한다. 이의 해결을 위하여 공개키를 통신 상대방간에 직접 전송한다면, 임의의 제3자에 의하여 쉽게 공격당한다[3]. 이러한 공개키 암호시스템의 문제점을 해결하기 위한 방법으로 Kohnfelder가 제안한 효과적인 방식을 소개한다[1].

센터는 일방향함수 f를 공개하고 역함수 f^{-1}를 비밀리에 보관한다.

가입자가 네트워크에 가입시에 각 가입자는 자신의 공개키 P 및 개인식별정보 ID를 센터에 등록한다. 물론 ID는 공개되어 있는 정보이며, 비밀키 S는 각 가입자가 비밀리에 보관한다. 센터는 $f^{-1}(ID, P)$를 계산하여 계산 결과를 가입자에게 전달한다. 이때, $f^{-1}(ID, P)$를 공개키 증명(public key certificate)이라고 한다.

가입자 A와 가입자 B는 다음과 같은 방법으로 비밀통신을 할 수 있다.

프로토콜 1. 공개키 증명을 이용한 비밀통신 프로토콜

순서 1. 가입자 A는 가입자 B에게 비밀통신을 요청한다.

순서 2. 가입자 B는 $f^{-1}(ID_B, P_B)$를 가입자 A에게 전송한다.

순서 3-1. 가입자 A는 $f \cdot f^{-1}(ID_B, P_B)$를 계산하여 가입자 B의 공개키 P_B를 확인 획득한다.

순서 3-2. 가입자 A는 가입자 B의 공개키 P_B로 메시지 M를 암호화하여 가입자 B에게 전송한다.

순서 4. 가입자 B는 자신의 비밀키 S_B로 비밀문을 복호화한다.

그러므로 Kohnfelder가 제안한 방식은 공개키 디렉토리가 필요하지 않은 방식이며, 센터도 가입자의 비밀키를 알지 못하므로 네트워크 가입자간의 비밀통신을 도청할 수 없으며 가입자간의 결탁의 문제도 없는 방식이다. 이 방식은 ID를 이용한 서명 및 ID를 이용한 키 분배로도 활용이 용이한 방식이다. 이 방식의 단점은 공개키 증명을 전송하기 위한 예비통신이 필요하다는 것과 키 파라메터의 변경이 불편하다는 것이다.

2.2 Shamir의 ID를 이용한 디지탈 서명

1984년 Shamir가 소개한 identity-based 방식[5]은 가입자의 idnetity ID 자체가 공개키 P이며 $(P=ID)$ 비밀키 S 자체가 공개키 증명 G이다$(G=S)$. 그러므로 시스템은 (ID, S)로 구성된다. 이 방식은 저장하거나, 검증할 공개키 증명 G가 별도로 없기 때문에 매우 흥미로운 방식이다. 보다 일반적인 identity-based 방식은 가입자의 공개키를 가입자의 identity와 관련된 어떤 값으로 대치하는 것이다.

Shamir가 제안한 최초의 ID를 이용한 디지탈 서명 방식을 소개하면 다음과 같다.

먼저 센터는 2개의 큰 소수 p, q 및 일방향함수 f를 선택하고, $n(=p \cdot q)$ 및 $\Phi(n)$과 서로소인 e를

계산한다. 센터는 n, e, f를 모든 가입자에게 공개하고, 가입자가 시스템에 가입시에 각 가입자는 자신의 개인식별정보 ID를 센터에 제출하면, 센터는 $ID=S^e \pmod n$인 S를 계산하여 가입자에게 비밀리에 전달한다.

가입자 A가 메시지 M에 대한 디지탈 서명(s, t)를 생성하여 가입자 B에게 전송하고, 가입자 B가 서명(s, t)를 검증하는 방법은 다음과 같다.

프로토콜 2. Shamir 의 디지탈 서명 프로토콜

〔디지탈 서명의 생성〕

순서 1-1. 가입자 A는 난수 r를 선택한다.

순서 1-2. 가입자 A는 $t=r^e \pmod n$ 및 $s=S_A \cdot r^{f(t, M)} \pmod n$를 계산한다.

순서 1-3. 가입자 A는 ID_A, M, (s, t)를 가입자 B에게 전송한다.

〔디지탈 서명의 검증〕

순서 2-1. 가입자 B는 $ID_A \cdot t^{f(t, M)}=s^e \pmod n$이 성립하는지 검증한다.

가입자 A의 ID_A에 대응되는 비밀키 S_A를 아는 가입자 A만이 메시지 M에 대한 서명(s, t)를 생성할 수 있으므로 가입자 A는 메시지 M을 가입자 B에게 자신이 보냈다는 것을 부인할 수 없다. 이 서명 방식은 RSA 방식에 비해 계산량이나 통신량이 두배로 늘어나므로 효율성은 낮은 방식이다. 이 서명 방식의 안전성은 ID_A의 e승근을 구하는 문제의 어려움에 근거하는데 만일 n의 소인수 p, q를 알 수 있다면 p와 q에 대한 ID_A의 e승근을 구할 수 있고, 중국인의 나머지 정리로 n에 대한 ID_A의 e승근을 구할 수 있다. 그러므로 e승근을 구하는 문제는 n을 인수분해하는 문제와 밀접한 관계가 있으며, 인수분해 문제는 매우 풀기어려운 문제로 알려져 있다.

3. ID를 이용한 개인 식별

ID 정보를 이용한 서명의 개념과 영지식 대화형 증명방식의 개념을 조합하여 실용적이면서 안전성이 높은 개인식별 방식은 Fiat와 Shamir 에 의해서 최초로 제안되었다. 이후 Fiat-Shamir 방식에 대한 많은 변형 및 개선책이 연구되어 왔다.

3.1 Fiat-Shamir의 개인식별

Fiat-Shamir 개인식별 방식[6]은 개인식별 정보 ID_i의 평방 잉여 s_i를 계산하여 가입자의 비밀키로 사용하였다. 이 방식의 안전성은 충분히 큰 두 소수 p, q의 곱인 n의 소인수 분해를 모를 때, 제곱근을 구하는 문제는 어려운 문제(NP 문제)라는 것에 근거한다.

사전 준비 과정에서 신뢰 센터는 소수 p, q를 선택하여 비밀리에 보관하고, 그 곱인 n을 공개한다. 카드 발급 과정에서 센터는 합법적인 사용자에게 카드를 발급할 때 그 사용자에 관한 개인정보(이름, id번호, 주소, 주민등록번호 등)와 카드에 관한 정보(유효기간 등)를 담고 있는 ID_i를 준비하고, mod n 상에서 ID_i의 평방근을 계산하여 그 역수 S_i를 각 가입자의 비밀키로 한다.

사실, 모든 ID_i가 mod n 상에서 평방근을 갖지는 않으므로, 이 문제의 해결책으로 임의의 스트링을 〔0, n〕으로 사상(mapping)하는 의사랜덤 함수(pseudo random function) h를 선택하여 공개하여 아래와 같이 비밀키를 생성한다.

① $P_j=h(ID_i, k_j)(j=1, \ldots, m)$을 구한다.

② 이 중에서 평방잉여를 갖는 k개의 P_j를 선택, 각 P_j의 가장 작은 제곱근 S_j를 k개 계산한다.

③ ID_i와 k개의 S_i, 각각의 j값을 카드에 담아 사용자에게 발급한다.

실제 가입자 A와 가입자 B가 개인식별을 행하는 프로토콜은 아래와 같다.

프로토콜 3. Fiat-Shamir의 개인식별 프로토콜 (순서 3-1에서 순서 6-1을 t회 반복)

순서 1-1. 가입자 A는 ID_A를 가입자 B에게 전송한다.

순서 2-1. 가입자 B는 $P_j=h(ID_A, k_j)(j=1, \ldots, k)$를 계산한다.

순서 3-1. 가입자 A는 $r\in_R Z_n^*$를 선택한다.

순서 3-2. 가입자 A는 $x=r^2(\mathrm{mod\ n})$를 계산하다.

순서 3-3. 가입자 A는 x를 가입자 B에게 전송한다.

순서 4-1. 가입자 B는 $(d_1, \ldots, d_k)\in_R \{0, 1\}$를 선택한다.

순서 4-2. 가입자 B는 가입자 A에게 $(d_1, \ldots, d_k)$를 전송한다.

순서 5-1. 가입자 A는 $y=r\prod_{d_j=1} S_j(\mathrm{mod\ n})$을 계산한다.

순서 5-2. 가입자 A는 y를 가입자 B에게 전송한다.

순서 6-1. 가입자 B는 $x=y^2\prod_{d_j=1} P_j(\mathrm{mod\ n})$이 성립하는지 검증한다.

가입자 A, B가 프로토콜을 수행하면, $y^2\prod_{d_j=1} P_j=r^2\prod_{d_j=1}(S_j^2\cdot P_j)=r^2=x(\mathrm{mod\ n})$

이 항상 성립한다. Fiat-Shamir 방식은 가입자 A가 가입자 B에게 전송하는 수치는 난수와 등가이며 가입자 A의 지식이 가입자 B에게 전송되지 않으므로 영지식이며 안전성은 매개 변수(security parameter) k, t에 의존한다. 제3자인 C가 A인척 위장하려면, 순서5-1의 y를 t회 정확하게 생성하여야 한다. 제3자인 C가 y를 1회 정확하게 생성할 확률은 2^k이며, y를 t회 정확하게 생성할 확률은 2^{kt}이므로 k와 t를 적정한 크기로 하면, 제3자인 C가 A인척 할 수 있는 확률은 무시할 수 있는 정도의 확률로 할 수 있다(security level$=2^{kt}$).

순서 5-1 및 순서 6-1에서의 계산을 간략히 하기 위해서 k의 값을 작게 선택하여 무시할 수 있는 정도의 확률에 도달하려면 t의 값은 매우 커야하므로 통신횟수가 매우 증가해야하는 약점이 있다.

만약 통신량을 감소하려면, 순서 3에서 가입자 A는 $h(x)$의 최초 128 비트 x^*를 전송하고, 순서 6의 검사식 우변에 함수 h를 작용시켜 획득한 결과의 최초 128비트 z^*와 x^*의 일치성을 검사하는 방법을 적용하면 된다. 통신량을 감소시키기 위하여 t회 동안 보낼 모든 x 및 d를 1회에 전송하는 병렬 방식은 영지식이 아니다.

Fiat-Shamir 방식의 문제점은 현재 스마트 카드 프로세서의 제약 조건들은 사용 알고리즘의 선택시 엄격한 제한을 수반하게 되는데 비해 반복 횟수와 증명자가 많은 메모리를 필요로 한다는 것이다.

Fiat-Shamir 방식은 스마트 카드의 마이크로프로세서(smart card microprocessor)와 인터페이스되는 산업 표준 퍼스널 컴퓨터간의 대화형 개인식별 방식(interactive identification scheme)으로 구현하려고 시도되었으며[7], 1988년 Micali와 Shamir는 증명자의 계산 복잡도에는 변화가 없으나, 검증자의 계산 복잡도를 2회 이하의 modular 곱셈으로 감소시킨 중앙 집중식 컴퓨터 네트워크에서 효율적인 방식을 제안하였다[8].

3.2 Ohta의 개인식별

Ohta의 ID를 이용한 개인식별 방식은 Fiat-Shamir 방식의 효율성을 개선한 방식으로 Fiat-Shamir 방식의 멱승 지수부를 기소수 L로 일반화시킨 방식으로 n의 인수를 모를 때 L 제곱근을 구하는 문제의 어려움을 이용한 것이다. Fiat-Shamir 방식의 문제점인 증명자와 검증자 사이의 반복 횟수를 1회로 개선하였으며, 적은 메모리로 개인식별이 가능한 장점을 가진 방식이나, 계산량에 있어서는 Fiat-Shamir 방식에 비하여 약 2~3배 정도 증가한다.

Ohta 방식은 사전 준비 과정에서 신뢰할 수 있는 센터가 소수 p, q를 비밀리에 선택하고, 그 곱인 n을 공개한다. 또한, $\Phi(n)$과 서로소인 L를 선택하여 공개한다.

카드발급 과정에서 센터는 가입자의 ID_i를 준비하고, GQ방식[9,10]에서는 mod n 상에서 ID_i의 L승

근을 계산하여 그 역수로 각 가입자의 비밀키 S_i로 하며, Ohta 방식[11]에서는 mod n 상에서 ID_i의 L 승근을 각 가입자의 비밀키 S_i로 한다. 실제로는 이 방식 역시 mod n 상에서 모든 ID_i가 L승근을 갖지는 않으므로 shadowed identity 개념을 이용한다.

프로토콜 4. Ohta의 개인식별 프로토콜

순서 1-1. 가입자 A는 $r \in_R Z_n^*$를 선택한다.

순서 1-2. 가입자 A는 $x=r^L \pmod n$를 계산한다.

순서 1-3. 가입자 A는 ID_A와 x를 가입자 B에게 전송한다.

순서 2-1. 가입자 B는 $d \in_R Z_L$를 선택한다.

순서 2-2. 가입자 B는 가입자 A에게 d를 전송한다.

순서 3-1. 가입자 A는 $y=rS_A^d \pmod n$을 계산한다.

순서 3-2. 가입자 A는 y를 가입자 B에게 전송한다.

순서 4-1. 가입자 B는 $y^L=xID_A^d \pmod n$이 성립하는지 검증한다.

가입자 A와 가입자 B가 위 프로토콜을 수행하면, $y^L=(r\cdot S_A^d)^L=r^L\cdot(S_A^L)^d=x\cdot ID_A^d \pmod n$이 항상 성립한다. Fiat-Shamir 방식에 비하여 비밀키가 k개에서 1개로 줄어들어 필요한 메모리를 감소시켰으며, Fiat-Shamir 방식에서는 순서 3-1에서 순서 6-1을 t회 반복하는데 반하여 확장 Fiat-Shamir 방식에서는 순서 1-1에서 순서 4-1을 1회 행하므로 통신 효율을 개선하였다(security level=$1/L$).

3.3 Girault의 개인식별

Chaum 등은 이산대수를 이용항 영지식 대화형 프로토콜을 제안하였으며[12,13] 여기서 아이디어를 얻어 1989년 Schnorr는 mod p 상에서의 이산 대수 문제를 이용하여 계산능력이 약한 스마트 카드에 적합한 새로운 개인식별 방식을 제안하였다[14,15]. 이 방식에서는 가입자가 네트워크에 가입할 때 센터가 그 가입자에 관한 개인 정보 ID_i와 신청자의 공개키 P_i 및 기타 유효일자 등의 데이터에 대한 서명(ISO/CCITT 용어로는 certificate라고 함)을 생성한다.

Fiat-Shamir 방식에서는 통신횟수가 t회 반복하는 데 반하여 Ohta 방식처럼 통신을 1회 행하므로 통신효율을 개선하였다. 그러나, 엄밀한 의미에서 Schnorr 방식은 영지식은 아니다. 또한, Schnorr 방식은 ID를 이용한 방식이 아니므로 센터가 certificate를 생성해야 하는 단점이 있으며 검증자가 이 certificate를 검증해야 하는 단점이 있다. 이러한 단점은 가입자의 공개키가 가입자의 identity ID인 indentity-based 방식[5]에서는 존재하지 않는다. 역으로 말하면, identity-based 구현시 실질적인 주요한 단점은 가입자가 자신의 비밀키를 선택할 수 없을 뿐만 아니라 가입자의 비밀키를 센터가 계산하며, 유효기간 동안 언제라도 센터가 재계산을 할 수 있다는 것이다.

mod p 상에서의 이산대수를 mod n 상에서의 이산대수로 확장한 개념은 Shmuely와 McCurley가 Diffie, Hellman의 공개키 분배방식에 적용하였다[16,17]. Diffie-Hellman 방식을 소인수분해 알고리즘이나, 이산 대수 알고리즘 중 어느 하나를 효과적으로 계산할 수 있는 암호해독가라도 공격이 불가능한 CDH(Composite Diffie Hellman)방식으로 변형하여 두가지 어려운 문제를 결합하여 안전성을 높였다.

이와 같은 개념으로 EUROCRYPT' 90에서 Brickell, McCurley와 Girault는 각기 다른 방법으로 mod p 상에서의 Schnorr 방식을 mod n 상으로 확장하였다[18,19]. 특히, Girault는 Schnorr 방식의 mod p 상에서의 이산대수를 mod n 상에서의 이산 대수로 확장하고, 각 가입자의 공개정보와 ID를 결합하여 센터가 효율적인 공개키를 생성하는 개인식별 방식을 제안하였다[19,20]. 본 논문에서는 Girault의 방법을 소개하기로 한다.

두 소수 $p=2fp'+1$, $q=2fq'+1$의 곱인 n을 법으로 하는 개인식별 방식으로 변형하자. 단, f, p',

q'는 각기 다른 소수이며, f는 200 bit, p'와 q'는 300 bit인 각기 다른 소수이며, 결국 n은 1000 bit의 합성수이다.

e는 $p-1$, $q-1$과 서로소인 공개정보이며 e의 길이는 20 bit에서 70 bit이다. d는 mod lcm($p-1$, $q-1$)상에서의 e의 승산역원이다.

Z_p 및 Z_q상에서 위수가 f인 원소 α를 정한다. 즉, mod n 상에서 α의 위수는 f이다. n, f, α, e는 센터의 공개정보이며, p, q, d는 비밀정보이다.

각 가입자는 자신의 비밀키 S_i를 선택하여, α^{S_i} (mod n)를 계산하여 센터에게 제출하면, 센터는 가입자의 공개키 $P_i=ID_i^{d}\cdot\alpha^{S_i}$(mod n)을 계산하고 certificate를 생성한다. 각 가입자의 공개키는 가입자의 identity 및 비밀키에 의존적이다. 또한, ID와 P의 관계는 $P^{e}\cdot ID\cdot h^{e}=1$(mod n)이 성립한다. 이때 $h=\alpha^{e}$(mod n)이다.

프로토콜 5. Girault의 identity-based 개인식별 프로토콜

순서 1-1. 가입자 A는 난수 $r\in_R \{1, 2, \ldots, f-1\}$를 선택한다.

순서 1-2. 가입자 A는 $x=h^{r}$(mod n)를 계산하다.

순서 1-3. 가입자 A는 ID_A와 P_A, Certificate, x를 가입자 B에게 전송한다.

순서 2-1. 가입자 B는 Certificate를 검증하여 가입자 A의 identification을 확인.

순서 2-2. 가입자 B는 난수 $c\in_R \{0, \ldots, e-1\}$를 선택한다.

순서 2-3. 가입자 B는 난수 c를 가입자 A에게 전송한다.

순서 3-1. 가입자 A는 $y=r+S_A\cdot c$(mod f)를 계산한다.

순서 3-2. 가입자 A는 y를 가입자 B에게 전송한다.

순서 4-1. 가입자 B는 $x=h^{y}\cdot(p^{e}\cdot ID_A)^{c}$(mod n)이 성립하는지 검증한다.

이 방식의 안전성을 생각하기 위하여 "가입자의 비밀키 S를 발견하여 정규 가입자인 척 할 수 있는 어려움의 정도는 무엇인가?", "센터의 비밀정보 d를 발견하여 신뢰 센터인 척 할 수 있는 어려움의 정도는 무엇인가?"의 2가지 질문에 대하여 생각하여 보자.

Schnorr 방식 같은 non-identity-based 방식에서는 생각할 수 있는 질문이 아니다. 왜냐하면, 대답이 certificate를 생성하는 서명 방식에만 의존하기 때문이다. 즉, 서명 방식은 개인식별 방식과는 완전히 독립적이기 때문이다. identity-based 방식에서 2개의 질문은 하나가 된다. 왜냐하면, S는 d를 이용하여 ID로부터 계산되고, d를 발견한다는 것은 S를 발견하는 유일한 방법으로 보이기 때문이다.

Girault의 identity-based 개인식별 프로토콜에서는 위의 2가지 질문이 분리된다. 왜냐하면, 앞에서도 언급했지만, d를 이용하여 S를 계산하는 것이 불가능하기 때문이다. n을 소인수분해하면, 신뢰 센터인 척 하는 것은 충분하며, mod n 상에서 이산 대수를 계산하면, 가입자인 척 흉내내는 것은 가능하다.

4. ID를 이용한 디지탈 서명

Shamir가 1984년 ID를 이용한 암호시스템의 개념을 제안하고, 그 실현 방법으로 디지탈 서명 방식을 소개한 이후 Fiat-Shamir 디지탈 서명 방식을 필두로 하여 Ohta, Guillou 등의 영지식 대화형 프로토콜에 바탕을 둔 각종 디지탈 서명 방식들이 제안되어 왔다.

4.1 Fiat-Shamir의 디지탈 서명

Fiat-Shamir 디지탈 서명 방식은 Fiat-Shamir 개인식별 방식과 동일한 준비 과정을 행하며 증명자가 메시지 M에 대하여 서명을 만들어 확인자에게 전송해야 하므로 개인식별 방식처럼

대화형 방식은 이용할 수 없다. 그러므로 증명자는 해쉬함수 f를 이용하여 서명하려는 메시지와 자신이 선택한 랜덤수에 의존하는 2진 벡터 $\{e_{ij}\}$를 생성하여 이용한다.

가입자 A가 메시지 M에 대한 디지탈 서명 (s, t)를 생성하여 가입자 B에게 전송하고, 가입자 B가 서명 (s, t)를 검증하는 방법은 다음과 같다.

프로토콜 6. Fiat-Shamir 디지탈 서명 프로토콜

〔디지탈 서명의 생성〕

순서 1-1. 가입자 A는 난수 $r_1, \ldots, r_t \in_R Z_n^*$를 선택한다.

순서 1-2. 가입자 A는 $x_i=r_i^2(1\le i\le t) \pmod n$를 계산하다.

순서 1-3. 가입자 A는 $f(M, x_1, \ldots, x_t)$를 계산하여 처음의 kt 비트 $e_{ij}(1\le i\le t, 1\le j\le k)$를 메시지 M에 대한 서명으로 한다.

순서 1-4. 가입자 A는 $y_i=r_i\prod_{e_{ij}=1} s_j \pmod n$을 계산한다.

순서 1-5. 가입자 A는 가입자 B에게 ID_A, M, $\{e_{ij}\}$ 및 y_i를 전송한다.

〔디지탈 서명의 검증〕

순서 2-1. 가입자 B는 $v_j=f(ID_A, j)(1\le j\le k)$를 계산하다.

순서 2-2. 가입자 B는 $z_i=y_i^2\prod_{e_{ij}=1} v_j \pmod n$을 계산한다.

순서 2-3. 가입자 B는 $f(M, z_1, \ldots, z_t)$를 계산하여 처음의 kt비트가 e_{ij}와 동일한가 검증한다.

가입자 A와 가입자 B는 이 프로토콜을 사용하여 가입자 B는 가입자 A의 서명이 정당한가 항상 확인할 수 있다. 이와 같은 서명 방식은 영지식 증명은 아니나, Feige와 Shamir가 전용 가능한 정보(transferable information) 개념을 제안하여 안전하다는 것을 증명하였다.

4.2 Ohta의 디지탈 서명

Ohta 디지탈 서명 방식은 Ohta 개인식별 방식과 동일한 준비 과정을 행하나, 해쉬 함수(hash function) h를 추가로 공개해야 한다.

가입자 A가 메시지 M에 대한 디지탈 서명 x, y)를 생성하여 가입자 B에게 전송하고, 가입자 B가 서명(x, y)를 검증하는 방법은 다음과 같다.

프로토콜 7. Ohta 디지탈 서명 방식

〔디지탈 서명의 생성〕

순서 1-1. 가입자 A는 난수 $r \in_R Z_n^*$를 선택한다.

순서 1-2. 가입자 A는 $x=r^v \pmod n$를 계산하다.

순서 1-3. 가입자 A는 해쉬함수 f를 이용하여 압축된 $f(M, x)=E$를 계산한다.

순서 1-4. 가입자 A는 $y=r\cdot S_A^E \pmod n$을 계산한다.

순서 1-5. 가입자 A는 가입자 B에게 ID_A, M, (x, y)를 전송한다.

〔디지탈 서명의 검증〕

순서 2-1. 가입자 B는 $f(M, x)=E$를 계산한다.

순서 2-2. 가입자 B는 $y^v=x\cdot ID_A^E \pmod n$가 성립하는 지 검증한다.

만약 L승근을 구하는 문제가 어렵다면 $x\cdot ID_A^E$의 L승근인 y를 구할 수 없으므로 비밀키 S_A를 모르는 제3자가 임의의 메시지 M에 대한 서명 (x, y)를 구하는 것은 불가능하다.

5. ID를 이용한 키 분배

ID를 이용한 키 분배방식에는 크게 대화형 방식과 비대화형 방식으로 분류할 수 있으며, 키분배 프로토콜 수행전 필요에 의하여 사전에 개인식별 프로토콜 등을 수행하는 경우 개인식별 프로토

콜의 랜덤정보를 이용하여 키 분배를 하는 프로토콜을 설계할 수도 있다[22]. 1984년 Shamir가 소개한 identity-based 방식에서의 가입자의 *ID* 자체를 공개키로 사용함으로써 공개키 분배방식에서의 공개키 관리 및 인증을 자연스럽게 해결한 Okamoto의 *ID*를 이용한 키 분배방식을 소개하기로 한다.

5.1 Okamoto의 키 분배방식

Okamoto는 Diffie-Hellman의 키 분배방식에 *ID*를 이용한 인증을 첨가한 방식을 제안하였다[22].

먼저 센터는 일방향함수로 RSA 암호계를 구성하기 위하여 2개의 소수 p, q 및 d를 비밀리에 보관하고, $n(=p\cdot q)$ 및 e를 공개한다. 또한, $GF(p)$ 및 $GF(q)$의 원시원소인 g를 공개한다.

가입자가 네트워크에 가입시에 각 가입자는 자신의 개인식별정보 *ID*를 센터에 등록한다. 센터는 $S=ID^{-d} \pmod n$를 계산하여 가입자에게 전달한다.

가입자 *A*와 가입자 *B*는 다음과 같은 방법으로 키를 공유할 수 있다.

프로토콜 8. ID를 이용한 키 분배 프로토콜

순서 1-1. 가입자 *A*는 난수 r_A를 선택한다.

순서 1-2. 가입자 *A*는 $c_A=S_A\cdot g^{r_A} \pmod n$를 계산하다.

순서 1-3. 가입자 *A*는 c_A를 가입자 *B*에게 전송한다.

순서 2-1. 가입자 *B*는 난수 r_B를 선택한다.

순서 2-2. 가입자 *B*는 $c_B=S_B\cdot g^{r_B} \pmod n$를 계산하다.

순서 2-3. 가입자 *B*는 c_B를 가입자 *A*에게 전송한다.

순서 3. 가입자 *B*는 공유키 $K_{AB}=((c_A)^e\cdot ID_A)^{r_B}=g^{r_Ar_B}$를 계산한다.

순서 4. 가입자 *A*는 공유키 $K_{AB}=((c_B)^e\cdot ID_B)^{r_A}=g^{r_Ar_B}$를 계산한다.

이 방식은 가입자가 비밀키의 파라메터인 r_i를 센터에 통하지 않고 용이하게 변경할 수 있으며, 센터가 가입자간의 통신을 도청할 수 없으며, 가입자간의 결탁 문제도 없는 방식이다.

6. 결 론

본고에서는 *ID*를 이용한 암호시스템 분야의 연구 기반을 마련하고자 전형적인 공개키 방식에서 공개키 디렉토리를 제거하는 방법인 certificated 방식과 identity-based 방식을 비교 설명하고, 1984년 Shamir가 *ID*를 이용한 암호시스템의 개념을 제안한 이래 *ID*를 이용한 대표적인 개인식별 방식 및 디지탈 서명 방식들을 안전성과 효율성 측면에서 비교 분석하였다. 또한, *ID*를 이용한 키 분배방식에는 크게 대화형 방식과 비대화형 방식으로 분류할 수 있는데 대표적인 대화형 방식인 가입자의 *ID* 자체를 공개키로 사용함으로써 공개키 분배방식에서의 공개키 관리 및 인증을 자연스럽게 해결한 Okamoto의 *ID*를 이용한 키 분배방식을 소개하였다.

참 고 문 헌

[1] W.Diffie, M.Hellman, "New directions in cryptography", IEEE Transactions on Information Theory, Vol.IT-22, pp. 644-654, Nov.1976.

[2] 권 창영, 원 동호, "Self-Certified 공개키 방식에 관한 고찰", 통신정보보호학회 학회지, 제3권, 제3호, pp.80-86, 1993. 9.

[3] S.Tsujii, K.Kurosawa, "ID-Based Cryptosystem", ISEC89-51, pp.25-31, 1989.

[4] D.E.Denning, "Cryptography and data security", P.170, Addison Wesley, 1982.

[5] Shamir, "Identity-Based Cryptosystems and Signature Schemes", Crypto' 84, pp.47-53, 1984.

[6] Fiat, Shamir, "How to Prove Yourself: Practical Solutions of Identification and Signature Problems", Crypto' 86, pp.186-194, 1986.

[7] H.J.Knobloch, "A Smart Card Implementation of the Fiat-Shamir Identification Scheme", Eurocrypt' 88, pp.87-95, 1998.

[8] S.Micali, A.Shamir, "An Improvement of the Fiat-Shamir Identification and Signature Scheme", Crypto' 88, pp. 244-247, 1988.

[9] L.C.Guillou, J.J.Quisquater, "A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing both Transmission and Memory", EUROCRYPT' 88, pp.123-128, 1988.

[10] L.C.Guillou, J.J.Quisquater, "A Paradoxical Identity-Based Signature Scheme Resulting from Zero-Knowledge" CRYPT' 88, pp.216-231, 1988.

[11] K.Ohta, T.Okamoto, "A Modification of the Fiat-Shamir scheme", CRYPT' 88, pp.233-243, 1988.

[12] D.Chaum, J.H.Evertse, J.van de Graaf, R.Peralta "Demonstrating Possession of A Discrete Logarithm without Revealing it" CRYPTO' 86, pp. 200-212, 1986.

[13] D.Chaum, J.H.Evertse, J.van de Graaf, "An Improved Protocol for Demonstration Possession of Discrete Logarithms and Some Generalizations", Eurocrypt' 87, pp.127-141, 1987.

[14] Schnorr, "Efficient Identification and Signatures for Smart Cards", Proceedings of Eurocrypt' 89, pp.686-689, 1989.

[15] Schnorr, "Efficient Identification and Signatures for Smart Cards", Proceedings of Crypto' 89, pp.239-252, 1989. J. of Cryptology, Vol.4, No.3, pp.161-174, 1991.

[16] Shmuely, "Composite Diffie-Hellman Public-Key Generating Systems Are Hard to Break", TR. No. 356, Computer Science Dept. Technion, IIT, 1985.

[17] McCurley, "A Key Distribution System Equivalent to Factoring", J. of Cryptology, Vol.1, No.2, pp.95-105, 1988.

[18] E.F.Brickell, K.S.McCurley, "An Interactive Identification Scheme Based on Discrete Logarithm and Factoring", Eurocrypt' 90, pp.63-71, 1990.

[19] M.Girault, "An Identity-based identification scheme based on discrete logarithms modulo a composite number", Eurocrypt' 90, pp.481-486, 1990.

[20] M.Girault, "Self-certified public keys", Advances in Cryptology EUROCRYPT' 91, pp.490-497, 1991.

[21] E. Okamoto, K.Tanaka, "Key Distribution System Based on Identification Information", Proc, GLOBECON 87, pp.108-111, 1987.

[22] 이 윤호, 양 형규, 권 창영, 원 동호, "*ID* 기반의 영지식 대화형 프로토콜을 이용한 개인 식별 및 키 분배 프로토콜에 관한 연구", 한국통신정보보호학회 논문지, 제2권, 제1호, pp.3-15, 1992. 6.

□ 著者紹介

권 창 영(權 蒼 英, Chang-Young Kwon) 정회원

1957년 4월 22일생
1983년 2월 성균관 대학교 수학교육과 졸업 (이학사)
1991년 2월 성균관 대학교 대학원 정보공학과 졸업 (공학석사)
1991년 3월 - 현재 성균관 대학교 대학원 정보공학과 박사과정 재학중
1982년 12월 - 1988년 9월 (주) KOLON 정보 SYSTEM실 팀장
1992년 3월 - 현재 대유공업전문대학 사무자동화과 전임강사
※ 주관심분야 : 암호학, 정보관리

김 경 신(Kyung-Shin Kim) 정회원

1960년 6월 1일생
1983년 2월 성균관 대학교 전자공학과 졸업 (이학사)
1985년 2월 성균관 대학교 대학원 전자공학과 졸업(공학석사)
1993년 3월 - 현재 성균관대학교 대학원 정보공학과 박사과정 재학중
1984년 12월 - 1991년 2월 (주)삼성전자 컴퓨터부문 선임연구원
1991년 3월 - 현재 연암공업전문대학 전자계산과 조교수
※ 주관심분야 : 정보보호 이론, 멀티미디어 응용 분야

원 동 호(元 東 豪, Dong-Ho Won) 종신회원

1949년 9월 23일생
1976년 2월 성균관 대학교 전자공학과 졸업 (공학사)
1978년 2월 성균관 대학교 대학원 전자공학과 졸업 (공학석사)
1988년 2월 성균관 대학교 대학원 전자공학과 졸업 (공학박사)
1978년 4월 - 1980년 3월 한국전자통신연구소 연구원
1985년 9월 - 1986년 8월 일본 동경공대 객원연구원
1982년 3월 - 현재 성균관대학교 공과대학 정보공학과 교수
1991년 - 현재 한국통신정보보호학회 편집이사
※ 주관심분야 : 암호이론, 정보이론