通信情報保護學會論文誌
第6卷 第3號, 1996. 9

개인정보에 기초한 서명 및 키 분배 통합 암호시스템의 제안

하 재 철*, 문 상 재*

Proposal of ID-Based Cryptosystems Integrating Digital Signature and Key Distribution.

Jae-Cheol Ha*, Sang-Jae Moon*

요 약

정보통신망에서 공개 키의 인증 문제를 비교적 쉽게 해결할 수 있고 디지탈 서명 및 키 분배를 하나의 시스템 내에서 구현할 수 있는 효율적인 비대칭 키 암호시스템이 요구될 수 있다. 본 논문에서는 개인정보에 기초하여 디지탈 서명과 키 분배를 통합하는 두 가지 형태의 암호시스템을 제안하고 계산량과 구현 측면에서 효율성을 분석한다. 그 하나는 ElGamal형 서명 기법을 이용하고 다른 하나는 RSA 기법을 이용하여 시스템을 구성한다. 두 암호시스템은 대화형 및 일방향 형태로 키를 분배할 수 있다.

Abstract

It would be desirable in network to implement an efficient asymmetric key cryptosystem which can not only solve the public key authentication problem but also integrate digital signature and key distribution. We propose two ID-based key distribution systems integrated with digital signature, and analyze them in computation and implementation. The first is based on the ElGamal-typed signature scheme, and the second is based on the RSA scheme. Both can be employed in one-pass and interactive key distribution systems.

1. 서 론

정보의 효율적인 관리와 교환을 위해서는 중요한 자원에 대한 출입을 통제하거나 통신 상대자를 확인하는 인증 서비스가 요구되며 정보의 무결성 검사와 송수신 사실의 부인을

* 경북대학교 전자전기공학부

방지하기 위한 디지탈 서명 서비스가 필요하다. 또한 데이터를 암호화하기 위한 키 분배 및 관리도 정보보호에 있어 기본적인 요소이다. 이러한 서비스들을 개별적인 시스템으로 구현하는 것보다 하나의 시스템내에서 통합적으로 구현하는 것이 효과적이다.

개인정보(identity, ID)에 기초한 암호법은 일종의 비대칭 키 암호법으로 유일한 개인정보를 공개 키로 사용하는 것이다. 일반에게 공인된 신상의 정보를 사용하므로 D-H(Diffie-Hellman)[1]이나 RSA(Rivest, Shamir, and Adleman)[2] 비대칭 키 암호법에서와 같이 개인정보와 관련이 없는 불규칙 정수 형태의 공개 키 화일을 인증하는 문제를 쉽게 해결할 수 있다. 개인정보를 공개 키 자체로 사용하는 것은 공개 키의 인증 문제를 해결하는데 가장 효과적이나 키 분배와 같은 다양한 형태의 보호 서비스를 제공하는 시스템을 구현하기가 쉽지 않다. 이러한 문제점을 극복하기 위해서 개인정보와 이를 간접적으로 관련시킨 공개 키를 사용하는 방법이 효과적이다.

통합 암호시스템을 설계하는 방법으로는 ElGamal 형태의 서명 기법을 이용하는 방법과 RSA 기법을 이용하는 방법으로 구분할 수 있다. H-Y(Harn-Yang)에 의해 제시된 AMV (Agnew, Mullin, and Vanstone) 서명을 이용한 통합 암호시스템[3]이 전자에 해당한다. 후자의 경우에는 각 서비스에 대한 시스템이 독립적으로 연구되었다.

본 논문에서는 개인정보에 기초하여 인증, 디지탈 서명 그리고 키 분배를 통합할 수 있는 두가지 형태의 암호시스템을 제안한다. 특히 키 분배는 적용 방법에 따라 대화형 및 일방향 형태로 구분하였으며, 대화형 키 분배는 키의 인증 여부에 따라 직접 인증 및 간접 인증 키 분배로 구분하였다. 첫번째 통합 암호시스템은 ElGamal형 서명 기법을 이용하였으며 인증 방식, 직·간접 인증 키 분배 및 일방향 키 분배 방식을 제안하였다. 두번째 통합 암호시스템은 RSA 기법을 이용하였으며 서명 방식, 직접 인증 및 일방향 키 분배 방식을 제안하였다. 그리고 두 시스템을 안전성 및 구현 측면에서 H-Y의 암호시스템과 비교 분석하였다.

2. 개인정보에 기초한 암호시스템

1984년 Shamir는 공개 키 디렉토리를 제거할 수 있는 개인정보에 기초한 암호시스템을 처음으로 연구 발표하였다[4]. 이 암호시스템은 일종의 비대칭 키 암호시스템으로 공개 키를 유일하면서 누구나 식별하기 용이한 개인정보로 대치한 시스템이다. 고유한 개인정보로는 성명, 주민등록 번호, 주소 그리고 전화번호 등이 있다. 그러므로 별도의 공개 키 화일을 관리하거나 공개 키를 증명할 필요가 없다.

개인정보에 기초한 암호시스템에서 시스템을 구성하는 기본 파라미터를 설정하고 비밀 키를 생성하는 키 관리 센타(key management center)는 절대적인 신뢰성이 요구된다(이하에서는 키 관리 센타를 센타라 약칭한다). 개인의 개인정보를 기초로 생성된 비밀 키와 시스템 관련 정보 등은 IC 카드와 같은 물리적으로 보호된 매체를 통해 발급된다.

Shamir는 개인정보에 기초한 암호시스템을 제안하면서 그 실현 방법으로 디지탈 서명 방식을 제시하였다. 이를 시초로 하여 F-S(Fiat-Shamir)의 인증 및 디지탈 서명 방식[5], 그리고 G-Q(Guillou-Quisquater)의 인증 및 디지탈 서명 방식[6] 등이 제안되었다. 이 중 G-Q 방식은 RSA 기법을 사용하여 생성된 비밀 키를 사용하므로 프로토콜 수가 적고 서명 길이가 짧아 효율적이다. 이 방식들은 개인정보 자체를 공개 키로 사용하므로 인증이나 서명에서 공개 키 관리 문제를 자연스럽게 해결하였다.

개인정보에 기초한 암호시스템은 키 인증 문제를 해결할 수 있는 장점이 있으나 개인정보를 공개 키 자체로 사용하는 조건이 키 분배

와 통합하는 데는 제한적인 요소가 된다. 즉, 개인 정보를 공개 키로 사용하면 D-H에서와 같이 공개 키가 공통의 밑수(base)를 가지지 못하므로 키 분배가 어려워진다. 그러므로 개인정보를 공개 키 자체로 사용하는 대신, 개인정보와 이에 기초한 공개 키를 사용하는 것이 효율적이다. 이 경우 사전에 통신자간 대화를 통해 개인정보와 관련된 정보를 교환한 후 세션 키를 생성한다는 의미에서 개인정보에 기초한 암호시스템의 본래 개념과는 약간 다르다.

개인정보를 공개 키 자체로 사용하는 대신 개인정보와 이에 기초한 공개 키를 사용하는 대표적인 대화형 키 분배 방법은 Günther 방식[7] 그리고 H-Y 방식[3] 등과 같이 ElGamal 형태의 서명 기법을 이용한 방법과 O-T (Okamoto-Tanaka) 방식[8]과 같이 RSA 기법을 이용한 방법으로 구분할 수 있다. 이 중 H-Y 방식은 AMV 서명법과 D-H형 키 분배법의 개념을 도입한 것으로서 하나의 시스템 내에서 인증, 디지탈 서명 및 키 분배를 통합적으로 수행할 수 있다.

3. ElGamal형 서명을 이용한 통합시스템

Harn-Xu는 기존의 발표된 서명 기법을 포함하여 ElGamal 형태의 디지탈 서명 기법을 일반화하였다[9]. 표 1은 일반화된 서명 기법의 서명 생성식과 검증식을 나타낸 것이다. 여기서 $\Phi(p)$는 소수 p에 대한 Euler 함수 값이며 g는 GF(p)상의 원시원이다. 일반화된 ElGamal 형태의 서명 방정식은 $aX = bk + c \bmod \Phi(p)$이다. 여기서 계수 (a, b, c)는 (m, r, s) 자체 혹은 그것의 수학적인 조합으로 이루어진다. 단, m은 서명할 메세지를 해쉬한 결과이며 r과 s는 메세지에 대한 서명이다. 또한 X는 사용자의 비밀 키이며 k는 불규칙 정수이다. 서명 검증식에서 Y는 사용자의 공개 키이며 이는 $g^X \bmod p$이다.

ElGamal 형태의 서명 방식을 사용하여 센타에서 개인정보에 기초한 서명 쌍을 생성하는 경우 X와 Y는 각각 센타의 비밀 키와 공개 키가 된다. 한 사용자가 등록하면 센타는

표 1. 일반화된 ElGamal 형태의 서명 방식

Table 1. Generalized ElGamal-typed signature schemes.

	Signature generation	Signature verification	
(1)	$mX = rk + s \pmod{\Phi(p)}$	$Y^m = r^r g^s \pmod p$	Harn
(2)	$mX = sk + r \pmod{\Phi(p)}$	$Y^m = r^s g^r \pmod p$	
(3)	$rX = mk + s \pmod{\Phi(p)}$	$Y^r = r^m g^s \pmod p$	
(4)	$rX = sk + m \pmod{\Phi(p)}$	$Y^r = r^s g^m \pmod p$	ElGamal
(5)	$sX = rk + m \pmod{\Phi(p)}$	$Y^s = r^r g^m \pmod p$	AMV
(6)	$sX = mk + r \pmod{\Phi(p)}$	$Y^s = r^m g^r \pmod p$	
(7)	$rmX = k + s \pmod{\Phi(p)}$	$Y^{rm} = rg^s \pmod p$	Moon, N-R
(8)	$X = mrk + s \pmod{\Phi(p)}$	$Y = r^{mr} g^s \pmod p$	Y-L
(9)	$sX = k + mr \pmod{\Phi(p)}$	$Y^s = rg \pmod p$	
(10)	$X = sk + rm \pmod{\Phi(p)}$	$Y = r^s g^{rm} \pmod p$	

서명식의 m을 ID로 대치하여 ID에 대한 서명 r과 s를 생성하여 사용자에게 전달한다. 센타의 공개정보 및 자신의 ID에 대한 서명 r과 s를 발급 받은 사용자는 s를 비밀 키로 사용하고 r은 ID와 관련한 공개정보로 사용한다.

인증, 서명 및 키 분배와 같은 응용 단계에서 이 암호시스템을 사용하기 위해서는 가급적 다음 성질을 만족하는 서명 방식을 사용하는 것이 효율적이다. 첫째, 공개하는 서명쌍 중 하나인 r과 ID만으로 공개 키를 계산할 수 있어야 한다. 둘째, 공개 키를 생성하는 계산량과 서명 검증 계산량이 상대적으로 적은 서명 방법을 이용하는 것이 효율적이다. 셋째, 비밀 키의 선택이 용이하며 다른 정보 보호 서비스와의 확장성이 좋은 서명 방식이어야 한다.

ElGamal 형태의 서명 방식 중 첫번째 성질을 만족하는 경우를 고려하면, 서명식에서 사용자의 비밀 키 s가 독립항일 때 사용자의 공개 키를 g^s로 센타의 비밀 키 X와 곱해진 형태일 때 공개 키를 Y^s로 사용할 수 있다. 이를 만족하는 서명 방식은 표 1에서 (1), (3), (5), (6), (7), (8) 그리고 (9)이다. 두번째 성질을 만족하는 경우를 보면, (1), (3), (5) 그리고 (6)방식은 공개 키를 생성하는데 2회의 멱승 연산이 필요한 반면 (7), (8) 그리고 (9)방식은 약 1회의 멱승 연산으로 가능하다. 그러나 (9) 방식은 비밀 키가 $\Phi(p)$과 서로 소(relatively prime)인 조건이 부가되며 서명 생성시 역수 계산이 필요하다. 또한 비밀 키 s와 불규칙 정수 k가 독립항일 때 broadband subliminal 서명이 용이하므로 결국 키의 선택성과 시스템의 확장성 측면까지 고려하면 Moon[10] 혹은 N-R(Nyberg-Rueppel) 서명 방식[11]이 위의 성질들을 만족한다고 볼 수 있다.

그러므로 이 서명 방식을 이용하여 개인정보에 기초한 인증, 디지탈 서명 그리고 키 분배를 통합할 수 있는 암호시스템을 구성하는 방안을 제안한다. 원 서명 방식에서와 같이 계산 효율을 높이기 위해 GF(p)보다 적은 부분체 GF(q)에서의 연산기법을 사용한다. 먼저 센타가 수행하는 시스템 구성과 사용자 등록 절차를 설명한 후 통신자간 수행하는 세부 응용 단계로 나누어 기술한다.

〔시스템 구성〕

① 센타는 소수 p를 선택하고 q | p-1인 소수 q를 선택한다.

② 센타는 $g = h^{(p-1)/q} \bmod p$인 원시원 g를 선택한다. 여기서, $g > 1$ 이고, h는 $0 < h < p$인 임의의 정수이다.

③ 비밀 키 X를 선택하고 공개 키 $Y = g^X \bmod p$를 계산한다. 또 일방향 해쉬함수 H를 선택한다. 여기서 H, p, q, g 그리고 Y는 각 사용자에게 공개하고 X는 비밀로 한다.

〔사용자 등록〕

사용자가 자신의 ID를 센타에 등록하면 센타는 원 서명 방식을 이용하여 ID에 대한 서명 s와 r을 사용자에게 발급한다.

① 센타는 $0 < k < q$인 k를 선택한 후 $r = g^k \bmod p$를 계산한다.

② 센타는 $EID = r \cdot H(ID)$를 구하고 $s = k - X \cdot EID \bmod q$를 계산한다.

③ 센타는 ID에 대한 서명 쌍인(s, r)을 사용자에게 발급한다.

이 시스템에서 두 통신자간에 교환하는 ID와 r로써 상대방의 공개 키를 생성할 수 있다. 즉 사용자의 공개 키는 $g^s = r \cdot Y^{-EID} \bmod p$이다. 이 서명 방식을 이용하면 1회의 멱승 연산으로 공개 키를 계산할 수 있다. 그러나 H-Y의 암호시스템에서는 표 1의 (5)인 AMV 서명을 이용한다. 그러므로 동일한 방식으로 센타에서 생성한 공개 정보 r과 ID를 이용하여 공개 키 $y^s = r^r g^{H(ID)} \bmod p$를 생성한다면 2회의 멱승 연산이 필요하다.

사용자 등록을 마친 후 A가 B에게 시도응

답형(challenge and response type)으로 신분을 증명하는 과정은 다음과 같다.

〔인증〕

① A가 B에게 자신의(ID, r)를 전송한다.

② B는 v ($0 < v < q$)를 선택하여 $W = g^v \bmod p$를 A에게 전송한다.

③ A는 $Z = W^s \bmod p$를 계산하여 B에게 전송한다.

④ B는 $(r \cdot Y^{-EID})^v = ? Z \bmod p$을 확인함으로써 A를 인증한다. 여기서 $EID = r \cdot H(ID) \bmod q$이다.

인증 과정에서 Schnorr의 인증 기법[12]을 그대로 사용할 수 있으나 제안하는 인증 방식이 전체 계산량 측면에서 효과적이다. 즉 Schnorr의 인증 방식이 순차적으로 이루어지는 반면, 제안 방식에서 단계 ④의 $(r \cdot Y^{-EID})^v$ 계산을 단계 ②가 완료된 직후 바로 수행할 수 있으므로 전체 계산 시간을 줄일 수 있다. 이 인증 방식에서 공개 정보나 통신 정보로부터 비밀 키를 계산하는 것은 이산대수(discrete logarithm) 문제이다. 또한 비밀 키 s나 공개 정보 r중 하나를 임의로 정한 후 시도할 수 있는 가장 공격(impersonation attack)도 역시 이산대수 문제로 귀결되어 이 인증 프로토콜은 안전하다.

〔디지탈 서명〕

서명자가 메세지 M에 서명을 하고자 할 때에는 센타가 발급한 비밀 키 s와 시스템 계수를 사용하여 원 서명 기법을 그대로 사용할 수 있다. 서명 확인에 필요한 공개 키를 구하는 문제는 서명자가 공개 정보 r을 서명 메세지와 함께 전송함으로써 해결된다. 즉 확인자는 $g^s = r \cdot Y^{-EID} \bmod p$를 계산하여 공개 키 g^s를 구할 수 있다.

〔대화형 키 분배(간접인증)〕

대화형으로 세션 키를 분배할 때 통신시마다 서로 다른 불규칙 정수를 발생하여 다른 키를 공유할 수 있어야 효과적이다. 직접적인 키의 인증없이 사용자 A와 B가 D-H의 키 분배 방식을 적용하여 불규칙 세션 키를 공유하는 과정은 다음과 같다. 제안하는 간접인증 키 분배 방식을 나타낸 것이 그림 1이며 두 통신자가 대칭적이므로 A의 경우만 기술한다.

① A는 v_A를 선택한 후 $W_A = g^{v_A} \bmod p$를 계산한다. 단, $0 < v_A < q$이다.

② A는(ID_A, r_A, W_A)를 전송하고 (ID_B, r_B, W_B)를 수신한다.

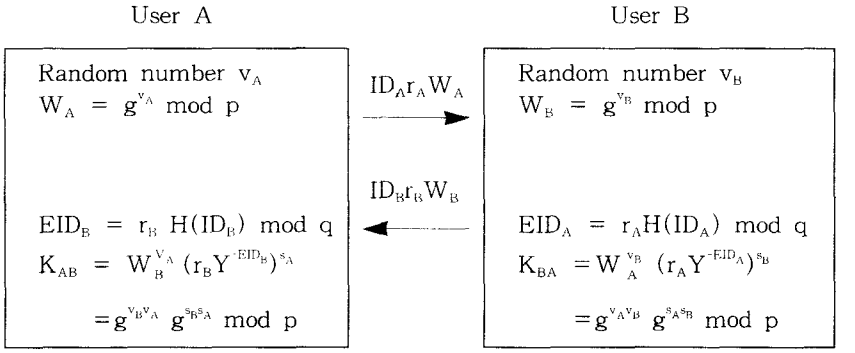


그림 1. 간접 인증 기능을 가진 키 분배

Fig. 1. Key distribution with indirect authentication.

③ A는 $EID_B = r_B \cdot H(ID_B) \bmod q$를 계산하고 세션 키를 다음과 같이 생성한다.

$$K_{AB} = W_B^{v_A} (r_B Y^{-EID_B})^{s_A} = g^{v_B v_A} \bmod p$$

이 키 분배 방식에서 전송 정보 W나 r로부터 비밀 정보 v나 s를 알 수 없으며 세션 키를 계산하는 것은 이산대수 문제와 같다. 또한 통신 후에 비밀 키 s가 노출되었고 전송 정보 W를 알고 있는 공격자라도 이전에 암호에 사용되었던 세션 키를 계산할 수 없어 perfect forward secrecy가 유지된다. 불법적인 제 3자가 A로 가장하여 공격하는 경우, W나 r을 위조하여 전송하더라도 A의 비밀 키 s_A를 알 수 없으므로 세션 키를 만드는 것은 불가능하다. 만약 세션 키를 $K_{AB} = W_B^{s_A} (r_B Y^{-EID_B})^{v_A} = g^{v_B s_A} g^{s_B v_A} \bmod p$와 같이 생성하더라도 비밀 정보를 알아 낼 수는 없으며 계산량은 제안 방식과 동일하다. 그러나 이 경우에는 통신 후에 비밀 키 s가 노출되었고 전송 정보 W를 알고 있는 공격자라면 이전에 암호에 사용되었던 세션 키를 계산할 수 있어 perfect forward secrecy가 유지되지 않는다.

〔대화형 키 분배(직접인증)〕

다음은 디지탈 서명 기법과 D-H 키 분배 방식을 적용하여 통신시마다 사용자 A와 B는 불규칙 세션 키를 공유 과정이며 그림 2에 나타내었다. 이 방식에서는 서명을 이용하여 불규칙 비밀 수를 인증하므로 직접 인증 기능이 제공된다.

① A는 v_A를선택하여 $W_A = g^{v_A} \bmod p$를 계산한다. 단 $0 < v_A < q$이다

② A는 $E_A = W_A \cdot H(W_A) \bmod q$를 계산한다.

③ A는 $\eta_A = v_A - s_A \cdot E_A \bmod q$를 계산한다.

④ A는 (ID_A, r_A, W_A, η_A)를 전송하고, (ID_B, r_B, W_B, η_B)를 수신한다.

⑤ A는 $EID_B = r_B \cdot H(ID_B) \bmod q$를 계산하고 W_B에 대한 서명을 확인한다.

$$W_B = g^{\eta_B} (r_B \cdot Y^{-EID_B})^{W_B \cdot H(W_B)} \bmod p$$

⑥ A는 세션 키 $K_{AB} = W_B^{v_A} = g^{v_A \cdot v_B} \bmod p$를 생성한다.

이 키 분배 방식은 불규칙 비밀 수 W를 서명 기법을 이용하여 직접 인증한 후 인증된 W에 D-H 키 분배 방식을 적용하였다. 그러므로 이 방식의 안전도는 원 서명의 안전도 및 D-H 키 분배 방식의 안전도와 동일하며 이는 이산대수 문제로 귀결된다.

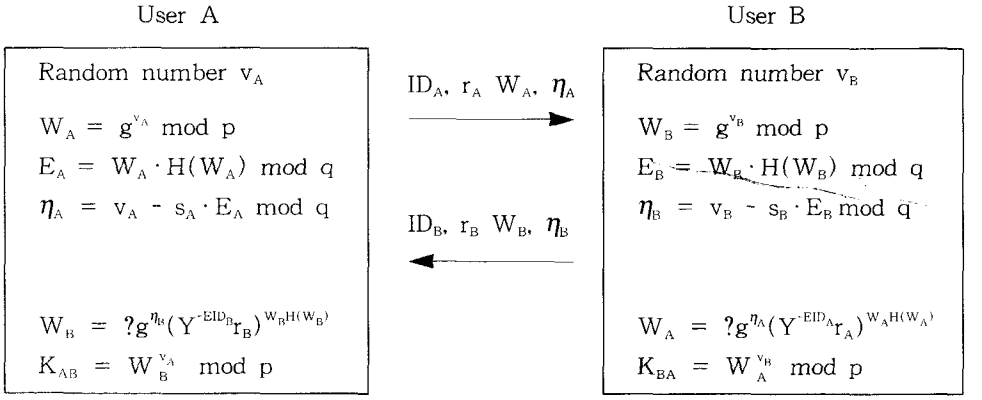


그림 2. 직접인증 기능을 가진 키 분배

Fig. 2. Key distribution with direct authentication.

〔일방향 키 분배〕

상기한 암호시스템에서 일방향으로 인증된 세션 키를 공유하는 방법을 제안한다. 만약, 통신자 A가 직접 인증 키 분배에서와 같이 $W_A = g^{v_A} \bmod p$를 서명하여 r과 함께 B에게 전송한다면 B는 서명 검증 후 D-H의 키 분배 방식에 적용하여 하나의 세션 키를 계산할 수 있다. 그러나 A는 B의 ID와 개인정보 관련 정보 r을 이용해야만 B의 실제 공개 키를 구할 수 있다. 그러므로 일방향 키 분배 시스템을 구현하기 위해서는 ID와 공개 키 관련 정보 r을 함께 관리하는 공개 화일이 있어야 한다. 공개 키 관련 정보 r은 센타에서 생성하므로 확인서는 필요하지 않으므로 검증 과정도 필요하지 않다. 이러한 조건하에서 일방향으로 키를 분배하는 과정은 다음과 같고 그림 3에 나타내었다.

① A는 v_A를 선택하여 $W_A = g^{v_A} \bmod p$를 계산한다. 단, $0 < v_A < q$이다.

② A는 $E_A = W_A \cdot H(W_A) \bmod q$를 구한다.

③ A는 $\eta_A = v_A - s_A \cdot E_A \bmod q$를 계산한다.

④ A는 B에게 (ID_A, r_A, W_A, η_A)를 전송한다.

⑤ A는 $EID_B = r_B \cdot H(ID_B) \bmod q$를 계산하고 세션 키 $K_{AB} = (r_B \cdot Y^{-EID_B})^{v_A} \bmod p = g^{s_B \cdot v_A} \bmod p$를 생성한다.

⑥ B는 $EID_A = r_A \cdot H(ID_A) \bmod q$를 계산하고 다음 식을 검증하여 W_A에 대한 서명을 확인한다.

$$W_A = g^{\eta_A}(r_A \cdot Y^{EID_A})^{W_A \cdot H(W_A)} \bmod p$$

⑦ B는 검증식이 성립하면 비밀 세션 키를 계산한다.

$$K_{BA} = W_A^{s_B} = g^{v_A \cdot s_B} \bmod p$$

일방향 키 분배 방식에서 공개 키 화일로부터 비밀 키를 찾아내는 것은 원 시스템을 해독하는 것과 동일하며 전송정보로부터 A의 비밀 키를 구하는 것은 직접인증 키 분배 방식에서와 같이 이산대수 문제로 동일하다. 또한 B의 비밀 키 s_B나 A의 비밀 수 v_A를 알지 못하고 세션 키를 알아내는 것도 이산 대수 문제로 귀착되어 안전하다.

4. RSA 기법을 이용한 통합시스템

본 장에서는 개인정보에 기초하여 RSA 기법을 이용한 인증, 디지탈 서명 및 키 분배를 통합할 수 있는 암호시스템을 제안한다. 시스템 구성 단계 및 사용자 등록 단계는 G-Q의 인증 및 서명 시스템을 이용하며 키 분배를 위한 GF(p)와 GF(q)의 원시원 g를 추가적으로 공개하는 것만 차이가 있다.

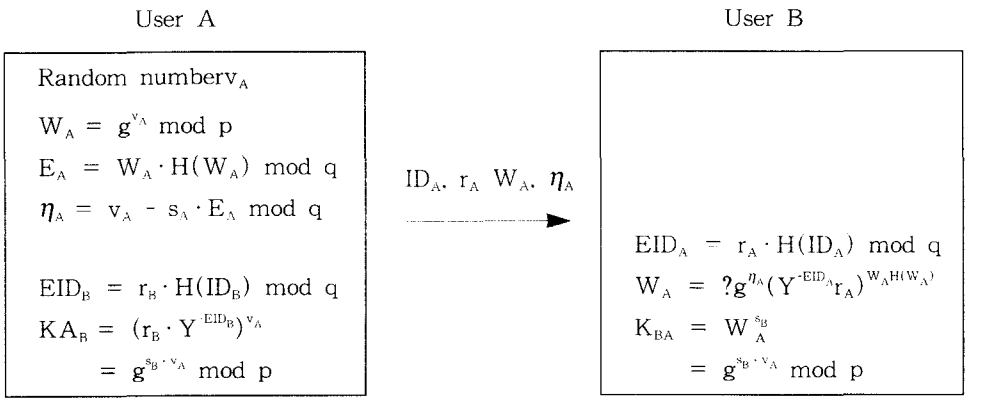


그림 3. 상호 인증 기능을 가진 일방향 키 분배

Fig. 3. One-pass key distribution with mutual authentication.

〔시스템 구성〕

① 센타는 두 소수 p 와 q를 생성한다.

② GF(p)와 GF(q)상의 원시원 g, N(= p·q) 및 ϕ(N)를 결정한다. 여기서 ϕ(N)은 (p-1)(q-1)이다.

③ 센타는 적당한 크기의 소수 e를 선택하고 e·d mod ϕ(N) = 1를 만족하는 d를 생성한다. 여기서 센타는 N, g 그리고 e를 공개하고 p, q, ϕ(N)그리고 d를 비밀로 한다.

〔사용자 등록〕

① 사용자가 개인정보 ID를 센타에 등록하면, 센타는 다음과 같이 사용자 비밀 키 S를 계산한다.

$J = Red(ID),\ S = J^{-d} \bmod N.$

즉, $S^e \cdot J \bmod N = 1$이다. 여기서 Red( )는 용장규칙(redundancy rule)이다.

② 센타는 N, g, e 그리고 비밀 키 S를 사용자에게 발급한다.

〔디지탈 서명〕

인증 및 디지탈 서명을 수행할 때에는 G-Q 방식을 그대로 적용 가능하다. 그러나 G-Q 서명의 단점은 메세지 해쉉시 불규칙 수 T와 메세지 M을 동시에 입력으로 사용한다는 것이다. 즉, 서명 쌍의 하나인 k가 k = H(T, M)와 같이 생성된다. 이와 같은 점은 개인정보에 기초한 암호시스템이 IC 카드 사용을 전제로 할 경우에 서명을 계산하는데 부적합하다. 즉 IC 카드 내에서 서명을 생성할 때 메세지를 주 전산장치로부터 수신하여 해쉬 함수를 구해야 한다. 이 경우 메세지가 크다면 IC 카드 내의 저장 능력이 크거나 일정한 크기로 나누어 전송하여 처리해야 하며 카드 내에 해쉬 함수 알고리듬이 있어야 한다. 그렇지 않으면 관련 데이타 T를 주 전산 장치로 보내어 해쉬 함수를 구한 후 그 결과 값을 다시 IC 카드로 보내어 서명 값을 생성해야 한다. 어느 경우든 주 전산 장치와 IC 카드 사이에 통신 프로토콜 설정과 데이타 전송 시간 때문에 실제로 서명이 지연된다. 그러므로 해쉬 함수의 입력을 다른 변수의 입력 없이 M만을 사용하여 주 전산 장치에서 해쉬 함수 값을 미리 계산하는 것이 효율적이다. 그러므로 키 분배와의 통합성을 고려하여 다음과 같은 서명 방식을 제안한다. 이를 나타낸 것이 그림 4이다.

〔서명 생성〕

① 서명자는 불규칙 정수 v(0 < v < N)를 생성하고 $T = v^e \bmod N$를 계산한다.

② 서명자는 메세지 M을 해쉉한 결과에 T와 곱한 후 e로 모듈라를 취함으로써 계산 효율을 높인다. 즉, $k = T \cdot H(M) \bmod e$이다. 이때 mod e 대신 계산량과 안전도를 고려하여 다른 해쉉이나 비트

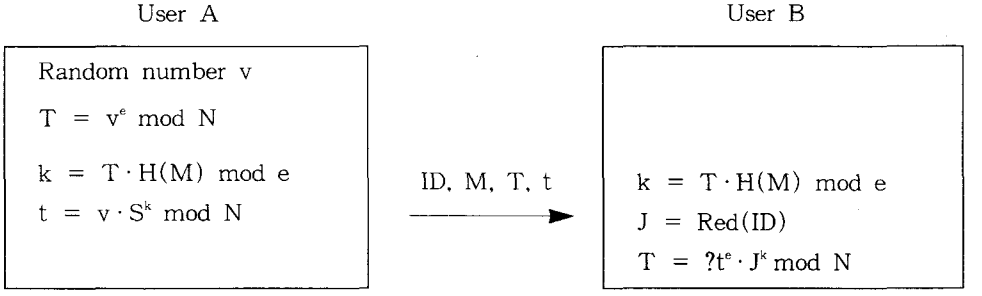


그림 4. 메시지 해쉬가 효율적인 디지탈 서명 방식

Fig. 4. Digital signature scheme with efficient message hash.

절단(truncation) 등의 방법으로 k의 비트 수를 조절할 수도 있다.

③ 서명자는 자신의 비밀 키 S, k 및 v를 이용하여 $t = v \cdot S^k \bmod N$ 계산한다.

④ 서명자는 자신의 ID, 메세지 M 그리고 서명 쌍 (T, t)를 검증자에게 전송한다.

〔서명 검증〕

① 검증자는 $k = T \cdot H(M) \bmod e$를 계산한다.

② 검증자는 서명자의 $J = Red(ID)$를 계산한다.

③ 검증자는 $T = t^e \cdot J^k \bmod N$를 확인하여 메세지를 인증한다.

검증은 수신 정보와 공개 정보를 이용하여 T를 재구성하는 과정으로 이루어지며 증명식은 다음과 같다.

$$t^e \cdot J^k = (v \cdot S^k)^e \cdot J^k = v^e \cdot (S^e \cdot J)k = v^e \bmod N = T$$

안전도 측면에서, 비밀 데이타인 S나 v를 계산하기 위해서는 공개 키 ID에서 S를 혹은 서명 T에서 v를 계산해야 하는데 이것은 mod N에 대한 e승근을 구하는 문제이고 결국 N의 소인수분해(factorization) 문제로 귀착된다. 서명 t를 먼저 정하고 ID와 메시지에 해당하는 T를 구할 수 있으면 위조가 되는데 이는 임의의 X에 대해 $T = X^e \bmod N$인 T를 구하는 어려운 문제이므로 안전성을 증명할 수 있다. 이 서명 방식의 계산량은 G-Q의 서명과 동일하며 메시지 해쉉을 효과적으로 할 수 있다.

〔대화형 키 분배(간접인증)〕

간접인증을 제공하면서 불규칙 세션 키를 분배하는 경우에는 O-T 방식[18]이 적용 가능하다. 즉, 통신자 A가 불규칙 정수 u_A $(0 < u_A < e)$를 생성한 후 $T_A = S_A \cdot g^{u_A} \bmod N$를 계산하여 ID_A와 함께 B에게 전송한다. 대화형으로ID_B와 T_B를수신한 A는 $J_B = Red(ID_B)$를 계산한 후 세션 키를 다음과 같이 생성한다.

$$K_{AB} = (T_B^e \cdot J_B)^{u_A} = g^{e \cdot u_B \cdot u_A} \bmod N$$
$$= (T \cdot J_A)^{u_B} = K_{BA}$$

〔대화형 키 분배(직접인증)〕

서명 기법을 이용하여 직접 인증을 제공하면서 대화형으로 키를 분배할 경우, 수신한 서명쌍 중 T를 이용하여 직접 D-H 키 분배 방식을 적용할 수 없다. 왜냐하면 T는 두 통신자가 발생한 서로 다른 밑수를 사용하기 때문이다. 이를 해결하는 방법은 두 통신자가 공통의 밑수를 가진 정보를 교환해야 한다. 즉, 서명 기법을 이용하여 대화형 키 분배 시스템을 구현하기 위해서는 서명 과정에서 생성하는 불규칙 정수 v를 $v = g^u \bmod N$로 계산하면 된다. 즉 $T = v^e = g^{u \cdot e} \bmod N$가 되어 D-H 키 분배 방식을 적용할 수 있다. 상기한 사실에 근거하여 통신자 A, B가 대화형으로 키를 공유하는 절차를 제안하면 다음과 같다. 그림 5는 이를 나타낸 것이다.

① A는 $u_A (0 < u_A < e)$를 생성하고 T_A를 계산한다. 즉, $v_A = g^{u_A} \bmod N$, $T_A = v_A^e \bmod N$이다.

② A는 T_A를 해쉉하고 $k_A = T_A \cdot H(T_A) \bmod e$를 계산한다.

③ A는 T_A에 대한 서명 $t_A = v_A \cdot S_A^{k_A} \bmod N$를 생성한다.

④ A는 ID_A, (T_A, t_A)를 전송하며 ID_B, (T_B, t_B)를 수신한다.

⑤ A는 $k_B = T_B \cdot H(T_B) \bmod e$와 $J_B = Red(ID_B)$를 계산한다.

⑥ A는 $T_B = t_B^e \cdot J_B^{k_B} \bmod N$를 검증하여 T_B의 서명을 확인한다.

⑦ A는 수신한 T_B에 자신의 불규칙 수를 멱승하여 세션 키를 계산한다.

즉, $K_{AB} = T_B^{u_A} \bmod N = g^{u_B \cdot e \cdot u_A} \bmod N$이다.

이 방식에서 서명 쌍 (T, t)의 일부인 T를 키 분배에 직접 사용하는 개념은 ElGamal 형태의 서명 방식을 사용하는 대화형 직접인증 키 분배 시스템과 유사하다. 두 통신자가 메세지에 대한 서명을 하면서 키를 공유할 경우에는 T대신 메세지 M 자체를 인증할 수 있다.

이 키 분배 방식은 불규칙 수 T를 서명 기법을 이용하여 직접 인증한 후 인증된 T에 D-H 키 분배 방식을 적용하였다. 그러므로 이 방식의 안전도는 제안한 서명의 안전도 및 D-H 키 분배 방식의 안전도와 동일하다.

〔일방향 키 분배〕

이 암호시스템을 이용하여 일방향으로 키를 분배하는 방법은 T-O(Tanaka-Okamoto)가 제안한 방식[13]을 사용할 수도 있다. 즉, 사용자는 N보다 작은 개인 비밀 키 h를 추가적으로 선택한 후 공개 키 관련 정보를 계산하여 ID와 함께 공개 화일에 등록한다. 즉, 공개 키 관련 정보는 $P = S \cdot g^h \bmod N$이다. 일방향으로 세션 키를 공유하는 경우, 공개 키는 $P^e \cdot Red(ID) = P^e \cdot J = S^e \cdot g^{h \cdot e} \cdot J = g^{h \cdot e} \bmod N$와 같이 생성한다. 그러므로 D-H 형 키 분배 방식을 적용할 수 있다. T-O 방식에서 사용자는 센타가 제공하는 비밀 키 S와 사용자가 선택하는 비밀 키 h를 모두 관리해야 하며 키 분배 방식에 따라 비밀 키를 다르게 선택해야 하는 것이 단점이다.

이러한 점을 개선하여 센타가 발급하는 하나의 비밀 키를 사용한 일방향 키 분배 방식을 제안한다. 센타는 각 사용자의 공개 키 관련 정보를 서명하여 이를 공개 화일에 등록한다. 즉, 각 사용자의 공개 키 관련 정보는 $P = (g^S \cdot (Red(ID))^{-1})^d = (g^s \cdot J^{-1})^d \bmod N$이다. 일방향으로 키를 분배하는 과정은 다음과 같고 그림 6에 나타내었다.

① A는 $u_A (0 < u_A < e)$를 생성하고 $T_A = S_A \cdot g^{u_A} \bmod N$를 계산하여 ID_A와 함께 B에게 전송한다.

② A는 공개 화일로부터 P_B와 ID_B를 찾아 다음과 같이 세션 키를 생성한다.

$$K_{AB} = (P_B^c \cdot J_B)^{u_A \cdot e} = g^{S_B \cdot e \cdot u_A} \bmod N$$

③ B는 전송된 정보 T_A와 ID_A로부터 다음과 같이 세션 키를 생성한다.

$$K_{BA} = (T_A^e \cdot J_A)^{S_B} = g^{u_A \cdot e \cdot S_B} \bmod N$$

이 키 분배 방식에서 공개정보 P로부터 비밀 키 S를 구하는 것은 이산대수 문제이다. 그리고 전송정보 T로부터 세션 키를 계산하기 위해서는 비밀 키나 비밀 불규칙 수 u를 알아

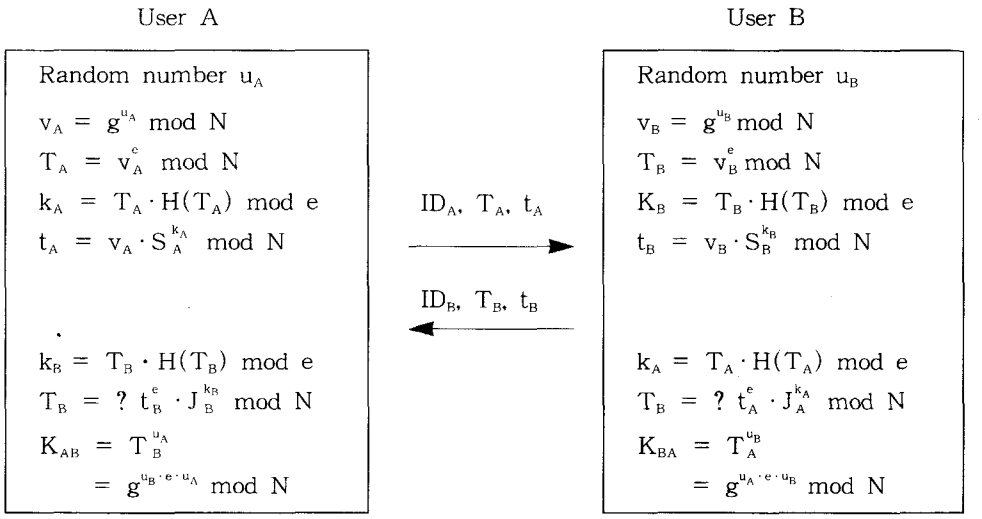


그림 5. 직접 인증 기능을 가진 키 분배

Fig. 5. Key distribution with direct authentication.

야 하며 이 또한 이산대수 문제이다. 불법적인 제 3자가 임의의 u'를 결정하고 A로 위장하는 경우를 고려하자. 제 3자는 B의 공개 정보를 이용하여 $g^{S_B \cdot e \cdot u'} \bmod N$를 계산하지만 B에게는 $T'^{e} \cdot J_A = g^{u' \cdot e} \bmod N$이 되는 T'을 계산하여 전송해야 한다. 이것은 센타의 비밀 키인 d를 알기전에는 계산상 불가능하며 임의의 수에 대한 e승근을 구하는 소인수 분해 문제로 귀결되므로 안전하다.

5. 비교 분석 및 고찰

본 장에서는 H-Y의 통합 암호시스템, Moon/N-R의 서명을 이용한 통합 암호시스템(제안 방식 1) 그리고 RSA 기법을 이용한 통합 암호시스템(제안 방식 2)을 비교한다. 이를 요약한 것이 표 2이다.

첫째, 안전도 측면에서 볼 때 하나의 소수법을 사용할 경우의 이산 대수 문제와 합성수

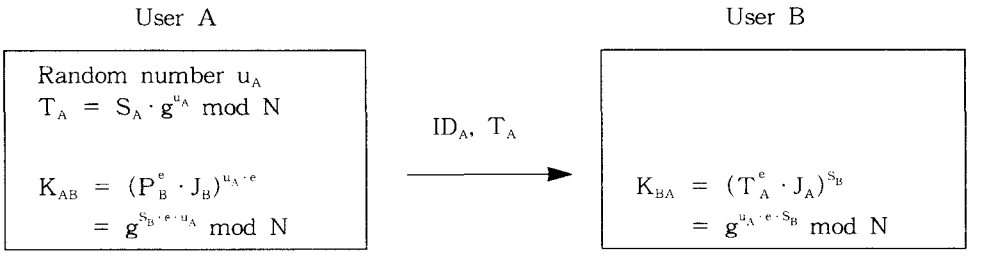


그림 6. 센타의 서명을 이용한 일방향 키 분배

Fig. 6. One-pass key distribution using center's signature

표 2. 디지탈 서명 및 키 분배 통합 암호시스템 비교
(n : p의 비트 수, m : q 및 e의 비트 수, H() 출력 비트)

Table 2. Comparison of cryptosystems integrating digital signature and key distribution.
(n : bit number of p, m : bit number of q or e, output bit number of H())

구 분			H-Y 방식	제안 방식 1	제안 방식 2
시스템 구성 기법			AMV	Moon, N-R	RSA
안전도			이산 대수	이산 대수	이산 대수 소인수 분해
계산량 (곱셈수)	서명	생성	1.5n(1.5n)	1.5m(1.5m)	3m(1.5m)
		확인	1.875n+1.5m	1.875m	1.75m
	키 분배(간접인증)		1.75n(0)	3.375m(1.5m)	4.5m(1.5m)
	키 분배(직접인증)		4.875n+1.5m(1.5n)	4.875m(1.5m)	7.75m(3m)
	키 분배(one-pass)		·	3.375m	3m
전송량 (비트)	서 명		3n	2n+m	2n
	키 분배(간접인증)		n2	n	n
	키 분배(직접인증)		3n2	n+m	2n
	키 분배(one-pass)		·	2n+m	n

N에 대한 소인수 분해의 계산 복잡도는 근사적으로 $\exp[\ln N \ln \ln N^{1/2}]$에 비례한다[14,15]. 제안 방식 1에서는 GF(p)의 부분체 GF(q)를 사용하므로 위수(order) q를 가진다. 실제 구현 시에는 계산 복잡도를 고려하여 p의 크기 n은 512비트 정도가 또한 Pollard 알고리듬[16]에 의한 공격을 고려하여 q의 크기 m은 160비트 정도가 안전도 측면에서 적당하다. 제안 방식 2에서는 합성수 N의 크기는 p의 크기와 동일하게 n비트로 가정하고 공개 정수 e의 크기는 안전도에 따라 가변적이나 q의 길이와 동일하게 m비트로 가정하여 비교하였다. 또한 일방향 함수의 출력 값은 모두 m비트이다.

제안 방식 1에서 센타에서 제공하는 비밀 키 S를 알기 위해서는 센타의 비밀 키 X와 비밀 정수 k를 알아야 한다. 사용자 A와 B가 결탁하여 s_A, s_B, r_A, r_B를 공개하여도 X나 k_A, k_B를 알 수 없다. 이는 디지탈 서명 원형에서 서명 쌍(s, r)만으로 사용자의 비밀 키나 불규칙 정수 k를 알지 못하는 것과 동일하다. 그러므로 이 암호시스템은 이산 대수 문제에 근거하여 안전하다. 인증, 디지탈 서명 및 키 분배방식에서의 안전도는 3장에서 기술한 바와 같이 이산 대수 문제로 귀착된다.

제안 방식 2의 안전도는 RSA 기법을 이용하므로 공개 정보를 이용하여 센타의 비밀 키를 알아내는 것은 소인수 분해의 난도로 볼 수 있다. 인증, 디지탈 서명 그리고 키 분배 시에는 전송 정보나 공개 정보로부터 비밀 정보를 알아내는 것은 이산 대수 문제이거나 혹은 mod N에 대한 e승근을 구하는 문제, 즉, N의 소인수 분해 문제이므로 안전하다.

둘째, 계산량 측면을 고려할 때 덧셈, 뺄셈, 역수 계산 그리고 해쉬 함수의 계산량은 멱승에 비해 적으므로 동일하게 제외하였다. X^a의 계산은 이진 멱승 방법에 의해 1.5n, $X^a \cdot Y^b$ 형태의 계산은 Schnorr의 계산식[12]에 의해 1.75n, $X^a \cdot Y^b \cdot Z^c$의 계산은 1.875n의 곱셈 계산수로 가정한다. 여기에서 n은 지수 a, b와 c의 비트 수이다. 표 2에서 대화형 키 분배 방식의 경우에는 한 명의 통신자가 수행하는 계산량이며 일방향 키 분배 방식의 경우에는 통신자 A는 사전에 계산할 수 있으므로 B의 계산량만 기술하였다. 예로서 n은 512 그리고 m은 160을 사용할 경우를 가정하면 직접 인증 키 분배 시에는 H-Y 방식은 약 2736번의 곱셈이 필요한 반면 제안 방식 1은 약 780번의 곱셈으로 처리가 가능하다. 그리고 제안 방식 2는 약 1240번의 곱셈이 필요하다. 또한 서명 생성이나 대화형 키 분배시 해쉬 함수가 사용되기 전의 계산은 사전에 처리할 수 있으므로 제안 방식의 실시간 계산량은 매우 감소한다. 사전 처리가 가능한 계산량은 표 2에서 괄호 안에 표시하였다. 만약 H-Y 방식을 GF(p)의 부분체 GF(q)를 사용하여 구현할 경우를 가정하면, 계산량은 표 2에서 n을 m으로 대치한 결과가 된다. 이때 제안 방식 1의 간접 인증 키 분배시의 계산량이 H-Y 방식에 비해 증가하는 것은 H-Y 방식에서 매 통신시 동일한 세션 키를 발생하는 점을 개선하여 불규칙 세션 키를 생성하는데 계산이 소요되기 때문이다.

셋째, 전송 정보량 측면에서는 ID정보와 메세지 전송을 제외함을 가정할 때 제안 방식 1은 H-Y 방식과 동일하거나 약간 적다. 제안 방식 1의 간접 인증 키 분배시의 전송량이 증가하는 것은 불규칙 수의 전송이 포함되기 때문이다. 제안 방식 2에서의 전송량은 H-Y 방식과 제안 방식 1에 비해 적다.

넷째, 구현 측면에서 보면 H-Y의 간접 인증 키 분배 시스템에서 동일한 세션 키가 생성되는 것과 비밀 키 s가 p-1과 항상 서로 소라는 제약조건이 단점이 된다. 그러나 제안 방식 1에서는 이 문제는 해결할 수 있다. 제안 방식 2는 G-Q 서명의 메시지 해쉬이 쉽도록 개선하고 키 분배와 통합할 수 있도록 구현하였다.

다섯째, 제안 방식 1에서 일방향으로 키를 공유할 때에서 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 위장할 수 있다. 그러나 제안 방식에서는 불법자가 ID와 r이 있는 공개 키 디렉토리에 접근하여 r을 자신의 것으로 대치하더라도 그에 상응하는 비밀 키를 생성할 수 없으므로 위장 공격이 불가능하다. 제안 방식 2에서는 ID와 공개 키 관련 정보 P를 관리해야 하는 점만 제외하고 제안 방식 1에서와 같이 공개 정보에 대한 센타의 서명을 이용하는 개념은 동일하다.

6. 결 론

본 논문에서는 개인정보에 기초하여 인증, 디지탈 서명 및 키 분배를 통합하는 방안에 대해 연구하였다. 먼저 개인정보에 기초한 통합 암호시스템을 분석하고 공개 키 계산이 효과적인 ElGamal 형태의 서명 방식에 근거하여 개선된 통합 암호방식을 제안하였다. 이 시스템에서의 인증 및 대화형 키 분배 방식을 개선하고 일방향 통신에 적합한 키 분배 방안도 고찰하였다. 그리고 G-Q의 서명 방식을 개선하여 RSA 기법을 이용한 새로운 디지탈 서명과 키 분배 방식들을 제안하였다. 이들을 비교 분석하여 제안 방식이 안전하며 계산량과 구현 측면에서 효율적임을 검증하였다. 개인 정보에 기초한 암호시스템은 센타에서 비밀 키와 관련한 정보를 모두 생성하므로 센타의 의존도가 높다. 그러므로 이 시스템은 사설망이나 금융망 등 일정한 폐쇄 사용자 그룹에 효과적인 암호시스템이다.

참 고 문 헌

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

[2] R. Rivest, A. Shamir, and L. Adleman, "On digital signatures and public key cryptosystems," *Comm. ACM.*, vol.21, pp.120-126, Feb. 1978.

[3] 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.

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

[5] 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.

[6] L. G. Guillou and J .J. Quisquater, "A paradoxical identity-based signature scheme resulting from zero-knowledge," *Crypto'88*, pp. 216-231, 1988.

[7] C. G. G nther, "An identity__based key-exchange protocol," *Eurocrypt'89*, pp.29-37, 1989.

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

[9] 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.

[10] 문상재, "전자서명 생성방법 및 그 확인방법," 특허출원번호 93-19946, 특허청, 1993년 9월

[11] K. Nyberg and R. A. Rueppel, "A new signature scheme based on the DSA giving message recovery," *1st ACM Conference on Computer and Communication Security*, No 3-5, Nov, 1993.

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

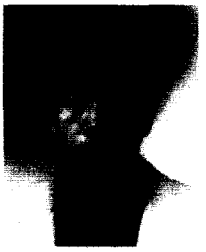
[13] K. Tanaka and E. Okamoto, "Key distribution system using ID-related information directory suitable for mail systems," *SECURICOM'90*, 1990.

[14] D. Coppersmith, A. M. Odlyzko, and R. Schroeppel, "Discrete logarithms in GF(p)," *Algorithmica*, vol. 1, no 1, pp. 1-15, 1986.

[15] R. D. Silverman, "The multiple polynomial quadratic sieve," *Math. Comp.*, vol. 48, pp. 329-339, 1987.

[16] J. Pollard, "Monte Carlo methods for index computation mod p," *Math. Comp.* vol. 24, pp. 918-924, 1978.

□ 著者紹介



하 재 철

1966년 8월 24일생
1985. 3 ~ 1989. 2 경북대학교 전자공학과 (전자공학 학사)
1989. 3 ~ 1991. 6 육군통신장교 근무
1989. 3 ~ 1993. 8 경북대학교 대학원 전자공학과 (석사)
1994. 3 ~ 현재 경북대학교 대학원 박사과정 재학중

※ 주관심분야 : 암호이론, 정보보호, 디지탈통신

문 상 재

통신정보보호학회 논문지 제3권 제2호 참조.