通信情報保護學會誌
第5卷 第3號, 1995. 9

디지탈 서명 방식의 비교

A Comparison of Digital Signature Systems

권 창 영*, 원 동 호**

요 약

최근 국내에서도 디지탈 서명에 대한 공개 제안 및 공청회가 활발히 진행되고 있다. 본 고에서는 암호학의 선진 각국에서 제안되어 다방면으로 광범위하게 그 안전성 및 실용성이 논의된 RSA, ESIGN, Feige-Fiat-Shamir, Micali-Shamir, Guillou-Quisquater, Ohta-Okamoto, DSA, Schnorr, Oka 등의 공개키 암호방식에 근거한 디지탈 서명 방식에 대하여 계산량 및 파라메터의 크기를 비교하고, 각각의 장단점을 분석하였다. 이는 향후 국내 디지탈 서명 방식의 표준 선정 작업시 보다 광범위한 검토가 필요함을 의미한다.

1. 서 론

암호의 기능은 보호(privacy) 기능과 인증(authentication) 기능으로 나눌 수 있다. 보호 기능이란 정보가 노출되어도 키가 없는 한 그 정보의 의미를 알 수 없도록 함으로써 정보를 보호하는 것이다. 한편, 계약이나 송금 등을 행하는 서비스에서 서명은 없어서는 안되는 중요한 요소이며, 전자 우편(electronic mail)이나 전자 송금(electronic funds transfer)과 같은 새로운 형태의 통신 서비스에서 문서의 서명, 날인에 해당하는 정보 및 송, 수신자간의 인증 기능을 갖추는 것은 분쟁을 해결하는 필수불가결한 요소이다[Won94].

* 대유공업전문대학 사무자동화과 전임강사
** 성균관대학교 정보공학과 교수

인증에는 메시지 인증과 사용자 인증이 있는 데 이 두 기능을 합친 것이 디지탈 서명이다. 메시지 인증은 정보가 변경되지 않고 본래의 정보 그대로임을 보증하는 기능이고, 사용자 인증은 정보 시스템에서 정보의 생성, 전송, 처리, 기억, 판단 등의 행위에 관여한 사용자 A가 바로 그 사용자임을 보증하는 기능으로써, 사용자 A가 사용자 B와 협조하여 A는 B에게 A임을 증명할 수 있으나, 제 3의 사용자 X는 A로 위장하여 B에게 A임을 증명할 수 없음을 보증하는 기능이다. 이와 같은 사용자 인증에 당사자인 B 자신도 제 3의 사용자 X에게 A임을 증명할 수 없다는 조건이 추가되었을 때 개인식별이 되며, 사용자 B가 B 자신에게조차도 사용자 A임을 증명할 수 없는 조건이 추가되었을 때 디지탈 서명이라 한다.

현재 여러 종류의 계약 문서, 은행의 예금

청구서, 신용카드의 매출전표 등에서 사용하고 있는 날인(도장)이나 서명을 정보화사회에서 전자적으로 구현할 때 사용하는 것이 디지탈 서명 방식이다.

디지탈 서명의 개념은 Diffie와 Hellman에 의해 처음 논의를 시작하여 다양한 연구 논문과 세미나 등에서 논의되어 왔다[DH76]. 일반적으로 디지탈 서명은 비트 스트링으로 표현되는 디지탈 신호이며, 특정 메시지가 송신되었음과 서명자가 이의 발신 측이라는 것을 증거로서 수신자가 간직할 수 있는 어떤 데이터를 포함하여야 한다.

즉, 수신자 또는 제 3자에 의한 서명의 위조와 송신자에 의한 메시지의 전송행위의 부인과 같은 두 가지 형태의 부정 행위를 방지하여야 한다. 또한, 사후에 서명의 정당성을 판정하여 그 분쟁을 조정할 수 있는 심판관에게 제시할 수 있는 증거로서 보관하여야 한다.

본고에서는 디지탈 서명 모델 및 디지탈 서명 방식의 일반적인 요구조건을 제시하고 기존의 디지탈 서명 방식 중 다방면으로 그 안전성 및 실용성이 논의된 RSA, ESIGN, Feige-Fiat-Shamir(이하 FSS), Micali-Shamir(이하 MS), Guillou-Quisquater(이하 GQ), Ohta-Okamoto(이하 OO), DSA, Schnorr, Oka 등의 공개키 암호방식에 근거한 디지탈 서명 방식에 대하여 비교 분석하였다.

2. 디지탈 서명 모델 및 디지탈 서명 방식의 요구 조건

디지탈 서명 모델은 대칭형 암호방식과 중재자를 사용한 모델, 공개키 암호방식을 이용한 모델 및 공개키 암호방식과 일방향 해쉬함수를 사용한 모델이 있다.

기존의 디지탈 서명 방식 중 대칭형 암호알고리즘과 중재자를 사용한 모델의 서명 방식은 다음과 같다. 서명자는 서명하려는 메시지 m을 자신의 비밀키로 암호화시켜 서명문 c를 중재자에게 전송한다. 중재자는 자신이 보유한 서명자의 비밀키를 이용하여 서명문 c를 복호화하여 메시지 m을 얻는다. 중재자는 검증자의 비밀키를 사용하여 메시지 m을 암호화시켜 서명문 c'를 검증자에게 전송한다. 검증자는 자신의 비밀키를 이용하여 서명문 c'를 복호화하여 메시지 m을 얻는다.

공개키 암호방식을 이용한 모델의 서명 방식은 다음과 같다. 서명자는 메시지 m을 자신의 비밀키를 사용 서명문 s를 생성하여 검증자에게 전송한다. 검증자는 공개키 디렉토리에 등록된 서명자의 공개키를 사용하여 서명문 s를 검증한다.

공개키 암호방식과 일방향 해쉬함수를 사용한 모델의 서명 방식은 공개키를 이용한 방식과 동일하나 서명 알고리즘의 효율성을 증가시키기 위하여 메시지 m의 서명문을 생성하는 대신에 일방향 해쉬함수(one-way hash

표1 암호기법의 분류

암 호 기 법				
정보보호 (Privacy)	인 증 (Authentication)			
. . .	메시지(Message) 인증	사용자(Entity) 인증	개별식별 (Identification)	디지탈 서명 (Digital Signature)

function) H를 이용하여 H(m)의 서명문 s를 생성한다. 그러므로 현실적으로 공개키 암호방식만을 이용하지 않고 해쉬함수를 같이 사용하는 것이 통례이다[WKYL93].

일반적으로 디지탈 서명 방식이 유용하고 안전하려면 아래의 5가지 조건을 만족하여야 한다.

요구조건 1) 위조 불가(unforgeable) 조건으로 합법적인 서명자만이 디지탈 서명을 생성할 수 있어야 한다.

요구조건 2) 서명자 인증(authentic) 조건으로 디지탈 서명의 서명자를 누구든지 검증할 수 있어야 한다.

요구조건 3) 부인 불가(repudiated) 조건으로 서명자는 후에 서명한 사실을 부인할 수 없어야 한다.

요구조건 4) 변경 불가(unalterable) 조건으로 서명한 문서(메시지)의 내용을 변경할 수 없어야 한다.

요구조건 5) 재사용 불가(not reusable) 조건으로 문서(메시지)의 서명은 다른 문서(메시지)의 서명으로 사용할 수 없어야 한다.

3. 공개키 암호방식을 이용한 디지탈 서명 방식

Diffie와 Hellman의 공개키 암호방식에 대한 논문에서 디지탈 서명에 대해 논의한 이래로 공개키 암호방식에 근거한 많은 디지탈 서명 방식이 제안되었다.

가장 널리 알려진 RSA 방식은 1978년 Rivest 등에 의하여 제안되었다[RSA78]. ESIGN은 1985년 Okamoto 등에 의해 처음 제안되어[OkSh85] 최종 버젼은 [Oka90]에서 제안되었다. Fiat-Shamir 방식[FS86]의 변형인 FFS 방식은 1987년에 제안되었으며, MS 방식은 1988에 제안되었다. 또한, Fiat-Shamir 방식의 변형인 GQ 방식[GQ88], OO 방식[OhOk88]은 1988년에 각기 독립적으로 제안되었다. ElGamal 방식[ElGa85]에 근거한 DSA 방식은 1991년 NIST에 의해 DSS(Digital Signature Standard)의 후보로 제안되었다[NIST91]. Schnorr 방식은 1989년에 제안되었으며[Sch89], Oka 방식은 1992년에 제안되었다[Oka92].

RSA, ESIGN, FFS, MS, GQ, OO 방식의 안전성은 소인수분해 문제에 근거하며 DSA, Schnorr, Oka 방식의 안전성은 이산대수 문제에 근거한다.

본고에서는 각각의 디지탈 서명 방식을 필요한 모듈러 승산 및 역원 계산량을 근거로 계산 시간을 비교하였으며, 키와 서명의 크기를 비교하고 각각의 장단점을 분석하였다.

본고에서 사용한 기호의 의미는 다음과 같다.

- Z_n : 0에서 n-1 사이 숫자의 집합
- Z_n^* : n과 서로소인 0에서 n-1 사이 숫자의 집합
- [M] : M 보다 크거나 같은 정수
- [M] : M 보다 작거나 같은 정수
- |X|: X의 비트 길이(즉, $\lfloor \log_2 X \rfloor + 1$)
- jM(|n|) : j번의 |n|비트 크기의 모듈러 승산 계산
- jI(|n|) : j번의 |n|비트 크기의 모듈러 역원 계산

3.1 RSA 방식

1) 파라메터

· 비밀키 : (p, q, d) p, q는 큰 소수, $d \in Z_{lcm(p-1, q-1)}$

· 공개키 : (n, e) $n = pq$, $ed = 1 (\mathrm{mod}\ lcm(p-1, q-1))$인 e

· 일방향 해쉬함수 : $H : Z \rightarrow Z_n$

2) 서명 생성

메시지 m에 대한 서명 s는 서명자에 의하여 다음과 같이 생성된다.

$$s = H(m)^d \pmod n$$

3) 서명 검증

서명된 메시지 (s, m)에 대한 검증은 다음의 등식이 성립되는지 검사한다.

$$H(m) = s^e \pmod n$$

3.2 ESIGN 방식

1) 파라메터

· 비밀키 : (p, q)

p, q는 큰 소수 (p > q)

· 공개키 : (n, k) $n = p^2q$, $k(k \geq 4)$

· 일방향 해쉬함수 : $H : Z \rightarrow Z_n$

2) 서명 생성

메시지 m에 대한 서명 s는 서명자에 의하여 다음과 같이 생성된다.

① 난수 $x(0 \leq x \leq pq-1)$를 선택한다.

② $w = [(H(m) - x^k \bmod n)/(pq)]$

③ $y = w/(kx^{k-1}) \bmod p$

④ $s = x + ypq$

3) 서명 검증

서명된 메시지 (s, m)에 대한 검증은 다음의 부등식이 만족되는지 검사한다.

$$H(m) \leq s^k \pmod n \leq H(m) + 2^{[2|n|/3)}$$

3.3 FFS 방식

1) 파라메터

· 비밀키 : (p, q, s_i)

p, q는 큰 소수,

$s_i \in Z_n (i = 1, \ldots, k)$

· 공개키 : (n, v_i) $n = pq$,

$v_i = 1/s_i^2 \pmod n$

$(i = 1, \ldots, k)$

· 일방향 해쉬함수 : $H : Z_n \times Z \rightarrow \{0, \ldots, 2^k-1\}$

(즉, $k = 128$)

2) 서명 생성

메시지 m에 대한 서명 (e, y)는 서명자에 의하여 다음과 같이 생성된다.

① 난수 $r \in Z_n$를 선택한다.

② $e = (e_1, \ldots, e_k)$

$= (H(r^2 \bmod n), m)$

③ $y = r \prod_{j=1}^{k} s_j^{e_j} \bmod n$

3) 서명 검증

서명된 메시지 (e, y, m)에 대한 검증은 다음의 등식이 만족되는지 검사한다.

$$e = H(y^2 \prod_{j=1}^{k} v_j^{e_j} \bmod n, m)$$

3.4. MS 방식

1) 파라메터

· 비밀키 : (p, q, s_i) p, q는 큰 소수,

$v_i = 1/s_i^2 \pmod n$인

$s_j \in Z_n$ $(i = 1, \ldots, k)$

· 공개키 : (n, v_i) $n = pq$,

v_i $(i = 1, \ldots, k)$는

Z_n 상에서 평방잉여인 처음 k개 소수들

(즉, $v_1 = 2$, $v_2 = 3$, $v_3 = 5$, . .)

· 일방향 해쉬함수 : $H : Z_n \times Z \rightarrow \{0, \ldots, 2^k-1\}$

(즉, $k = 128$)

2) 서명 생성

메시지 m에 대한 서명 (e, y)의 생성은 FFS와 동일하다.

3) 서명 검증
서명된 메시지 (e, y, m)에 대한 검증은 FFS와 동일하다.

3.5 GQ/OO 방식

1) 파라메터
· 비밀키 : (p, q, s) p, q는 큰 소수, $s \in Z_n$
· 공개키 : (n, L, v) $n = pq$, 양수 L(즉, $|L| = 128$), $v_1 = 1/s^L \pmod n$
· 일방향 해쉬함수 : $H : Z_n \times Z \rightarrow Z_L$

2) 서명 생성
메시지 m에 대한 서명 (e, y)는 서명자에 의하여 다음과 같이 생성된다.
① 난수 $r \in Z_n$를 선택한다.
② $e = H(r^L \bmod n, m)$
③ $y = rs^e \pmod n$

3) 서명 검증
서명된 메시지 (e, y, m)에 대한 검증은 다음의 등식이 만족되는지 검사한다.

$$e = H(y^L v^e \bmod n, m)$$

3.6 DSA 방식

1) 파라메터
· 시스템 파라메터 : (p, q, g)
$q|(p-1)$, $2^{511} < p < 2^{512}$, $2^{159} < q < 2^{160}$인 소수 p, q 위수가 q인 $g \in Z_p$
(즉, $g \neq 1$, $g^q = 1 \pmod n$)
· 비밀키 : (s) $s \in Z_q$
· 공개키 : (v) $v = g^s \pmod p$
· 일방향 해쉬함수 : $H : Z_p \times Z \rightarrow \{0, \ldots, 2^t-1\}$ (즉, $t = 128$)

2) 서명 생성
메시지 m에 대한 서명 (e, y)는 서명자에 의하여 다음과 같이 생성된다.
① 난수 $r \in Z_q$를 선택한다.
② $e = (g^r \pmod p) \pmod q$
③ $y = ((H(m) + se)/r) \pmod q$

3) 서명 검증
서명된 메시지 (e, y, m)에 대한 검증은 다음의 등식이 만족되는지 검사한다.

$$e = (g^{H(m)/y} v^{e/y} \pmod p) \pmod q$$

3.7 Schnorr 방식

1) 파라메터
· 시스템 파라메터 : (p, q, g)
$q|(p-1)$, $p \geq 2^{512}$, $q \geq 2^{140}$ 인 소수 p, q 위수가 q인 $g \in Z_p$
· 비밀키 : (s) $s \in Z_q$
· 공개키 : (v) $v = 1/g^s \pmod p$
· 일방향 해쉬함수 : $H : Z_p \times Z \rightarrow \{0, \ldots, 2^t-1\}$ (즉, $t = 128$)

2) 서명 생성
메시지 m에 대한 서명 (e, y)는 서명자에 의하여 다음과 같이 생성된다.
① 난수 $r \in Z_q$를 선택한다.
② $e = H(g^r \pmod p, m)$
③ $y = r + se \pmod q$

3) 서명 검증
서명된 메시지 (e, y, m)에 대한 검증은 다음의 등식이 만족되는지 검사한다.

$$e = H(g^y v^e \pmod p, m)$$

3.8 Oka 방식

1) 파라메터

· 시스템 파라메터 : (p, q, g_1, g_2)
$q|(p-1)$, $p \geq 2^{512}$, $q \geq 2^{140}$인
소수 p, q 위수가 q인 g_1, g_2

· 비밀키 : (s_1, s_2) $s_1, s_2 \in Z_q$

· 공개키 : (v) $v = g_1^{-s_1} g_2^{-s_2} \pmod p$

· 일방향 해쉬함수 : $H : Z_p \times Z \rightarrow$
$\{0, \ldots, 2^t-1\}$ (즉, $t = 128$)

2) 서명 생성

메시지 m에 대한 서명 (e, y_1, y_2)는 서명자에 의하여 다음과 같이 생성된다.

① 난수 $r_1, r_2 \in Z_q$를 선택한다.

② $e = H(g_1^{r_1} g_2^{r_2} \pmod p, m)$

③ $y_1 = r_1 + es_1 \pmod q$,
$y_2 = r_2 + es_2 \pmod q$

3) 서명 검증

서명된 메시지 (e, y_1, y_2, m)에 대한 검증은 다음의 등식이 만족되는지 검사한다.

$$e = H(g_1^{y_1} g_2^{y_2} v^e \pmod p, m)$$

4. 디지탈 서명 방식의 비교 분석

본고에서는 RSA의 n 값을 512 비트로 가정하며 ESIGN에서의 n 값을 576 비트로 가정한다. FFS, MS, GQ, OO에서의 n 값은 512 비트로 가정한다. DSA에서의 p는 512 비트, q는 160 비트로 가정하고, Schnorr 및 Oka에서의 p는 512 비트, q는 140 비트로 가정한다. 추가적으로 RSA에서의 e = 3으로 ESIGN에서의 k = 8로 가정한다.

여기서 유독 ESIGN에서의 n 값만을 576 비트로 가정한 이유는 576 비트인 $n = p^2q$을 소인수분해하는 것이 512비트 $n = pq$를 소인수분해하는 것에 필적하기 때문이다.

FFS, MS, GQ, OO, Schnorr, Oka의 시큐리티 파라메터는 128로 가정한다. 즉, FFS, MS에서는 k = 128, t = 1로 가정하고, GQ, OO에서는 |L| = 128로 가정한다. 또한, Schnorr, Oka에서는 t=128로 가정한다.

4.1 계산량 비교

각 디지탈 서명 방식의 서명 생성 및 검증시 필요한 계산량의 비교는 표 2.와 같다.

각 디지탈 서명 방식에서 서명 생성시 사전계산을 하는 경우 필요한 계산량의 비교는 표 3.과 같다.

표 2 디지탈 서명 방식의 계산량 비교

방 식	서명 생성시 계산량	서명 검증시 계산량
RSA	750M(512)	2M(512)
ESIGN	3M(576) + I(192) 〈 5M(512)	3M(576) 〈 4M(512)
FFS	66M(512)	66M(512)
MS	66M(512)	2M(512)
GQ/OO	385M(512)	224M(512)
DSA	240M(512) + I(160) 〈 241M(512)	280M(512) + I(160) 〈 281M(512)
Schnorr	210M(512)	242M(512)
Oka	245M(512)	261M(512)

표 3 디지탈 서명 방식의 서명 생성시 계산량 비교(사전계산)

방 식	사전 계산량	서명 생성시 계산량
RSA	-	750M(512)
ESIGN	5M(512)	거의 0
FFS	-	66M(512)
MS	-	66M(512)
GQ/OO	192M(512)	193M(512)
DSA	241M(512)	거의 0
Schnorr	210M(512)	거의 0
Oka	245M(512)	거의 0

4.2 파라메터 크기의 비교

각 디지탈 서명 방식의 공개키, 비밀키 및 서명의 크기를 비교하면 표 4.와 같다.

표 4 파라메터의 크기 비교

방 식	공개키의 크기 (비트)	비밀키의 크기 (비트)	서명의 크기 (비트)
RSA	514 (512 + 2)	512	512
ESIGN	578 (576 + 2)	384 (192 + 192)	576
FFS	66048 (512 + 512 * 128)	65536 (512 * 128)	640 (128 + 512)
MS	약 2500 (512 + 약2000)	65536 (512 * 128)	640 (128 + 512)
GQ/OO	1152 (512 + 512)	1152	640 (128 + 512)
DSA	1696 (152 + 160 + 512 + 512)	160	320 (160 + 160)
Schnorr	1676 (512 + 140 + 512 + 512)	140	268 (128 + 140)
Oka	2188 (512 + 140 + 512 + 512 + 512)	280 (140 + 140)	408 (128 + 140 + 140)

각 디지탈 서명 방식의 공개키 중 RSA의 e, ESIGN의 k, MS의 $(v_1, \ldots, v_k)$, DSA와 Schnorr의 (p, q, g), Oka의 (p, q, g_1, g_2)는 모든 사용자가 공유하거나, 시스템 파라메터일 수 있다.

4.3 종합 검토

본고에서 다룬 디지탈 서명 방식의 안전성을 제공하는 암호학적 문제 및 각각의 장단점을 종합적으로 비교 검토하면 다음의 표 5.와 같다.

표 5 디지탈 서명 방식의 비교

	안전성 근거	단 점	장 점	비 고
RSA	소인수분해 문제 (승산역원)	· 승산횟수가 많음 · 사전계산 불가능	· 충분한 안전성 검토 · 가장 널리 사용됨	
ESIGN	소인수분해 문제	· 안전성 검토기간이 짧다.	· 사전계산 가능 · 서명 생성시간이 빠르다.	· 일본에서 표준화 추진중
FS 및 변형	소인수분해 문제 (제곱근)	· 고신뢰센터 필요 · 키의 크기가 길다 · 통신량이 많다	· 사전계산 기능 · ID-based(공개키 디렉토리 불필요)	
GQ/QO	소인수분해 문제 (L 승근)	· 고신뢰센터 필요	· ID-based(공개키 디렉토리 불필요)	· FS의 확장키의 크기는 줄었으나, 계산량이 증가
ElGamal	이산대수 문제	· 서명의 길이가 길다 · 랜덤변수의 비밀성 요구	· 사전계산 가능	
DSA	이산대수 문제	· 검증시 계산량 많음 · 랜덤변수의 비밀성 요구	· 사전계산 가능	· 미국에서 표준 제안(NIST)
Schnorr	이산대수 문제	· 검증시 계산량 많음 · 랜덤변수의 비밀성 요구	· 사전계산 가능 · 서명의 길이가 짧다	
Oka	이산대수 문제	· 검증시 계산량 많음	· 사전계산 가능	· 안전성 증명 가능

5. 결 론

안전성은 암호화 알고리즘에서 고려하여야 할 가장 중요한 요소 중의 하나이다. 현재까지 FFS, OO, Oka 방식은 해쉬함수가 이상적으로 랜덤하다는 가정하에서 그 안전성을 증명할 수 있다. RSA, ESIGN, MS, GQ, DSA, Schnorr 방식은 안전성을 명쾌하게 증명할 수 없지만, 그 안전성을 다방면으로 검토했기 때문에 대부분의 암호학자들은 안전하다고 믿고 있다. 이 방식들의 안전성은 최초 제안한 이래로 안전성에 대해 문제점이 지적되지 않고 지나간 기간에 비례한다고 할 수 있다. 가장 오래된 RSA는 14년이 되었으며, DSA(ElGamal)은 10년, ESIGN은 7년, MS와 GQ는 4년, Schnorr는 3년이 지났다. 이미 안전성에 문제가 있다고 공격당한 거의 모든 방식들은 최초 제안후 몇 년만에 공격을 당했다.

그러므로 최근 진행되고 있는 한국형 디지탈 서명 방식의 공개 제안 및 선정 문제는 좀 더 시간을 가지고, 보다 광범위하고 활발히 진행되는 것이 바람직할 것이다.

1985년 Goldwasser 등이 영지식 대화형 증명의 개념[GMR85, GMW86]을 제안한 이래로 각종 인증 방식 및 그 응용에 활발히 연구가 진행되고 있다[KLW93]. 특히, 스마트 카드를 이용하는

개인식별 방식 및 디지탈 서명 방식에 대하여 많은 연구가 되어왔다. 디지탈 서명 방식은 신용 카드, 신분증명 카드, 전자 현금 등의 스마트 카드를 활용하는 응용 분야에서 매우 중요한 역할을 담당하게 될 것이다. 그러므로, 국내 디지탈 서명 표준안으로 선정되어 가장 일반적으로 널리 사용될 디지탈 서명 방식은 아마도 스마트 카드에서도 구현시 효과적이어야 할 것이다. 만약 이 문제가 간과되어 스마트 카드에서 구현시 비효과적인 디지탈 서명 방식이 국내 표준으로 선정된다면, 이 국내 표준은 중요한 역할은 담당하지 못할 것이다.

또한, 앞에서 언급한 디지탈 서명 프로토콜의 요구조건은 전형적인 디지탈 서명 프로토콜에서의 가장 기본적인 요구조건이다. 사실상 디지탈 서명이 많은 응용 업무에서 활용될 것은 자명한 사실이므로 적용 환경 및 적용 업무에 따라서 여러 가지 추가적인 요구조건이 등장할 것이다. 이러한 추가적인 요구조건을 만족하는 특수한 디지탈 서명 프로토콜에 대한 연구는 매우 가치있는 연구 분야이다. 특히, Blind signature, Undeniable signature, Group signature, Fail-stop signature, Multiple signature, Nominative signature, Entrusted undeniable signature 등의 특수한 디지탈 서명에 대한 연구가 보다 활발히 진행되어야 할 것으로 사료된다.

참 고 문 헌

[DH76] W.Diffie, M.E.Hellman, "New Directions in Cryptography," IEEE Trans. on Inform. Theory, vol.IT-22, pp.644-654, 1976.

[ElGa85] T.ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Trans. on Inform. Theory, vol.IT-31, pp. 469-472, 1985.

[FFS88] U.Feige. A.Fiat, A.Shamir, "Zero knowledge Proofs of identity," The 19th ACM STOC, pp.210-217, 1988.

[FS86] U. Fiat, A. Shamir, "How to Prove Yourself : Practical Solutions to Identification and Signature Problems," Crypto'86, pp. 186-194, 1986.

[GMR85] S.Goldwasser, S.Micali, C.Rackoff, "The Knowledge Complexity of Interactive Proof Systems," The 17th ACM STOC, pp.291-304, 1985.

[GMW86] O.Goldreich, S.Micali, A.Wigderson, "Proofs that Yield Nothing But their Validity," Proceedings of Crypto'86, pp.171-185, 1986. "Proofs that Yield Nothing But Their Validity or All Languages in NP Have Zero Knowledge Proofs," Tech. Rep.#544, Israel Institute of Technology, Department of Computer Science, 1989.

[GQ88] 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.

[KLW93] 권 창영, 이 인숙, 원 동호, "영지식 대화형 증명 방식 및 응용 프

로토콜," 대한전자공학회 학회지 (정보기술 특집), 제 20권, 제 2호, pp.101-114, 1993. 2.

[MS88] S.Micali, A.Shamir, "An Improvement of the Fiat-Shamir Identification and Signature Scheme," Crypto'88, pp.244-247, 1988.

[NIST91] "Specification for a Digital Signature Standard," National Institute for standards and Technology, Federal Information Standard Publication XX, draft, 1991.

[OhOk88] K.Ohta, T.Okamoto, "A Modification of the Fiat-Shamir Scheme," Crypto'88, pp.233-243, 1988.

[Oka90] T.Okamoto, "A Fast Signature Scheme Based on Congruential Polynomial Operations," IEEE Trans. on Inform. Theory, vol.IT-36, No.1, pp.47-53, 1990.

[Oka92] T.Okamoto, "Provably Secure and Practical Identitification Schemes and Corresponding Signature Sch-emes," Crypto'92, pp.31-53, 1992.

[OkSh85] T.Okamoto, A.Shiraishi, "A Digital Signature Schemes Based On Quadratic Inequalities," Proceeding of Symposium on Security and Privacy, IEEE, pp.123-132, 1985.

[RSA78] R.Rivest, A.Shamir, and L.Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Comm. ACM, Vol.21, No.2, pp.120-126, 1978.

[Sch88] C.P.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.

[Won94] 원 동호, "디지탈서명의 정의와 개념," 디지탈서명 표준화 워크샵 자료집, pp.11-29, 1994. 4.

[WKYL93] 원 동호, 권 창영, 양 형규, 이 경호외, "공중통신망에 적합한 한국형 디지탈 서명 메카니즘의 실용화 기술개발 및 표준화에 관한 연구," 한국통신 연구개발단 '93 장기기초연구과제, 최종보고서, 1993.12.

□ 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)
1994년 8월 성균관 대학교 대학원 정보공학과 졸업 (공학박사)
1982년 12월 - 1988년 9월 (주)KOLON 정보 SYSTEM실 팀장
1992년 3월 - 현재 대유공업전문대학 사무자동화과 전임강사
※ 주관심분야 : 암호학, 정보관리

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