ID를 이용한 디지탈 서명 방식에 관한 연구

○이 임 영*, 강 창 구**, 김 대 호**

* : 순천향대학교 컴퓨터학부

** : 한국전자통신연구소

A Study on ID-based Digital Signature Scheme

Im-yeong Lee*, Chang-goo Kang**, Dae-ho Kim**

* : Soonchunhyang University, Dept. of Computer Science and Engineering

** : Electronics and Telecommunications Research Institute

요 약 문

본 고에서는 기존의 Shamir의 ID를 이용한 디지탈 서명 방식에 대하여 분석하여, 이 방식이 서명자가 서명 생성시 동일한 랜덤수를 두번 이상 사용할 경우 서명자의 비밀 정보가 노출될 수 있음을 보인다. 또한 이러한 문제점을 해결할 수 있는 새로운 ID를 이용한 디지탈 서명 방식을 제안하고, 제안된 방식의 안전성과 효율성을 분석하고자 한다.

I. 서론

향후 정보화 사회에 있어서는 종래의 종이 서류에 의한 문서 수발 업무 등이 컴퓨터 통신망을 통해 신속하고 경제적으로 이루어지고, 정보 전송시 상대방의 신분을 확인하거나 사용자의 정당성을 인증하고 송수신자간에 일어날 수 있는 제반 분쟁을 해결할 수 있도록 통상적인 인감 도장과 같은 역할을 해줄 수 있는 제도나 절차가 필연적으로 요구된다.

이러한 디지탈 메시지를 전송할 때 필요한 서명방식으로 디지탈 서명(Digital Signature) 기법이 있으며, 공개키 암호 시스템을 이용한 많은 디지탈 서명 방식이 제안되었다[1-4,9]. 그러나 공개키 암호 시스템이 키 관리가 편리하고 보다 많은 정보 서비스 기술을 제공할 수 있다고 하여도 상대를 인증 하기 위해서는 공개키를 인증 해야 하는 문제가 발생한다. 공개키 암호 시스템에서 공개키는 공통키 암호 시스템에서 사용되는 키와 달리 제3자에게 노출된다고 하여도 암호 시스템의 안전성에 영향을 주지 않으나, 공개키 내용이 불법적으로 변경되어서는 안되므로 인증된 공개키를 공개 기록집(public directory)으로 만들어서 항시 보유하여야 한다[10,13].

1984년 Shamir는 주소, 이름 등 각 개인이 식별할 수 있는 ID(identification)을 이용한 암호 시스템을 제안하였다. 이러한 ID를 이용한 암호 시스템은 송수신자간에 공개키나 비밀키를 교환할 필요가 전혀 없고, 또 키의 리스트나 제 3자에 의한 서비스도 필요로 하지 않는 방법으로, 임의의 사용자간에 안전하게 통신이 가능하고 또한 서로 서명을 인증할 수 있는 새로운 암호 시스템이다. 이 방법은 신뢰할 수 있는 키 생성 센터를 가정하고 있다. 키 생성 센터를 설치하는 유일한

목적은 신규로 사용자가 정보 네트워크에 가입할 때 그 사용자의 이름이나 주소, 전화번호 등의 고유 정보(ID)를 받아 센터 고유의 비밀 알고리즘을 이용하여, 그 ID에 대응하는 비밀키를 생성하고 개인별로 사용하는 스마트 카드에 기록하여 발행하는 일을 한다. 이 카드 안에 들어있는 비밀 정보에 의해 통신 상대가 변하더라도 사용자는 독자적으로 자기가 보내는 메시지를 암호화하던지 서명을 할 수가 있으며, 자기가 받은 암호문의 복호나 서명의 인증을 할 수 있다.

ID를 이용한 암호 시스템은 새로운 사용자가 네트워크에 가입할 경우에도 이미 발행된 카드의 비밀 정보를 갱신할 필요가 없고, 센터는 사용자의 활동을 통제할 필요도 없으며 사용자의 리스트도 보관하지 않는다. 카드의 발행을 모두 종료한 후에는 센터를 폐쇄할 수가 있고, 폐쇄 후에도 네트워크는 완전히 분산된 형태로 활동을 할 수 있다[5],[6].

본고에서는 ID를 이용한 디지탈 서명 방식에 대하여 논하기로 한다. ID를 이용한 디지탈 서명 방식으로 Shamir방식[10], Ohta방식[8], ISO(안)[7] 등이 알려져 있으나, 모든 방식이 사용자의 랜덤수를 두 번 이상 사용하면 각 사용자의 비밀 정보가 노출되는 문제점을 지적하고자 한다. 그러한 경우 사용자는 센터로부터 새로운 비밀 정보를 받아야 하는 불편함이 있다. 본고에서는 사용자가 랜덤수를 두 번 이상 사용하더라도 비밀 정보가 노출되지 않는 새로운 ID를 이용한 디지탈 서명 방식을 제안하고, 제안된 방식의 안전성과 효율성을 분석하고자 한다.

II. Shamir ID를 이용한 디지탈 서명 방식

Shamir는 1984년 ID를 이용한 암호에 대한 기본 개념을 처음 제안하면서 그 실현 방법으로 다음과 같은 ID를 이용한 서명 방식을 소개하였다[10].

먼저 신뢰할 수 있는 센터(Trusted Center; 이후 TC라 함)는 다음과 같이 키를 생성한다.

(1) p, q는 랜덤하게 선택한 큰 소수이고, $N=p\cdot q$이다.

(2) f는 일 방향 함수이다.

(3) N의 오일러 함수값 $\phi(N)=(p-1)(q-1)$이고, $\gcd(L, \phi(N))=1$인 L를 계산한다.

(4) 각 사용자 A의 개인 식별 정보를 ID_A라 할 때

$$ID_A = S_A^L \mod N$$

을 계산한다.

(5) N, f, L, ID_A는 모든 사용자에게 공개하고, S_A는 사용자 A만 보유하고, p, q는 TC만 보유한다.

서명자(A)는 다음과 같은 서명문을 작성한다.

(1) A는 랜덤한 수 R를 선택하여

$$X = R^L \mod N$$

을 계산한다.

(2) 메세지 M과 X에 대하여 일 방향 함수를 취한 값을 다음과 같이한다.

$$E=f(M,X)$$

(3) A는 자신의 비밀 정보 S_A과 랜덤수 R 및 해쉬값 E를 이용하여 다음과 같이 서명문을 작성한다.

$$Y = S_A R^E \mod N$$

(4) 서명자 A는 자신의 개인 식별 정보 ID_A와 메세지 M 및 서명문(Y,X)를 B에게 보낸다.

확인자(B)는 ID_A, M, (Y,X)가 다음과 같은 조건을 만족하는지 확인한다.

$$Y^L = ID_A \cdot X^E \mod N$$

즉 위식의 우변은 $ID_A \cdot X^E = S_A^L \cdot R^{L \cdot E} = (S_A \cdot R^E)^L \mod N$ 임으로 좌변의 Y^L과 일치한다.

이러한 Shamir 방식 이외에도 유사한 방식으로 Ohta 방식, ISO에서 표준화(안) 등이 제안되고 있으며, 표 1은 이러한 방식들을 요약한 것이다.

표 1. ID를 이용한 디지탈 서명 방식 비교

	TC의 키 생성	서명자의 비밀 정보	서명문 생성	서명문 확인
공 통	n(=p q) f : 일방향함수 L : 소수	S	. R 생성 . $X=R^L$ 계산 . E=f(M,X) 계산	공개 정보 : N, f, L, ID_A Y, X
Shamir 방식	. $ID=S^L$		. $Y=S\ R^E$	. $Y^L=ID\ X^E$
Ohta 방식	. $ID=S^L$		. $Y=R\ S^E$	. $Y^L=X\ ID^E$
ISO 안	. $ID^{-1}=S^L$		. $Y=R\ S^E$	. $Y^L=X\ ID^{-E}$

III. 기존의 ID를 이용한 디지탈 서명 방식에 대한 분석

본 절에서는 기존의 ID를 이용한 디지탈 서명 방식에 대한 문제점에 대하여 언급하고자 한다. Shamir방식에서 동일한 랜덤수 R을 두번 사용할 경우 안전성의 위험에 대하여 살펴보기로 한다. 서명자가 동일한 랜덤수 R를 사용함으로서 동일한 X를 얻게 될 것이다. 그러므로 메세지 M_1에 대하여 $E_1 = f(M_1, X)$을 얻어 서명 확인자는 $Y_1^L = ID \cdot X^{E_1}$로 확인하며, 메세지 M_2에 대하여 $E_2 = f(M_2, X)$을 얻어 서명 확인자는 $Y_2^L = ID \cdot X^{E_2}$로 확인한다.

이러한 경우 2개의 서명 확인식으로 부터 다음의 식을 얻을 수 있다.

$$ID = Y_1^L \cdot X^{-E_1} = Y_2^L \cdot X^{-E_2}$$

$$X^{(E_1 - E_2)} = (Y_2 / Y_1)^{-L}$$

위식의 양변에 다음의 t를 구하여 곱하면 다음과 같다.

$$X^{(E_1-E_2)\cdot t}=(Y_2/Y_1)^{-L\cdot t} \qquad 단,\ t=(E_1-E_2)^{-1} \mod L$$

또한 위의 t의 조건으로부터 위식의 좌변의 지수승 부분은 $(E_1-E_2)\cdot t=l\cdot L+1$과 같이 쓸 수 있으므로 위식은 다음과 같다.

$$X^{l\cdot L+1}=(Y_2/Y_1)^{-L\cdot t}$$

$$X=(Y_2/Y_1)^{-L\cdot t}\cdot(X)^{-l\cdot L}$$

$$R^L=(Y_2/Y_1)^{-L\cdot t}\cdot(X)^{-l\cdot L}$$

$$R=(Y_2/Y_1)^{-t}\cdot(X)^{-l}$$

그러므로 2개의 서명 확인식으로 부터 서명자의 랜덤수 R을 알 수 있다. 따라서 이러한 R로부터 서명문 생성식($Y=S\cdot R^E$)을 이용하여 사용자의 비밀 정보 S를 쉽게 알 수 있다.

또한 Ohta방식 및 ISO(안)에서도 위와 같은 방법을 사용함으로서 표2와 같이 사용자의 비밀 정보를 알 수 있다.

표2. 각 방식의 노출 정보

	도출식	결과식	노출 정보
Shamir 방식	$(\frac{Y_2}{Y_1})^L=X^{-(E_1-E_2)}$	$R=(Y_2/Y_1)^{-t}\cdot(X)^{-l}$	랜덤수R 및 비밀정보 S
Ohta 방식	$(\frac{Y_2}{Y_1})^L=ID^{-(E_1-E_2)}$	$S=(Y_2/Y_1)^{-t}\cdot(ID)^{-l}$	비밀정보 S
ISO 안	$(\frac{Y_2}{Y_1})^L=ID^{(E_1-E_2)}$	$S=(Y_2/Y_1)^{t}\cdot(ID)^{l}$	비밀정보 S

다음은 Shamir 방식인 경우 비밀 정보 S가 노출되는 예를 보이고 있다. 먼저 p=7, q=11, 사용자의 ID=67인 경우 서명자가 동일한 랜덤수 R을 사용하는 경우에 대하여 생각하여 보자.

< TC에서의 비밀 정보 생성 >

TC는 사용자의 ID(=67)를 이용하여 다음과 같은 사용자의 비밀정보를 생성한다.

$$ID=S^L \mod N \qquad 67=9^5 \mod 77$$

사용자의 비밀 정보 S(=9)를 비밀리에 사용자에게 전달하며, L(=5)과 N(=77)를 공개하며, p(=7)와 q(=11)의 값은 TC만이 비밀리에 보관한다.

< 서명자의 서명문 생성 >

서명자는 랜덤한 수 R(=10)를 선택하여 다음 식을 계산한다.

$X = R^L \mod N$ $\quad 54=10^5 \mod 77$

2개의 메세지 M_1과 M_2에 대하여 해쉬 함수를 취한 값 E_1(=17)과 E_2(=13)를 이용하여, 서명문 Y_1과 Y_2는 다음과 같이 생성한다.

$$Y_1 = S \cdot R^{E_1} \mod N \qquad 9 \cdot 10^{17} = 24 \mod 77$$

$$Y_2 = S \cdot R^{E_2} \mod N \qquad 9 \cdot 10^{13} = 13 \mod 77$$

제 3자는 TC의 공개 정보 N(=77), L(=5)과 메세지 M_1에 대한 공개 정보 Y_1(=24), E_1(=17), X(=54), ID(=67)과 메세지 M_2에 대한 공개 정보 Y_2(=13), E_2(=13), X(=54), ID(=67)를 이용하여 서명자의 랜덤수 R를 다음과 같이 구한다.

먼저 t는 다음과 같다.

$$t = (E_1 - E_2)^{-1} \mod L \qquad (17-13)^{-1} = 4 \mod 5$$

또한 $(E_1 - E_2) \cdot t = l \cdot L + 1$이므로 l은 다음과 같다.

$$l = \frac{(E_1 - E_2) \cdot t - 1}{L} \qquad \frac{(17-14) \cdot 4 - 1}{5} = 3$$

그러므로 R은 다음과 같이 쓸 수 있다.

$$R = (Y_2 / Y_1)^{-t} \cdot (X)^{-l} \qquad (13/24)^{-4} \cdot 54^{-3} = 4$$

따라서 TC의 비밀 정보 S는 다음과 같이 계산한다.

$$Y = S \cdot R^E \mod N \qquad 24 = S \cdot 10^{17} \mod 77$$

그러므로 서명자의 비밀 정보 S는 9이다.

IV. 새로운 ID를 이용한 디지탈 서명

본 절에서는 기존의 ID를 이용한 디지탈 서명 방식의 문제점인 동일한 랜덤수를 두번 사용할 경우 발생하는 비밀 정보의 노출을 막을 수 있는 새로운 방식을 제안하고자 한다.

먼저 TC는 다음과 같이 키를 생성한다.

(1) p, q는 랜덤하게 선택한 큰 소수이고, $N = p \cdot q$이다.

(2) f는 일 방향 함수이다.

(3) N의 오일러 함수값 $\phi(N)=(p-1)(q-1)$이고, $\gcd(L, \phi(N))=1$인 L를 계산한다.

(4) 각 사용자 A의 개인 식별 정보를 ID_A라 할 때

$ID_A = S_A^L \mod N$

을 계산한다.

(5) N, f, L, ID_A는 모든 사용자에게 공개하고, S_A는 사용자 A만 보유하고, p, q는 TC만 보유한다.

서명자(A)는 다음과 같은 서명문을 작성한다.

(1) A는 랜덤한 수 R를 선택하여

$$X = R^L \mod N$$

을 계산한다.

(2) 메세지 M과 X에 대하여 일 방향 함수를 취한 값을

$$E = f(M, X) \mod N$$

라 한다.

(3) A는 자신의 비밀 정보 S_A와 랜덤수 R 및 해쉬값 E를 이용하여 다음과 같이 서명문을 작성한다.

$$Y = (S_A \cdot R)^E \mod N$$

(4) 서명자 A는 자신의 식별 정보 ID_A와 메세지 M 및 서명문(Y,X)를 B에게 보낸다.

확인자(B)는 ID_A, M, (Y,X)가 다음과 같은 조건을 만족하는지 확인한다.

$$Y^L = (ID_A \cdot X)^E \mod N$$

즉 위식은 우변의 항이 $(ID_A \cdot X)^E = S_A^{L \cdot E} \cdot R^{L \cdot E} = ((S_A \cdot R)^E)^L \mod N$ 임으로 좌변과 일치함을 알 수 있다.

V. 제안 방식에 대한 고찰

1. 안전성

제안 방식의 안전성은 기존 방식들과 동일하게 N의 소인수 분해를 알지 못할 때 mod N에서의 L-th root를 구하는 어려움에 근거를 두고 있다. 어떤한 방식이라도 (p, q, S_A)의 비밀성은 합성수 N의 소인수 분해의 곤란성에 기반을 두고 있다. 만일 공격자가 N을 소인수 분해한다면 S_A를 알게되어 사용자 A로 위장할 수 있다. N의 소인수 분해는 현재 알려진 알고리즘으로 $\exp((2+O(1))\sqrt{\log(N)\log(\log(N))})$의 시간이 걸린다. 그러므로 설계자는 위장의 공격을 방지하게끔 p와 q의 크기를 선택하여야 할 것이다.

또한 기존 방식 등에서의 서명 확인식에 지수승이 아닌 항이 존재 함으로서 그 항을 중심으로 다음과 같이 변환 시킬 수 있을 것이다.

$$Y^L = ID \cdot X^E$$
$$ID = Y^L \cdot X^{-E}$$

그러면 특별한 경우(같은 R을 두번 사용할 경우) 두개의 서명 확인식으로부터 다음과 같은 서로 동치가 되는 수식이 성립함으로서 안전성의 위협을 받게 된다.

$$Y_A^L \cdot X^{-E_A} = Y_B^L \cdot X^{-E_B}$$

그러나 제안한 방식에서는 서로 동치가 되는 수식이 성립하지 않음으로 동일한 R을 두번 사용하여도 안전하다고 할 수 있다.

2. 계산량

이러한 ID를 이용한 디지탈 서명 방식에서 서명자가 서명을 행하고자 할 때에는 개략적으로 모듈러 N에서 두번의 지수승(Shamir 방식인 경우; R^L, R^E)과 한번의 곱셈(Shamir방식인 경우; $S_A \cdot R^E$)이 필요하다. 본 제안 방식도 기존의 방식들과 동일한 계산량이 요구됨을 알 수 있다.

표3. 본 방식과 타 방식의 수식 비교

	서명 생성식	서명 확인식
Shamir 방식	$Y = S_A \cdot R^E \mod N$	$Y^L = ID \cdot X^E \mod N$
제안 방식	$Y = (S_A \cdot R)^E \mod N$	$Y^L = (ID \cdot X)^E \mod N$

VI. 결론

본고에서는 ID를 공개키로 사용하기 때문에 공개키를 인증할 필요도 없고, 따라서 공개 기록집을 작성하지 않아도 되는 ID를 이용한 디지탈 서명 방식에 대하여 검토하였다. 먼저 기존의 ID를 이용한 디지탈 서명 방식으로 Shamir 서명 방식, Ohta 서명 방식, ISO 표준(안) 방식에 대하여 분석하고, 이들 세 가지 방식은 서명자가 서명 생성시 랜덤수를 두번 이상 사용할 경우 서명자의 비밀 정보가 노출될 수 있음을 보였다. 또한 이러한 위협에 대하여 견딜 수 있는 새로운 ID를 이용한 디지탈 서명 방식을 제안하고 검토하였다.

본고에서 제안한 방식의 안전성은 큰 합성수 N의 소인수 분해를 알지 못할 때 모듈러 N에서의 L-th 제곱근을 구하는 어려움에 근거를 두고 있으며, 계산량은 서명 생성시 두번의 지수승 계산과 한번의 곱셈 그리고 서명 확인시 한번의 지수승과 한번의 곱셈이 요구된다. 따라서 본 제안 방식은 기존의 방식과 같은 안전성 및 계산량을 유지함으로서 기존 방식보다 안전하고 효율적인 ID를 이용한 디지탈 서명 방식임을 보였다.

- 참고 문헌 -

1. Akl, S. G., "Digital Signatures : a tutorial survey", IEEE Compute, No.16, pp.27-35, 1983
2. Denning, D. E., "Protecting Public Keys and Signature Keys", IEEE Compute, 16, pp.27-35, 1983.

3. Diffie, W. and Hellman, M. E., "New Directions in Cryptography", IEEE Trans. Inform. Theory, Vol. IT-22, No.6, pp.644-654, 1976.
4. ElGamal, T., "A public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithm", IEEE Trans. on Inform., Vol. IT-31, No. 4, pp.469-472, 1985.
5. Feige, U. and Shamir, A., "Zero-knowledge Proofs of Identity", Proc. of 19th ACM Symposium on Theory of Computing, pp.121-132, 1987.
6. Fiat, A. and Shamir, A., "How to Prove Yourself, practical solutions to identification and signature problem", Proc. of Crypto '87, Lecture Notes in Computer Science 263, pp.186-199, 1987.
7. Ohta, K. and Okamoto, T., "A Modification of the Fiat-Shamir Scheme", Crypto '88, pp.233-243, 1988.
8. ISO Digital Signature with appendix-Part 2:Identity-based mechanisms, ISO/IEC JTC 1 /SC 27/WG2 N378, 1996.
9. Rivest, R. L., Shamir, A. and Adleman, L., "A Method for Obtaining Digital Signature and Public Key Cryptosystem", Comm. ACM, Vol. 21, No.2, pp.120-126, 1978.
10. Shamir, A., "Identity based Cryptosystems and Signature Schemes", Proc. of Crypto'84, Lecture Notes in Computer Science 196, pp.47-53, 1985.
11. Stinson, D.R., Cryptography ; Theory and Practice, CRC Press, 1995.
12. 한국전자통신연구소, 현대 암호학, 1991.
13. 이임영,최용락,이강수,소우영, 통신망 정보보호, 그린출판사, 1996