제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

「무선 환경에 적합한 타원곡선상의 복원형 전자서명에 관한 연구」

김근옥*, 안상만*, 오수현*, 원동호*
* 성균관대학교 정보통신공학부
e-mail : {kokim, smahn, shoh, dhwon}@dosan.skku.ac.kr

A Study on a Message Recovery Signature based on Elliptic Curves for Wireless Environment

Keun-Ok Kim*, Sang-Man Ahn*, Soohyun Oh*, Dongho Won*
* School of information and communication Engineering, Sungkyunkwan University

요 약

PKI(Public Key Infrastructure)의 발달과 함께 전자서명의 필요성 또한 대두되고 있다. 전자서명이 무선 PKI환경에서도 사용되기 위해서는 최소한의 서명 생성·검증 시간과 적은 저장 공간, 적은 대역폭의 사용 등의 조건을 만족해야 한다. 본 논문에서는 서명 생성·검증 시간을 줄여주기 위해서 타원곡선 상의 연산을 이용하고, 대역폭의 감소를 위해서 서명의 크기를 최소화해서 보내줄 수 있는 복원형 전자서명에 대해서 알아볼 것이다.

1. 서론

인터넷의 발달과 함께 대부분의 사람들이 컴퓨터를 접할 수 있게 되면서, 인터넷을 통한 상거래 문화가 널리 자리잡고 있다. 하지만, 전자상거래라는 특성상 물건을 사고 파는 사람이 서로에 대한 어떠한 정보도 가지지 못하기 때문에 대금을 지불한다든지 할 경우 이에 따르는 보안문제가 필수불가결하다. 이러한 문제를 보완해 줄 수 있는 방법중에 하나가 전자서명이다. 전자서명은 위조불가, 서명자 인증, 부인불가, 재사용불가, 변경불가등 전자상거래를 통해 발생할 수 있는 문제를 해결하기에 적합한 조건을 가지고 있다.

요즘들어 무선 단말기의 보급과 함께 무선 인터넷 시장의 급속한 발달로 무선 인터넷상에서의 전자서명또한 고려해봐야 할 문제로 대두되고 있다. 하지만, 무선인터넷상의 제약 조건을 만족시키기 위해서는 기존 유선상에서 사용되던 전자서명 방식을 그대로 사용하는데는 무리가 따른다. 우선 무선 단말기 용량의 제한으로 서명을 생성/검증하는데 걸리는 시간을 최소화 해야 하며, 무선 전송상의 문제를 줄이기 위해서 적은 대역폭을 사용해야 한다. 이러한 조건에 알맞은 전자서명이 타원곡선을 이용한 복원형 전자서명이다.

타원곡선상의 연산을 통해서 키 크기를 줄여주고, 연산속도를 증가시킴으로써 서명을 생성·검증하는데 걸리는 시간을 줄여주며, 통신할 때 메시지의 길이를 최소화해줌으로써 적은 대역폭을 사용해서 통신이 가능하게 해준다.

서명된 메시지의 길이가 짧다는 타원곡선상의 전자서명의 장점 때문에 ID-based PKI system이나 키 교환(key exchange)프로토콜에 사용되기에 알맞다.

타원곡선을 이용한 복원형 전자서명은 1996년 Nyberg Rueppel이 처음으로 제안한 복원형 전자서명 방식을 타원곡선상에 적용시킨 ECNR이 있으며, 1997년 Atsuko Miyaji가 제안한 복원형 전자서명을 타원곡선상에 적용시킨 ECMR이 있다. 2000년 Pintsov와 Vanstone이 제안한 ECAO와 1997년 Handbook of applied cryptography에 소개된 ECPV가 있다. 본 논문에서는 우선 복원형 전자서명의 서명 생성·검증 과정에 대해서 2장에서 기술하고, 3

장에서는 위에서 소개한 타원곡선상의 복원형 전자서명에 대해서 알아보고, 4장에서는 각 전자서명의 효율성을 분석하고자 한다.

2. 관련 연구

복원형 전자서명은 보내고자 하는 메시지를 서명해서 보낸 후에 메시지를 복원해서 이를 검증한다. 이러한 복원형 전자서명을 생성하는 과정과 검증하는 과정은 다음과 같다.

2.1 복원형 전자서명의 생성

복원형 전자서명의 생성과정은 먼저 randomizer와 pre-signature를 생성한후 메시지를 적당한 크기로 나누고, data input을 생성한다. 그런 후에 서명을 생성한다.

2.2 복원형 전자서명의 검증

서명된 message를 복호화 한 후에, 서명의 크기를 검증하고 pre-signature와 data input을 다시 생성하고, 이를 통해 메시지를 다시 생성해서 메시지의 redunduncy를 확인한다.

2.3 복원형 전자서명의 특징

복원형 전자서명은 받은 데이터를 통해서 메시지를 복원하고, 복원 결과 만들어진 메시지의 redunduncy를 확인해서 서명의 정당성 여부를 판별하는 특징을 가지고 있다. 복원형 전자서명은 적은 대역폭을 가지고 통신을 할 수 있기 때문에 무선 환경에 적합한 전자서명 방식이라고 할 수있다. 하지만, 메시지를 적당한 크기로 잘라서 각각의 조각에 서명을 해야하는 번거로움이 있기 때문에 부가형 전자서명 방식에 비해 서명을 생성하는데 걸리는 시간이 많지만, 계산을 효율적으로 해줄 수 있는 타원곡선상에서 복원형 전자서명을 이용할 경우 서명생성 시간을 줄일 수 있다.

3 복원형 전자서명의 종류

타원곡선을 이용한 복원형 전자서명에는 다음과 같은 종류가 있다.

3.1 ECNR

ECNR은 1996년 Nyberg-Reuppel이 복원형 전자서명을 처음으로 제안한 이후에 이를 타원곡선 상에 적용시킨 프로토콜이다. ECNR은 해쉬를 사용하지 않고도 서명 생성/검증을 할 수 있다는 장점이 있고 기존의 RSA나 ElGamal에서도 서명 생성/검증이 가능하기 때문에 별도의 알고리즘이 필요하지 않다.

□ ECNR 의 키 생성 과정

- $k \in \{2, \ldots, n-2\}$ 선택
- $(x_1, y_1) = kG$ 계산

위의 과정에서 k값은 randomizer이며, kG값은 선행 서명을 생성하기 위해 생성한 값이다.

□ ECNR 의 서명 생성 과정

- $\Pi = \pi(kG) \pmod n$
- $r = d + \Pi \pmod n$
- $s = k - x_A r \pmod n$

위의 과정에서 Π값은 선행 서명이 되며, r과 s가 실제 서명 값이 된다. 서명을 모두 생성한 후 k값을 초기화하고, 만약 생성한 서명값 중 0이 나오면 k를 다시 선택한다.

□ ECNR 의 서명 검증 과정

- $R_1' = s'G + r'Y_A$
- $\Pi' = \pi(R_1') \pmod n$
- $d' = r' - \Pi' \pmod n$

서명 검증의 초기 과정은 전송되어온 서명 값을 먼저 검증한다. r과 s의 값이 mod n상에서 계산되었기 때문에, 이 구간에 포함되는지 여부를 확인한다. 서명 값이 mod n안에 속하는지 여부를 확인 한 후, 속할 경우에 선행 서명인 Π'를 먼저 생성하고 이를 이용해서 메시지인 d값을 복원하게 된다. ECNR의 경우 모든 메시지를 복원하는 short redundancy를 이용하기 때문에 복원된 d값과 원래 메시지와의 redundancy를 비교해서 서명의 정당성 여부를 판별하게 된다.

3.2 ECMR

ECMR은 1996년 Atsuko Miyaji가 제안한 복원형 전자서명을 타원곡선 상에 적용시킨 프로토콜로 ECNR에서 사용하지 않았던 해쉬함수를 사용하게 된다. 이 과정을 통해서 유한체에서 정의한 타원곡선위의 점을 압축시켜줌으로써 서명할 메시지의 크기를 줄여주는 역할을 한다.

□ ECMR 의 키 생성 과정

- $k \in \{2, \ldots, n-2\}$ 선택
- $(x_1, y_1) = kG$ 계산

ECMR의 키 생성 과정은 ECNR의 키 생성 과정과 동일하다.

□ ECMR 의 서명 생성 과정

- $\Pi = Hash(kG) \pmod n$

- $r = d \; XOR \; \Pi$
- $s = (rk - r - 1)/(x_A + 1) \pmod{n}$

위의 과정에서 선행 서명인 Π값을 생성할 때, 출력으로 데이터 부분인 d의 길이와 같은 길이가 나올 수 있는 Hash 함수를 이용하여 XOR 연산을 XOR 연산을 통해 서명을 생성한다. 그렇기 때문에 선행 서명을 이용해서 생성한 r값은 d의 크기와 같게 되었다. 이러한 과정을 통해서 ECMR의 서명 중 r 값의 크기가 $\{0,1\}^{len_n}$만큼 작아지게 되는 것이다.

서명을 모두 생성한 후에는 위의 프로토콜과 마찬가지고 k값을 초기화하며, s값이 0이 나올 경우 k값을 다시 선택해야 한다.

□ ECMR 의 서명 검증 과정

- $R_1' = (1 + r' + s')/(r')G + s'/r' Y_A$
- $\Pi' = Hash(R_1')$
- $d' = r' \; XOR \; \Pi' \pmod{n}$

서명 검증시에는 먼저 서명자에게 받은 r값과 s값이 알맞은 범위에 들어가는지를 확인해야 한다. 특히 ECMR같은 경우 r값의 범위를 확인해야 한다.

1996년 Atsuko Miyaji는 자신의 논문 "A message recovery signature scheme equivalent to DSA over elliptic curves"에서 ECMR이 타원곡선상에 적용시킨 다른부가형 전자서명과도 같은 안전성을 가지고 있음을 증명하였다.

3.3 ECAO

ECAO는 메시지의 부분적인 부분만 복원해서 비교하는 long redundancy를 이용해서 서명을 생성하고 검증하기 때문에 다음과 같은 조건이 필요하다.

□ ECAO의 조건

- $Hash(\{0,1\}^* \rightarrow \{0,1\}^{len})$ *where* $len \geq \max(8L_2, 8L_F - 8L_2, \; number \; of \; bits \; of \; n)$
- $Hash_1(\{0,1\}^* \rightarrow \{0,1\}^{8L_2})$
- $Hash_2(\{0,1\}^{8L_2} \rightarrow \{0,1\}^{8L_F - 8L_2})$
- $Hash_3(\{0,1\}^* \rightarrow \{1, \ldots, n-2\})$
- $d = Hash_1(M_{rec}) \| (Hash_2(Hash_1(M_{rec})) \; XOR \; M_{rec})$

위의 과정에서 M_{rec}와 M_{clr}은 각각 복원할 수 있는 메시지의 부분과 복원할 수 없는 메시지의 부분을 의미한다.

□ ECAO의 키 생성 과정

- $k \in \{2, \ldots, n-2\}$ 선택
- $(x_1, \; y_1) = kG$ 계산

키 생성 과정은 ECMR 과 같다.

□ ECAO 의 서명 생성 과정

- $r = d \; XOR \; x_1$
- $\Pi = Hash_3(r \| M_{clr})$
- $s = k - x_A \Pi \pmod{n}$

위의 과정에서 r 생성시 d의 값의 크기는 $8L_F$가 되므로 전체 r값 또한 $8L_F$가 된다. 이 과정에서 s값이 0이 나왔을 경우, k를 다시 선택한다.

□ ECAO 의 서명 검증 과정

- $\Pi' = Hash_3(r' \| M_{clr})$
- $(w_x, w_y) = s'G + \Pi' Y_A$
- $d' = r' XOR \; w_x$
- $M_{rec} = [d']_{8L_F - 8L_2} \; XOR \; Hash_2([d']^{8L_2})$
- $[d']^{8L_2} = Hash_1(M_{rec})$

ECAO의 경우 long redundancy를 이용하기 때문에 복구 가능한 메시지를 복구한 후에 보내진 메시지와 함께 메시지의 redundancy를 확인한다.

3.4 ECPV

ECPV는 위에서 소개한 방식들과는 다른 방법으로 서명을 생성/검증한다. 우선 대칭키를 만들어주는 함수인 KDF를 이용해서 만든 대칭키 SYM을 가지고 메시지를 암호화하고, 이 암호문을 서명과 함께 보내주는 방식으로 통신을 한다. ECPV의 조건을 보면 다음과 같다.

□ ECPV의 조건

- SYM: 대칭키 암호
- KDF :대칭키를 만들어주는 함수
- d를 SYM을 이용해서 암호화한 값을 C라 함

□ ECPV의 키 생성 과정

- $k \in \{2, \ldots, n-2\}$ 선택
- $J = (x_1, \; y_1) = kG$ 계산

키 생성 과정은 ECMR 과 같다.

□ ECPV 의 서명 생성 과정

- $s = k - x_A h \pmod{n}$
- C : d를 SYM을 이용해서 암호화한 값
- M_2 : 전체 메시지에서 M_1을 뺀 부분

ECPV에서는 서명 생성시 s값만을 생성하며, C와 M_2값을 함께 전송해준다.

서명 생성후 s값이 0이 나왔을 경우, k값을 다시

선택해 준다.

□ ECPV 의 서명 검증 과정

- $h = Hash(C \| M2)$
- $R_1' = sG + hY_A$

보내진 값들로부터 M_1을 계산하고, 받은 M_2와 값께 원래의 메시지를 복원한 다음 redundancy를 확인해서 서명을 검증한다.

4. 복원형 전자서명의 효율성 비교

복원형 전자서명이 적은 대역폭을 사용하고 기존의 알고리즘을 그대로 이용할 수 있다는 장점이 있지만, 여전히 부가형 전자서명에 비해 메시지를 알맞은 크기로 잘라서 각각에 대해서 서명을 해야 하기 때문에 서명을 생성/검증하는데 걸리는 시간이 오래걸린다.

타원곡선상에서 정의된 복원형 전자서명의 효율성을 알아보기 위해서 서명의 크기와 pass 그리고 타원곡선상의 주요 연산인 scala multiplication의 횟수를 비교하였다.

<표 1> 타원곡선상의 복원형 전자서명의 효율성 비교

		ECNR	ECMR	ECAO	ECPV
서명 크기	r	n	$\{0,1\}^{len\_n}$	$\{0,1\}^{8L_F}$	-
	s	n	n	n	n
pass		1	1	1	1
scala multiplication	서명자	1	1	1	1
	검증자	2	2	2	2

(단, $n > len\_n > 8L_F$)

위에서 정의한 타원곡선 상의 복원형 전자서명들은 각 프로토콜의 효율성을 위해서 연산을 줄이기보다는 복원될 메시지의 크기와, 서명값의 크기를 줄여줌으로써 통신량과 서명을 생성·복원할 때 소요되는 시간을 줄여주는 방향으로 정의되고 있다.

ECNR의 경우 메시지를 mod n 연산했기 때문에 서명의 크기가 메시지의 길이와 같은 n이 되며, ECMR은 메시지 d와 XOR연산을 하기 때문에 d의 크기인 len_n이 되며, ECAO는 조건에 맞게 d값을 계산하면, d의 크기가 $8L_F$가 되어 위의 프로토콜들보다는 적은 크기의 서명을 생성할 수 있다. 마지막으로 ECPV는 서명을 단지 s값만 생성하고 메시지를 암호화해줌으로써, 서명의 크기를 줄여줄 수 있었다.

5. 결론

무선 인터넷의 발달과 함께 무선상의 전자상거래가 자리잡고 있으며, 안전한 전자상거래를 위해서는 보안문제를 생각하지 않을 수 없다. 이를 보완해줄 수 있는 것이 전자서명 방식인데, 무선 환경이라는 제약조건 때문에 적은 연산량과 적은 저장용량에 적합한 전자서명이 필요하게 되었다.

현재 대부분의 무선 환경에서는 서명을 생성/검증하는데 상대적으로 적은 시간이 소요되는 부가형 전자서명 방식을 사용하고 있지만, 기존의 알고리즘을 그대로 사용할 수 있고, 통신할 때 적은 대역폭을 사용할 수 있는 복원형 전자서명 또한 무선환경에 적합한 서명방법이라 할 수 있다.

하지만, 무선상에서는 서명을 생성/검증하는데 걸리는 시간이 가장 중요하기 때문에 타원곡선을 이용한다든지, 메시지의 양과 서명의 값을 줄여줄 수 있는 방향으로 복원형 전자서명이 발전된다면, 앞으로 무선 환경에서도 부가형 전자서명만큼 사용될 수 있을 것이다.

참고문헌

[1] ISC/CD 15946-4 , Digital signatures giving message recovery, 2001

[2] IEEE P1363a/D2, Standard Specifications for Public Key Cryptography, 2000

[3] Atsuko Miyaji, "A message recovery signature scheme equivalent to DSA over elliptic curves, ASIACRYPT'96

[4] Atsuko Miyaji, "Another countermeasure to forgeries over message recovery signature" , IEICE Trans., Fundamentals. vol. E80-A, No.11, 1997

[5] Leon A.Pintsov and Scott A. Vanstone, "Postal Revenue Collection in the Digital Age", LNCS 1962, pp. 105

[6] Chen-Chi Lin and Chi-Sung Laith, "Cryptanalysis of Nyberg-Rueppel's Message Recovery Scheme" , IEEE Communication Letters, Vol.4, no.7, pp.231-232, July 2000

[7] Kaisa Nyberg and Rainer A. Rueppel, "Message Recovery for signature Schemes Based on the Discrete Logarithm Problem", Eurocrypt '94, LNCS 950, pages 182-193

[8] M. Abe and T. Okamoto, "A signature scheme with message recovery as secure as discrete logarithm", Advances in Cryptology-Asiacrypt'99, LNCS pp. 378-389, 1999