情 報 保 護 學 會 誌
第 14 券 第 2 號, 2004. 4

ISO/IEC JTC1/SC27의 전자서명 표준

이 필 중*, 박 동 진**

요 약

본 고에서는 ISO/IEC JTC1/SC27에서 만들어졌거나 진행 중인 전자서명 표준에 대해서 살펴본다. 해당되는 표준은 9796의 part 2, 3과 14888의 part 1, 2, 3과 15946의 part 2, 4이다. 각 문서들이 다루고 있는 내용과 개정 방향을 살펴보고, 각각의 알고리즘들을 간단히 설명한다.

Ⅰ. 서 론

인터넷과 컴퓨터의 발달에 따라서 전자서명은 이미 많은 곳에서 쓰이고 있다. 여러 가지 다양한 전자서명 기법들이 제안되었으며 그것들의 안전도 역시 증명되고 있다. 이에 따라서 안전한 전자서명 알고리즘에 대한 표준화도 일부에서 이루어지고 있다. 본 고에서는 ISO/IEC JTC1/SC27에서 표준화되고 있는 전자서명 알고리즘들을 소개한다.

ISO/IEC JTC1에서 표준은 우선 WD(Working Draft)을 만들고 여러 국가의 전문가들의 교정을 통해서 CD(Committee Draft)를 만들게 된다. 이런 과정을 거쳐서 CD는 DIS(Draft International Strandard)로 바뀌게 된다. 그리고 DIS는 국가 단체(NB: National Body)들의 75%의 동의를 거쳐 IS(International Standard)가 된다. 채택된 IS 문서는 4년 후 해당 SC에서 재검토하고 5년째 되는 해에 다시 5년 동안 그것을 IS로 채택할 것인지를 결정한다. 현재 ISO/IEC JTC1/SC27에서 전자서명 알고리즘을 표준화하고 있는 문서는 다음과 같다.

- ISO/IEC IS 9796-2, Information technology - Security techniques - Digital signature schemes giving message recovery - Part 2: Integer factorization based mechanisms (revision)
- ISO/IEC WD 9796-3, Information technology - Security techniques - Digital signature schemes giving message recovery - Part 3: Discrete logarithm based mechanisms (revision)
- ISO/IEC IS 14888-1, Information technology - Security techniques - Digital signature with appendix - Part 1: General
- ISO/IEC WD 14888-2, Information technology - Security techniques - Digital signature with appendix - Part 2: Integer factorization based mechanisms (revision)
- ISO/IEC WD 14888-3, Information technology - Security techniques - Digital signature with appendix - Part 3: Discrete logarithm based mechanisms (revision)
- ISO/IEC IS 15946-2, Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 2: Discrete signatures
- ISO/IEC FDIS 15946-4, Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 4: Digital signatures giving message recovery

* 포항공과대학교 전자전기공학과/KT 기술연구소 (pjl@postech.ac.kr)
** 포항공과대학교 전자전기공학과 (djpark@oberon.postech.ac.kr)

EC-KCDSA가 ISO/IEC 15946-2에서, 그리고 ECKNR이 ISO/IEC 15946-4에서 이미 표준화가 되었고, SEED, KCDSA, AMP, Cha-Cheon algorithm 등이 현재 표준화 중에 있다.

본 고에서는 이들 문서를 살펴본다. 우선 Ⅱ장에서는 이해를 돕기 위해 표준들이 다루고 있는 전자서명 알고리즘들을 분류해서 설명한다. 그리고 각각의 문서의 현 상황을 Ⅲ장에서 다룰 것이다. 아울러 이 장에서는 2003년 10월의 프랑스 파리에서 열린 SC27/WG2의 회의 결과에 따라서 표준문서가 어떤 식으로 변화될지도 살펴보겠다. 그리고 Ⅳ장에서 실제 전자서명 알고리즘에 대한 설명을 할 것이다.

Ⅱ. 전자서명의 분류

SC27에서는 여러 가지 전자서명 알고리즘들에 대한 표준화가 진행되고 있다. SC27은 이들 알고리즘을 몇 가지 기준에 의해 분류하고 있다. 이 기준에 따라서 알고리즘들은 ISO/IEC 9796, ISO/IEC 14888, ISO/IEC 15946에 나누어서 표준화가 되고, 다시 part 가 나누어진다. 각각의 문서 내에서도 이런 성질별로 구분 지어져서 설명되고 있다.

1. 메시지 복원 여부

가. Mechanism giving message recovery

여기에 속하는 알고리즘들은 서명 값에서 메시지의 일부분을 복구할 수 있다. 이런 알고리즘들은 현재 ISO/IEC 9796과 ISO/IEC 15946-4에서 표준화 되고 있다. 해당되는 알고리즘에는 RSA, Rabin, NR, ECMR, ECAO, ECKNR이 있다.

나. Mechanism with appendix

여기에 속하는 알고리즘들은 서명 값에서 메시지를 복구할 수 없다. 따라서 서명 값과 별도로 메시지 전체가 같이 보내진다. ISO/IEC 14888과 ISO/IEC 15946-2에서 표준화가 되고 있다. 해당되는 알고리즘에는 RSA, Rabin, GQ1, GQ2, GPS, ESIGN, DSA, KCDSA, Pointcheval-Vaudenay, EC-DSA, EC-KCDSA, EC-GDSA, IBS-1, IBS-2이 있다.

2. 기반을 두는 hard problem

가. 소인수분해문제

소인수분해문제의 어려움에 기반을 두는 서명 알고리즘들이다. ISO/IEC 9796-2와 ISO/IEC 14888-2에서 다루고 있다. 해당되는 알고리즘에는 RSA, Rabin, GQ1, GQ2, GPS, ESIGN이 있다.

나. 이산대수문제

이산대수문제의 어려움에 기반을 두는 서명 알고리즘들이다. 여기서의 이산대수문제는 상당히 넓은 의미로 쓰인다. 그래서 타원곡선 상에서의 이산대수문제와 (bilinear) Diffie-Hellman problem도 이 영역에서 다루고 있다. ISO/IEC 9796-3, ISO/IEC 14888-3, ISO/IEC 15946에서 다루고 있다. 해당되는 알고리즘에는 NR, ECMR, ECAO, ECKNR, DSA, KCDSA, Pointcheval-Vaudenay, EC-DSA, EC-KCDSA, EC-GDSA, IBS-1, IBS-2이 있다.

3. 타원곡선 사용 여부

ISO/IEC JTC1/SC27에서는 타원곡선을 다루기 위해 ISO/IEC 15946를 만들어서 타원곡선을 이용한 전자서명 알고리즘들을 표준화 하였다. 그리고 또한 ISO/IEC 9796-3과 ISO/IEC 14888-3에서도 몇 종류의 알고리즘을 다루고 있다. 2003년 프랑스 파리회의에서 타원곡선상의 알고리즘을 특별한 문서로 다루지 않기로 결정하였다. 해당되는 알고리즘은 ECMR, ECAO, ECKNR, EC-DSA, EC-KCDSA, EC-GDSA, IBE-1, IBE-2이 있다.

4. 공개키를 얻는 방식

서명 검증을 위해서는 서명자의 서명키에 해당하는 검증키가 필요하다. 이때 서명자의 신원(identity)과 검증키간의 관계에 따라서 다음의 두가지 방식이 존재한다.

가. 신원 기반의 알고리즘

사용자의 신원에서 공개키를 직접 구할 수 있다. 1998년에 제정된 ISO/IEC 14888-2이 이런 알고리즘을 다루었다. 새로 개정되는 표준에서는 이런 알고리즘이 기반을 두는 문제에 따라서 ISO/IEC 14888-2와 ISO/IEC 14888-3에 나누어서 표준화될 예정이다. 해당하는 알고리즘은 GQ1, IBS-1, IBS-2이 있다.

나. 공개키 기반의 알고리즘

이 방식의 알고리즘은 사용자의 신원과 공개키를 연결하기 위해 인증서(certificate)를 사용한다. 현재 사용하고 있는 대부분의 전자서명 방식이 여기에 해당된다. 해당되는 알고리즘에는 RSA, Rabin, GQ2, GPS, ESIGN, NR, ECMR, ECAO, ECKNR, DSA, KCDSA, Pointcheval-Vaudenay, EC-DSA, EC-KCDSA, EC-GDSA이 있다.

5. 서명 값의 난수성

가. Randomized mechanism

매번 다른 서명 값을 얻는다. 대부분의 전자 서명 알고리즘이 이곳에 속한다. ISO/IEC JTC1/SC27에서는 이 방식을 따르는 알고리즘들을 권장하고 있다.

나. Non-randomized mechanism

같은 메시지에 대해 서명키가 같을 경우 서명 값이 일정하다. 난수 발생기가 없는 상황이나 이전 버전과의 호완성이 필요한 경우와 같이 특별한 조건에서만 사용하는 것을 권장하고 있다. RSA과 Rabin이 특정한 padding을 사용할 때 이 범주에 해당된다.

Ⅲ. 상 황

각 표준 문서들의 현재 상황을 알아본다.

• ISO/IEC 9796: Digital signature schemes giving message recovery

이 표준은 메시지 복원형 전자서명 알고리즘을 다루고 있다.

Part 1: Mechanisms using redundancy

안정성에 문제가 제기되어서 2000년에 폐기되었다.

Part 2: Integer factorization based mechanisms (revision)

1997-09-01에 첫 번째 버전이 IS가 되었고, 개정된 문서가 2002-10-01에 다시 IS가 되었다 [12]. RSA와 Rabin을 메시지 복원형으로 사용하는 방법을 표준화하였다.

Part 3: Discrete logarithm based mechanisms (revision)

2000-04-15에 첫 번째 버전이 IS가 되었다 [13]. 현재는 개정작업 중이며 WD이다 [14]. 기존의 내용과 15946-4의 내용을 통합하는 문서가 될 예정이다. 현재 버전의 문서에는 NR, ECMR, ECAO이 포함되어 있고, 다음 WD에 ECKNR이 추가될 예정이다.

• ISO/IEC 14888: Digital signature with appendix

이 표준은 부가형 전자서명 알고리즘들을 다루고 있다. 1999년 첫 번째 버전이 표준화 되었다 [15, 16, 17]. 2003년 프랑스 파리회의의 결과로 전면적인 개정이 결정되었다. 원래 part 2는 identity-based mechanisms이었고, part 3은 certificate-based mechanisms이었다. 개정되는 문서는 ISO/IEC 9796과 같이 기반을 두는 hard problem을 기준으로 part를 나누기로 하였다.

Part 1: General

1998-12-15에 IS가 되었다 [15]. 부가형 전자서명의 일반적인 모델을 설명하고 있다. 다른 part가 개정되면 그것을 반영하도록 개정될 예정이다.

Part 2: Integer factorization based mechanisms (revision)

현재 WD에 있는데 [18], 앞으로 CD는 2005-05, FDIS는 2006-11, IS는 2007-05를 목표로 표준화가 진행 중이다. RSA, Rabin, GQ1, GQ2, GPS, ESIGN이 표준화 중이다. GPS 알고리즘이 개정안에서 추가 되었다.

Part 3: Discrete logarithm based mechanisms (revision)

현재 WD에 있는데 [19], 앞으로 CD는 2005-05, FDIS는 2006-11, IS는 2007-05를 목표로 표준화가 진행 중이다. DSA, KCDSA, Pointcheval-Vaudenay, EC-DSA, EC-KCDSA, EC-GDSA, IBS-1, IBS-2를 다루고 있다. ISO/IEC 15946-2에 있던 EC-DSA, EC- KCDSA, EC-GDSA가 이 문서로 옮겨서 표준화 중에 있다. 그리고 pairing 연산을 사용하는 IBS-1과 IBS-2를 이 문서에서 같이 표준화 하고 있다.

• ISO/IEC 15946: Cryptographic techniques based on elliptic curves

이 표준문서는 타원곡선을 사용한 암호 기술들을 표준화할 목적으로 만들어졌다. 하지만 이제 더 이상 타원곡선을 특별한 기술로 볼 필요가 없다고 판단해서 새로이 개정되는 버전에서는 part 1만을 남기로 하였다. 따라서 이 표준에서 다루고 있는 전자서명 알고리즘들은 ISO/IEC 9796이나 ISO/IEC 14888로 옮겨질 예정이다.

Part 2: Digital signatures

2002-12-01에 IS가 되었다 [20]. 이 문서에 있는 내용은 ISO/IEC 14888-3에 합쳐진 후에 이 문서를 제거할 예정이다. 다루고 있는 전자서명 알고리즘은 EC-DSA, EC-GDSA, EC-KCDSA이다.

Part 4: Digital signatures giving message recovery

2000-05에 WD를 시작으로 2000-11에 CD, 2002-11에 FDIS가 되었다 [21]. 2004-5에 IS가 될 예정이다. 이 문서에 있는 내용은 ISO/IEC 9796-3에 합쳐진 후에 이 문서를 제거할 예정이다. 다루고 있는 전자서명 알고리즘은 ECNR, ECMR, ECAO, ECPV, ECKNR를 다루고 있다.

Ⅳ. 알고리즘 설명

이 절에서는 실제 전자 서명 알고리즘들을 살펴보겠다. 본 고에서는 알고리즘이 동작하는 원리만을 소개할 것이기 때문에 데이터의 형태 변화, 구체적인 format, 변수의 선택 등은 다루지 않을 것이다. 다양한 변종이 있을 경우에는 가장 대표적인 것을 예로 들어 설명할 것이다. 소인수분해문제의 어려움에 기반을 두는 알고리즘에서는 CRT나 multiprime을 사용하지 않는 방식으로 설명할 것이다.

• 공통 표기법

이 절에서는 M은 메시지를 의미하고, $h()$는 해쉬함수를 의미한다. 프라임 부호($'$)나 별 부호($*$)가 붙은 값은 서명 검증과정에서 받은 값이나 재 계산된 값을 의미한다.

$MSB(A,B)$는 A의 왼쪽에서 B bits를 취한 값이고, $LSB(A,B)$는 A의 오른쪽에서 B bits를 취한 값을 의미한다.

타원곡선상의 점 P가 주어졌을 때 P_x는 x 좌표값을, P_y는 y 좌표값을 의미한다.

• RSA [26]/Rabin [25]

가장 많이 쓰이는 전자서명 알고리즘이다. 메시지 복원형과 부가형 모두에서 표준화 되었다. 본 고에서는 RSA 부가형만을 설명한다.[1] Rabin 시스템은 RSA 시스템과 비슷하여 설명을 생략한다.

- 도메인 변수 생성:

큰 소수 p, q를 생성하고 $n = pq$을 계산한다. 검증에 쓰일 적당한 지수 v를 선택하고 서명에 쓰일 지수 $s = v^{-1} \bmod \phi(n)$를 계산한다. 그리고 메시지를 원하는 형태의 정수로 바꾸어 줄 formating 함수를 선택한다. ISO/IEC 14888-2에는 다음의 두 가지 format를 제시하고 있다. $Format_1()$은 PSS (Probabilistic Signature Scheme) [2]를 표준화한 것이다. 이 방식은 난수 salt를 사용해서 같은 M에 대해서도 다양한 결과가 나오게 만들어 준다. $Format_2()$는 이전 버전의 알고리즘과의 호환성을 위해 남겨둔 것이다. 표준 문서에서처럼 앞으로의 설명에서는 첫 번째 함수를 사용하는 것을 가정하겠다.

- 서명 생성:

$F = Format_1(h(M))$

$S = F^s \bmod n$

서명 값은 S가 된다.

- 서명 검증:

$F' = S'^v \bmod n$

$h(M)$값을 다시 계산하고, 이 값이 F'에 포함되어 있는 $h(M)$값과 같으면 유효한 서명으로 인정한다.

• GQ1 [8, 9]

GQ scheme은 Guillou와 Quisquater에 의해 제안되었다. 영지식 인증 기법을 변형하여 만들었다. 그 중 GQ1은 신원 기반의 전자 서명 알고리즘이다.

- 도메인 변수 생성:

큰 소수 p, q를 생성하고 $n = pq$을 계산한다. 공개될 지수 v를 선택하고 개인키를 추출할 때 쓰일 지수

1) 메시지 복원형으로 쓸 때는 F가 복원하고자하는 메시지를 포함하게 한다.

$s = -v^{-1} \bmod \phi(n)$를 계산한다. 그리고 W와 M에서 H를 계산할 방식을 결정한다. (표준 문서에는 네 가지 방식이 있는데, 본 고에서는 첫 번째 방식인 $H = h(W \| M)$으로 설명하겠다.) 또한, 사용할 formating 함수를 결정한다. $Format_1'()$은 $Format_1()$에서 난수값을 사용하지 않는 변종을 의미한다.

- 개인키 추출:

ID에 해당하는 개인키 $D_{ID} = G_{ID}^{s} \bmod n$를 만들어준다. 이때 G_{ID}는 $Format_1'(ID)$으로 계산되고 누구나 계산 가능한 값이다.

- 서명 생성:

$[2, n-1]$에서 임의의 정수 K를 선택한다.

$W = K^{v} \bmod n$

$H = h(W \| M)$

$R = MSB(H, |v| - 1)$

$S = K \times D_{ID}^{R} \bmod n$

서명 값은 (R, S)가 된다.

- 서명 검증:

$G_{ID} = Format_1'(ID)$

$W = S^{v} G_{ID}^{R} \bmod n$

$H' = h(W' \| M)$

$R^{*} = MSB(H', |v| - 1)$

R'와 R^{*}가 같으면 유효한 서명으로 인정한다.

• GQ2 [10]

GQ1와 비슷한 방식으로 서명 값을 생성한다. 하지만 GQ1과는 달리 공개키 기반의 전자서명 알고리즘이다. 계산 방식은 설명하지 않겠다.

• GPS [6, 24, 7]

Girault, Poupard, Stern에 의해 제안된 영지식 기술을 응용해서 만들어진 메시지 부가형 전자서명 알고리즘이다. 영지식 인증 기법을 변형하여 만들었다. 표준에서 설명하는 세 가지 방식 중에서 본 고에서는 첫 번째 방식을 설명한다.

- 도메인 변수 생성:

RSA와 같은 방식으로 modulus n을 선택한다. 그리고 $[2, n-1]$에서 g를 선택한다. 160 bits의 임의의 정수를 선택해서 사용자의 서명키 Q로 삼는다. 공개키는 $Y = g^{Q} \bmod n$가 된다.

- 서명 생성:

400 bits의 임의의 정수 r를 선택한다.

$W = g^{r} \bmod n$

$H = h(W \| M)$

$R = MSB(H, 160)$

$S = r - R \times Q$

- 서명 검증:

$W = Y^{R} \times g^{S} \bmod n$

$H' = h(W' \| M)$

$R^{*} = MSB(H', 160)$

R'와 R^{*}가 같으면 유효한 서명으로 인정한다.

• ESIGN [5]

Fujioka, Okamoto, Miyaguchi에 의해 제안된 메시지 부가형 전자서명 알고리즘이다.

- 도메인 변수:

4 이상의 공개된 지수 v를 선택한다. 소수의 크기를 결정하는 정수 π를 선택한다. $(2^{\pi})/2 < p_1 < p_2 < 2^{\pi}$을 만족하는 소수 p_1과 p_2를 선택해서 사용자의 서명키로 가진다. p_1과 p_2을 이용해서 modulus $n = p_1 p_2^2$을 계산해서 공개한다.

- 서명 생성:

$U = r^{v} \bmod n$

$V = (vr^{v-1})^{-1} \bmod p_2$

$F = Format_2(M)$

$S = r + (|(2^{2\pi}F - U/(p_1 p_2)| V \bmod p_2) p_1 p_2 \bmod n$

서명 값은 S가 된다.

- 서명 검증:

$F' = S^{v} \bmod n$

$F^{*} = Format_2(M)$

F'와 F^{*}가 같으면 유효한 서명으로 인정한다.

• NR [23]

Nyberg-Rueppel에 의해 제안된 메시지 복원형

전자서명 알고리즘이다.

- 도메인 변수:

1024 bits 정도의 큰 소수 p를 선택한다. $p-1$을 나누는 160 bits 정도의 소수 q를 선택한다. $GF(p)$ 상의 원소 중에서 위수가 q인 정수 G를 선택한다. $[2, q-2]$에서 서명키 x를 선택한다. 검증키는 다음의 두 가지 방식 중에 한 가지를 선택해서 생성한다. 첫 번째 방식은 검증키를 $Y = G^x \bmod p$로 계산한다. (이때는 P, Q를 다음과 같이 두자. $P := G$, $Q := Y$) 두 번째 방식은 검증키를 $Y = G^{x^{-1}} \bmod p$로 계산한다. (이때는 P, Q를 다음과 같이 둔다 $P := Y, Q := G$)

- 서명 생성:

본 고에서는 복원할 수 있는 메시지의 최대 길이를 L_{rec}로 정의한다. 그리고, 메시지 M은 충분히 길어서 복원할 수 있는 부분인 M_{rec}와 M_{clr}으로 나뉘는 것으로 본다. 이 보다 짧은 경우는 M 자체가 M_{rec}이 된다고 생각하면 된다.

$[2, q-2]$에서 임의의 정수 k를 선택한다.

$\Pi = P^k \bmod p$

$t = \Pi \bmod q$

$d = MSB(h(M), |q| - L_{rec}) \mid M_{rec}$

$r = d + t \bmod q$

$s = k - xr \bmod q$

서명 값은 (r, s)이다. M 대신에 M_{clr}을 보낸다.

- 서명 검증:

$\Pi' = P^s Q^{r'} \bmod p$

$t' = \Pi' \bmod q$

$d' = r' - t' \bmod q$

$M_{rec}' = LSB(d', L_{rec})$

$M' = M_{rec}' \mid M_{clr}$

$MSB(d', |q| - L_{rec})$와 $MSB(h(M'), |q| - L_{rec})$가 같으면 유효한 서명으로 인정한다. 이때 복구된 메시지는 M'이 된다.

• ECMR [22]

Miyaji에 의해 제안된 타원곡선을 이용하는 메시지 복원형 전자서명 알고리즘이다.

- 도메인 변수:

160 bits 위수 q를 가지는 타원 곡선으로 이루어지는 군을 선택한다. 서명키와 검증키 생성 방법은 NR과 일치한다. 다만 사용하는 군이 다르므로 $G^x \bmod p$ 방식의 연산을 타원곡선 위에서의 연산인 xG으로 바꾸어 준다.

- 서명 생성:

$[2, q-2]$에서 임의의 정수 k를 선택한다.

$\Pi = kP$

$t = h(\Pi)$

$d = MSB(h(M), |q| - L_{rec}) \mid M_{rec}$

$r = d \oplus t$

$s = (rk - r - 1)(x + 1) \bmod q$

서명 값은 (r, s)가 된다. M 대신에 M_{clr}을 보낸다.

- 서명 검증:

$\Pi' = ((1 + r' + s')/r')P + (s'/r')Q$

$t' = h(\Pi')$

$d' = r' \oplus t'$

$M_{rec}' = LSB(d', L_{rec})$

$M' = M_{rec}' \mid M_{clr}$

$MSB(d', |q| - L_{rec})$와 $MSB(h(M'), |q| - L_{rec})$가 같으면 유효한 서명으로 인정한다. 이때 복구된 메시지는 M'이 된다.

• ECAO [1]

Abe-Okamoto에 의해 제안된 타원곡선을 이용하는 메시지 복원형 전자서명 알고리즘이다.

- 도메인 변수:

ECMR의 도메인 변수와 키 쌍을 그대로 사용한다. 추가로 다음의 세가지 해쉬 함수를 사용한다.

$h_1: \{0,1\}^* \rightarrow \{0,1\}^{|q| - L_{rec}}$

$h_2: \{0,1\}^* \rightarrow \{0,1\}^{L_{rec}}$

$h_3: \{0,1\}^* \rightarrow [1, q-1]$

- 서명 생성:

$[2, q-2]$에서 임의의 정수 k를 선택한다.

$R = kP$

$d = h_1(M_{rec}) \| (h_2(h_1(M_{rec})) \oplus M_{rec})$

$r = d \oplus LSB(R_x, |q|)$

$\Pi = h_3(r \mid M_{clr})$

$s = k - x\Pi \bmod q$

서명 값은 (r, s)가 된다. M 대신에 M_{clr}을 보낸다.

- 서명 검증:

$\Pi' = h_3(r' \mid M'_{clr})$

$R' = s'P + \Pi' Q$

$d' = r' \oplus LSB(R_x', |q|)$

$M'_{rec} = LSB(d', L_{rec}) \oplus h_2(MSB(d', |q| - L_{rec}))$

$MSB(d', |q| - L_{rec})$와 $h_1(M'_{rec})$값을 비교해서 같을 경우 서명이 올바른 것으로 확인한다.

• ECKNR

한국에서 제안한 EC-KCDSA에 기반한 메시지 복원형 전자서명 알고리즘이다. ISO/IEC 9796-3의 다음 WD에서 포함될 예정이다.

- 도메인 변수:

160 bits 위수 q를 가지는 타원 곡선으로 이루어지는 군을 선택한다. $[2, q-2]$에서 서명키 x를 선택한다. 검증키는 $Y = (x^{-1} \bmod q)G$으로 계산 한다.

- 서명 생성:

$[2, q-2]$에서 임의의 정수 k를 선택한다.

$R = kY$

$\Pi = h(R)$

$d = MSB(h(M), |q| - L_{rec}) \mid M_{rec}$

$r = d \oplus \Pi \oplus h(h(Y_x \mid Y_y) \mid M_{clr})$

$s = k - x\,r \bmod q$

서명 값은 (r, s)가 된다. M 대신에 M_{clr}을 보낸다.

- 서명 검증:

$R' = s'P + r'Q$

$\Pi' = h(R')$

$d' = r' \oplus \Pi' \oplus h(h(Y_x \mid Y_y) \mid M'_{clr})$

$M_{rec}' = LSB(d', L_{rec})$

$M' = M_{rec}' \mid M_{clr}$

$MSB(d', |q| - L_{rec})$와 $MSB(h(M'), |q| - L_{rec})$가 같으면 유효한 서명으로 인정한다. 이때 복구된 메시지는 M'이 된다.

• DSA [4]

NIST에 의해 FIPS PUB 186으로 표준화된 메시지 부가형 전자서명 알고리즘이다. RSA와 함께 가장 많이 쓰이는 전자 서명 알고리즘의 하나이다.

- 도메인 변수:

1024 bits 정도의 큰 소수 p를 선택한다. $p-1$을 나누는 160 bits 정도의 소수 q를 선택한다. $GF(p)$상의 원소 중에서 위수가 q인 정수를 G로 선택한다. $[2, q-2]$에서 서명키 x를 선택한다. 검증키는 $Y = G^x$가 된다.

- 서명 생성:

$[2, q-2]$에서 임의의 정수 k를 선택한다.

$\Pi = G^k \bmod p$

$r = \Pi \bmod q$

$s = (k^{-1}(h(M) + xr)) \bmod q$

서명 값은 (r, s)가 된다.

- 서명 검증:

$a = s'^{-1}\, r' \bmod q$

$b = s'^{-1} h(M) \bmod q$

$\Pi' = Y^a G^b \bmod p$

r'과 Π' mod q의 값이 같으면 유효한 서명으로 인정한다.

• KCDSA [27]

TTA에 의해 표준화된 메시지 부가형 전자서명 알고리즘이다. DSA에 비해 효율적이고, random oracle model에서 안전도가 증명된 장점이 있다.

- 도메인 변수:

1024 bits 정도의 큰 소수 p를 선택한다. $p-1$을 나누는 160 bits 정도의 소수 q를 선택한다. $GF(p)$상의 원소 중에서 위수가 q인 정수를 G로 선택한다. $[2, q-2]$에서 서명키 x를 선택한다. 검증키는 $Y = G^{x^{-1}}$가 된다.

- 서명 생성:

[2, $q-2$]에서 임의의 정수 k를 선택한다.

$\Pi = G^k \bmod p$

$r = h(\Pi)$

$v = r \oplus h(LSB(Y, 512) \| M) \bmod q$

$s = x(k - v) \bmod q$

서명 값은 (r, s)가 된다.

- 서명 검증:

$v' = r' \oplus h(Y' \| M) \bmod q$

$\Pi' = Y^{s'} G^{v'} \bmod p$

r'과 $h(\Pi')$가 일치하면 유효한 서명으로 인정한다.

• Pointcheval-Vaudenay

DSA와 비슷한 전자서명 알고리즘이다. $h(M)$ 대신에 $h(r \| M)$을 사용하는 알고리즘이다. 이로 인해서 random oracle model에서 안전도가 증명되었다.

• EC-DSA

DSA의 타원곡선 버전이다. $GF(p)$상의 연산을 타원곡선 연산으로 대체하여 쉽게 얻을 수 있다.

• EC-KCDSA [28]

KCDSA의 타원곡선 버전이다. ISO/IEC IS 15946-2과 ISO/IEC WD 14888-3에 동시에 포함되어 있다. 이중 후자가 국내 표준과 일치한다. KCDSA와 기본 알고리즘은 일치하지만 사용하는 변수 등이 일부 다르다.

• EC-GDSA

독일 표준의 전자 서명 표준이다. EC-KCDSA와 키 생성은 같지만 서명 생성/검증이 조금 다른 알고리즘이다.

- 도메인 변수:

ECKNR과 같은 변수와 서명키, 검증키를 사용한다.

- 서명 생성:

[2, $q-2$]에서 임의의 정수 k를 선택한다.

$\Pi = kG$

$r = \Pi_x$

$s = x(kr - h(M)) \bmod q$

서명 값은 (r, s)가 된다.

- 서명 검증:

$a = r'^{-1} h(M) \bmod q$

$b = r'^{-1} s' \bmod q$

$\Pi' = aY + bG$

r'과 Π_x'의 값이 같으면 유효한 서명으로 인정한다.

• IBS-1 [11]

Hess에 의해 제안된 신원 기반의 전자서명 알고리즘이다. IBS-1과 IBS-2는 타원곡선 연산과 함께 다음의 Bilinear map을 사용한다. 이 연산은 주로 (modified) Weil (or Tate) pairing을 이용해서 구현된다.

- Bilinear map

G_1과 G_2를 큰 소수 q를 위수로 가지는 군이라고 하자. IBS-1에서 사용하는 map $e: G_1 \times G_1 \rightarrow G_2$은 다음 세 가지 성질을 만족해야 한다.

가. Bilinear: 모든 $P, Q \in G_1$와 $a, b \in Z$가 $e(aP, bP) = e(P, Q)^{ab}$를 만족한다.

나. Non-degenerate: G_1에서 항등원이 아닌 모든 $P, Q \in G_1$에 대해서 $e(P, Q)$는 G_2에서 항등원이 아니다.

다. Computable: 어떤 $P, Q \in G_1$에 대해서도 $e(P, Q)$를 계산하는 효율적인 알고리즘이 존재한다.

- 도메인 변수 생성:

큰 소수 q를 위수로 가지는 G_1과 G_2을 선택한다. 이 때 두 군 사이에는 bilinear map $e: G_1 \times G_1 \rightarrow G_2$이 존재해야 한다. [2, $q-2$]에서 임의의 정수를 선택해서 마스터 키 s로 삼는다. 군 G_1에서 임의의 원소 P를 선택한다. sP를 계산해서 P_{pub}로 한다. 다음의 두가지 암호학적 해쉬 함수를 선택한다: $h_1: \{0,1\}^* \rightarrow [1, q-1]$, $h_2: \{0,1\}^* \rightarrow G_1$.

- 개인키 추출:

사용자의 ID가 주어지면 누구나 $Q_{ID} = h_2(ID)$를

계산할 수 있다. 이 값이 사용자의 공개키 역할을 한다. 사용자의 개인 서명키는 $D_{ID} = sQ_{ID}$가 된다.

- 서명 생성:

$[2, q-2]$에서 임의의 정수 k를 선택한다.

$\Pi = e(D_{ID}, P)^k$

$r = h_1(M \| \Pi_x)$

$S = (k-r)D_{ID}$

서명 값은 (r, S)가 된다.

- 서명 검증:

$\Pi' = e(S', P)e(Q_{ID}, P_{pub})^{r'}$

$r^* = h_1(M \| \Pi_x')$

r'과 r^*가 같으면 유효한 서명으로 인정한다.

• IBS-2 [3]

Cha-Cheon에 의해 제안된 신원 기반의 전자서명 알고리즘이다.

- 도메인 변수 및 개인키 생성:

IBS-1과 같은 변수와 키들을 사용한다.

- 서명 생성:

$[2, q-2]$에서 임의의 정수 k를 선택한다.

$R = kQ_{ID}$

$t = h_1(M \| R_x)$

$S = (k+t)D_{ID}$

서명 값은 (R, S)가 된다.

- 서명 검증:

$t' = h_1(M \| R_x')$

$e(P, S')$의 계산 결과와 $e(P_{pub}, R' + t'Q_{ID})$의 계산 결과가 같으면 유효한 서명으로 인정한다.

V. 결 론

본 고에서는 ISO/IEC JTC1/SC27에서 표준화 중인 전자 서명 알고리즘들을 살펴보았다. 이 소위원회를 통해서 다양한 전자 서명 알고리즘이 현재 표준화 되었거나 표준화 중임을 알 수 있었다. 그리고 국내에서 제안한 알고리즘도 많이 포함되어 있음을 알 수 있다.

이런 작업을 원활히 하기 위해 보다 많은 국내 전문가들의 참여가 요구된다. 이를 통해 국제 표준 기구 내에서의 대한민국의 위상 강화와 국내 기술의 국제 표준화라는 두 가지의 결실을 모두 얻게 되기를 기대한다.

참 고 문 헌

[1] M. Abe and T. Okamoto, "A signature scheme with message recovery as secure as discrete logarithm", Asiacrypt '99, LNCS 1716, pp. 378-389, Springer-Verlag, 1999.

[2] M. Bellare and P. Rogaway, "The exact security of digital signatures: How to sign with RSA and Rabin", Eurocrypt '96, LNCS 1070, pp. 399-416, Springer-Verlag, 1996.

[3] J. C. Cha and J. H. Cheon, "An identity-based signature from gap Diffie-Hellman groups", PKC 2002, LNCS 2567, pp. 18-30, Springer-Verlag, 2002.

[4] FIPS PUB 186, "Digital Signature Standard", U.S. National Institute of Standards and Technology, 1994.

[5] A. Fujioka, T. Okamoto and S. Miyaguchi, "ESIGN, an efficient digital signature implementation for smart cards", Eurocrypt '91, LNCS 547, pp. 446-457, Springer-Verlag, 1992.

[6] M. Girault, "Self-certified public keys", Eurocrypt '91, LNCS 547, pp. 490-497, Springer-Verlag, 1992.

[7] M. Girault and J. C. Pailles, "On-line / off-line RSA-like", Workshop on Cryptography and Coding, 2003.

[8] L.C. Guillou and J.-J. Quisquater, "A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory", Eurocrypt '88, LNCS 330, pp. 123-128, Springer-Verlag, 1988.

[9] L. C. Guillou and J.-J. Quisquater, "A paradoxical identity-based signature scheme resulting from zero-knowledge", Crypto '88, LNCS 403, pp. 216-231, Springer-Verlag, 1988.

[10] L.C. Guillou, M. Ugon and J.-J. Quisquater, "Cryptographic authentication protocols for smart cards", Computer Networks Magazine, Vol 36, pp. 437-451, North Holland Elsevier Publishing, 2001.

[11] F. Hess, "Efficient identity based signature schemes based on pairings", SAC 2002, LNCS 2595, pp. 310-324, Springer-Verlag, 2002.

[12] ISO/IEC IS 9796-2: 2002, "Information technology - Security techniques - Digital signature schemes giving message recovery - Part 2: Integer factorization based mechanisms (revision)", ISO/IEC JTC1/SC27, 2002.

[13] ISO/IEC IS 9796-3: 2000, "Information technology - Security techniques - Digital signature schemes giving message recovery - Part 3: Discrete logarithm based mechanisms", ISO/IEC JTC1/SC27, 2000.

[14] ISO/IEC 1st WD 9796-3: 2003, "Information technology - Security techniques - Digital signature schemes giving message recovery - Part 3: Discrete logarithm based mechanisms (revision)", ISO/IEC JTC1/SC27, 2003.

[15] ISO/IEC IS 14888-1: 1999, "Information technology - Security techniques - Digital signatures with appendix - Part 1: General", ISO/IEC JTC1/SC27, 1999.

[16] ISO/IEC IS 14888-2: 1999, "Information technology - Security techniques - Digital signatures with appendix - Part 2: Identity-based mechanisms", ISO/IEC JTC1/SC27, 1999.

[17] ISO/IEC IS 14888-3: 1999, "Information technology - Security techniques - Digital signatures with appendix - Part 2: Certificate-based mechanisms", ISO/IEC JTC1/SC27, 1999.

[18] ISO/IEC 1st WD 14888-2: 2004, "Information technology - Security techniques - Digital signatures with appendix - Part 2: Integer factorization based mechanisms (revision)", ISO/IEC JTC1/SC27, 2004.

[19] ISO/IEC 1st WD 14888-3: 2004, "Information technology -Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms (revision)", ISO/IEC JTC1/SC27, 2004.

[20] ISO/IEC IS 15946-2: 2002, "Information technology - Security techniques - Cryptographic techniques based on elliptic curves: Part 2 - Digital signatures", ISO/IEC JTC1/SC27, 2002.

[21] ISO/IEC FDIS 15946-4: 2002, "Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 4: Digital signatures giving message recovery", ISO/IEC JTC1/SC27, 2002.

[22] A. Miyaji, "Another Countermeasure to Forgeries over Message Recovery Signature", IEICE Trans., Fundamentals, vol. E80-A, No.11(1997), pp. 2192-2200, 1997.

[23] K. Nyberg and R. A. Rueppel, "Message recovery for signature schemes based on the discrete logarithm problem", Designs Codes and Cryptography, 7(1996), pp. 61-81, 1996.

[24] G. Poupard and J. Stern, "Security analysis of a practical "on the fly" authentication and signature generation", Eurocrypt '98, LNCS 1403, pp. 422-436, Springer-Verlag, 1998.

[25] M. O. Rabin, "Digital signatures and public-key functions as intractable as

factorization", Technical Report MIT/LCS/TR-212, MIT Laboratory for Computer Science, January 1979.

[26] R. L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", in Communications of the ACM, vol 21-2, pp. 120-126, 1978.

[27] TTAS.KO-12.0001/R1, "부가형 전자서명 방식 표준 - 제2부 : 인증서 기반 전자서명 알고리즘", 한국정보통신기술협회 (TTA), 2000.

[28] TTAS.KO-12.0015, "부가형 전자서명 방식 표준 - 제3부 : 타원곡선을 이용한 인증서 기반 전자서명 알고리즘", 한국정보통신기술협회 (TTA), 2001.

〈著 者 紹 介〉

이 필 중 (Pil Joong Lee)
정회원

1974년 2월 : 서울대학교 전자공학과 학사
1977년 2월 : 서울대학교 전자공학과 석사
1982년 6월 : U.C.L.A System Science, Engineer
1985년 6월 : U.C.L.A Electrical Engineering, Ph.D.
1980년 6월~1985년 8월 : Jet Propulsion Laboratory, Senior Engineer
1985년 8월~1990년 2월 : Bell Communications Research, M.T.S.
1990년 2월~현재 : 포항공과대학교 전자전기공학과 교수
1996년 2월~1997년 2월 : NEC Research Institute 방문 연구원
2000년 9월~2003년 8월 : 포항공과대학교 정보통신연구소 연구소장 (정보통신대학원장 겸임)
2004년 1월~2004년 12월 : 한국정보보호학회 회장
2004년 1월~2004년 12월 : 한국통신 연구소 방문연구원
〈관심분야〉 정보보호전반

박 동 진 (Dong Jin Park)
학생회원

2000년 2월 : 포항공과대학교 전자전기공학과 학사
2000년 3월~현재 : 포항공과대학교 전자전기공학과 박사과정
〈관심분야〉 정보보호, 암호이론, 알고리즘 구현