An Efficient Variant Signature Scheme on ECDSA

[1]M.Prabu and [2]R.Shanmugalakshmi
[1]Anna University-Coimbatore, Tamil Nadu, India.
[2]Department of CSE, Government College of Technology, Coimbatore, India
prabu_pdas@yahoo.co.in

***Abstract*- This paper describes a new variant level of Signature Scheme on ECDSA. In support of this scheme, a study of on a number of schemes was done. The number of scheme includes Lamport, Schnorr, DSA etc., In this study three schemes, DSA, ECDSA and Variant ECDSA are taken for a comparative study. From that comparison, the paper tries to develop a new scheme on ECDSA. Finally, It was found out that, Variant signature on ECDSA is better than other schemes. . We give a brief preamble to the Signature Algorithm in chapter 1 and then give the Concepts of the Elliptic Curve version of DSA. Finally a Variant of ECDSA will be given in chapter 9.**

***Keywords*- DSA, Lamport, Schnorr, ECDSA, Signature Scheme**

I.INTRODUCTION

The term "Signature" is used to establish the initial level of security. The person should send message with his Signature. It is one kind of authentication and security. The Digital Signature Algorithm was specified and converted to standard level by U.S Federal Information Processing Standard. This level is called as Digital Signature Standard. Its security is backed on the computational intractability of the DLP in prime order.

A. Signature Schemes

A Signature Scheme, which is also called Digital Signature. A Signature Scheme is a method of signing a message stored in electronic form. The Signature Schemes can be classified into two components, First, a Signing Algorithm which permits a user to sign in a message securely and Verification Algorithm which permits to verify the signed message. It is a well-know fact that, Digital Signature can be verified using Verification Algorithm. Anyone cane verify a digital Signature.

A Signature is part of the physical document being singed. Conventional Signature holds a copy of a singed paper document can usually be same form the original message

Though the conventional Signature has the same resemblance of the digital Signature. The ECDSA is the elliptic curve analogue of the DSA.

II. HASH FUNCTIONS

Hash function can provide assurance of data integrity.

A. Hash functions properties

A common method for realizing a MAC is the use a so called keyed hash function techniques. A MAC (Message Authentication Code) can be created and verified using a keyed hash Techniques. A hash function is a deterministic function which maps a bit string of an arbitrary length to a hashed value, which is a bit string of a fixed length.[10]

Mixing Transformation

In any input x, the output hashed value h(x) should be computationally indistinguishable from a uniform binary string in the interval $(0, 2^{|h|})$.[10]

Collision resistance

It should be computationally infeasible to find two inputs x, y with x=y such that h(x) =h(y).

Pro-Image resistance

Given hashed value h, it should be computationally infeasible to find an input string x such that h=h(x).

Practical efficiency

Given input string x, the computation of h(x) can be done in time bounded by a small degree polynomial in the size of x.The mixing transformation and collision-resistance properties of a hash function can be realized by using operations similar to those used in the design of a block of cipher Algorithm.[10]

III.HASH WITH MESSAGE DIGEST

Always, Signature schemes widely entreated with very fast public cryptographic hash function. The hash function h= {0, 1}*→ Z[8]. It will take a message arbitrary length and procedure a message digest of a specified size. The message digest of a specified using a Signature scheme like (P, A, K, S, V) where Z≤ P. In case, Alice keen to sign a message x, which is a bit string of arbitrary length, she first construct the message digest Z=h(x) and then computer the Signature on Z namely $y=sig_k(z)$[12]

Message	**x**	**x ε {0, 1} ***
Message Digest	z=h(x)	x **ε** Z
Signature	$y=sig_k(z)$	y**ε** Y

IV. ELGAMAL SIGNATURE SCHEME

ElGamal Signature scheme, which was described in 1985. A modification of this scheme has been adopted as the Digital Signature scheme (or DSA) by the National Institute of standards and Technology (NIST)[7]. ElGamal works out an ingenious digital Signature schemes. At the same time ElGamal public-key cryptosystem inspiring great follow-up research and application interest for now a days. It is also origin of many further digital Signature schemes which belong to the family of ElGamal Signature schemes. The ElGamal Signature is non-deterministic. This means that there are many valid Signatures for any size of given message and the Verification must be able to accept any of these valid Signature as authentic[2].

Generation Phase:
Domain parameters (n, o, m, x)
Public Key: (n, o, m)
Private Key: x

Select K € Z_{p-1} k, $m=o^x \bmod n$

Signature Algorithm:

$Sig_b (a, b) = (\delta, \gamma)$

$\gamma= o^b \bmod n$
$\delta= (a-x\ \gamma)^{k-1} \bmod (n-1)$

Verification Algorithm:

$Ver_b (a, (\delta, \gamma) \leftrightarrow m^{\gamma} \gamma^{\delta}=o^a \bmod n$

V. SCHNORR SIGNATURE SCHEME:

The Schnorr Signature scheme modifies the ElGamal Signature scheme in an ingenious way so that a log 2 q-bit Signature, but the computations are done in Z_p.Key sizes were similar to the ElGamal key sizes. The Schnorr Scheme integrates a hash function directly into the Signing Algorithm[5][4].

Generation Phase:
Parameters for Schnorr (n, o, x, m, s)
Public key: {n, o, m, s}
Private Key: {x}

Signing Algorithm:
$Sig_b (a, b) = (\delta, \gamma)$

$\gamma= h (x|| o^b)$

$\delta= b+x\ \gamma \bmod s$

Verification Algorithm:

$Ver_b (a, (\delta, \gamma) \leftrightarrow h (x|| o^{\delta} m^{-\gamma}) = \gamma=$ true

VI. LAMPORT SIGNATURE SCHEME

A simple way to construct a provably secure one-time Signature from a one-way function. The one-way Signature scheme based on an arbitrary one-way function. The Scheme, which is known as one-time Signature.[1][10]

One-way Algorithm
Let K be a positive integer and let P= {0, 1}* suppose f .Y→ Z is a one-way function and let $A =Y^k$.
Let $y_{i,j} \in Y$ be chosen at random, 1≤i≤k; j=0,1 and let $z_{i,j} =f(y_{i,j})$,1≤i≤k,j=0,1.
For k= ($y_{i,j}$, $z_{i,j}$: 1≤i≤k, j=0, 1) define
Signing Algorithm

$Sig_k(x_1 \ldots x_k) = (y_1, x1\ldots\ldots\ldots\ldots..y_k,x_k)$.

A Signature ($a_1,\ldots\ldots a_k$) on the message ($x_1,\ldots x_k$) is verified as follows

Verification Algorithm:
$Ver_k ((x_1\ldots x_k), (a_1\ldots a_k)) =$true↔ f(ai)= z_i,x_i, 1≤i≤k.

It is quite elegant, But it is not of practical use one problem is the size of the signature produces.

VII. DIGITAL SIGNATURE SCHEME

The DSA (Digital Signature Algorithm) was proposed in August 1991 by U.S. National Institute of Standards and Technology (NIST)[9] and was specified in a U.S. Government Federal Information Processing Standard (FIPS 186) called the Digital Signature Standard (DSS). The DSA can be viewed as a variant of the ElGamal Signature scheme. Its security is based on the intractability of the discrete logarithm Problem in prime-order subgroup of (Z/*p*Z) ×.[3]

.

Digital Signature Algorithm:

Generation Phase:
Select p, q, x, q|p.1, and 1 ≤ x < q. Select h € [1, p.1], compute
$g = h^{(p.1)/q} \pmod p$
$y = g^x \pmod p$
Public key: (p, q, g, y),
Private Key: {x}
Signing Algorithm:
$r = (g^k \bmod p) \pmod q$
$s = k^{-1}(H (m) +xr) \pmod q$
(r, s) is the Signature of m.

Verification Algorithm:
$w = s^{-1} \pmod q$
u1 = H (m) w (mod q)
u2 = rw (mod q)
$v = (g^{u1}y^{u2} \bmod p) \pmod q$
v = r→accept the Signature.

VIII. ECDSA: ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM

The Elliptic Curve Digital Signature Algorithm (ECDSA) is a variant of the Digital Signature Algorithm (DSA) which uses Elliptic curve cryptography.

Generation Phase:
Select Ep(a,b), x, and $1 \leq x < n$.
Select G ϵ Ep(a,b) with order n and compute Q = dG
Public key: (Ep(a,b), p,G,n,Q)
Private Key: x

Signature Algorithm
Select k, $1 \leq k < q$.
kG = (x1,y1), r = x1 (mod n)
$s = k^{-1} (H(m)+xr) \pmod n$
(r, s) is the Signature of m.

Verification Algorithm
$w = s^{-1} \pmod n$
u1 = H(m)w (mod n)
u2 = rw (mod n)
u1G+u2Q = (x2,y2),
$v = x_2 \pmod n$
v = r→ accept the Signature.

IX. VARIANT ON ECDSA

Scheme:

Select E_p (a,b), x, and $1 \leq x < n$.
Select G ϵ E_p(a,b) with order n and compute
Q = dG
Public key: (Ep(a,b), p,G,n,Q)
Private Key: x
Signature Algorithm:
Select k1, k2, $1 \leq k1, k2 < n$.
k1G = (x1, y1), r1 = x1(mod n)
k2G = (x2,y2), r2 = x2(mod n)
$s = k^{-1} + (H(m)k2+x(r1 .r2)) \pmod n$
(r1, s) is the Signature of m.

Verification Algorithm:
$w = s^{-1} \pmod n$
u1 = H(m)wk2(mod n)
u2 = (r1 .r2)w(mod n)
u1G+u2Q = (x3,y3),
$v = x_3 \pmod n$
v = r1 → accept the Signature.

X. ANALYSIS OF SIGNATURE SCHEMES

	DSA	ECDSA	Variant ECDSA
Generation Syntax	Select p, q, x, q|p.1, and $1 \leq x < q$. Select h ε [1, p.1], compute $g = h^{(p.1)/q} \pmod p$ $y = g^x \pmod p$	Select Ep(a,b), x, and $1 \leq x < n$. Select G ε Ep(a,b) with order n and compute Q = dG public key : (Ep(a,b), p,G,n,Q) private key : x	Select Ep(a,b), x, and $1 \leq x < n$. Select G εEp(a,b) with order n and compute Q = dG public key : (Ep(a,b), p,G,n,Q) private key : x
Signature Algorithm	Public key: (p, q, g, y) Private Key: {x} Signing Algorithm: $r = (g^k \bmod p) \pmod q$ $s = k^{-1}(H(m)+xr) \pmod q$(r, s) is the Signature of m.	Select k, $1 \leq k < q$. kG = (x1,y1), r = x1 (mod n) $s = k^{-1} (H(m)+xr) \pmod n$ (r, s) is the Signature of m.	Select k1, k2, $1 \leq k1, k2 < n$. k1G = (x1,y1), r1 = x1(mod n) k2G = (x2,y2), r2 = x2(mod n) $s = k^{-1} + (H(m)k2+x(r1 .r2)) \pmod n$ (r1, s) is the Signature of m.
Verification Algorithm	$w = s^{-1} \pmod q$ u1 = H (m) w (mod q) u2 = rw (mod q) $v = (g^{u1}y^{u2} \bmod p) \pmod q$ v = r→accept the Signature.	$w = s^{-1} \pmod n$ u1 = H(m)w (mod n) u2 = rw (mod n) u1G+u2Q = (x2,y2), $v = x_2 \pmod n$ v = r→ accept the Signature.	$w = s^{-1} \pmod n$ u1 = H(m)wk2(mod n) u2 = (r1.r2)w(mod n) u1G+u2Q = (x3,y3) $v = x_3 \pmod n$ v = r1 → accept the Signature.

Why Variant ECDSA scheme is better than other scheme:

This scheme says,

Variant ECDSA generated Signature (r1, s1) and (r1, s2) on two different messages m1 and m2 with same security key k1, k2. We implemented to two levels of digital Signatures because the process is a complex one. It also makes to increase our security level.

XI. CONCLUSION

We compare the performance of ECDSA with securely Variant ECDSA in the way of Signing Algorithm and Verification Algorithm. In this Variant ECDSA, we introduced a two-level-value in Verification and Signing Algorithms. In existing ECDSA, it is used to bind a single value in Verification and Signing Algorithm. The variant ECDSA is interacted with two values and compared with the same level of computation time. The above information is useful for next generation security level on ECDSA.

XII. .ACKNOWLEDGEMENT

We thank for the anonymous reviewers of this paper for their valuable comments, and they are reflected on the final version of this paper.

REFERENCES

[1]. D. Johnson and A. Menezes (August 1999)" "The Elliptic Curve Digital Signature Algorithm (ECDSA)," *Technical Report CORR* 99-34, Centre for Applied Cryptograpic Research (CACR), University of Waterloo

[2]. Hung-Zih Liao and Yuan-Yuan Shen "On the Elliptic Curve Digital Algorithm" Tunghai Science Vol.8:109-126

[3]. National Institute of Standards and Technology, *Digital Signature Standard*, FIPS Publication 186, 1994.

[4]. National Institute of Standards and Technology (1997), *Entity Authentication using Public Key Cryptography*, FIPS Publication 196.

[5]. C. Schnorr (1991), "Efficient signature generation by smart cards," *Journal of Cryptology*, 43, 161-174.

[6]. NIST (2001), "Digital Signature Standard," *FIPS* 186-2, http://csrc.nist.gov/ publiscations/fips/fips186-2/fips186-2-change1.pdf,

[7] NIST (2002), "Secure Hash Standard," *FIPS PUB* 180-2, http://csrc.nist.gov/publiscations/fips 2/fips180-2withchangenotice.pdf,

[8]. NIST (2003), "Recommendation on Key Management," *DRAFT Special Publication* 800-57,http://csrc.nist.gov/CryptoToolkit/kms/guideline-1-Jan03.pdf, .

[9]. M. Rabin (1979), "Digitalized signatures and public-key functions as intractable as factorization," *MIT/LCS/TR-212, MIT Laboratory for Computer Science*.

[10]. Douglus R.Stinson "Cryptography theory and practice ", chapman, hall Publichsers.2002

[11]. D. Galindo, S. Martin and J.L. Villar (2004), "Evaluating elliptic curve based KEMs in the light of pairings," http://eprint.iacr.org/2004/084.pdf.

[12] William Stallings "Cryptography and Network Security", 4th Edition,