International Journal of Engineering & Technology, 7 (2.32) (2018) 264-268

SPC

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

MSEC Scheme for Providing Secure Data Transformation Using Coding Technique

Ram Kumar.J[1], Veena Avutu[2], Anurag.V[3]

[1,2,3]Department of CSE, K L E F, Vaddeswaram, Guntur, Andhra Pradesh, India
**Corresponding author E-mail: ramkumar@kluniversity.in*

Abstract

The MSEC which is the short from of Multiple Signature Elliptic curve Algorithm by using coding tchnique. It can be Digital Signature Algorithm (DSA) elliptic curve analogue. In 1999, the acknowledgement done such as standard of the ANSI. After that in 2000, it again acknowledged like benchmarks of the IEEE as well as NIST. Like this it again acknowledged in the year 1998 in the name of standard of ISO, as well as it was under thought to incorporate in some of other principles of ISO. unlike logarithm of standard discrete problem as well as number of issues of factorization, none of the calculation of the sub exponential-time can called to issue of the elliptic bend discrete logarithm. Similarly per-keybit quality can be generously much prominent if consider the calculation which uses bends of elliptic. This implemented system if or executing the ANSI X9.62 ECDSA on the bend of elliptic P-192, as well as talking regarding the relevant V of the security. Classes A as well as Subject D.4.6v Descriptors which is Operating Systems: Security as well as Protection – getting for controlling, control of the confirmation cryptographic; E.3 [Data]:cryptosystem of the Data Encryption which is the Public key and standards. Algorithms, of the General Terms Security.

***Keywords**: DSA, ECDSA. 1, integer factorization, elliptic curve cryptography, discrete logarithm problem.*

1. Introduction

Identity of the Cryptography: component e ε G exists, which known as character, to the extent of a*e= e * a = a to the G ε a each one. 4. converse Presence: to the a ε G each one having component i.e b ε G which having goal end i.e a * b = b * a = e. So the backwards of a is the component b. in addition to gather G called as abelian when a * b = b * a to a, G and a each. Here cryptology managing branch which having the calculations outline to encrypt as well as unscramble, that ae planning for guaranteeing mystery and message legitimacy. DSA stated in the year 1991 in U.S.NIST which is the short form of National Institute of Standards and Technology determining Government of the U.S. Standards of the Federal Information Processing i.e IPS 186 known like DSS which is Digital Signature Standard. The security depending on discrete logarithm issue computational obstinacy (DLP) in Zp * prime-arrange subgroups. plans of Advanced mark are intending for giving partner of the computerized for manual written marks. In the mark plan of the advanced must be non-forgeable existentially on the chosenmessage of assault. The small key size of EC-DSA, that prompting the calculation time of speedier as well as diminishment in the power of the preparing, room of the storage as well as capacity of the data transfer. It making perfect ECDSA to gadgets which are obliged, for an illustration, mobile phones pagers as well as cards of the shrewd. The ECDSA which is short form of Elliptic Curve Digital Signature Algorithm was bend of elliptic DSAmple. In year 1992, the first implemented system is the ECDSA of Scott Vanstone since NIST's asking to open remarking over its 1st proposition to the DSS. This can acknowledged in the year 1998 like the ISO standard, after that in the year 199, acknowledged like ANSI which is the short form American National Standards Institute i.e ANSI X9.62; as well as recognized like IEEE which is the short form of Institute of Electrical and Electronics Engineers i,e IEEE 1363-2000 in the year 2000. As well as the standard of FIPS i.e FIPS 186-2 planning of the Digital mark may use for giving to accompany administrations of the basic cryptographic: data uprightness root of the information validation which is non-denial. In implemented paper, 1st we start plans of the cryptography in the light no of factorization (IF) as well as logarithm of discrete (DL) in the segment of 2. In the area of 3, we discussed regarding the ECC clearly. In the segment of 4, we demonstrating execution as well as results. Facilitate in the area of 5 as well as 6 we are looking finishing up the separately.

2. Schemes of Cryptographic

2.1 Integer Factorization

$$n = p * q \tag{1}$$

It can be difficult for n to give p & q. Hence it is infeasible for deciding P & q for given n. RSA is the one of good calculation method. this algorithm given as per following

1. Take 2 extensive prime numbers, p & q which are 1024 bit

2. Register the n = p * q and z = (p-1) * (q-1).

3. Select a number, e, with no fundamental variables, d, to the such extent which is e * d - 1 can separable with z. in general key people is matching of (n, d) numbers . After: c = me mod n (2) instant message the encryption done, c m = album mod n (3)that needed use of private key, (n, d). To take the Integer Factorization

problem is the Field Sieve Number i.e calculation a of the subexponential & running of time is exp[1.923*(log n)1/3*(log log n)2/3] [2].

2.2 Discrete Logarithm

A loga(b) which is the normal logarithm which is condition a x = b answer over the numbers of the complex.When g & h are G components then x condition is g x = h call as discrete logarithm into a fundamental g of h to gather G, i.e. log(g(h)). The gathering operation * characterized over G sets.

1. **Conclusion:** (a * b ε G) to each one a, b ε G.

2. **Associativity**:{ a * (b * c) = (a * b) * c} to every a, b ε G.

3. **Presence** for G request means the G quantity.

The problem of this discrete logarithm is for discovering the n-1, along goal end gx = h (mod p), to give g ε Z*p of the request of n and h ε Z*p. have running of time {exp[1.923*(log n)1/3*(log log n)2/3]} [2].

3. Cryptography of an Elliptic Curve

ECC vented by Neal Koblitz& Victor Miller in the year 1985. ECC is discrete logarithm cryptography relative. Fig 1 represents the elliptic bend E on Zp that can framework of the Cartesian arrange with shape condition : y 2 ={x 3 + hatchet + b (8) E(Zp)} set comprising focuses (x, y), (x ε Zp),(y ε Zp),. Each b offers another bend of elliptic. For developing the bend of ellipse the gatherings as well as limited fields, are basics.

3.1 Groups A group for an operation

*G element paris describes it.. The functions satisfying the below properties:

Closure: (a * b ε G) to each a, b ε G. **Associativity**: {a * (b * c) = (a * b) * c} to each a, b ε G.

Identity Existence: e and G, known as identity, so e * a = a * e = a to each a ε G.

inverse Existence: Every a ε G here b ε G so a * b = b * a = e. b knowns as a inverse.

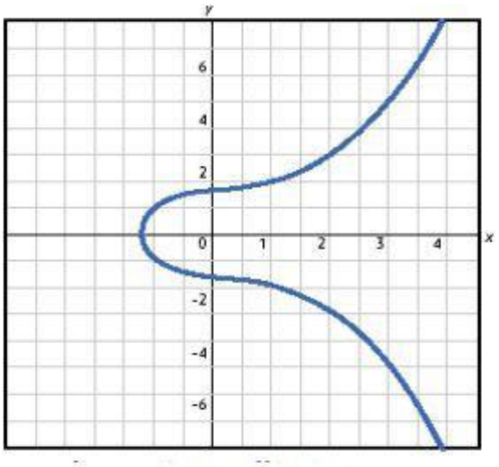


Figure 1. An Elliptic Curve

3.2 Finite Field

The field of finite having the elements set together along with the multiplication, & addition that fulfill the properties of the certain arithmetic. d. When q=pm here p represents prime & m represents the positive integer, so p known as the Fa characteristic as well as m known as Fq extension.

3.2.1 Fp - Prime Field Assume p is Prime Number.

Fp known as prime field, having integers set [{0,1,2,….,p-1}] along through below arithmetic operations:

Addition: When a, b ε Fp now a+b=r, here r - remainder If a+b divided with p & 0 ≤ r ≤ p-1 called like p - addition modulo.

Multiplication: When a, b ε Fp Now a.b=s, Here s - remainder If a.b divided with p as well as (0 ≤ s ≤ p-1)called as multiplication of modulo p

Inversion: in Fp, a is non 0 elements than a inverse is modulo p_, represented with a-1 , which c a unique integer ε Fp to a.c=1

3.2.3 Domain Parameters

The ECDSA domain parameters having chosen E elliptic curve represented on Fq of p, as well as a fundamental point G ε E(Fq). parameters of the Domain is either shared with entities groups, or particular to the one user. For summarizing, parameters of the domain comprises of:

1. a - size of field q, here q=p, is odd or prime, or q=2m

2.FR sign represented for Fq elements 3. 2 elements of field s a &b in the Fq having equation for elliptic curve E on Fq' (i.e., y2 = x 3 + ax + b in the case p>3, and y2 + xy = x3 + ax + b in the case p=2)

4. G=(xG, yG) is finite points of the order of prime in E(Fq)

5. ε order point G, along n>2160 & n>4√q

6. cofactor h= #E(Fq)/n

3.3 Elliptic Curves functions On Finite Fields

The major functions is the Point multiplication that obtained with 2 fundamental curve of elliptic operations. addition of the

1. Point, addition of 2 points J & K for obtaining other point L L= J + K,

Here one inversion as well as three multiplication requires.

2. doubling of the Point, add a J point to itself for getting other L point L = 2J,

Here one inversion as well as four multiplication requires

3.3.1 Addition of the Point

Means adding 2 points i.e J& K over curve of elliptic for getting other L point on similar one .

Assume J a K are 2 points curve of the over elliptic represents on the Figure 2.

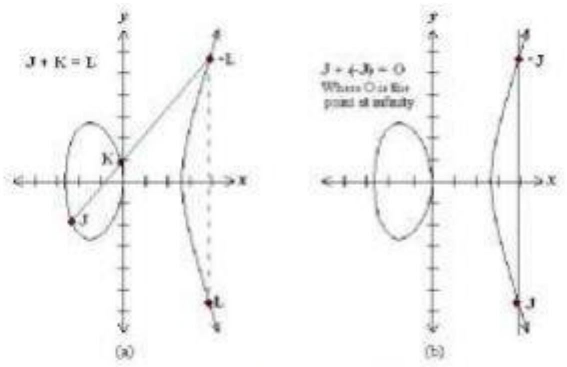


Figure 2. Point Addition

3.3.2 Doubling of Point

Point doubling means adding J point which is presented on curve of elliptic to itself for obtaining other L point on same curve of elliptic. For doubling a J point for getting L, means finding L = 2J, Take J point over curve of the elliptic represented in Fig 3. When J point y coordinate is not a zero . So that J tangent line intersecting the curve of elliptic exactly on one or more L point. The L point reflection the with respecting to the x-axis provides L point, that is doubling the point J result that is L = 2J. When Point J, y coordinate is 0 when tangent at the point of intersects O infinity. Therefore 2J = O If yj=0. Fig represents the doubling of point

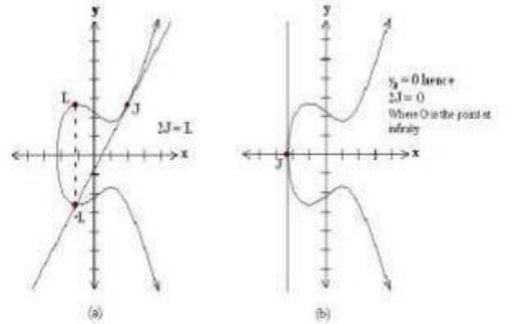


Figure 3. Point Doubling

3.3.3 Formulae for Algebraic

Fp (P+O=O+P=P) for P ε E(Fp) If P=(x, y) ε E(Fp) now {(x, y)+(x,-y)}=O. {(–P is the point denoted by (x,-y)}, known as P negative, identify the –P is point on curve. addition of the Point

Assume P={(x1, y1) ε E(Fp) }& Q={(x2, y2) ε E(Fp)} , here P≠ ± Q. Now P+Q={(x3, y3)} here x3= [{(y2-y1)/(x2-x1)}2 – x1-x2] & y3= [{(y2-y1)/(x2-x1)}(x1- x3) –y1] doubling the Point Assume P={(x1, y1) ε E(Fp)} here P≠ -P. now 2P=(x3, y3) here x3=[{(3x1 2 +a)/2y1} 2 -2x1] & y3=[{(3x1 2 +a)/2y1} 2 (x1-x3) –y1]

3.3.4 Formulae for Algebraic

Over F2 m{ P+O=O+P=P} to each P ε E(F2 m) When P={(x, y) ε E(Fp)} then {(x, y)+(x, -y)}=O. ((x, -y) point denotes by –P, known P negative, identify –P as the point of indeed on curve. Addition of point Assume P={(x1, y1) ε E(F2 m)} & Q={(x2, y2) ε E(F2 m) }, Here (P≠ ± Q). Now P+Q={(x3,y3)} here x3= [{(y2+y1)/(x2+x1)}2 + {(y2+y1)/(x2+x1)}+ x1 + x2 +a] where y3= [{(y2+y1)/(x2+x1)}(x1+x3) +x3 + y1]Doubling of Point Assume P={(x1,y1) ε E(F2 m)} here P≠ -P. Then 2P={(x3,y3)} here x3={x1 2 +(b/ x1 2)} & y3={x1 2 +{x1+(y1/x1)}x3 + x3}

4. Results & Implementation

Algorithm of the Elliptic Curve Digital Signature is for over elliptic curve P-192 can be mandate with the help of the ANSI X9.62 in the language C. To create a domain parameters, key generation, generation of signature as well as verification of signature over curve of the elliptical, this implemented system having the required modules. generation of key, ECDSA have three phases signature generation, key generation and :A is the key pair which is the entity associating with the parameters for EC set domain D= (q, FR, a, b, G, n, h). Every entity of A follows:

1. Choose an integer d randomly in the[1, n- 1] e interval.

2. Q = dP. - Compute

3. where Q = public key of A's , d = private key o f A's

Signature Generation of the ECDSA:. For signing m which is the message, A is entity along with parameters of domain D={ (q, FR, a, b, G, n, h) } as follow:

1. Choose a random integer i.e k in{ [1, n-1]} interval .

2. Computing the kP =(x1, y1) & r= (x1 mod n) .

When (r= 0) afterwards back to the 1st step.

3.(k -1)mod n. - Compute

4. s= [k -1 {h (m)+ dr}] mod n Computing Here h is SHA-1. When s = 0, then back to 1st step.

5. The message m signature first integers pair (r, s).

Verification ECDSA Signature:

For verifying A's signature i.e (r, s) on the m, B provides A's domain parameter authenticated copy D ={ (q, FR, a, b, G, n, h) & Q} public key as well as follow

1. Verify r as well as s integers in {[1, n-1]} interval

2. w = {s -1mod n & h (m)} Computing

3. u1 ={ h(m)w mod n} & u2 ={ rw mod n}. Computing

4. (u1P + u2Q) =(x0, y0) & v= (x0 mod n) computing

5. Accepting signature v = r only.

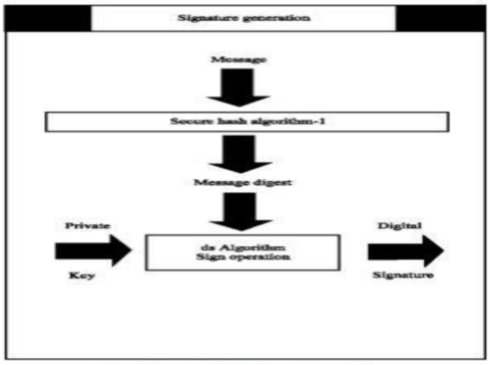


Figure 4. Signature Generation

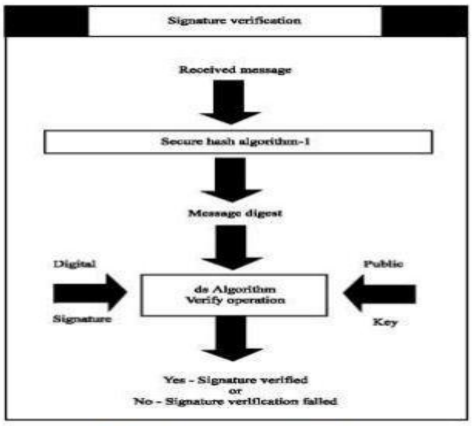


Figure 5. Signature Verification

Results

In given results are for highlighting to provided values set. Result of the SHA-1 represented with set keys of private as well as public SHA–1 of Input: “a”

Output of the SHA:
86f7e437faa5a7fce15d1ddcb9eaeaea377667b8 Input: “ABC”
Output of the SHA:
3c01bdbb26f358bab27f267924aa2c9a03fcfdb8 Generation of the Key Pair: 198 bit random key which is private as well as corresponding

5. RSA and DSA Comparision

this tough to do two types of operations one is forward operation that is tractable, second one is inverse operation that is intractable. The difference degree among these depends on key pairs size. exponential increase in inverse operation linear increase in forward operation and size of key increases represented in Figure 6.

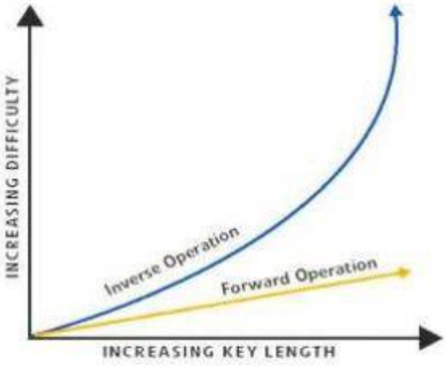
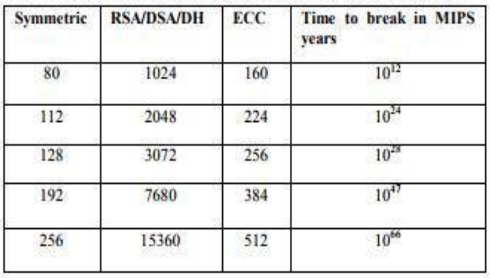


Figure 6. Difficulty of forward, inverse operation against key length

5.1 Table Represents ECC & RSA Comparisondsa

Table 1 Key comparison of Symmetric, RSA/DSA/DH, ECC



Symmetric	RSA/DSA/DH	ECC	Time to break in MIPS years
80	1024	160	10^{12}
112	2048	224	10^{24}
128	3072	256	10^{28}
192	7680	384	10^{47}
256	15360	512	10^{66}

5.1 Comparisons of ECC with the RSA

1. Time of the sub-exponential are taken by RSA where the time of full exponentials took by ECC. For illustration, RSA along with 1024 bits key size taking MIP of 3x1011 years with the perfect calls like attack. In ECC, key size of the 160 bit taking MIP years of 9.6x 10^11

2. The security which is same level offered by ECC with the help of key sizes. which are smaller

3. RSA size of DATA smaller compared to the ECC.

4. Size of key and data is the one of the Encrypted message function of key to the RSA as well as ECC, The key size of ECC less compared to key size of RSA, hence ECC encrypted message is small in size. .

5. ECC have small Computational power

5.2 ECDSA & DSA 1 Comparison

The ECDSA as well as DSA 1 are according to the scheme of the ElGamal signature as well as using similar signing equation: i.e s = k-1({h (m) + dr}) mod n.

2. Generation of values are difficult like the parameters of the system in both

3. DSA as well as the ECDSA using SHA-1 like hash function of sole cryptographic.

4. The d which is the private key as well as the k value which is per-signature in the ECDSA can be defined like unique as well as unpredictable than random DSA [11].

5.3 ECC Pros

Hence, ECC having best advantages compared to other system of cryptography

1. offering effective as well as implementations of the compact to the operations of the cryptography want smaller chips.

2. as there are chips in small size so that generation of the heat also less as well as the consumption of the power.

3. Best compatible for low bandwidth, power computing and memory systems

6. Conclusion

ECDSA which is the Algorithm of the Elliptic Curve Digital Signature this is one of the Elliptic Curve Cryptography variant implemented like the another for establishing public key of the systems like the Algorithm of the Digital Signature (DSA) as well as the RSA which is the short form of the Rivest Shamir Adleman ; having recently obtained attention a lot in the industry as well as academia. Primary reason of ECDSA attractiveness fact where here we donot have the algorithm of the sub exponential called as for solving the problem of elliptic curve discrete logarithm over perfect selecting curve of the elliptic. Therefore, it taking complete time of exponential for solving if excellent perfect algorithm called to solve underlyof RSA integer factorization as well as DSA discrete logarithm problem in two taking the time of sub exponential. The key produced with implementation of high secured as well as consuming lower bandwidth since low key size utilised with curves of elliptic. Like that parameters which are smaller may use in ECDSA compared to other systems which are competitive like RSA as well as DSA but with the help of levels of equivalent security. Some of the advantages of small key size including the power of higher processing, space for storage as well as bandwidth. All these things making the ECDSA become ideal to constrained environment like the pagers, cellular phones PDAs, as well as smart cards. In another environments, these pros are important where there are processing of the power, space for the storage, bandwidth/ consumption of the power lack.

References

[1] Vanstone, S. A., 1992. Responses to NIST's Proposal Communications of the ACM, 35, 50-52.

[2] Vanstone, S. A., 2003. Next generation security for wireless: elliptic curve cryptography. Computers and Security, vol. 22, No. 5.

[3] Koblitz, N., 1987. Elliptic curve cryptosystems. Mathematics of Computation 48, 203-209.

[4] Miller, V., 1985. Use of elliptic curves in cryptography. CRYPTO 85.

[5] Certicom ECC Challenge. 2009. Certicom Research

[6] Hankerson, D., Menezes, A., Vanstone, S., 2004. Guide to Elliptic Curve Cryptography. Springer.

[7] Botes, J.J., Penzhorn, W.T., 1994. An implementation of an elliptic curve cryptosystem. Communications and Signal Pro-cessing. COMSIG-94. In Proceedings of the 1994 IEEE South African Symposium, 85 -90.

[8] An intro to Elliptical Curve Cryptography[On-Line

[9] Gupta, V., Stebila, D., Fung, S., Shantz, S.C., Gura, N., Eberle, H., 2004. Speeding up Secure Web Transactions Using Elliptic Curve Cryptography. In Proceedings of the 11th Annual Network and Distributed System Security Symposium (NDSS 2004). The Internet Society, 231-239.

[10] Raju, G.V.S., Akbani, R., 2003. Elliptic Curve Cryptosystem And Its Application. In Proceedings of the 2003 IEEE International Conference on Systems Man and Cybernetics (IEEE-SMC), 1540-1543.

[11] Johnson, D.B., Menezes, A.J., 2007. Elliptic Curve DSA (ECDSA): An Enhanced DSA. Scientific Commons.