International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 11, November-2014

Survey on NP-Hard Problems of Digital Signature Schemas

Rashad Elhabob[1]
Computer science department
Faculty of Mathematical Sciences
University of Khartoum
Khartoum ,Sudan

Abdalla Adel[1]
Computer science department
Faculty of Mathematical Sciences
University of Khartoum
Khartoum ,Sudan

Ma'moun Omer [1]
Computer science department
Faculty of Mathematical Sciences
University of Khartoum
Khartoum,Sudan

Dr. Hwida Elshoush[2]
Computer Science Department
Faculty of Mathematical Sciences
University of Khartoum
Khartoum, Sudan

***Abstract*— A study for public-key digital signature schemes that based on different mathematical NP hard problems. That problems influence in performance and reliability of digital signature schemes. In this paper we make a survey on mathematical NP hard problems of digital signature schemes and present the powerful and practical of some schemes depending on its security level.**

Keywords—Cryptography, Digital Signature, Hard Problem.

I. INTRODUCTION

Digital signature is a verification mechanism based on the public-key scheme, and it provides:

a. Data integrity (the assurance that data has not been changed by an unauthorized party).
b. Authentication (the assurance that the source of data is as claimed).
c. Non-repudiation (the assurance that an entity cannot deny commitments).

Generally, every public-key digital signature schemes is based on a mathematical problem. This problem is known as NP (Non-deterministic polynomial) hard problem. The problem is considered to be an NP hard mathematical problem if the validity of a proposed solution can be checked only in polynomial time.

Basically, public-key digital signature schemes are successfully classified into many major types depending on the NP mathematical hard problem shown in (Fig1). These problems are the integer factorization problem (IFP), the discrete logarithm problem (DLP), the Elliptic Curve discrete logarithm problem (ECDLP), the chaotic maps hard problem In the present e-commerce and e-government era, digital signatures have become more and more important According to this what the suitable schema used and in what class that algorithm fall after this study [1][4][6][7].

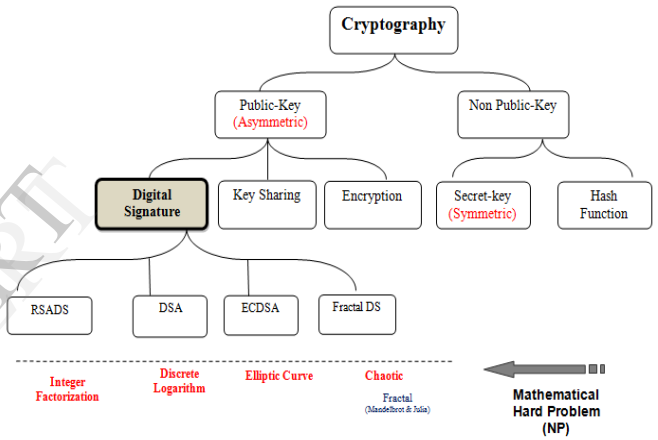

Fig.1. major type's public-key digital signature schemes depending on the NP mathematical hard problem [4]

I. DIGITAL SIGNATURE BASED ON INTEGER FACTORIZATION

The factoring a positive integer *n* means finding positive integers *u* and *v* such that the product of *u* and *v* equals *n*, and such that both *u* and *v* are greater than 1. Such *u* and *v* are called *factors* (or *divisors*) of *n*, and *n* =*u* .*v*is called a *factorization* of *n*. Positive integers that can be factored are called *composites*. Positive integers greater than 1 that cannot be factored are called *primes*. For example, *n* = 15 can be factored as the product of the primes *u* = 3 and *v* = 5, and *n* = 105 can be factored as the product of the prime *u* = 7 and the composite *v* = 15. A factorization of a composite number is not necessarily unique: *n* = 105 can also be factored as the product of the prime *u* = 5 and the composite *v* = 21. But the *prime factorization* of a number writing it as a product of prime numbers is unique, up to the order of the factors: *n* = 3 . 5. 7 is *the* prime factorization of *n* = 105, and *n* D=5 is the prime factorization of *n* = 5[8][9].

A. Rsa Digital Signature Scheme

In the RSA digital signature algorithm, the private key is used to sign the message. The signed message will be sent to the receiver with the sender's electronic signature. To verify the contents of digitally signed data, the recipient generates a new verification key from the signed message that was received, by using his public key, and compares the verified value with the original message value. If the two values match, then the message is verified and authenticated [4].

B. The RSA Digital Signature Algorithms:

1) *Key generation algorithm (generated by receiver)*

a. Choose two prime numbers (p, q) randomly, secretly, and roughly of the same size.
b. Compute the modulus n as follows: $n = p \times q$.
c. Compute the $\Phi(n)$, as follows: $\Phi(n) = (p-1) \times (q-1)$.
d. Choose the key e, such that $1 < e < \Phi(n)$, and $GCD\ (e, \Phi(n)) = 1$.
e. Compute the private key d, such as $d = e^{-1} \bmod \Phi(n)$.
f. Send the public (n, e).

2) *Signature and verification algorithms:*

g. Determine the message m to be signed such that 0 < m < n.
h. Sign the message as follows: s = md mod n.
i. Send the signature s with the message m to Bob (receiver).

3) *Verification (receiver):*

j. Obtain the keys (d, n).
k. Obtain s, m from Alice.
l. Compute u as follows: u = se mod n.
m. Verify the message m as follows: is m= u-1?.

II. DIGITAL SIGNATURE BASED ON DISCRETE LOGARITHM

The Discrete Logarithm Problem (DLP) has been the subject of interest among many mathematicians and cryptographers in recent times because of its computational difficulty.

Definition: The Discrete Logarithm Problem states: Given a multiplicative group G and elements g , h ϵ G, find an integer n, if it exists, such that $g^n = h$ ". This number n is the discrete logarithm of h to the base g, written more concisely as $n=\log_g(h)$.

In 1976, Whitfield Diffie and Martin Hellman published a paper in which they proposed the Discrete Logarithm Problem as a good source of a "one-way" function [10]. That marked the inception of the Discrete Logarithm Problem in cryptography. For the purpose of this study, we may think of a "one-way" function as a function $f : X \rightarrow Y$ for which given x ϵ X, it is easy to compute f(x), however, given y ϵ Y, it is difficult to compute a value x ϵ X such that f(x) = y, at least for most values of y [2]. In other words, from the standpoint of realistic computability, the function f is not invertible, without further information, and it is for this reason that such function is otherwise known as a "trapdoor" function.

A. Digital Signature Algorithm (DSA):

DSA is an alternative to the ElGamal signature scheme. Knowing that tow schemes based on same mathematical hard problem "Discrete logarithm problems (DL)", but DSA more security because it's bases on complexity of the discrete logarithm problem in the field of Zp, where p is a prime [3].

B. The DSA Algorithms:

1) *Key generation algorithm (generated by receiver)*

a. Choose a prime number (p), where $2L-1 < p < 2L$ for $512 \le L \le 1024$ and L a multiple of 64.
b. Choose a prime numbers (q), where q divisor of ($p - 1$), and $2159 < q < 2160$.
c. Compute g as follows: $g = (h(p-1)/q) \bmod p$, where $1<h<(p-1)$, and $g > 1$.
d. Choose a random integer x, with $0 < x < q$.
e. Compute y as follows: $y = g^x \bmod p$.
f. Send (p, q, g, and y)

2) *Signing and verifying algorithms*

g. Determine the message m to be signed such that: 0 < m < p.
h. Choose a random integer k, with 0 < k < q.
i. Compute r as follows r = (gk mod p) mod q.
j. Compute s as follows: s = ((k-1) (SHA-1(m) + x r)) mod q.
k. The signature is (r, s).
l. Send the signature(r, s) and the message to the receiver.
m. k-1 is a multiplicative inverse of k in Zq.

3) *Verifying (receiver)*

n. Obtain the keys (p, q, g, and y).
o. w = s-1 mod q.
p. u1 = ((SHA-1(m)) w) mod q.
q. u2 = (r w) mod q.
r. v = ((gu1 yu2) mod p) mod q.
s. Verify the message m as follows: is v= r?.

III. DIGITAL SIGNATURE BASED ON ELLIPTIC CURVE

Elliptic Curve provides public-key primitives using much shorter key lengths for a given security level than other cryptosystems such as RSA, Digital Signature Algorithm (DSA), or Diffie-Hellman. This is a decisive advantage in the context of embedded devices where resources (power, memory, frequency, bandwidth, etc.) are generally limited. Thus, many applications are currently switching to ECC as security requirements increase over the years and traditional key lengths become prohibitive in the embedded context.

Elliptic Curves are mathematical constructions, An elliptic curve can be defined over any field (of real , relational or complex numbers) , but generally speaking the elliptic curve used in cryptography are defined over finite fields[11]like what show in figure 2.

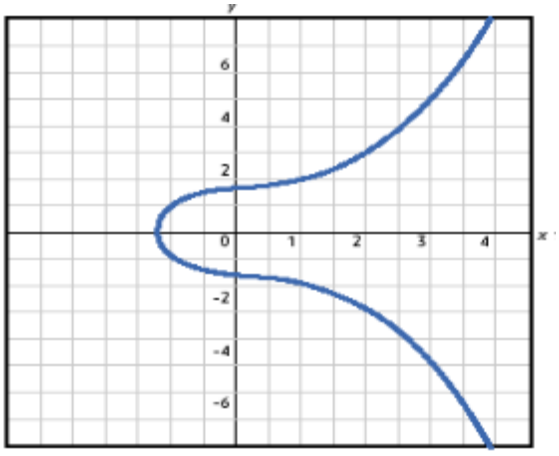

Fig2: finite fields represented in graph[3]

A. *Finite Field*

A finite field consists of a finite set of elements together with two binary operations called addition and multiplication, which satisfy certain arithmetic properties. The order of a finite field is the number of elements in the field. There exists a finite field of order q if and only if q is a prime power. If q is a prime power, then there is essentially only one finite field of order q; this field is denoted by F_q. There are, however, many ways of representing the elements of F_q. Some representations may lead to more efficient implementations of the field arithmetic in hardware or in software. If q=pm where p is a prime and m is a positive integer, then p is called the characteristic of F_q and m is called the extension degree of F_q.

1) *Prime Field Fp:*

Let p be a prime number. The finite field F_p called a prime field, is comprised of the set of integers {0,1,2,….,p-1} with the following arithmetic operations:

- **a)** *Addition:* If a, b ε F_p then a+b=r, where r is the remainder when a+b is divided by p and $0 \le r \le p-1$ known as addition modulo p.
- **b)** *Multiplication:* If a, b ε F_p then a.b=s, where s is the remainder when a.b is divided by p and $0 \le s \le p-1$ known as multiplication modulo p.
- **c)** *Inversion:* If is a non-zero element in F_p, the inverse of modulo a modulop, denoted by a 1, is the unique integer c ε F_p for which a.c=1.

2) *Binary Field F2m :*

The field F2m, called a characteristic two finite field or a binary finite field, can be viewed as a vector space of dimension m over the field F2 which consists of the two elements 0 and1. That is, there exist m elements α0, α1,…, αm-1 in F2m such that each element α can be uniquely written in Equation (1):

α= a0 α0+a1 α1+…….+am-1 αm-1, where ai ε{0,1}……(1)

Such a set {α0, α1,…, αm-1} is called a basis of F2m over F2. Given such a basis, a field element α can be represented as the bit string (a0 a1 …….+am-1) Addition of field elements is performed by bitwise XOR-ing the vector representations. The multiplication rule depends on the basis selected. ANSI X9.62 permits two kinds of bases: polynomial bases and normal bases.

B. *Domain Parameters of ECDSA(elliptic curve DSA) :*

The domain parameters for ECDSA [3] consist of a suitably chosen elliptic curve E defined over a finite field F_q of characteristic p, and a base point G ε E(F_q). Domain parameters may either be shared by a group of entities, or specific to a single user. To summarize, domain parameters are comprised of:

1) a field size q, where either q=p, an odd prime, or $q=_2^m$
2) an indication FR (field representation) of the representation used for the elements of F_q
3) (optional) a bit string seed E of length at least 160 bits
4) two field elements a and b in F_q which define the equation of the elliptic curve E over F_q' (i.e., y2 = x3 + ax + b in the case p>3, and $y^2 + xy = x^3 + ax + b$ in the case p=2)
5) two field elements xG and yG in Fq which define a finite point G=(xG, y14) of prime order in E(Fq)
6) the order ε of the point G, with n>2160 and n>4√q and
7) the cofactor h= E(Fq)/n.

C. *Elliptic Curves Digital Signature Algorithm over Finite Fields:*

The main operation is Point multiplication is achieved by two basic elliptic curve operations.

- Point addition, adding two points J and K to obtain another point L i.e. L= J + K, require 1 inversion and 3 multiplication operation.
- Point doubling, adding a point J to itself to obtain another point L i.e. L = 2J, requires 1 inversion and 4 multiplication operation.

1) *Key Pair generation*

Public key systems require the selection of a public key and a private key as inputs to the encryption and decryption schemes respectively . The public and private keys are algebraically related to each other by Q = [m]P where Q is the public key , m is the private key and P is the primitive (base) point of (P). The order of (P) is denoted by |(P)|.

Input: all necessary parameter for P ϵ E (F_q) .

Output: public key Q and private key m.

a)Select a random m , 0 < m < |(P)|.
b) Compute Q = [m]P.
c)return (Q, m).

2) *Elliptic Curve Digital Signature Generation*

Input: All necessary parameters for P ϵ E(F_q) , private key k , message M , a suitable Hash function.

Output: Signature (s_0 , s_1).

d) Select a random m , 0 < m < |(P)|.
e)Compute [M]P and treat the r-coordinate as integer im.
f) Set s0 = im (mod|(P)|). if s0 = 0 go to step 1.
g) Compute s1 = K-1(H(M)+Ks0) (mod|(P)|) . if s1 = 0 go to step 1.
h) return (s0, s1).

3) *Elliptic Curve Digital Signature Verification*

Input: All necessary parameters for PϵE(F_q), public key Q, Signature (s_0 , s_1), the message M, the Hash function H.

Output: r = {true, False} for the acceptance or the rejection of (s_0, s_1), respectively.

i) Set r = False.
j) if 0 < s0,s1 < |(P)| is satisfied then
k) Compute t0 = s1-1s0(mod|(P)|) , t1 = s1-1H(M) (mod|(P)|).
l) Compute T = [t0]P+[t1]Q.
m) if T ≠ 0 then
n) Treat the x-coordinate of T as an integer iT.
o) if s0 ≡ iT (mod|(P)|) then
p) r = True.
q) end
r) end
s) end
t) return r.

IV. DIGITAL SIGNATURE BASED ON CHOATIC MAPS

From early times, cryptography based on chaos theory has been studied widely. Chaotic maps have been used in the design of symmetric encryption protocols, S-boxes, and hash functions. Recently, chaotic systems have also been used for key agreement schemes [13][14][15].

A. Chaotic maps problems:

Let P and Q be integers and p be prime. The general second-order linear recurrence relation is in this Equation (2):

$$Ta(M) = P \times Ta-1(M) + Q \times Ta-2(M) \ (a \geq 2) \quad (2)$$

Where Ta (M) ∈ GF(p) for all a. The recurrence relation function of chaotic maps is defined to be in Equation (2)
With initial conditions T0 (M) =1 and T1 (M) = M. It is easy to see that the chaotic maps function is a special type of second-order linear recurrence relation as defined in previous equation, with P = 2M and Q=−1.
The Chebyshev polynomials exhibit the following two important properties:

1) The semi-group property:
   Tr (Ts(x)) = cos(r cos−1(cos(s cos−1(x)))) = cos(rs cos−1(x)) = Tsr (x) = Ts(Tr (x)) (3)
   where r and s are positive integer numbers and x ∈ [−1, 1].
2) When the degree a > 1, the Chebyshev polynomial map:
   Ta(x): [−1, 1] → [−1, 1] of degree a is a chaotic map with the invariant density f (x) $= \frac{1}{\pi\sqrt{1-x^2}}$ (4)
   forLyapunov exponent λ = ln a >0.

B. Anew digital signature algorithm based on chaotic maps:

Kai Chain and Wen-Chung Kuo propose a new Digital Signature Algorithm and give implementation of a digital signature algorithm based on both cryptographic and chaotic system characteristics [15].

1) System Parameters

First there will be exploring for system parameters as follow:

- h1(.) is a strong one-way hash function whose output is an integer of which the length is t -bit. Here, we assume t = 128 as the output length of the standard hash function.
- h1v(.) is a strong one-way hash function whose output is a vector which has t elements and every element belongs to {0,1}.
- h2(β, γ) is a strong one-way hash function whose input is two integers β and γ , its output is an integer which length is t -bit.
- p is a large prime such that a factor of p − 1 is the product of two large primes p' and q' ex: n'=p'.q'and n'|p-1
- g is an element in GF(p) whose order modulo p is n' , and G is the multiplicative group generated by g. Note that the two large primes p' and q' are kept secret for all users in the system.

2) User's Keys Generation Phase

a) include set of keys u1,u2,u3,…,ut ∈[1,n']with t length that represent a set of private keys and after that calculate the corresponding public keys k1,k2,k3,…,kt by : kiui 2 =1mod n'
b) choose a secret key u ∈ [1,n'] randomly from the previous set

3) Signature Generation Phase:

To sign a message M the singer must implement this procedure:

c) choose two integers R and r randomly such that gcd(r,n')=1 and compute K= TR(α)mod p.
d) If h2(M,K) = 0, then go to Step 1 and select another random number R; otherwise go to Step 3.
e) Calculate the following: x ≡ 2−1(r + _h22 (M,K) +RK2)r −1)mod n
f) Compute h1v(x) = e = (e1, e2, . . . , et), where ei∈ {0, 1} for all i.
g) Calculate the following: $y = 2^{-1}\, u \prod_{i=1}^{t} u_i^{ei}\ (r - h2\ \ 2M,K + RK2r - 1 \bmod n'$
h) signature of M signed by the signer is (K,x,y).

4) Signature Verification Phase:

The verifier (destination) verify that (K, x, y) is a valid signature of M signed by the signer , he/she will first calculate h1v(x) = e = (e1, e2, . . . , et) and h2(M,K), and then checks to see whether the following equivalence holds or not.

$$\left(\left[T_{x^2-h_2^2(M,K)}(\propto)\right]^2 + \left[T_{y^2}\prod_{i=1}^{t} K_i^{ei}(z)\right]^2 + \left[T_{K^2}(K)\right]^2\right) \bmod p = \left(T_{x^2-h_2^2(M,K)}(\propto) T_{y^2}\prod_{i=1}^{t} K_i^{ei}(z) T_{K^2}(K) + 1\right) \bmod p \quad (5)$$

The verifier always accepts the signature as valid If the signer and verifier follow the signature protocol above, and the receiver is ensured that the message is indeed signed by the signer. Otherwise, the signature is invalid.

C. Security analysis:

The security of this schema depend on finding the key (K, x, y) and it have a good security because of computational complexity A drawback of our method is that it requires high computational resources.

V. DIGITAL SIGNATURE BASED ON TWO NP-HARD PROBLEMS

The securities of digital signature algorithms are based on the difficulty of solving some NP-hard problems. These algorithms stay secure as long as the problem, on which the algorithm is based, stays unsolvable. The most used hard problems for designing a signature algorithm are prime factorization (FAC) and Discrete Logarithm (DL) problems. For improving the security, the algorithms may be designed based on multiple hard problems. Definitely, the security of such algorithms is longer than algorithms based on a single problem. This is due to the need of solving both the problems simultaneously. Many digital signature algorithm have been designed based on both FAC and DL [5][17][18][19].

A. MERDSA:

KapilMadhur and others propose Modified ElGamal over RSA Digital Signature Algorithm (MERDSA)[20] proposed digital signature algorithms based on two hard problems-the prime factorization problem and the discrete logarithm problem. A new digital signature algorithm based on combined application of DL and FAC is described as follows:

1) Key Generation

a) Choose a large prime p such that computing discrete logarithms modulo p is difficult and two large prime numbers p1 and q1 such that p < n where n = p1 × q1.
b) Choose random numbers k and v such that 1 < k, v <p−1.
c) Choose random number b such that 1 < b < n − 1.
d) Choose a primitive root g inZ^p.
e) Calculate φ(n) = (p1 − 1) × (q1 − 1).
f) Choose e and x such that e, x Zφ(n) .

g) Calculate d such that $d \times e \bmod \varphi(n) = 1$.
h) Calculate c such that $b^x \times c \pmod{n} = 1$.
i) Calculate u, w, and t as follows: $u = g^k \bmod p$,
$w = g^y \bmod p$,
$t = u^w \bmod p$,
j) Public key is (e, x, c, g) and private key is (k, v, t, b, d).

2) Signature Generation:

k) Choose an integer z such that $1 < z < (p - 1)$ and it is relative prime to $(p - 1)$ i. e. $\gcd(z, p - 1) = 1$. z should be different for every message m and is not public. Here H (.) is a one way hash function.
l) Calculate:
$h = g^z \bmod p$,
$s1 = H(m)^d \bmod n$,
$s2 = (H(m) \times b^s 1) \bmod n$,
$s3 = ((((H(m) - kw - hv) \times z^{-1})) \bmod (p - 1))$.

If $\gamma = 0$ and/or $s1 = 0$ and/or $s2 = 0$ and/or $s3 = 0$ and/or $H(m) \equiv (kw + hv) \bmod (p - 1)$ then repeat step 1 and 2 else tuple $(\gamma, h, s1, s2, s3)$ is the signature of m.

Here $-kw$, $-hv$ are additive inverse of kw and hv respectively and z^{-1} is the multiplicative inverse of z with respect to mod $(p - 1)$.

3) Signature Verification

m) Calculates H (m) using the received message m at receiver's end.
n) If $g^{H(m)} \times s^{1 \times x} \equiv (\gamma \times h^s 3 \times s^2 \times c^s 1 \bmod n) \bmod p$
Then the signature is valid else reject the signature.

B. Security analysis:

The performance of the proposed algorithm is found to be competitive to the most of the digital signature algorithms which are based on multiple hard problems, butIt is observed that if an oracle O breaks the FAC and DL then it can break the proposed algorithm also, if given the public key of the scheme and a message m.

VI. CONCLUSIONS

In this paper we give the reader basic concepts which are related to the concepts in digital signature cryptosystem. As well, we studied some digital signature schemes (Table I) which are based on different mathematical hard problems as classified earlier. Those classifications help the reader to be familiar with the public-key digital signature cryptosystem. On the other hand, the security protection of the discussed digital signature schemes depend on the mathematical NP-hard problems and the randomness of the output generated. As a result we recommend that to use two NP-hard problems digital signature and chaotic map as one problem because of its complexity and hardness to break.

TABLE I.Comparisons ofMathematical NP- hard problem in term of efficiency and performance

Mathematical NP- hard problem	Algorithm	Efficiency	Typical key size for high performance
INTEGER FACTORIZATION	RSA digital signature schema	Slower than other	large key size which is typically 1024 - Bit
ON DISCRETE LOGARITHM	DSA	System security depend on maintaining the confidentiality of private key	large key size which is typically 1024 - Bit
ELLIPTIC CURVE	Elliptic Curves Digital Signature Algorithm over Finite Fields.	It's more difficult than other mathematical problems	Small key size which is typically 128 - Bit
CHAOTIC MAPS	Anew Digital Signature Algorithm based on chaotic maps	The system provides high level of security , in term of key size and execution time	Small key size which is typically 128 - Bit
COMBINATION OF TWONP-HARD PROBLEMS	MERDSA	The performance of the proposed algorithm is found to be competitive to the most of the digital signature algorithms which are based on multiple hard problems	large key size which is typically 1024 - Bit

REFERENCES

[1] Yadav .Srivastava. and Trehan , DIGITAL SIGNATURE, international journal of engineering and management sciences ,p I.J.E.M.S., VOL.3(2) 2012: 115 – 118
[2] McCurley K.S., The Discrete Logarithm Problem, Cryptology and Computational Number Theory, volume 42, pages 49-74, American Mathematical Society, 1990.
[3] D. Johnson, A. Menezes, S. Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)", Certicom Corporation, 2001.
[4] M. Ahmad , "Comparison Study On Np-Hard Problem Based Digital Signature Schemes" , International Science and Technology Conference, Istanbul, 7-9 December 2011.
[5] Swati Verma1,* and Birendra Kumar Sharma2, A New Digital Signature Scheme Based on Two Hard Problems, International Journal of Pure and Applied Sciences and Technology, pp. 55-59, 5(2) (2011).
[6] Fashoto S.G, Gbadeyan J.A and Okeyinka E.A, Application of Digital Signature for Securing Communication Using RSA Scheme based on MD5, Proceedings of the International Conference on Software Engineering and Intelligent Systems , Ota, Nigeria, July 5th-9th , 2010.
[7] GunjanJain , Digital Signature Algorithm, International Journal of Innovations in Computing, (ISSN : 2319-8257) Vol. 1 Issue 1
[8] ARJEN K. LENSTRA , Integer Factoring, Designs, Codes and Cryptography, 19, 101–128 (2000)
[9] Ismail E.S, N.M.F. Tahat and R.R Ahmad , A New Digital Signature Scheme Based on Factoring and Discrete Logarithms, Journal of Mathematics and Statistics 4 (4): 222-225, 2008
[10] Diffie, W. and Hellman, M., New Directions in Cryptography, IEEE Trans. Information Theory (1976), 472-492
[11] M. W. Paryasto, S. Sutikno, A. Sasongko, "Issues in Elliptic Curve Cryptography Implementation", Internetworking Indonesia Journal, Vol. 1, No. 1, 2009.
[12] He, D., Chen, Y., Chen, J.: Cryptanalysis and improvement of an extended chaotic maps-based key agreement protocol. Nonlinear Dyn.69(3), 1149–1157 (2012).

[13] Lee, C.C., Chen, C.L., Wu, C.Y., Huang, S.Y.: An extended chaotic maps-based key agreement protocol with user anonymity. Nonlinear Dyn.69(1), 79–87 (2012).
[14] Zhang, L.: Cryptanalysis of the public key encryption based on multiple chaotic systems. Chaos Solitons Fractals 37(3), 669–674 (2008).
[15] Kai Chain · Wen-Chung Kuo , A new digital signature scheme based on chaotic maps, An International Journal of Nonlinear ,Dynamics and Chaos in Engineering Systems ,ISSN 0924-090X , 22 July 2013
[16] Christophe Guyeuxand Jacques M. Bahi , Topological chaos and chaotic iterations Application to Hash functions ,
[17] Z. Shao. Security of a new digital signature scheme based on factoring and discrete logarithms. International Journal of Computer Mathematics, 82(10):1215-1219, 2005.
[18] S.F. Tzeng, C.Y. Yang, and M.S. Hwang.A new digital signature scheme based on factoring and discrete logarithms. International Journal of Computer Mathematics, 81(1):9-14, 2004.
[19] S. Wei. A New Digital Signature Scheme Based on Factoring and Discrete Logarithms.Progress on Cryptography, pages 107-111, 2004.
[20] M. Kapil,y. Jitendra and v. Ashish , Modified ElGamal over RSA Digital Signature Algorithm (MERDSA), International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 8, August 2012