VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

J- COMPONENT
(REVIEW 1)

Information Security Analysis and Audit

Topic : **Acquiring Digital Signatures from Elliptic Curve Cryptography**

Reg no : **18BIT0168**
Name: Ashu Goyal
Slot : G1
Faculty: Prof. Sumaiya Thaseen I.
Digital Signature :

LITERATURE SURVEY

Research Paper 1 : Implementation of Elliptic Curve Digital Signature Algorithm

International Journal of Computer Applications (0975 – 8887) Volume 2 – No.2, May 2010

Authors : Aqeel Khalique || Kuldip Singh || Sandeep Sood

Department of Electronics & Computer Engineering, Indian Institute of Technology Roorkee

Technique Implemented and its motivation :
The Elliptic Curve Digital Signature Algorithm (ECDSA) is the elliptic curve analogue of the Digital Signature Algorithm (DSA). It was accepted in 1999 as an ANSI standard, and was accepted in 2000 as IEEE and NIST standards. It was also accepted in 1998 as an ISO standard, and is under consideration for inclusion in some other ISO standards. Unlike the ordinary discrete logarithm problem and the integer factorization problem, no sub exponential-time algorithm is known for the elliptic curve discrete logarithm problem.

Architecture / Pseudo Code:
Elliptic Curve Digital Signature Algorithm is implemented over elliptic curve P-192 as mandated by ANSI X9.62 in C language. The Project contains necessary modules for domain parameters generation, key generation, signature generation, and signature verification over the elliptic curve. ECDSA has three phases, key generation, signature generation, and signature verification.

Step1 : In key generation, an entity A's key pair is associated with a particular set of EC domain parameters D= (q, FR, a, b, G, n, h). E is an elliptic curve defined over Fq , and P is a point of prime order n in E(Fq), q is a prime. After key generation next phases are signature generation and signature verification are as follows:

Step2 : ECDSA Signature Generation: To sign a message m, an entity A with domain parameters D= (q, FR, a, b, G, n, h) does the following: 1. Select a random or pseudorandom integer k in the interval [1, n-1]. 2. Compute kP =x1, y1 and r= x1 mod n (where x1 is regarded as an integer between 0 and q-1). If r= 0 then go back to step 1. 3. Compute k -1mod n. 4. Compute s= k -1 {h (m)+ dr} mod n, where h is the Secure Hash Algorithm (SHA-1). If s = 0, then go back to step 1. 5. The signature for the message m is the pair of integers (r, s).

Step3 : ECDSA Signature Verification: To verify A's signature (r, s) on m, B obtains an authenticated copy of A's domain parameters D = (q, FR, a, b, G, n, h) and public key Q and do the following 1. Verify that r and s are integers in the interval [1, n-1]. 2. Compute w = s -1mod n and h (m) 3. Compute u1 = h(m)w

mod n and u2 = rw mod n. 4. Compute u1P + u2Q =(x0, y0) and v= x0 mod n. 5. Accept the signature if and only if v = r

Performance Analysis :

messages.

Table 1. Comparable Key Size (in bits) [3]

Symmetric Algorithms	ECC	RSA
80	163	1024
112	233	2240
128	283	3072
192	409	7680
256	571	15360

Table 2. Key Generation Performance [3]

Key Length (bits)		Time (s)	
RSA	ECC	RSA	ECC
1024	163	0.16	0.08
2240	233	7.47	0.18
3072	283	9.80	0.27

The degree of difference between the difficulties of these operations depends on the size of the key pairs. The inverse operation increases exponentially whereas the forward operation increases linearly as the key size increases as in Figure 6. Increase in key length give rise to complexity issues in both operations. Thus ECC is preferred as it provides same level security at 160 bit key length as of 1024 bit key length in RSA.

Research Paper 2 : RSA Encryption and Digital Signature Algorithm

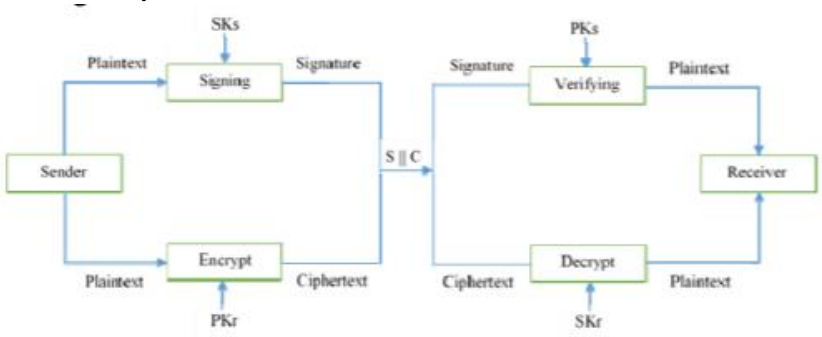
2018 4th International Conference on Science and Technology (ICST), Yogyakarta, Indonesia

Authors : Farah Jihan Aufa || Endroyono || Achmad Affandi
Departement of Electrical Engineering Institut Teknologi Sepuluh Nopember
Surabaya, Indonesia

Technique Implemented and its motivation :

This paper discusses the performance analysis of each method, and combination of both RSA and DSA methods so it can improve its security system with a relatively fast time. The structure of the distribution in this paper is: It contains the theory of RSA algorithm and DSA algorithm and describes the proposed system model. The Rivest-Shamir-Adleman (RSA) algorithm is most widely used for public key encryption approaches. Digital signature is an authentication mechanism that allows the sender of message to attach the code as digital signature. Generally, digital signature is formed by retrieving the hash of the message and encrypting the message with the sender's private key. This signature guarantees the source and integrity of the message.

Architecture / Pseudo Code:



System Model

The blend calculation of the proposed technique is a mix of RSA and DSA calculations so the messages sent are scrambled as well as carefully marked so as to expand the security level of their messages.

Step 1 : Combination key generation

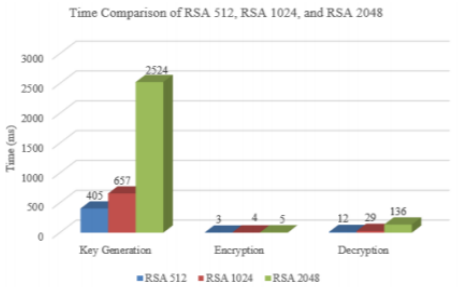
Step 2 : Encryption and Signing

Step 3 : Decryption and Verifying

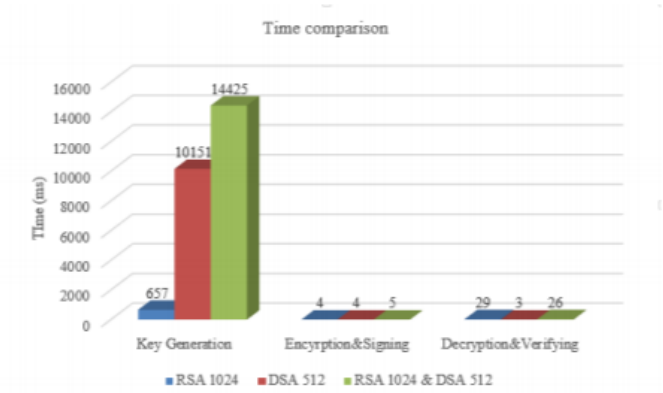
Performance Analysis / Time Comparison:

	RSA-1024		ECC-160	RSA-1536		ECC-192	RSA-2048		ECC-224
Time (ms)	9.79		3.67	22.24		2.63	61.62		6.08
Performance ratio	1	:	2.6	1	:	8.5	1	:	10.1
Key-size ratio	6.4	:	1	8	:	1	9.14	:	1
Speedup	1	:	17.5	1	:	30.1	1	:	48.7

Fig. 4 Response time v/s transaction request for ECC and RSA



Time Comparison of RSA 512, RSA 1024, and RSA 2048



Total Time Comparison of The Methods

The Time comparison of key generation, encryption and signing, decryption and verifying. Total time required RSA 1024 is 690 ms. The total time required DSA 512 is 10158 ms. And the total time required by the combination method of RSA 1024 and DSA 512 is 14455 ms.

In this paper, a combination method of RSA 1024 and DSA 512 has been performed since the calculation time is generally quick. Acquired time for key age is 33.5% more slow than RSA and DSA age time independently. It has 60% quicker computational time in encode and marking measure. Also, for decoding and confirming time, it has a 23% quicker than RSA and DSA independently.

Research Paper 3 : Implementation of Elliptic Curve Digital Signature Algorithm Using Variable Text Based Message Encryption.

International Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 5

Authors: Jayabhaskar Muthukuru, Prof. Bachala , Sathyanarayana

Research Scholar, Department of Computer Science & Technology,Professor, Sri Krishnadevaraya University, INDIA

Technique Implemented and its motivation :

The sender produces the mark of a given message utilizing his mystery key; the recipient at that point checks the mark by utilizing sender's open key. The ECDSA have a littler key size, which prompts quicker calculation time and decrease in preparing power, extra room and transfer speed. This makes the ECDSA ideal for obliged gadgets, for example, pagers, mobile phones and smart cards. The Elliptic-Curve Digital Signature Algorithm (ECDSA) is a Digital Signature Scheme dependent on ECC.
Confidentiality, Authentication and Non-repudiation are the three properties of Digital Signature authenticated schemes.

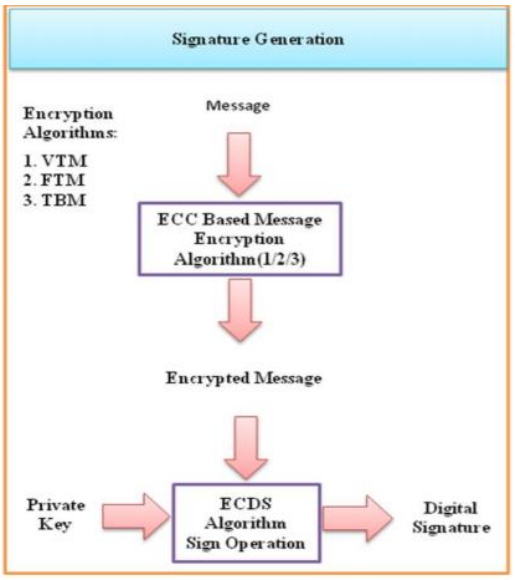
Architecture / Pseudo Code:

Signature Generation steps:

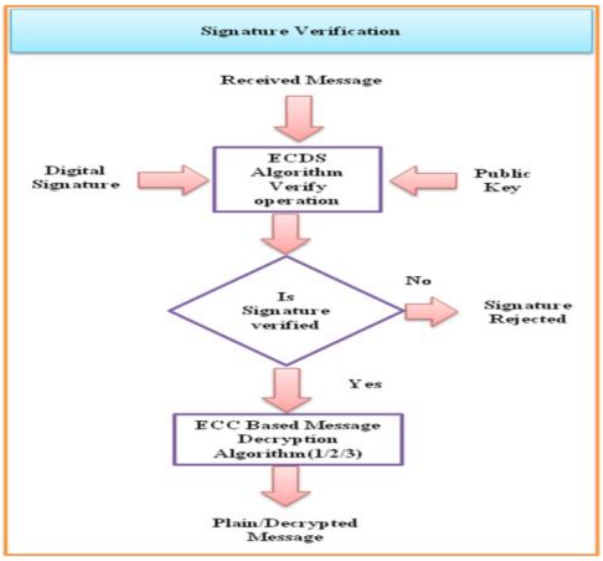
1. Encrypt the message using EC Encryption algorithm which is VTM/FTM/TBM
2. Compute signature for Encrypted message using Algarithm-4
3. Send the digitally signed message

Signature Verification Steps:

1. Verify Signature using Algarithm-5.
2. If verification fails then reject the signature
3. If verification success, then decrypt the message using respective EC Decryption Algorithm.



Signature Generation Process

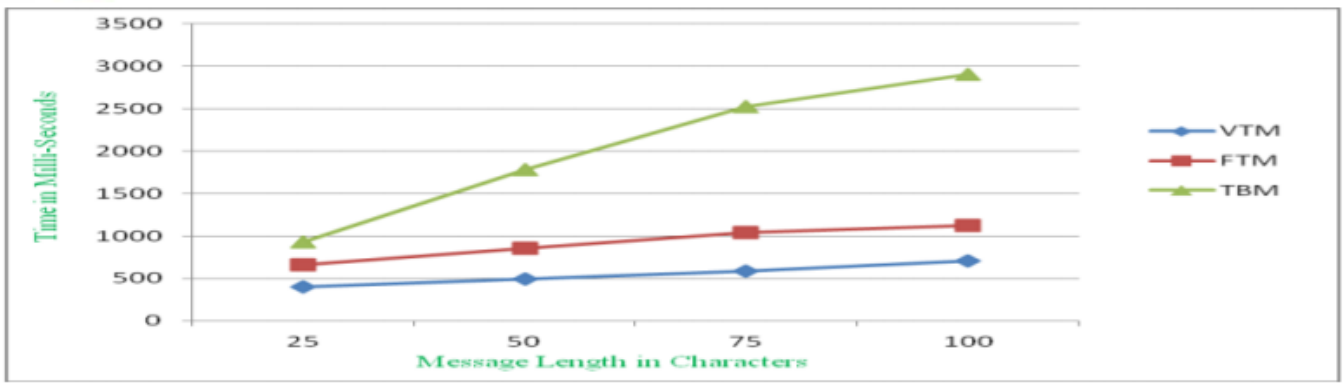


Signature Verification Process

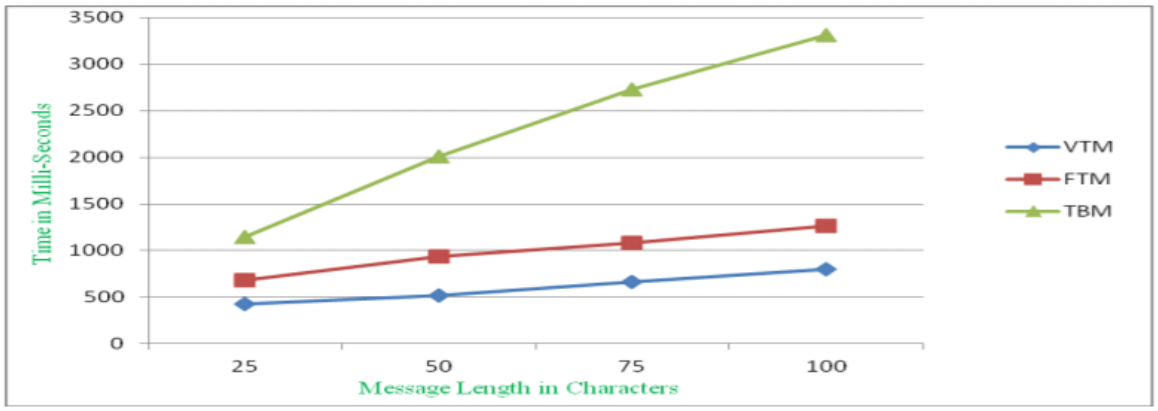
Performance Analysis / Time Comparison:

	RSA-1024		ECC-160	RSA-1536		ECC-192	RSA-2048		ECC-224
Time (ms)	9.79		3.67	22.24		2.63	61.62		6.08
Performance ratio	1	:	2.6	1	:	8.5	1	:	10.1
Key-size ratio	6.4	:	1	8	:	1	9.14	:	1
Speedup	1	:	17.5	1	:	30.1	1	:	48.7

After implantation of given algorithm we found that performance of ECDSA utilizing Variable Size Text Message Encryption is better when contrast and ECDSA utilizing FTM Encryption and TBM Encryption. The explanation is VTM based ECDSA utilized less number of point increments and increases contrast and other two strategies. Performance of ECDSA is conversely corresponding to key size, and security of the security of the system depends upon key size.



Performance comparison of various ECDSA methods for over EC P-192



Performance comparison of various ECDSA methods for over EC P-256

In this paper we have executed ECDSA for different space boundaries, in the wake of watching the outcomes when the key size builds then multifaceted nature increments and execution diminished. Subsequent to looking at VTM, FTM and TBM based ECDSA strategies, ECDSA utilizing Variable Text Message Encryption is better when contrasting and Fixed Length Text Message and Text Based Encryption utilized ECDSA. The primary explanation is, the speed of scalar duplication which assumes a significant part in the effectiveness of entire framework . In VTM based ECDSA technique, number of scalar duplications are decreased, so this strategy is effective when contrasted and FTM and TBM based strategies

Research Paper 4 : The Improvement of digital signature algorithm Based on elliptic curve cryptography

Authors : Qiuxia Zhang , Zhan Li , Chao Song
HuangHe Science and Technology College, morden education technical center ZhengZhou, China

Technique Implemented and its motivation :
digital signature innovation an ever increasing number of shows its significant situation in data security. The elliptic curve cryptography having higher security is applied to the field of digital signature has become the center which individuals give increasingly more consideration. In this paper, the first

advanced mark innovation research is dissected. We acquire another digital signature conspire through improving the first advanced mark plot, and upgraded the security of the advanced mark.

Architecture/Pseudo Code of improved scheme:

In order to increasing the safety, we can embed the information of signature into a point on the ellipse. This paper would improve the scheme. In this paper we take the method of signing before encrypting, namely after calculating 's' in the signature process of original scheme, increased one step that encrypting s with signer's private key ,and then sent the encrypted result to the verifier. Verifier verifies the encrypted result before verifying the signature.

The improved scheme process

1) The signature process If user A want to sign for the news, the signature process is as follows:

a) firstly Randomly select an integer $k, 0 < k < n$, calculate $R = kG = (x, y)$, $r = x \bmod n$ if $r = 0$ then return (1).

b) calculate $e = h(m)$; $s_1 = (ke + (r + \oplus e)d)G$; $s_2 = s_1 d$

c) Sent (r, s_1, s_2) as the signature of message m to the verifier.

2) The validation process firstly, verifier verify the encrypted result 2 s before verifying the signature. The process is as follows:

a) Verify the equation $s_2 G = S_1 Q$, if the equation was established ,go to process (5),else refuse the signature.

b) calculate $e = h(m)$, $u = r \oplus e \bmod n$;

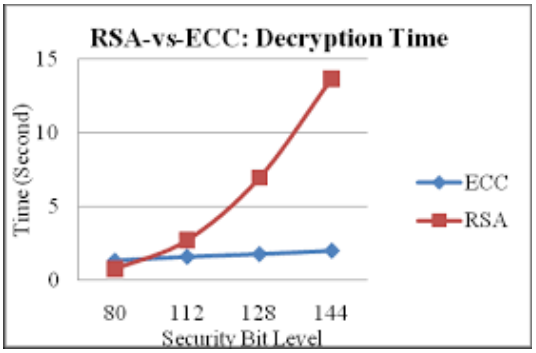
c) calculate $X = e^{-1}(s - uQ) = (x_1, y_1)$;

d) calculate $r_1 = x_1 \bmod n$ if the equation was established ,receive the signature or refuse.

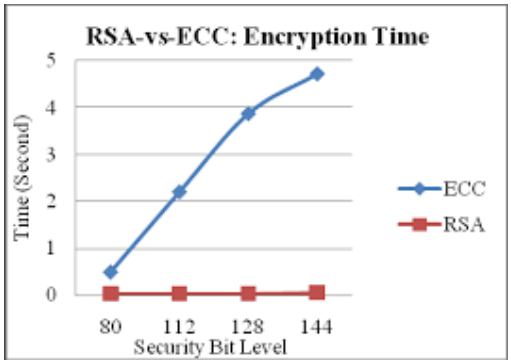
Performance and Security Analysis :

	RSA-1024		ECC-160	RSA-1536		ECC-192	RSA-2048		ECC-224
Time (ms)	9.79		3.67	22.24		2.63	61.62		6.08
Performance ratio	1	:	2.6	1	:	8.5	1	:	10.1
Key-size ratio	6.4	:	1	8	:	1	9.14	:	1
Speedup	1	:	17.5	1	:	30.1	1	:	48.7

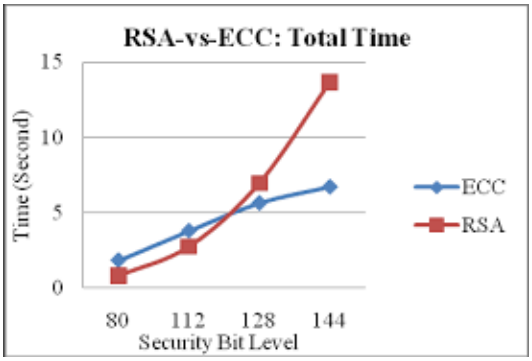
Now look to the performance of ECC vs RSA at encryption, decryption and total time.



Decryption Time



Encryption Time



Total Time

The improved plan despite everything take the technique for inserting the data of mark into a point on the circle when compute 1s in the mark cycle. However, expanded a cycle that the underwriter scrambling the mark. Verifier need checking the ciphertext of mark 2s before confirm the mark. It isn't achievable that the aggressor endeavoring to manufacture the mark by supplanting the message. So the improved plan can prevent forgery. With the rapid development of information technology, RSA public key cryptography has been not well meet the demand for high security so we are making towards ECC and trying to optimizing it further.

Research Paper 5 : An Efficient Elliptic Curve Digital Signature Algorithm (ECDSA)

2013 International Conference on Machine Intelligence Research and Advancement

Authors : Shweta Lamba || Monika Sharma
Technological Institute of Textile & Sciences Bhiwani, India

Technique Implemented and its motivation :

Elliptic curve can be applied to cryptography as it is secure to the best of current information. Elliptic curve cryptography (ECC) is a way to deal with open key cryptography, in light of the logarithmic structure of elliptic curves over limited fields. The Elliptic Curve Digital Signature Algorithm is the Elliptic Curve simple to the more generally utilized Digital Signature Algorithm (DSA). It is the utilization of ECC to computerized signature age and confirmation. Its security depends on the elliptic curve discrete logarithm problem.

The *motivation* behind this algorithm is that it provides more security as only two points are shared publically and generating point is private, this algorithm is more secure against intruders.

Architecture/Pseudo Code of improved scheme:

Construct a digital signature of a document. Let z be an integer that represents a hash of the document M which is to be signed. The digital signature s is calculated by first calculating the elliptic curve point k ×G and retaining only its x-coordinate modulo n, if the modulo operation produces a zero value then opt a different value of k. And then by means of formula s = (z× d) × k−1 (mod n), s is computed, where k−1 is the multiplicative inverse of k modulo n that can be obtained with the Extended Euclid's Algorithm.

this algo have 4 main steps :

1. Key-Pair Generation
2. Signature Generation
3. Signature Verification
4. Correctness of Algorithm

PUBLIC AND PRIVATE PARAMETERS OF PROPOSED ECDSA

Private Parameters	Public parameters
private key G (generating point)	Public key Q
Random integer 'k'	x-coordinate of point (x_1, y_1)
Elliptic curve parameter 'a, b'	Message hash 'z'
Field characteristic 'q'	Signature (s)
Order of field 'n'	Random number 'd'

Performance and Security Analysis :

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}

It is less Complex Algorithm : Dissimilar to existing ECDSA, the signature generation using proposed ECDSA comprises computing the value of parameter ‘s’ only. Integer 'r' isn't determined in this calculation. Additionally signature confirmation comprises of one point multiplication operation though existing calculation have two point multiplication and one point addition operation.

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] W. Stalling, “Cryptography and Network Security: Principles and Practice”, 5ft ed, Prentice Hall, 2011
[4] Ali Sadikin, “Implementation of RSA 2048-bit and AES 256-bit with Digital Signature for Secure Electronic Health record Application”, in International Seminar on Intelligent Technology and Its Application, 2016
[5] Navneet Randhawa, Lolita Singh, A Systematic Way to Provide Security for Digital Signature Using Elliptic Curve Cryptography, IJCST Vol.2, Issue 3, Sep-2011, 185-188
[6] Jayabhaskar Muthukuru, Bachala Sathyanarayana, Fixed and Variable Size Text Based Message Mapping Techniques Using ECC, GJCST Vol.12, Issue 3, Feb-2012, 25-30
[7] T.Elgamal. A public-key cryptosystem and a signature scheme based on discrete logarithms[J].TEEE Transaction on Information Theory, 1985,(31):469-472.
[8] Long Dong-yang, Wang Chang-ji, Wu Dan. Application coding and computer cryptography [M].BeiJing:Tsinghua university press,2005.169-171.
[9] Ms. P. G. Rajeshwari and Dr. K. Thilagavathi, “An Efficient Authentication Protocol Based on Elliptic Curve Cryptography for Mobile Network,” IJCSNS, vol 9, feb 2009.
[10] Tilahun Kiros and Kumudha Raimond,” An Efficient Modified Elliptic Curve Digital Signature Algorithm,” Journal of EEA, vol 26, 2009
[11] Aqeel Khalique, Kuldip Sihgn and Sandeep Sood,” Implementation of Elliptic Curve Digital Signature Slgorithm,” International Journal of Computer Applications, vol 2, no. 2, may 2010.
[12] Dipti Aglawe and Samta Gajbhiye,” Software Implementation of Cyclic Abelian Elliptic Curve using MATLAB,” International Journal of Computer Applicatios, vol 42, no. 6, march 2012.