A Hybrid Security Model for Data Exchange Using Elliptic Curve Cryptography and Message Digest Algorithm

Juber Mirza[1], Avdesh Kumar Sharma[2]
[1, 2] Department of Computer Science & Engineering
[1, 2] SVITS- SVVV Indore

Abstract- *Now in these days the means of computation is changed due to high computational resource availability. Due to this the traditional way of computing is not much efficient to adopt for new generation computing therefore, it is required to enhance the traditional technique in order to design efficient and compatible technique for new scenarios. The given study is intended to enhance the traditional cryptographic approach in order to make adoptable and compatible for different computational needs.*

In order to provide solution for cryptographic techniques the elliptical curve cryptography is explored and enhanced for designing a hybrid cryptographic technique. The proposed hybrid cryptographic algorithm incorporates the ECC algorithm and MD5 hash generation algorithm. The ECC algorithm uses a private key for encrypting data, therefore in the proposed algorithm the manual private key is replaced with the MD5 generated 128 bit hash code. The implementation of the proposed cryptographic algorithm is performed using the JAVA environment and the NETBEANS IDE.

After implementation of the desired algorithm the performance of the system are estimated using different performance parameters such as memory consumption, time consumption, data validity and the storage overhead. The obtained results demonstrate the designed hybrid ECC algorithm is efficient and effective. Additionally that is adoptable for different file formats such as image and text data.

Keywords- Security, Message Digest Algorithm, MD 5, Cryptography

I. INTRODUCTION

The cryptography is an art of data hiding that can be also stated as the art of preserving information by transforming it (encrypting it) into an unreadable format (for human eyes), called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called code-breaking, although modern cryptography techniques are virtually unbreakable. As the Internet and other forms of electronic communication become more prevalent, electronic security is becoming increasingly important. Cryptography is used to protect e-mail messages, credit card information, and corporate data. One of the most popular cryptography systems used on the Internet is Pretty Good Privacy because it's effective and free. Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and recipient have, and public-key systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses.

In this study the available elliptical curve cryptography is analysed and new ECC inspired hybrid encryption scheme is proposed, basically the encryption algorithms are mathematical models that are manipulating the data to hide them. Therefore encryption algorithms are varying according to the data formats. Thus for encryption and decryption of two data formats are a complex issue in this study. In addition of that successfully data recovery from modified message is also a complex task in presence of different data formats. Therefore a new innovative solution is tried to find in this proposed study work. The proposed solution incorporates study of a hash generation algorithm for efficient key generation process and ECC algorithm that support the efficient cypher generation process.

II. PROPOSED WORK

To achieve more security, this section proposed a new cryptography algorithm with an integrated scheme to improve data security. The hybrid cryptographic algorithm uses an integrated scheme to achieve authentication, Using ECC encryption-decryption methodology and the MD5 hash generation algorithm. To develop a more efficient and more secure cryptographic algorithms. It is suitable for all devices due to their confines in memory capacity, computing power,

cryptographic support and key sizes. It is lighter and secure encryption system for the secure file transferring system.

2.1 Key Generation Module

This module include MD5 algorithm

2.1.1 MD 5 algorithm

MD5 algorithm is an essential contribution in data security, which generates a 128 bit length hash for complete data. Therefore it is much essential in data manipulation and transmission error check. Sometimes it is used for key generation process in different hybrid algorithms. The MD5 algorithm includes 5 step processes for generating hash.

Steps 1 –append padded bits:

- The message is padded so that its length is congruent to 448, modulo 512.
  - Means extended to just 64 bits shy of being of 512 bits long.
- A single "1" bit is appended to the message, and then "0" bits are appended so that the length in bits equals 448 modulo 512.

Step 2 –append length:

- A 64 bit representation of b is appended to the result of the previous step.
- The resulting message has a length that is an exact multiple of 512 bits.

Step 3 – Initialize MD Buffer

- A four-word buffer (A,B,C,D) is used to compute the message digest.
  - Here each of A, B, C, D, is a 32 bit register.
- These registers are initialized to the following values in hexadecimal:
  - word A: 01 23 45 67
  - word B: 89 ab cd ef
  - word C: fe dc ba 98
  - word D: 76 54 32 10

Step 4 –Process message in 16-word blocks.

- Four auxiliary functions that take as input three 32-bit words and produce as output one 32-bit word.
  - F(X,Y,Z) = XY v not(X) Z
  - G(X,Y,Z) = XZ v Y not(Z)
  - H(X,Y,Z) = X xor Y xor Z
  - I(X,Y,Z) = Y xor (X v not(Z))
- Process message in 16-word blocks cont.
  - if the bits of X, Y, and Z are independent and unbiased, the each bit of F(X,Y,Z), G(X,Y,Z), H(X,Y,Z), and I(X,Y,Z) will be independent and unbiased.

Step 5 –output

- The message digest produced as output is A, B, C, D
-
- That is, output begins with the low-order byte of A, and end with the high-order byte of D

This section provides the detailed discussion about the MD5 hash generation algorithm. The next section includes recent made efforts and applications of ECC algorithm.

2.1.2 Data Encryption/Decryption by using ECC

The propose solution includes the development of security system using traditional encryption scheme (ECC) and the MD5 hash generation algorithm. The private key generation of the ECC algorithm here accepts self-generated keys for encryption and that key is incorporated with the cypher for secure file exchange. In addition of that the algorithm is able to extract key from the given cypher and cross check the validity of the data.

The diagram figure 2, First of all the system will accept input file and apply for ECC encryption process on the input file and also apply MD5 algorithm that will generate 128 bit key. Both cipher text and 128 bit key will send. Then on the decryption side it will get Cipher text and 128 bit key. Apply ECC decryption process on the cipher text and get original message. Now it will apply MD5 Algo on the message and get 128 bit key. If received 128 bit key and generated 128 bit key are same then massage will accept otherwise massage will discard. To understand the process of the proposed methodology, first required illustrating the traditional ECC encryption and decryption process.

2.1.3 Encryption Process

Input:

If Q= public key

P= a point in curve

d= private key

M= original message

K= random number

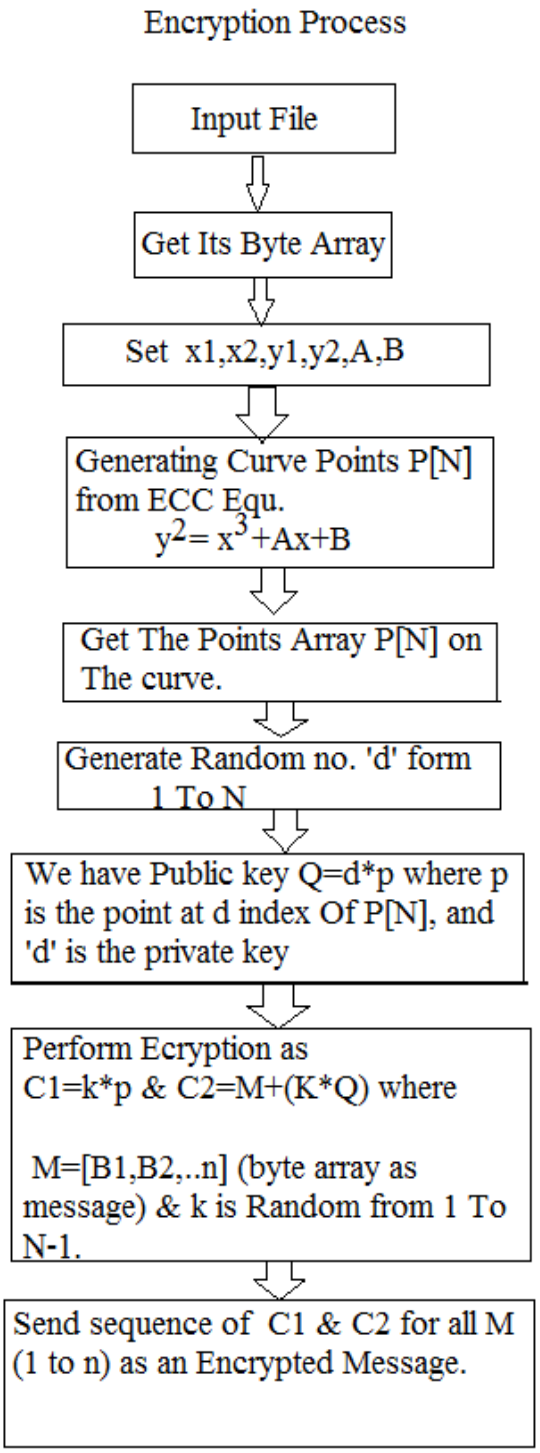

Figure 2.1 Encryption process

Then using above parameters we get the two cypher texts blocks which are denoted using $C_1$and C_2

$$C_1 = K.P$$

$$C_2 = M + KQ$$

2.1.4 Decryption Process

Using the above equations the message can be defined as:

$$M = C_2 - d * C_1$$

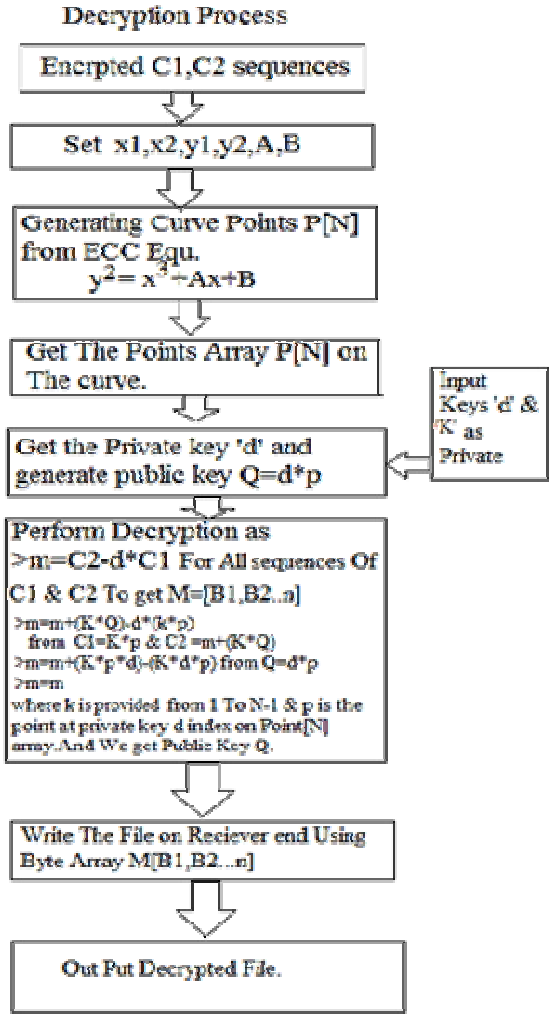

Figure 2.2 Decryption process

$$M = C_2 - KQ$$

At the network scenarios the cypher $C_1$and C_2 is sanded on network and the recovery of the original message can be found using the below given expression.

$$M = C_2 - d * C_1$$

$$C_2 - d * C_1 = (M + KQ) - d * (K * p)$$

In next step

$$C_2 - d = M + KQ$$

$$C_2 = M + KQ$$

$$M = M$$

III. PROPOSED ALGORITHM

The proposed hybrid elliptical cryptographic model can be defined using the figure 1.3. That incorporates whole system with their subcomponents. The proposed system is described as:

Input file: that the user input files which is required to encrypt using developed elliptical curve cryptography. This file provided as input into two different algorithm namely MD5 for hash generation and at ECC algorithm for encryption.

MD5: that is implementation of MD5 algorithm, which accepts user input data for hash generation. The generated 128 key used as private key for ECC algorithm.

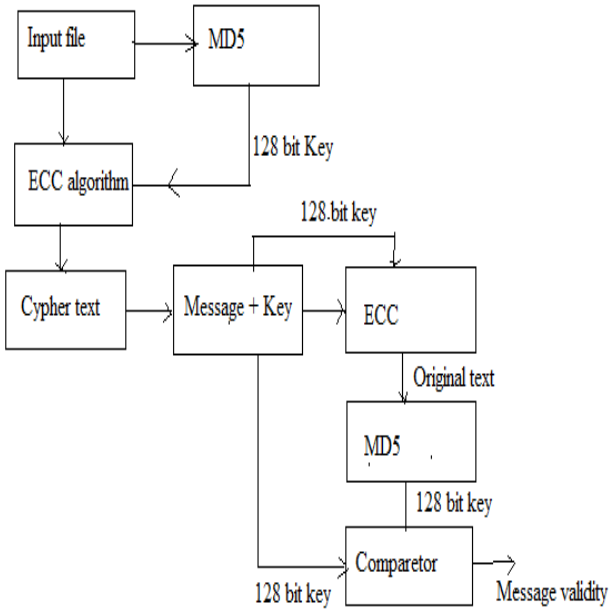

Figure 3.1 Proposed Algorithms

ECC algorithm: the ECC algorithm accepts user input file for encryption with a private key generated by MD5 hash algorithm. Using these input parameters algorithm generate cypher text.

Cypher text: that is pre-cypher text means some additional information are additionally added to the encrypted data.

Message and key: final cypher text is generated in this phase using 128 bit message digest and cypher text.

ECC: that is decryption phase of the algorithm here system separate encrypted message and key and generates the original data.

MD5: recovered data is again produces into MD5 algorithm and hash key is generated.

Comparator: comparator compare the generated 128 bit key to available 128 bit key, if both keys are similar then during communication data is not manipulated.

IV. EXPECTED OUTCOMES

The desired system is a hybrid cryptographic model, after implementation of the desired model the following outcomes expected form study.

An implementation of hybrid encryption algorithm: using the ECC algorithm and MD5 hash generation algorithm a new hybrid algorithm is found.

Performance analysis of developed technique: the performance analysis in different experiments and performance parameters provides the effectiveness of the designed system.

Literature collection: different research articles for exploring the ECC methodology are collected; this can helpful for exploring more the encryption technique.

The next section provides the information about the remaining document organization.

V. RESULTS ANALYSIS

After implementation of desired hybrid ECC algorithm the performance is evaluated and listed in this chapter. That includes the evaluation parameters and experimentation results for the implemented cryptographic technique. The result of all encrypted file represented in table 5.1 and all decrypted file in table 5.2

Table 5.1: File encryption time, memory and file size

Time in Ms	Memory in Kb	File size in kb
268.0	43770.1328125	121.0
181.0	31880.34375	17.0
57.0	59744.5703125	135.0
19.0	35060.390625	45.0
291.0	40374.609375	235.0

In the table 5.1 demonstrate the information about File size, Memory in Kb and Time in MS of all encrypted files.

Table 5.2: File decryption time, memory and file size

Store-overhead	Time in Ms	Memory in Kb	File size in kb
17.0	137.0	40685.140625	121.0
17.0	28.0	55643.9453125	17.0
17.0	92.0	44499.1484375	135.0
17.0	36.0	20400.890625	45.0
17.0	417.0	45579.734375	235.0

In the table 5.2 demonstrate the information about File size, Memory in Kb and Time in MS of all Decrypted files.

5.1 Memory Consumption

The amount of main memory required processing the encryption algorithm and decryption algorithm is known as memory consumption. The given diagram 5.1 demonstrates the comparative memory consumption of encryption and decryption process.

And the given encryption

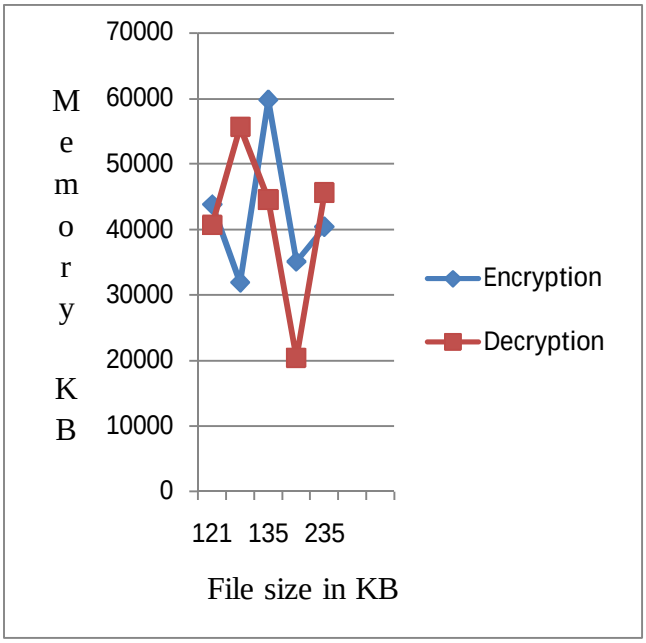

Figure 5.1 Memory consumption

The amount of main memory consumed during the cryptographic process is demonstrated using Y axis in the figure 5.1 and X axis prides the number of different experiments performed with increasing file size. The obtained results demonstrate the amount of main memory during both process is much similar.

5.2 Time Consumption

The amount of time required to successfully encrypt a file and decrypt a file is known as time consumption. The figure 5.2 provides the comparative encryption time and decryption time of the proposed algorithm.

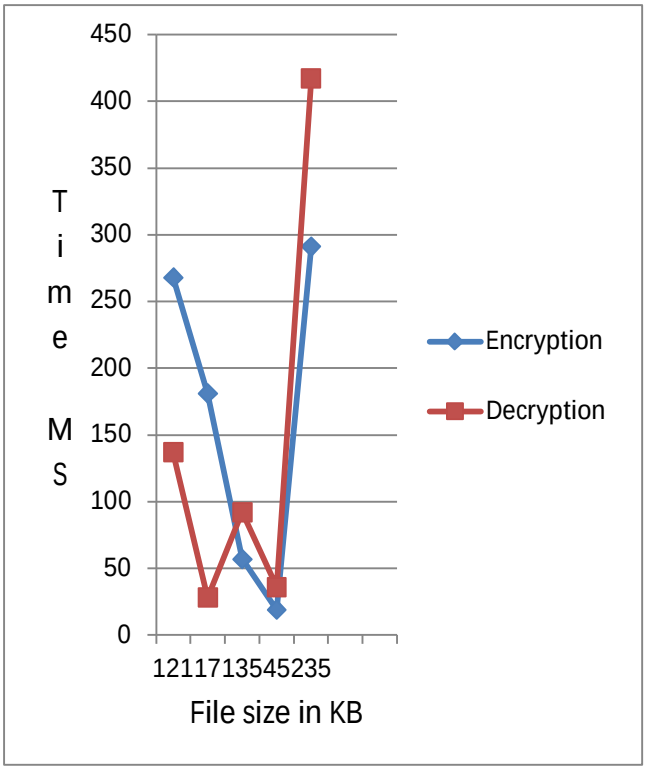

Figure 5.2 Time consumption

The amount of time consumed during both processes is given using figure 5.2 According to the given results the encryption process takes less time as compared to the decryption time. But not much additional time is required. In the given diagram X axis provides the number of experiments performed and the Y axis provides the amount of time consumed in milliseconds.

5.3 Storage Overhead

The amount of additional cypher size from the original files which is desired to encrypt is known as storage overhead. Given figure 5.3 demonstrate the algorithm's storage overhead, as the original file size is increase the amount of storage overhead is same. The X axis provides the number of different experiments performed with increasing files size and the Y axis includes the storage over head in terms of bytes.

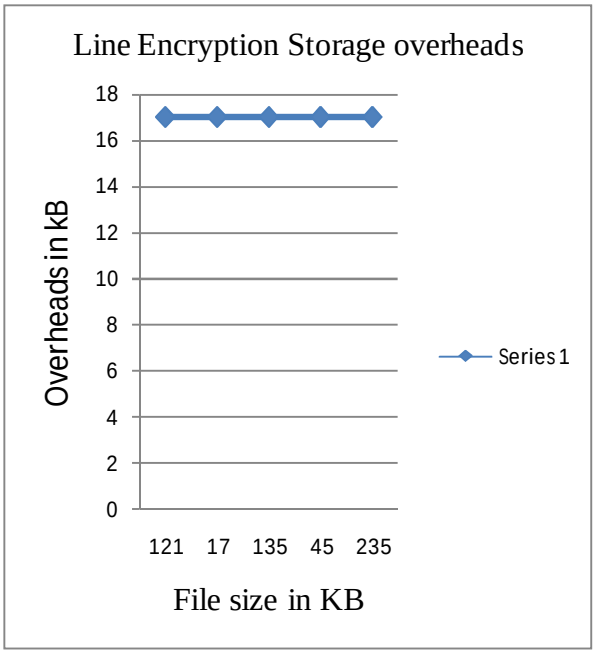

Figure 5.3 Storage overhead

5.4 Data Validity

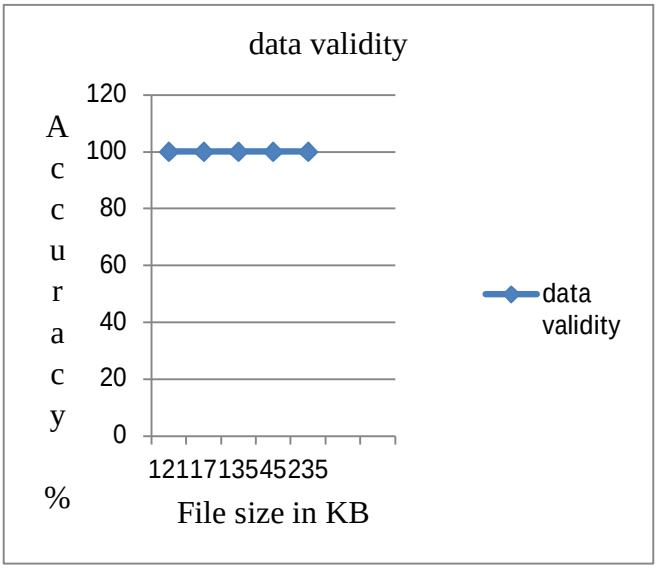

Figure5.4 Data validity

The amount of data accurately recovered after decryption of the encrypted file is termed as data validity. The data validity of the system is given using 5.4 results shows that the system able to recover 100% accurate data during decryption process.

In the given figure 5.4 X axis represents the number of experiments performed with the system and Y axis demonstrate the accuracy percentage.

VI. CONCLUSION AND FUTURE WORK

Given chapter draws the conclusion of the proposed work, which includes the observed facts about ECC and improved ECC algorithm. In addition of that according to the facts proposed technique future extension is also provided.

6.1 Conclusion

The security in the domain of communication is an essential due to outside attackers and malicious users. During communication or data transmission the data is travelled in unsecured and untrusted environment. Therefore, the security becomes more essential during various online applications such as internet or mobile banking, online payments. In this context a secure and lightweight security algorithm helps in improving the data security. In this proposed study the ECC (elliptical curve cryptography) technique is investigated. Additionally to improve security in ECC a new hybrid algorithm is designed. The proposed hybrid cryptographic scheme includes traditional ECC algorithm and MD5 hash generation algorithm.

Implementation of proposed cryptographic algorithm is provided using visual studio dot environment. After implementation of proposed technique performance of the cryptographic algorithm is evaluated in terms of memory consumption and time consumption. The evaluated performance demonstrates the effectiveness of the proposed technique which consumes less resource and provides improved security using the ECC algorithm. The performance of the system is summarized using the given table 6.1.

Table 6.1 performance summery

S. no.	Parameter	Remark
1	Memory consumption	Memory consumption during both cryptographic process is evaluated during different experiments. The memory consumption of the system is adoptable and consumes less memory
2	Time consumption	The less time consumed during process the evaluated time is obtained in terms of milliseconds. Therefore in less time algorithm able to produce cypher text and able to recover them
3	Storage overhead	A small amount of storage overhead is detected in terms of bytes. But that parameter increase as the amount of data is increase to be encrypt
4	Data validity	The receiver end obtain 100% data validity during decryption process

According to the obtained results the performance of the proposed hybrid ECC algorithm is adoptable and demonstrates the effectiveness of proposed technique.

6.2 Future Extension

The proposed hybrid encryption algorithm is adoptable due their efficiency in terms of time and space complexity. In near future the proposed algorithm is implemented with the real time system for enhancing security.

Using hybrid approach where for enhancing the algorithm ECC and MD5 algorithm is consumed. In place of randomly generation of keys MD5 algorithm is used for key generation. Which enhance the strength of cypher text.

REFERENCES

[1] Gururaja.H.S., M.Seetha, Anjan.K.Koundinya,"Design and Performance Analysis of Secure Elliptic Curve Cryptosystem ",International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013

[2] Jitendra Sharma and Prashant Shukla, “ECC Cipher Processor Based On Knapsack Algorithm”,ISSN 2224-5774 (print) ISSN 2225-0492Vol.3, No.2, 2013- National Conference on Emerging Trends in Electrical, Instrumentation & Communication Engineering

[3] K. Immanuvel Arokia James, A.Karthikeyan and M. J. Carmel Mary Belinda, "A survey of low power elliptic curve cryptography for smart network",(Elixir International Journal Accepted: 29 January 2013

[4] Dr.T.P.Saravanabava, M.Gandhi, “SECURITY IN WIRELESS SENSOR NETWORKS-REAL TIME IMPLEMENTATION IN ARM 9”, IJAIR Vol. 2 Issue 5 ISSN: 2278-7844

[5] Young Sil Lee1,, Esko Alasaarela, HoonJae Lee, "Efficient Encryption Scheme based on Elliptic Curve Cryptography (ECC) and Symmetric algorithm in Wireless Body Area Networks (WBANs)",Advanced Science and Technology Letters Vol.38 (Embedded Ubiquitous 2013), pp.36-39

[6] Georgios Evangelidis,Ferran Diego, Radu Horaud, “From Video Matching to Video Grounding", International Conference on Computer Vision, Workshop on Computer Vision in Vehicle Technology (2013)

[7] Dr.K.Ravikumar, A.Udhayakumar, "Secure Multi-Party Negotiation: An Analysis for Electronic Payments in Mobile Computing",ACEEE Int. J. on Network Security , Vol. 5, No. 1, January 2014

[8] Sruti Agarwal, Sangeet Saha, Rourab Paul, Amlan Chakrabarti, “Performance Evaluation of ECC in Single and Multi-Processor Architectures on FPGA Based EmbeddedSystem”, ICCN-2013/ICDMW-2013/ICISP-2013 January 16, 2014

[9] Hatem M. Abdul Kader, Mohie M. Hadhoud, Salah M El-Sayed, Diaa Salama AbdElminaam, "Performance Evaluation Of New Hybrid Encryption Algorithms To Be Used For Mobile Cloud Computing",INTERNATIONAL JOURNAL OF TECHNOLOGY ENHANCEMENTS AND EMERGING ENGINEERING RESEARCH, VOL 2, ISSUE 4 63ISSN 2347-4289

[10] Sumanjit Das, Santosh Kumar Sahu, Santosh Narayan Pati, “A Novel Sign-crypto Scheme Based on ECC with Public Verification and Encrypted Message Authentication”, International Journal of Advanced Research inComputer Science & Technology (IJARCST 2014)© 2014, IJARCST All Rights Reserved 72Vol. 2 Issue 1 Jan-March 2014

[11] Better Privacy and Security in E-Commerce: Using Elliptic Curve-Based Zero-Knowledge Proofs, Sultan Almuhammadi, ieeexplore.ieee.org/Xplore/home.jsp

[12] A New Encryption Algorithm over Elliptic Curve,S. Han, E. Chang, W. Liu, ieeexplore.ieee.org/Xplore/home.jsp

[13] Access Control and Key Management Scheme based on Bilinear Pairings over Elliptic Curves for Mobile Agent, 1 Chia-Hui Liu, 2 Yu-Fang Chung, ieeexplore.ieee.org/Xplore/home.jsp

[14] An Asymmetric Authentication Protocol for Mobile Devices Using Elliptic Curve Cryptography, Mrs. S. Prasanna Ganesan, ieeexplore.ieee.org/Xplore/home.jsp

[15] Elliptic Curve based Key Generation for Symmetric Encryption, S. Maria Celestin Vigila1, K. Muneeswaran2, 2011 IEEE,

[16] Elliptic Curves Cryptosystems Approaches, Ion TUTANESCU, Constantin ANTON, Laurentiu IONESCU, Daniel CARAGATA, 2012 IEEE

[17] Elliptic Curves Cryptographic Techniques, Ali Makki Sagheer2012 IEEE