iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** III **Month of publication:** March 2018

DOI: http://doi.org/10.22214/ijraset.2018.3652

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

Security through Elliptic Curve Cryptography in UID for Fetching Relevant Information Only

Aman Verma (M.Tech CSE)[1], Sweeti Sah (M.Tech CSE)[2], Ram Singar Verma (Assistant Professor CSE)[3]
[1, 2, 3,] *M.Tech Student, BBAU, Vidya Vihar Raibareily Road Lucknow*

Abstract: ***Today we are able to secure our data and information over the internet because of various security techniques used and implemented to meet the user need. ECC (Elliptic Curve Cryptography) is more popular asymmetric key cryptography algorithm which can be implemented in both hardware and software. ECC is quite similar to RSA. This paper will describe the theory of ECC, the role in UID and also the comparison with other security algorithms. The major goal of any security algorithm is to achieve confidentiality, Integrity, Authentication. To achieve security through ECC, it uses arithmetic algorithms as the core operations. Cryptography can be used in wired and wireless network both. In terms of UID, the biometric information of any person can be secured by using elliptic curve cryptography.***
Index terms: Security, ECC, UID, Boimetrics, cryptography, RSA

I. INTRODUCTION

With the increase in the number of computer application globally. There is a need of security for keeping our information secure that is electronically being transferred from one location to another. In keeping our messages secure cryptography plays a major role which includes encryption and decryption of messages means converting the plain text into cipher text and vice versa. There are two types of cryptography mainly symmetric key cryptography and asymmetric key cryptography.

Although the symmetric key is efficient, but asymmetric is more secure. In 1975, Diffe, Hellman and Merkle introduced the idea of public key cryptography. ECC is public key cryptography, which is more complex than RSA. There exist only a single algorithm for RSA but ECC can be implemented in different ways. If ECC is implemented in software than it require moderate speed, but more power consumption and has very limited physical security. If ECC is implemented in hardware, then it is more secure because it cannot be easily read and modified by the intruder which can be very advantageous to user who needs to protect their UID data from intruders.

II. LITERATURE REVIEW

Elliptic Curve Cryptography most secure public key cryptography. During communication the user should have pair of keys that is public key which is distributed to all users and private key which is owned by particular user. There are several operations associated with these keys to increase security.

"Prospective Utilization of Elliptic Curve Cryptography for security enhancement" [2] specified that the cryptographic keys can be made smaller, faster and efficient instead of using conventional methods of key generation and describes the use of elliptic curve cryptography for communication network.

"Achieving authentication and integrity using Elliptic Curve Cryptography architecture" [4] This paper specified the sensitivity of data which needs to be protected during communication from intruders when communication is between two parties. Elliptic curve architecture is based on discrete logarithmic problems.

"Elliptic Curve Cryptography in securing networks by mobile authentication" [1] It proposes an authentication mechanism which is better for low power mobile devices. It uses elliptic curve cryptography system mechanism for generating pass code for mobile. It has both computation efficiency and communication efficiency and require single elliptic curve scalar point multiplication.

"Effective implementation of GF (P) Elliptic Curve Cryptography computations using parallelism" [3] It analyzed the effect of parallelism which is available in two common Elliptic Curve Cryptography. To implement the multiplications of large bit, partitioning and pipeline folding done on single Xiliniux FPGA. The speed up factors can be doubled by using m-ary over binary algorithm.

"Literature survey on Elliptic Curve Encryption Techniques" [7] This paper specified on stopping the unauthorized access to information. The recent way of providing security from intruders is ECC. This paper presents various scalar multiplication with respect to feature, weight, efficiency. This public key based mechanism provide encryption, digital signature and key exchange algorithms.

©IJRASET (UGC Approved Journal): All Rights are Reserved

"Comprehensive Security system for mobile network using Elliptic Curve Cryptography over GF (p)" [5] There are several mobile devices and all vary in computation capability, security etc. Hence the Role of ECC can be divided into two parts, one for designing the API which generate a secret key fro communication and the other is web service which is created to distribute this key to validate the user.

"An Efficient SDRP with Elliptic Curve Integrated Encryption Scheme" [6] This paper describes the security over WSN (wireless sensor nodes). It uses the reprogramming algorithms like SDRP distributed reprogramming protocol. In this Integrated Encryption Scheme provide strong security to wireless sensor network. Only authenticated users will be allowed to modify the system reprogramming. Also the different session keys will be introduced for both owner and other users as they can have multiple views of network and can preserve their own privacy.

"Review on secure and distributed reprogramming protocol" [9] This paper presents wireless reprogramming in sensor networks. Reprogramming is the process of loading new code image to sensor nodes. To ensure security every code update must be authenticated to protect from intruders by installing malicious script into the network. To secure reprogramming the protocol uses identity based cryptography. Elliptic Curve Integrated Encryption Scheme ensures authorization and security in wireless networks.

"An efficient implementation for key management techniques using smart card and ECIES cryptography" [8] This paper specifies the popularity of ECC by reducing the number of keys bit which is required in comparison to other cryptosystem. This paper focused on smart card techniques using ECIES cryptographic algorithm.

"Analysis of Elliptic Key Algorithms" [10] This paper specified that ECC is having maximum security and more efficient performance. The random number (R) is encrypted for the security purpose. ECIES provides advantage over this random number. ECIES (Elliptic Curve Integrated Encryption Technique) is a hybrid scheme.

"A Comparative Analysis of Public Key Cryptography" [11] This paper reviews on public keys like RSA and ECC. ECC is more efficient than RSA as it offer the same security but with smaller keys and faster computation. ECC takes less time for encryption as well as decryption and ECC improves the SSL performance. The RSA algorithm was based on three popular theorems which are Fermat's Little Theorem, Euler's Theorem and Chinese Remainder Theorem but ECC is based on discrete logarithm problems.

"Issues in Elliptic Curve Cryptography Implementation" [12] This paper describes the brief explanation on ECC theory. ECC has less overhead compared to RSA and provide same level of security as RSA. The only disadvantage is its attractiveness and lack of maturity.

III. OBJECTIVES

A. *Confidentiality*

The data should be confided to the real or original user and also assuring that only authorized user can be allowed to access the information.

B. *Integrity*

The data must be altered by the original user. The intruder should not modify the content while any operation.

C. *Authentication*

This is the security measure related to Identification over the network. The person who is accessing the data should be real identity person.

D. *Non-Repudiation*

If the communication over the network has taken place then the party in a communication cannot deny falsely that the part of the actual communication happened.

IV. TYPES OF CRYPTOGRAPHIC ALGORITHM

A. *Symmetric Key (Secret):* Same key for encryption and decryption.

B. *DISADVANTAGE:* Scalable

Two different keys are required for encryption and decryption

C. *Asymmetric Key (Public):* Different Key for encryption and decryption.

©IJRASET (UGC Approved Journal): All Rights are Reserved

D. Advantage: Only one key is required so attacker can easily decrypt
E. Disadvantage: Slowe The size of the encrypted text is too large.
F. Hash Function: Use of mathematical transformation.

V. RSA (RIVEST, ADI SHAMIR AND LEONARD ADLEMAN)

In 1977, RSA was discovered at MIT, first published at 1978 and is practically and widely used for secure data transmission. In this we do factoring of two large prime number. There is higher security and the use of digital signature makes it even more secure and safe.

A. There Are Two Types Of Function
1) Encryption function: Conversion of plain text to cipher text and vise versa with the help of private key.
2) Key Generation: Factoring of modulu n is equivalent to determining private key from RSA public key.

B. Algorithm
1) Choose two large prime numbers P and Q.
2) Compute n=P*Q
3) Choose public key e, gcd(ϕ(n),e) = 1; 1<e<ϕ(n)
4) Select private key d, d*emodϕ(n)=1
5) Public key (n,e) and private key (n,d).

C. Disadvantages
1) Slower encrypting speed.
2) Slower in generating the key.
3) Less efficient for decryption.
4) The length of the message should be less.
5) Every time RSA is initialized with two large prime numbers.
6) Not suitable for wireless sensor network
7) Lengthy Keys.

VI. ECC (ELLIPTIC CURVE CRYPTOGRAPHY)

In 1985, Victor Miller (IBM) and Neil Koblitz discovered ECC. ECC is based on discrete logarithms
and can be used for smart cards. It take less time for encryption as well as decryption of any message. There are few operations that are performed by ECC are subtraction, addition, multiplication and doubling. Out of which multiplication takes more time.
In terms of operation, ECC is comparatively slower than RSA but In terms of security ECC is faster compared to RSA.

Security (Bits)	RSA Key Size	ECC Key Size
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

Table 1: Security Comparison based on Key Size[11]

©IJRASET (UGC Approved Journal): All Rights are Reserved

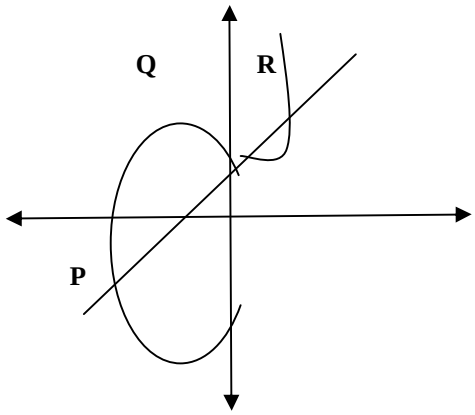
Elliptic curve equation over finite field Fp:

$$Y^2 = X^3 + ax + b \bmod P$$

Y, X, a and b are all within Fp (p is a integer modulo p).
a and b is the coefficient which determines the points on the curve.
Curve Coefficient has to fulfill one condition i.e.

$$4a^3 + 27b^3 \text{ not equal to zero}$$

This condition will ensure that the curve will not contin any singularities.



$$Y^2 = X^3 + ax + b$$

Fig1: ECC Curve

A. Advantages

1) Shorter encryption key
2) Faster
3) Less computing power
4) Occupies less memory.
5) Decryption is faster

B. Disadvantages

1) Encrypted message has larger size.
2) Complex
3) Difficult to implement.
4) Encryption and key generation is slower

C. The Advantage of Ecc over Rsa

Can be used for wireless devices where memory, computing power and battery is limited. But the computation of both RSA and ECC is same $0(n^3)$
Where 'n' is the key length in bits.

VII. ECC ROLE IN UID

The maximum security can be achieved through ECC and RSA. But here the role of ECC is represented in UID. As there can be various IDs of any person but each ID is unique to that person. The information of any person like biometric information, personal details are stored. These details are very important to each person which needs security. ECC can provide the security to these information related to UID with shorter keys.

VIII. ECC ISSUES

Breaking the encryption with ECC should be very advance. ECC consists of few operations and also define the protocols that define how addition, subtraction, doubling and multiplication are performed.

©IJRASET (UGC Approved Journal): All Rights are Reserved

Among all the above operations, multiplication is very time consuming in ECC cryptographic scheme. The main research topic in ECC is the software and hardware implementations. These ECC operations are performed in the three layer. In the upper layer, there can be various algorithm for doing multiplication. In the middle layer there exists various combination of coordinates system and finite field representation. The curve operations come under this middle layer. At last the lower level is about finite field operations and finite field arithmetic. Various functions which can be applied to it are:

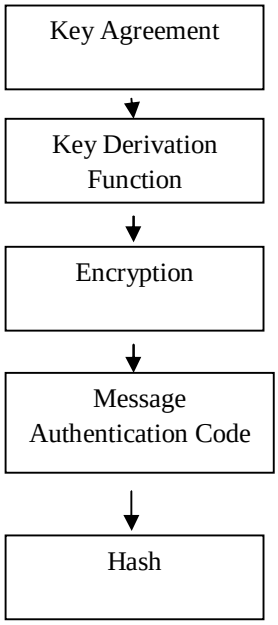


Fig 2: Various Functions of ECC

IX. PROPOSED WORK

UID has various information which can be viewed to any user through internet. So the role of ECC is to secure the details of user as some details will be viewed to user and some details will be displayed in encrypted form. The ECC will hide or encrypt the details of user through its encrypting technique.

This can be done to various Identity cards like Aadhar Card, License Card, Pan Card and many more. Currently with the increasing attacks it is important to provide security such as availability, confidentiality, integrity, authentication.

X. CONCLUSION

Hence this paper will describe the security in UID through ECC by displaying only relevant data to external user and detailed data to only real user. The external user if wants to view the detailed data then it would be encrypted through ECC for security purpose.

Hence ECC has proven less overheads as compared to RSA and has greater security and performance to secure the information even though it lack maturity and attractiveness then also it good for security purpose.

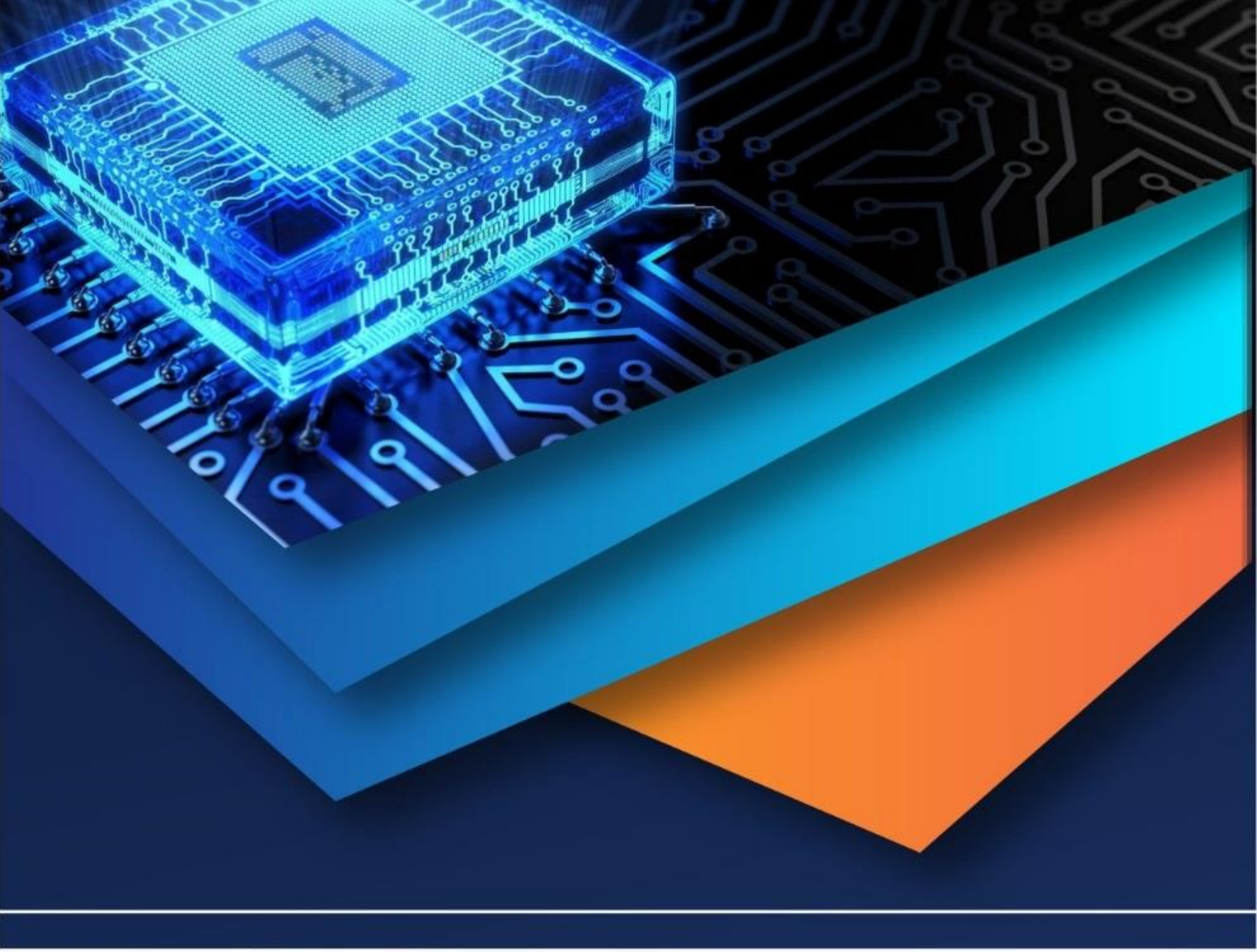
REFERENCES

[1] Manoj Prabhakar ,"Elliptic Curve Cryptography in securing networks by mobile authentication", International Journal on Cryptography and Information Security, September 2013
[2] Sonali Nimbhorkar and Dr. L. G. Malik, "Prospective utilization of Elliptic Curve Cryptography for Security enhancement", International Journal of Application or Innovation in Engineering and Management, January 2013.
[3] N. Sivasankari and M. Kannan, "Effective implementation of GF (p) Elliptic Curve Cryptography Computations using parallelism", International Journal of Emerging Technology and Advanced Engineering, November 2013
[4] Ms. Manali Dubal and Ms. Aaradhana Deshmukh, "Achieving authentication and integrity using Elliptic Curve Cryptography architecture", International journal of Computer Applications, May 2013
[5] Ruchika Markan and Gurvinder Kaur "An Efficient SDRP with Elliptic Curve Integrated Encryption Scheme", International Journal of Advanced Research in Computer Science and Software Engineering, November 20
[6] Ruchika Markan and Gurvinder Kaur, "Literature survey on Elliptic Curve Encryption Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, September 201
[7] Kaalidoss Rajamani and Dr. A. Arul L. S, "Survey: Elliptic Curve Cryptography using scalar multiplication algorithm", International Journal of Innovative Research in Advanced Engineering, March 2014.

©IJRASET (UGC Approved Journal): All Rights are Reserved

[8] Neha Gupta, Harsh Kumar Singh, Anurag Jain, "An efficient implementation for key management technique using smart card and ECIES cryptography", International Journal of Control Theory and Computer Modelling, November 2013.
[9] Ruchika Markan and Gurvinder Kaur, "Review on secure distributed reprogramming protocol", International Journal of Advanced Research in Computer Science and Software Engineering, August201
[10] S.Nithya, Dr. E. Geogre Dharma Prakash Raj, "Analysis of Elliptic Key Algorithms" , International journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3 Issue 8, August 2014.
[11] Ajit Karki, "A Comparative Analysis of Public Key Cryptography", International Journal of Modern Computer Science (IJMCS) Volume 4, Issue 6, December, 2016.
[12] Marisa W. Paryasto, Kuspriyanto, Sarwono Sutikno and Arif Sasongko, "Issues in Elliptic Curve Cryptography Implementation", Internetworking Indonesia journal, Vol. 1/No. 1 (2009)

©IJRASET (UGC Approved Journal): All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)