IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Elliptic Curve Cryptography Implementation For Strengthening The Security Of Mobile Network

DR. SUKALYAN GOSWAMI

Professor, Department of Computer Science and Engineering

University of Engineering and Management, Kolkata, India

Abstract: Recently, the mobile industry has experienced an extreme increment in number of its users. The GSM network with the greatest worldwide number of users succumbs to several security vulnerabilities. Security is a burning and intelligent issue. It will always remain relevant as it is important in all types of applications. GSM Security flaws have been identified several years ago. Some of these flaws have been fixed by the 3GPP but others are left to discussion. Most of the RSA–based hardware and software products and standards require big key length for higher security level. In this paper we will be focusing on the comparison of working procedure of elliptic curve cryptography and RSA algorithm in GSM network to how it's a better promise for a faster and more secure method of encryption in comparison to the current standards in the Public-Key Cryptographic algorithms of RSA.

Index Terms **– Elliptic Curve Cryptography, RSA, GSM, Cryptography.**

I. INTRODUCTION

Mobile phones are used on a daily basis by hundreds of millions of users, over radio links. Fixed phones offer some level of physical security (i.e. physical access is needed to the phone line for listening in). Unlike a fixed phone, with a radio link, anyone with a receiver is able to passively monitor the airwaves. Therefore, it is highly important that reasonable technological security measures are taken to ensure the privacy of user's phone calls and text messages (data) as well to prevent unauthorized use of the service [1] [2]. GSM is the 900 MHz radio system using a common world-wide standard. The system used by PCN (DCS 1800) is technically identical, except for the frequency. GSM was designed to grow and meet the needs of new technologies. GSM is currently composed of EDGE, 3GSM, and GPSR. Each member of the family is designed to solve a particular need. EDGE is an upper level component used for advanced mobile services such as downloading music clips, video clips, and multimedia messages. GPSR is designed for "always-on" systems that are needed for web-browsing. 3GSM is the GSM running on third generation standards for multimedia services [3]. It allows full roaming from operator to operator if mutual bilateral agreements are in place [4]. However, being the internet an open and insecure network, some anxiety has been raised in transmitting sensitive information. The solution lies in using cryptography and secures authentication protocols that guarantee the confidentiality, authentication and integrity of communications. Such protocols, like SSL [7] and SET [8], already exist and are widely used in current e-commerce applications. Most of them are based in RSA public key cryptography. A protocol is developed which is based exclusively on elliptic curve cryptography, an asymmetric cryptography that performs well in resource constrained platforms and maintain the high

security level that one can achieve with the protocols in use today [6]. This paper concentrates on the drawbacks of RSA algorithm and why elliptic curve cryptography algorithm is preferred to RSA.

II. WHY GSM SECURITY IS REQUIRED?

Global System for Mobile Communications, GSM, is an advanced mobile phone system used around the world. GSM has many benefits over its predecessors in terms of security, capacity, clarity, and area coverage. GSM aimsto provide a secure connection for communication. Since its advent in the early 1980's it has grown into a family ofservices to provide everything from mobile voice to mobile data. The best way to appreciate security is by looking at how chaotic and dangerous a mobile communications system would be without security. Atany given moment, anybody could eavesdrop into your conversation. Your bank account information, dailyschedule, and any other information you may disclose on the phone would be at risk. Besides listening in, at any given moment, a hacker could impersonate your user information to make calls that would later amount to thousands of dollars in service charges. The list goes on and on. GSM was designed to address security problems like those listed above [3]. The security methods standardized for the GSM System make it the most secure cellular telecommunications standard currently available. Although the confidentiality of a call and anonymity of the GSM subscriber is only guaranteed on the radio channel, this is a major step in achieving end-to-end security. The subscriber's anonymity is ensured through the use of temporary identification numbers. The confidentiality of the communication itself on the radio link is performed by the application of encryption algorithms and frequency hopping which could only be realized using digital systems and signaling. The security architecture of GSM was originally intended to provide security services such as anonymity, authentication and confidentiality of user data and signaling information [5].

The security goals of GSM are as follows:

- Authentication of mobile users for the network,
- Confidentiality of user data and signalling information,
- Anonymity of subscriber's identity,
- Using SIM (Subscriber Identity Module) as a security module [5].
- Keys are securely stored [3].

III. CURRENT WORKS ON GSM SECURITY USING RSA ALOGITHM

The RSA public key cryptosystem was proposed by and named after R.L. Rivest, A. Shamir and L. Adlemanin 1978. Public key cryptography is based on the creation of mathematical puzzles that are difficult to solve without certain knowledge about how they were created. The creator keeps that knowledge secret (the private key) and publishes the puzzle (the public key). The public keyconsists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n andthe private (or decryption) exponent d which must be keptsecret [3]. Encryption and decryption are performed by identical modular exponentiation operations using apublic and private key pair. The input X is represented asa sequence of integers in the range [0, M − 1] and then weneed to raise it to the Eth power modulo M. This operation can be computed by repeated modular multiplications and squares using the R-L binary method [5]. It is optimized for speed by allowing multiplications and squares to be performed in parallel. The inputs are initially converted to the Montgomery domain. Each bit ofthe exponent is then scanned from right to left and a multiplication performed if the bit is one. A squaring is performed on each step of the iteration. At the end of eachexponentiation, the output _Y is mapped back to normal representation [11].

$$Y = X*E \pmod{M} \qquad (1)$$

c = m*e mod n*c

This can be done quickly using the method of exponentiation by squaring. Bob then transmits c to Alice [3].

A. *Decrypting messages* [3]

Alice can recover m from c by using her private key d in the following procedure**:**

m = c^d mod n

Given m, she can recover the original message M. The decryption procedure works as:

c^d ≡ (me)^d ≡m^(ed) (mod n)

RSA is not secure if the same message is encrypted to several receivers, to completely break RSA one needs to find the prime factors. In practice, RSA has proved to be quite slow, especially for key generation algorithm. Furthermore, RSA is not well suited for limited environments like mobile phones and smart cards without RSA co-processors because it is hard to implement large integer modular arithmetic on such environments [16]. RSA algorithm encryption used in file encryption for small files, any file with asymmetric key encryption into its text can be more convenient to communicate and manage, and it has broad development prospects [17].

IV. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic curve cryptography is an approach to public key cryptography based on algebraic structures of elliptic curves over finite fields. [8][20] Elliptic curves defined over a finite-field provide a group structure that is used to implement the cryptographic schemes. The elements of the group are the rational points on the elliptic curve, together with a special point O (called the "point at infinity"). [10] The mathematical operations of elliptic curve cryptography are defined over the elliptic curve

y^2 = x^3 + ax + b, where
4a^3 + 27b^2 ≠ 0

Each value of the ‘a’ and ‘b’ gives a different elliptic curve. All points (x, y) which satisfies the above equation plus a point at infinity lies on the elliptic curve. The public key is a point in the curve and the private key is a random number. The public key is obtained by multiplying the private key with the generator point G in the curve. The generator point G, the curve parameters ‘a’ and ‘b’, together with few more constants constitutes the domain parameter of elliptic curve cryptography. [14] We can use elliptic curve cryptography to construct a new cryptosystem. If A wants send message to B. First, A chooses an elliptic curve and a point G on it, note that both A and B should know G. Then A encodes message to the point Pm on the curve. B choose a random number a (B's private key), and compute a*G (B's public key), and announce it. Then A chooses another random number k, and compute

Pm + k*(a*G) and k*G,

C= (k*G, Pm + k*a*G)

to B. When B receives C, he can compute

Pm=Pm - k*a*G - a*k*Q

and get Pm, then decode Pm to the message. Because of the ECDLP, it is very hard for attackers to get Pm [12]. Elliptic curve cryptography provides higher level of security due to its complex mathematical operation.

Mathematics used for elliptic curve cryptography is considerably more difficult and deeper than mathematics used for conventional cryptography. In fact this is the main reason, why elliptic curves are so good for cryptographic purposes, but it also means that in order to implement elliptic curve cryptography more understanding of mathematics is required. A short introduction to mathematics behind elliptic curve cryptosystems is given below [12].

A. Mathematics behind ELLIPTIC CURVE CRYPTOGRAPHY

Cryptographer noticed that elliptic curves behaved conveniently when operations were performed with prime modulus. That means cryptographer elliptic curve is in the form

$$y^2 \bmod p = (x^3+ax+b) \bmod p$$

Where,

$$4a^3+27b^2 \neq 0$$

and p is a prime number and a, b is the parameter of the curve. Here variables and coefficient are all restricted to elements of a finite field. There are two families of elliptic curve are used in cryptography application:

1. Prime Curves over Zp
2. Binary Curves over GF (2^m).

In Binary curve defined over GF (2^m), the variables and co-efficient all take on values in GF (2^m) and in calculation performed over GF (2^m).

In Prime Curve over Zp we use a cubic equation in which the variables and co-efficient all take on values in the set of integers from 0 through (p-1) and in which calculations are performed modulo p.

B. Arithmetic Operation in ELLIPTIC CURVE CRYPTOGRAPHY

The rule of mathematical operation on elliptic curve is different from the rule conventional mathematical operations. If we want to add two points of elliptic curve then we have to use are some rules which are as follows

Rules of Addition:

Rule 1. Infinity + Infinity = infinity.
Rule 2. (x1, y1) + Infinity = (x1, y1).
Rule 3. (x1, y1) +(x1, -y1) = Infinity.
Rule 4. If $x1 \neq x2$ then
(x1, y1) +(x2, y2) =(x3, y3).
Where
x3 =(λ2-x1-x2) mod p, y3 = (λ(x1-x3)-y1) mod p And
λ = ((y2-y1)/(x2-x1)) mod p

Rule 5. (Doubling):
If $y1 \neq 0$, then
(x1,y1) +(x1,y1) = 2(x1,y1)=(x3,y3).
Where
x3 = (λ^2-2x1)mod p
y3 = (λ(x1-x3)-y1) mod p And
λ = ((3x1^2+a)/2y1) mod p.

Rule of Subtraction:

(x1, y1) - (x2,y2) = (x1, y1) + (x2, - y2).

Rule of Multiplication:

Suppose P is a point on elliptic curve P=(x, y)

Thus 8*P =P+P+P+P+P+P+P+P
=2P+2P+2P+2P
=4P+4P

C. *Point on ELLIPTIC CURVE CRYPTOGRAPHY*

For any operation on elliptic curve, first of all wehave to find the all point of that curve [10]. Thus for finding the point on the curve firstly we have to chose anyelliptic curve.

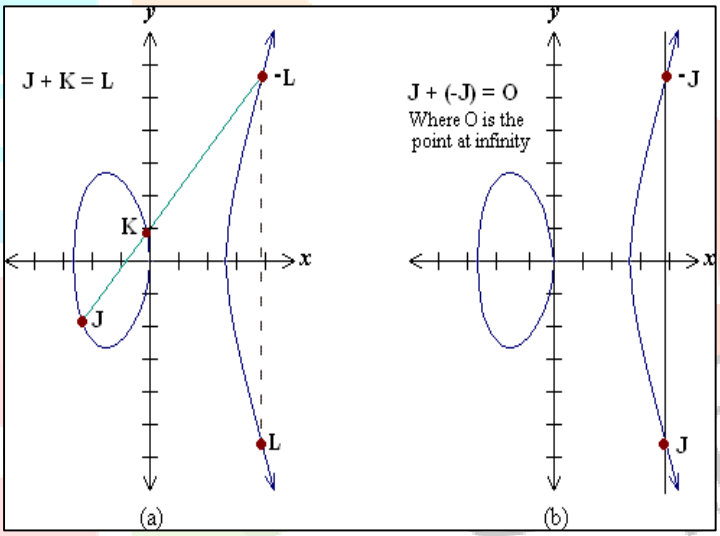
Suppose

y^2 mod p=(x^3+ax+b) mod pis an elliptic curve Where

$4a^3+27b^2 \neq 0$

Then points on this curve are the set Ep (a, b) consisting of all pairs of integers (x, y), which satisfy the above equation together with the point Zero. Method for finding the points on the curve is as follows

- .Determine the L.H.S of elliptic curve. For all (x,y) € Zp.
- Determine the R.H.S of elliptic curve. For all(x,y) € Zp.
- Choose the Pair of corresponding value of x andy as a pair for all x, y € Zp for which L.H.S. =R.H.S.
- All pairs of such (x, y) are the point on the curve[13].



D. *ELLIPTIC CURVE CRYPTOGRAPHY algorithm*

- At first we will take a curve in the form

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

Where a and b are curve parameters.

- We then choose a prime number.
- Using point adding and point doubling we compute the points on the curve.
- Select a generating point out of those points whose order should be large.
- Then take a random number less than order of generating point as a private number for each entity. This will be a secret key.
- This entity will then generate its public key by multiplying the generating number with the secret number and will publish the point. [15]

V. APPLICATIONS OF ELLIPTIC CURVE CRYPTOGRAPHY ALGORITHM

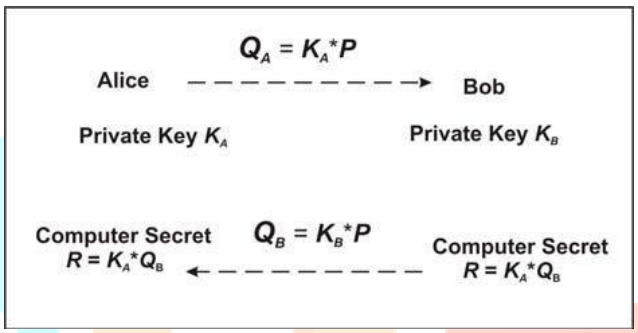
A. *Diffe-hellman*

The Diffe-Hellman protocol is the basic public-key cryptosystem proposed for secret key sharing. If A and B first agree to use a specific curve, field size, and type of mathematics. They then share the secret key by process as follows. We can see that we just need scalar multiplication in order to implement the Diffe-Hellman protocol.

Diffe-Hellman Protocol algorithm:

- A and B each chose random private key ka and kb
- A and B each calculate ka*P and kb*P, and send them to opposite side.
- A and B both compute the shared secret

  Q = ka (kb*P) = kb (ka*P) [11][18]



Diffe-Hellman Protocol based on ECC

B. *Elliptic curve digital signature algorithm*

EC Digital Signature Algorithm is the elliptic curve analogue of the DSA; this protocol needs not only the elliptic curve operations, such as scalar multiplication, field multiplication and field inverse multiplication, but also integer multiplication, inverse operation, modular operation and a hash function. In the ECDSA, A (Alice) generates the signature with his secret key and B (Bob) verifies the signature with A's public key. Algorithm.3 is the ECDSA protocol which A signs the message m and B verifies A's signature [10].

ECDSA Protocol algorithm:

- Key generation : (A)

  1: Select a random integer d from [1; n -1]. 2: Compute Q = d.P.

  3: A's public key is Q; A's private key is d.

- Signature generation : (A)

  1: Select a random integer k from [1; n - 1].

  2: Compute k*G = (x1; y1) and r = x1(mod n). 3: If r = 0 then go to step 1.

  4: Compute [k^ (-1)] (mod n).

5: Compute s = [k^ (-1)] (SHA - 1(m) + dr) (mod n).

  6: If s = 0 then go to step 1.

7: Send m and (r; s), which is A's signature for the message m, to B.

- Signature verification : (B)

1: Verify that r and s are integers in [1; n -1].

2: Compute e = SHA - 1(m).

3: Compute w = [s^ (-1)] (mod n). 4: Compute u1 = [e * w] (mod n)
And u2 = [r * w](mod n).

5: Compute u1P +u2Q = (x1; y1) and v = x1(mod n).

6: If s = 0 then go to step 1.

7: Accept the signature if and only if v = r.

VI. COMPARISON OF RSA AND ELLIPTIC CURVE CRYPTOGRAPHY ALGORITHM

As analyzed before, in the wireless condition, the equipment's recourse, power and compute capacity all are limited. So the encryption system in it must be low power and RAM consumption. But current the most popular algorithm RSA does not satisfy it. The elliptic curve cryptography is more effective than RSA. There are some comparisons between elliptic curve cryptography and RSA .

ECC key size	163	283	409	571
RSA key size	1024	3072	7680	15360
Key size ratio	1:6	1:11	1:19	1:27

Table 1: The Key Size Ratio

From table 1, we can see the elliptic curve cryptography needs small key size but can achieve the same security level as a big key size of RSA. A typical example is that a 163-bit elliptic curve cryptography key can do as well as, in the same condition, 1024-bit RSA key [19].

Algorithm	**Signature**		**Key Exchange**	
	Sign	**Verify**	**Client**	**Server**
RSA1024	304	11.9	15.4	304
ECDSA160	22.82	45.09	22.3	22.3
RSA2048	2302.7	53.7	57.2	2302.7
ECDSA224	61.54	121.98	60.4	60.4

Table 2: Energy cost of digital signature and key exchange computations [mJ].

Table 2 shows us the energy cost of RSA and ECDSA (a signature algorithm of elliptic curve cryptography). From here we can clearly see that elliptic curve cryptography has much better performance than RSA. The elliptic curve cryptography can give a total solution for the security problems in the wireless communication, such as authentication, signature, and key exchange. The ECDSA is the elliptic curve analogue of DSA. It is a very important one of elliptic curve cryptography. The security of 322-bit ECDSA is equal to the 1024-bit RSA signature, and the length of ECDSA certification is 62 bytes, while that of RSA is 256 bytes, DSA is 168 bytes [12]. There is huge importance of shorter key lengths especially in applications having limited memory resources because shorter key length requires less memory for key storage purpose. Elliptic curve cryptosystems also require less hardware resources than conventional public-key cryptography. Now at the security level elliptic curve cryptography is more secure than RSA. RSA can be cracked successfully, uses 512 bits

and for elliptic curve cryptography the number of bits is 97, respectively. It has been analyzed that the computation power required for cracking elliptic curve cryptography is approximately twice the power required for cracking RSA. Elliptic curve cryptography provides higher level of security due to its complex mathematical operation. Mathematics used for elliptic curve cryptography is considerably more difficult and deeper than mathematics used for conventional cryptography. In fact this is the main reason, why elliptic curves are so good for cryptographic purposes, but it also means that in order to implement elliptic curve cryptography more understanding of mathematics is required. [13] The inverse operation of elliptic curve cryptography which known as the Elliptic Curve Discrete Logarithm Problem (ECDLP) gets harder, faster, against increasing key length than do the inverse operations in Diffie Hellman and RSA. As security requirements become more stringent and as processing power get cheaper and more available, elliptic curve cryptography becomes the more practical system for use. And as security requirements become more demanding, and processors become more powerful. This keeps elliptic curve cryptography implementations smaller and more efficient than other implementations. Elliptic curve cryptography can use a considerably shorter key and offer the same level of security as other asymmetric algorithms using much larger ones. Moreover, the difference between elliptic curve cryptography and its competitors in terms of key size required for a given level of security becomes dramatically more pronounced, at higher levels of security[10].

VII. CONCLUSION

This paper shows that it is possible to implement the authentication protocol using elliptic curve cryptography in resource constrained mobile devices with reasonable performance compared to RSA. It gives a brief comparative point between elliptic curve cryptography and RSA. The elliptic curve cryptosystem has a better performance than traditional cryptosystem with high speed, low computation, and resource consumption. So it is very suitable for the wireless environment. But because of not all the wireless communication protocol have introduced elliptic curve cryptography, and the elliptic curve cryptography's fast hardware implementation is also being researched, the use of elliptic curve cryptography in wireless communication is more in academic than in industry now.

REFERENCES

[1] Rehab El Nemr, Imane Aly Saroit Ismail, S. H. Ahmed: Action- Triggered Public-Key cryptography for GSM systems with Phone- Dependent end-to-end encryption, Vol (5), Issue (2), June 2006, www.icgst.com/cnir/Volume5/Issue2/P1140626001.pdf

[2] Jeremy Quirke, "Security in the GSM system", May 2004, www.it.iitb.ac.in/~kavita/GSM_Security_Papers/Security in the GSM system 01052004.pdf

[3] Tuan Huynh and Hoang Nguyen: Overview of GSM and GSM Security Department of Electrical Engineering and Computer Science Oregon State University June 06, 2003, http://www.d-cell.com/setyobudianto/resources/gsm/overview_gsm_security.pd f

[4] Brookson, C, GSM MoU Security Rapporteur, British Telecommun. plc, London:GSM security: a description of the reasons for security and the techniques Issue Date: 1994, On page(s): 2/1 - 2/4, Date of Current Version: 06 August 2002

[5] Mohsen Toorani, Ali Asghar Beheshti Shirazi: Solutions to the GSM Security Weaknesses, Issue Date: 16-19 Sept. 2008, pp. 576-581, Date of Current Version: 20 January 2009, ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4756489

[6] Mrs. S. Prasanna Ganesan: An Efficient Protocol for Resource Constrained Platforms Using ECC, Vol.2 (1), 2009, pp. 89-91, www.enggjournals.com/ijcse/doc/IJCSE10-02-01-16.pdf

[7] The Secure Sockets Layer (SSL) Protocol Version 3.0, ISSN: 2070-1721, August 2011, tools.ietf.org/html/rfc6101.

[8] Secure Electronic Transaction (SET) Protocol, Vol. 6, www.isaca.org/Journal/Past-Issues/2000/Volume-6/Pages/Secure-Electronic-Transaction-SET-Protocol.aspx

[9] Devon Ritter: Elliptic-curve-cryptography.pdf

[10] Moncef Amara and Amar Said: Elliptic Curve Cryptography and its applications, Issue Date: 9-11 May 2011, pp. 247-250, Date of Current Version: 27 June 2011

[11] Francis Crowe, Alan Daly and William Marnane: A Scalable Dual Mode Arithmetic Unit for Public KeyCryptosystems, Proceedings of the International Conference on Information Technology:

Coding and Computing (ITCC'05) 0-7695-2315- 3/05, ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=01428523

[12] Jia Xiangyu Wang Chao: The Application of Elliptic Curve Cryptosystem in Wireless Communication, 2005 IEEE, ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1618234

[13] Avanindra Kumar Lal, Sandip Dutta: ECC Based Biometric Encryption for Network Security, JOURNAL OF COMPUTING, VOLUME 3, ISSUE 6, JUNE 2011, ISSN 2151-9617

[14] Anoop MS: Elliptic Curve Cryptography, www.tataelxsi.com/whitepapers/ECC_Tut_v1_0.pdf?pdf_id=public_key_TEL.pdf

[15] Vivek B.Kute, P. R. Paradhi, G. R. Bamnote: A SOFTWARE COMPARISON OF RSA AND ECC, Vol. 2, No. 1, May 2009, ISSN: 0974-1003, www.researchpublications.org/IJCSA/issue4/2009-IJCSA-02-01-15.pdf

[16] Sameer Hasan Al-Bakri, M.L. Mat Kiah, A.A. Zaidan, B.B. Zaidan, Gazi Mahabubul Alam: Securing peer-to-peer mobile communications using public key cryptography: New security strategy, Vol.6(4), pp. 932-938, 18 February 2011.

[17] Wang Suli, Liu Ganlai: File encryption and decryption system based on RSA algorithm, Issue Date: 21-23 Oct. 2011, pp. 797- 800, Date of Current Version: 28 November 2011, ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6086320

[18] Xu Huang, Pritam Shah, and Dharmendra Sharma: Fast Algorithm in ECC for Wireless Sensor Network, March 17-19, 2010, Proceedings of the International Multiconference of Engineers and Computer Scientists 2010 Vol II, IMECS 2010.

[19] Masood Habib, Tahir Mehmood, Fasee Ullah, Muhammad Ibrahim: Performance of WiMAX Security Algorithm (The Comparative Study of RSA Encryption Algorithm with ECC encryption Algorithm), 13-15th Nov. 2009, Vol. 2, pp. 108-112, ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5360117

[20] The Case for Elliptic Curve Cryptography-NSA/CSS, 15 Jan. 2009, www.nsa.gov/business/programs/elliptic_curve.shtml