Vol. 5(18) Special Issue, Dec. 2015, PP. 2577-2584

Contents list available at IJMEC

International Journal of Mechatronics, Electrical and Computer Technology (IJMEC)

Journal Homepage: www.aeuso.org

PISSN: 2411-6173 - EISSN: 2305-0543

An ElGamal Encryption Scheme of Pauli Spin ½ Matrices and Finite Machines

B. Ravi Kumar[1], A.Chandra Sekhar[1] and G.Appala Naidu[2]

[1]*Department of Mathematics, GIT, Gitam University, Visakhapatnam, India*

[2]*Department of Mathematics, Andhra University, Visakhapatnam, India*

***Corresponding Author's E-mail:** ravikumarbrk6@gmail.com*

Abstract

Cryptography is used for encryption and decryption of data using mathematics. Cryptography transmits the information in an illegible manner such that only intended recipients will be able to decrypt the information. In the recent years, researchers developed several new encryption methods. We too have mange to develop a new method that is, ElGamal encryption scheme, which uses points on the elliptic curve, finite state machines and Pauli spin matrices. This method makes our system invulnerable to attacks from a hacker who does not possess appropriate decoding them.

Keywords: *ElGamal, Pauli spin ½ matrices, Finite state machine, Encryption, decryption..*

1. Introduction

In the year 1985, Victor Miller and Neal Koblitz first introduced the Elliptic curve cryptography. In the year 1985. Elliptic curve cryptography has proven its security by withstanding a generation of attacks. In the recent years, as the wireless communication has grown rapidly, the numerous companies have adopted elliptic curve cryptography as an innovative security technology. Elliptic curve poses a shorter encryption key compared to other techniques, which allows it to be faster and less power consuming. It provides almost the same security as '1024'-bit RSA encryption key [1] [2] [3] [4] [8]. In general, cubic equations for elliptic curves take the following form, known as Weierstrass equation [5]: where g, h, I, j, k are real numbers and x, y take on values in the real numbers. For our purpose, it is sufficient to limit ourselves to equations of the form where x, y, g, h belongs to R, Q, C or Fp. Also include in the definition of an elliptic curve is a single element denoted by O and called the point at infinity or the zero point. There is also a requirement that the discriminant.

2. The ElGamal Cryptosystem

Two communicating parties 'A' and 'B' initially agree upon the Elliptic curve $E_p(x, y)$ and p is sufficiently large prime number and (x,y) is the point on the Elliptic curve. For secure communication over insecure channels, both A and B fix a point C(x_1, y1). A initially selects the private key 'K_A' and generates the public key $P_A = K_A \times C.$ Next 'B' selects the private key K_B and generates the public key $P_B = K_B \times C.$ Now 'A' wants send the message M to B. For this purpose A chooses a random integer 'n'

Article History:

IJMEC DOI: 649123/10175

Received Date: Sep. 09, 2015

Accepted Date: Dec. 15, 2015

Available Online: Dec. 24, 2015

now A encrypts M as $CT_m = \{nC, M + nP_B\}$ and sends to B. Then 'B' decrypts the CT_m as $M + nP_B - K_B(nC) = M + n(K_B C) - K_B(Cn) = M$ [12].

3. Finite state Machine

Automata theory is a key to software for verifying systems of all types that have a finite number of distinct states, such as communication protocols or protocol for secure exchange of information. Finite state machines (FSM), also known as finite state automaton (FSA), at their simplest, are models of the behaviors of a system or a complex object, with a limited number of defined conditions or modes, where mode transitions change in circumstance[6][7].

A deterministic finite automation (DFA) is a quintuple $M = (Q, \sum, q_0, \delta, F)$, where

- Q is a finite set of states.
- $\sum$ is a finite set of input symbols.
- q_0 is the start state indicated by an arrow $\rightarrow$.
- δ is a transition function $\delta : Q \times \sum \rightarrow Q$ i.e., $\delta(q_0, a) = q_i \in Q.$
- $F \subset Q$ is a finite set of final states.

Generally, the input symbols of being either letters or digits. I.e., and is the set of strings formed out of Sometimes we refer strings as languages also. We say that a string x is accepted by a DFA if The set of languages accepted by a DFA 'M' is denoted by L(M). In a DFA, there will be only one transition out of each state on the same input symbol. The nondeterministic finite automaton (NDFA) is also a mathematical model where are as in DFA except is a transition function from In NDFA there may be Moore machine is a sextuple Where are as before and is an output function and is the set of output symbols. On a More machine the output depends on the transition.

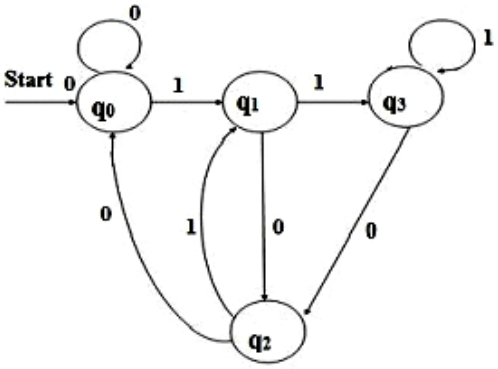

Fig. 1: Moore Machine with residue mod4

Transition table, as well as transition diagram can also represent Moore machine. In this paper, consider Moore machine, which calculates residue mod4.

4. Pauli Spin ½ Matrices

The Pauli spin matrices are set of three 2x2 complex matrices $\sigma_1, \sigma_2, and\ \sigma_3$ which are Hermitian and unitary matrices represents the intrinsic angular momentum components of spin ½ particles in quantum mechanics.

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Let $p = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, q = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, r = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$

We braid entangle these 2x2 matrices to form the set R are formed as follows.

$$R_{01} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & -1 \end{pmatrix}, R_{02} = \begin{pmatrix} p & q \\ s & r \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 \end{pmatrix},$$

$$R_{03} = \begin{pmatrix} p & r \\ s & q \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & -1 \end{pmatrix}, R_{04} = \begin{pmatrix} q & p \\ r & s \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & -1 \end{pmatrix},$$

$$R_{05} = \begin{pmatrix} q & s \\ r & p \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & -1 \end{pmatrix}, R_{06} = \begin{pmatrix} q & p \\ s & r \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 \end{pmatrix},$$

$$R_{07} = \begin{pmatrix} r & p \\ q & s \end{pmatrix} = \begin{pmatrix} 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & -1 \end{pmatrix}, R_{08} = \begin{pmatrix} r & s \\ p & q \end{pmatrix} = \begin{pmatrix} 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix},$$

$$R_{09} = \begin{pmatrix} r & s \\ q & p \end{pmatrix} = \begin{pmatrix} 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, R_{10} = \begin{pmatrix} s & q \\ p & r \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \end{pmatrix},$$

$$R_{11} = \begin{pmatrix} s & r \\ p & q \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, R_{12} = \begin{pmatrix} s & r \\ q & p \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

This set R of twelve 4x4 non singular matrices is used to encrypted the message [13][14].

5. PROPOSED ALGORITHM

Alice wants to send the message to Bob using elliptic curve ElGamal encryption by using Pauli spin ½ matrices. Alice chooses the elliptic curve $y^2 = x^3 + gx + h$ over the field z_p .

Choose the point G on the elliptic curve. Alice selects a private key 'a' and generates the public key A='aG' and Bob selects a private key 'b' and generates the public key B= 'bG'.

5.1 Encryption:

Step 1: Alice chooses a random integer k, and keeps it secret.
Step 2: She Computes kG.
Step 3: Alice selects the Bob's public key $B = bG.$
Step 4: Compute $kB = k(bG) = l.$
Step 5: Compute $aB = a(bG) = m.$
Step 6: Alice wants to send the message q_i to Bob.
Step 7: Alice wants to convert the message into the points on the elliptic curve. She chooses a point Q, which is a generator of the elliptic curve. By using ASCII characters of upper case letter into the points on the elliptic curve.

Let $A = \{1P, 2P, 3P.....255P\}$
$B = \{set\ of\ all\ ASCII\ characters\}$

Alice defines one to one correspondence $f : A \to B$ by $f(nP) = x_n$
Where n=1,2.....255 and $\{x_1, x_2, x_3, ...x_{255}\}$ *are the ASCII characters.*

Step 8: Generates the following 4×4 matrix with entries are the points on the elliptic curve.

$$m_1 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_5 & a_6 & a_7 & a_8 \\ a_9 & a_{10} & a_{11} & a_{12} \\ a_{13} & a_{14} & a_{15} & a_{16} \end{pmatrix}$$

, and so on additional which is obtained depending upon the length of the message.

Step 9: Alice selects $m,$ where's' is the x-coordinate of m and the binary value's' is secret key.

Step 10: Alice define Moore machine with input is secret key.

Compute $q_{k+1} = q_k \times [R_{(\text{sec}rect\ code\ in\ decimal\ form \bmod 12)}]^{output q_{k+1}\ \ state}$

The resultant sets of points are

$R = \{q_1(x_1, y_1), q_2(x_2, y_2), q_3(x_3, y_3).....q_i(x_i, y_i)$

Where i=1, 2, 3 ……

Step 11: Compute $C_i = q_i + l + m..$

Step 12: Now Alice sends the encrypted message (kG, C_i) to Bob.

5.2 Decryption:

To recover the plain text q_i from C_i, Bob do the following:

Step 1: First Bob selects the Alice public key A=aG.

Step 2: Compute bA=b(aG)=m.

Step 3: Now Bob computes the inverse element of b(aG) is - b(aG).

Step 4: Add - b(aG)to the second part of the message: $q_i + kbG + abG - abG = q_i + kbG.$

Step 5: Multiply the Bob's own private key 'b' with the first part of the message kG, we get: kbG.

Step 6: Now Bob computes the inverse element of kbG which is –kbG.

Step 7: Bob adds -kbG to the second part of the message: $q_i + kbG - kbG = q_i$.

Step 8: After decryption, the obtained points are stored in 4×4 matrix.

$$S_1 = \begin{pmatrix} q_1 & q_2 & q_3 & q_4 \\ q_5 & q_6 & q_7 & q_8 \\ q_9 & q_{10} & q_{11} & q_{12} \\ q_{13} & q_{14} & q_{15} & q_{16} \end{pmatrix},....$$

Step 9: Bob selects m, where s is the x-coordinate of m which is the secret key and the binary value is input key.

Step 10: Now Bob multiplies q_i with inverse of key metrics 'R' and Bob applies the reverse process and by using ASCII characters of upper case letters, he can recover the message.

6. EXAMPLE

Alice wants to send the message to Bob using elliptic curve ElGamal encryption by using Pauli spin ½ matrices. Alice chooses the elliptic curve $y^2 = x^3 - 4$ over the field z_{271}. Then the points on the elliptic curve are

E={0,(1,57),(1,214),(2,2),(2,269),(5,11),(5,260),(6,36),(6,235),(7,135),(7,136),……

……..(264, 174), (269,114), (269,157)}.

The number of points on the elliptic curve are 271 and the prime number is 271. Therefore each point is a generator of an elliptic curve E[9][10][11].

Choose the point G=(68,136) on the elliptic curve. Alice selects a private key 'a'=6, and generates the public key A='aG' = 6(68,136)= (85, 199) and Bob selects a private key 'b'=8 , and generates the public key B= 'bG' = 8(68,136)= (122 , 259) .

6.1 Encryption:

Step 1: Alice chooses a random integer k =4, and keeps it secret.

Step 2: Compute kG= 4(68,136)= (250 , 189).

Step 3: Alice selects the Bob's public key B=bG= (122, 259).

Step 4: Compute kB=k(bG)=4(122 , 259)= (132,248).

Step 5: Compute aB=a(bG)=6(122 , 259)= (215,157)=m.

Step 6: Alice wants to send the message q_i to Bob.

Step 7: Alice wants to convert the message into the points on the elliptic curve. She chooses a point Q=(172,240) which is generator of the elliptic curve. By using ASCII characters, upper case letter converted into the points on the elliptic curve.

$I \to 73(172,240) = (183,38),\quad N \to 78(172,240) = (69,18),$
$T \to 84(172,240) = (126,260),\quad E \to 69(172,240) = (225,189),$
$R \to 82(172,240) = (168,235),\quad N \to 78(172,240) = (69,18),$
$A \to 65(172,240) = (64,246),\quad T \to 84(172,240) = (126,260),$
$I \to 73(172,240) = (183,38),\quad O \to 81(172,240) = (93,5),$
$N \to 78(172,240) = (69,18),\quad A \to 65(172,240) = (64,246),$
$L \to 76(172,240) = (120,261),\quad 1 \to 61(172,240) = (97,235),$
$2 \to 62(172,240) = (55,93),\quad 3 \to 63(172,240) = (256,259).$

Then the points are
$T = \{(183,38),(69,38),(126,260),(225,189),(168,235),(69,18),(64,246),(126,260),$
$(183,38),(93,5),(69,18),(64,246),(120,261),(97,235)(55,93)(256,259)\}$

Step 8: To create 4×4 matrix with entries are the points on the elliptic curve.

$$m_1 = \begin{pmatrix} (183,38) & (69,18) & (126,260) & (225,189) \\ (168,235) & (69,18) & (64,246) & (126,260) \\ (183,38) & (93,5) & (69,18) & (64,246) \\ (120,261) & (97,235) & (55,93) & (256,259) \end{pmatrix}$$

Step 9: Alice selects $m = (215,157),$ where $s = 215$ and the binary value of 215 is 11010111which is input key.

Step 10: Alice define Moore machine with input is secret key. And compute

$q_{k+1} = q_k \times [R_{(\text{sec}rect\ code\ in\ decimal\ form \bmod 12)}]^{output q_{k+1}\ \ state}$

S. No	I/P Binary Form	I/P In Decimal Form mod 12	Present state	O/P	Key Matrix	Cipher text
1	1	1	q_1	1	R_{01}	$\begin{pmatrix} (203,174) & (150,49) & (157,43) & (258,77) \\ (227,155) & (205,64) & (6,36) & (156,100) \\ (164,259) & (5,260) & (106,194) & (105,73) \\ (182,258) & (172,31) & (163,200) & (205,64) \end{pmatrix}$
2	1	3	q_3	3	R_{03}	$\begin{pmatrix} (231,43) & (157,3) & (83,171) & (231,43) \\ (214,191) & (185,178) & (126,260) & (214,191) \\ (208,176) & (85,199) & (108,10) & (208,176) \\ (119,211) & (205,64) & (166,246) & (119,211) \end{pmatrix}$

3	0	6	q_2	2	R_{06}	$\begin{pmatrix}(182,258) & (49,207) & (219,120) & (49,64)\\ (97,235) & (38,160) & (208,176) & (38,111)\\ (157,268) & (95,210) & (58,157) & (95,61)\\ (58,114) & (172,240) & (250,189) & (172,31)\end{pmatrix}$
4	1	1	q_1	1	R_{01}	$\begin{pmatrix}(219,20) & (183,38) & (182,258) & (196,136)\\ (28,57) & (1,57) & (95,61) & (215,157)\\ (231,228) & (2,2) & (67,189) & (173,23)\\ (167,253) & (218,13) & (108,10) & (73,226)\end{pmatrix}$
5	0	2	q_2	2	R_{02}	$\begin{pmatrix}(59,109) & (260,205) & (149,98) & (30,80)\\ (28,214) & (194,130) & (219,120) & (65,130)\\ (158,170) & (133,95) & (256,12) & (5,11)\\ (161,31) & (212,72) & (221,210) & (107,173)\end{pmatrix}$
6	1	5	q_1	1	R_{05}	$\begin{pmatrix}(183,233) & (35,253) & (183,38) & (68,136)\\ (140,11) & (36,168) & (140,260) & (229,220)\\ (214,191) & (234,66) & (214,80) & (215,157)\\ (43,261) & (34,238) & (43,10) & (67,82)\end{pmatrix}$
7	1	11	q_3	3	R_{11}	$\begin{pmatrix}(161,240) & (256,12) & (256,259) & (213,269)\\ (182,258) & (201,95) & (235,43) & (133,95)\\ (237,248) & (183,38) & (226,210) & (166,25)\\ (234,205) & (6,235) & (106,194) & (153,120)\end{pmatrix}$
8	1	11	q_3	3	R_{11}	$\begin{pmatrix}(213,2) & (97,235) & (75,97) & (122,259)\\ (40,103) & (228,200) & (40,168) & (257,49)\\ (140,11) & (147,45) & (140,260) & (235,228)\\ (48,205) & (71,27) & (48,66) & (237,248)\end{pmatrix}$

Then the points are

$$R = \{(213,2)(97,235)(75,97)(122,259)(40,103)(228,200)(40,168)(257,49)(140,11)(147,45)(140,260)(235,228)\\ (48,205)(71,27)(48,66)(237,248)\}.$$

Step11: Compute $C_i = q_i + kbG + abG$.

$C_1 = (213,2) + (132,248) + (215,157) = (54,3),$ $C_2 = (97,235) + (132,248) + (215,157) = (59,109),$

$C_3 = (75,97) + (132,248) + (215,157) = (195,168),$ $C_4 = (122,259) + (132,248) + (215,157) = (231,228),$

$C_5 = (40,103) + (132,248) + (215,157) = (258,77),$ $C_6 = (228,200) + (132,248) + (215,157) = (65,141),$

$C_7 = (40,168) + (132,248) + (215,157) = (192,155),$ $C_8 = (257,49) + (132,248) + (215,157) = (173,23),$

$C_9 = (140,11) + (132,248) + (215,157) = (196,136),$ $C_{10} = (147,45) + (132,248) + (215,157) = (214,91),$

$C_{11} = (140,260) + (132,248) + (215,157) = (54,268),$ $C_{12} = (235,228) + (132,248) + (215,157) = (91,244),$

$C_{13} = (48,205) + (132,248) + (215,157) = (123,116),$ $C_{14} = (71,27) + (132,248) + (215,157) = (251,111),$
$C_{15} = (48,66) + (132,248) + (215,157) = (157,268),$ $C_{16} = (237,248) + (132,248) + (215,157) = (182,258).$

Step12: Now Alice sends the encrypted message consisting of pair of points
$\{((250,189),(54,3))((250,189),(59,109)),((250,189),(195,168))\ ((250,189),(231,228))(250,189),(258,77))(250,189),(65,141))$
$(250,189),(192,155))(250,189),(173,23))(250,189),(196,136))\ (250,189),(214,91))(250,189),(54,268))(250,189),(91,244))$
$(250,189),(123,116))(250,189),(251,111))(250,189),(157,268))\ (250,189),(182,258))\}.$
to Bob.

6.2 Decryption:

Bob applies the reverse process and recovers the message “INTERNATIONAL123”.

CONCLUSIONS

In the proposed work, the plain text has been transformed to points on the elliptic curve one to one mapping and their ASCII characters. The secret key has been generated using Pauli spin 1/2 matrices and the encryption process uses the finite state machines and the ElGamal encryption taking security, confidentiality, and authenticity into consideration. The obtained cipher text becomes quite difficult to break or to extract the original information even if the algorithm is known.

References

[1] N.Koblitz. Elliptic curve Cryptosystem Mathematics of computation, 48203- 209, 1987.
[2] A text book of Guide to elliptic curve Cryptography by Darrel Hancott Vanstone.
[3] N. Koblitz. Hyper Elliptic Cryptosystem. International Journal of Cryptography, 139-150, 1989.
[4] An introduction to the theory of Elliptic Curves by Joseph H. Silverman brown University and NTRU Cryptosystems.
[5] A text book of Cryptography and Network Security by William Stallings.
[6] Adesh K.Pandey. Reprint 2009, “An introduction to automata theory and formal languages S.K.Kararia & sons. New Delhi.
[7] Johan E.Hopcroft, Rajeev Motwin, Jeffrey D.Uiman. “Introduction to automata theory,language, and computation ” Vanstone 3 rd impression, 2007 CRC press, Dorling Kindersley (India)Pvt.Ltd.
[8] http://www.certicom.com/index.php/ecc-tutorial.
[9] P.A.Jyotirmie, B.Ravi Kumar,A.Chandra Sekhar, S.Uma Devi “A One to one Correspondence in elliptic Curve Cryptography” International Journal of Mathematical archive-4(3),2013: 300- 304.
[10] B.krishna Gandhi, A.Chandra Sekhar,S.Srilaksmi. “Cryptography Scheme for Digital Signals using Finite State Machines” International Journal of Computer Applications, September, 2011.
[11] K.R.Sudha , A.chandra Sekhar ,Prasad Reddy P.V.G.D. “Cryptography Protection of Digital Signals using Some recurrence relations” International Journal of Computer Science and Network security, Vol (7) no 5 may 2007, 203-207.
[12] T.ElGamal, “A public-key cryptosystem and a signature scheme based on discrete logarithms”, IEEE Transactions on Information Theory, on Information Theory, 469- 472, 1985.
[13] D.Sravan Kumar, CH.Suneetha and A.Chandra Sekhar “Encryption of data streams using Pauli spin ½ matrices”International Journal of Engineering Science and Technology Vol 2(6), 2010, 2020-2028.
[14] B.Krishna Gandhi, A.Chandra Sekhar and S.Srilakshmi “Encryption of data streams using Pauli spin ½ matrices and Finite state machine” International journal Computer Applications vol 37(2), January 2012.