International Journal of Information & Network Security (IJINS)
Vol.2, No.3, April 2013, pp. 190~196
ISSN: 2089-3299

A Novel Encryption Scheme of Amazigh Alphabet Based Elliptic Curve using Pauli Spin ½ Matrices

F. Amounas* and E.H. El Kinani**
* R.O.I Group, Informatics Department Moulay Ismaïl University, Faculty of Sciences and Technics Errachidia, Morocco
** A.A Group, Mathematical Department Moulay Ismaïl University, Faculty of Sciences and Technics Errachidia, Morocco

Article Info

Article history:

Received Nov 30th, 2012
Accepted Dec 12th, 2012

Keyword:

Elliptic Curve Cryptography,
Pauli Spin 1/2 matrices,
Linear block,
Encryption, Decryption

ABSTRACT

A new secure Elliptic Curve Cryptosystem based on Pauli spins ½ matrices will be proposed in this paper. It includes (i) public key generation on the elliptic curve and its declaration for data encryption of Amazigh characters and (ii) private key generation and its use in data decryption depended on Pauli spins ½ matrices. An overview of Pauli spins ½ matrices has been discussed. Much attention has been given here on the coding of Amazigh alphabets to data stream. Finally, we describe how to encrypt the data by ECC technique using Pauli spins ½ matrices.

Corresponding Author:

E.H. El KINANI
Mathematical Department
Moulay Ismaïl University,
Faculty of Sciences and Technics, Box 509 Errachidia, Morocco
E-mail: elkinani_67@yahoo.com

1. INTRODUCTION

With the explosion of networks and the huge amount of data transmitted along, securing data content is becoming more important. Data encryption is widely used to ensure security in open networks such as the Internet. With the fast development of cryptography research and computer technology, the capabilities of cryptosystems such as of RSA and Diffie-Hellman are inadequate due to the requirement of large number of bits. The cryptosystem based on Elliptic Curve Cryptography is becoming the recent trend of public key cryptography.

The message is converted into an incomprehensible data in the process of encryption. The confidential data is generally encrypted to protect it from attackers [1,2].The receiver of the message needs an algorithm to retrieve the plaintext. To make the procedure more secure the algorithm is devised so that the retrieval of the message from the encrypted data is possible only for a person holding a private key. This process is generally referred to as decryption.

In our previous work [3], we investigate the implementation of elliptic curve cryptosystem using Tifinagh characters. Furthere, we have provided a new mapping method based on non-singular matrices in [4]. In [5] we provide more secure digital signature scheme by using Boolean permutation based elliptic curve cryptography (ECC). In [6] we describe an elliptic curve cryptosystem using code computing For Tifinagh alphabet.

In the present paper, we provide a new secure scheme based ECC using Pauli spin ½ matrices. Here, we are creating synthetic data value on the 55 alphabets of Amazigh, based on hexadecimal code. Encryption as cipher text use invertible square matrix, blocking the message according to the selected square matrix. At

decryption we use the inverse of the square matrix. The choice of the matrices is based on the selected bits on random point. More precisely, we propose an algorithm for encoding the Amazigh alphabets to data stream. Next, we will encrypt these numbers based ECC technique using Pauli spin ½ matrices.

The remainder of this paper is arranged as follows: we start with brief review of elliptic curve followed by Pauli spin ½ matrices in section 3. Next, we describe the encoding of the Amazigh alphabet in section 4. In section 5 we propose an algorithm based elliptic curve using Pauli spin ½ matrices. The security of the proposed method is studied in 6. The paper is concluded in Section 7.

2. BRIEF REVIEW OF ELLIPTIC CURVE

The Weiestrass equation defining an elliptic curve over finite field F_p, is as follows:

$$y^2 = x^3 + ax + b, \quad (1)$$

where x, y are elements of the field F_p, and a, b are integer modulo p, satisfying the following equation:

$$4a^3 + 27b^2 \neq 0 \bmod p \quad (2)$$

An elliptic curve E over F_p consist of the solutions (x,y) defined by Equations (1) and (2), along with an additional element noted O, which is the point of elliptic curve at infinity. The set of points (x,y) are said to be affine coordinate point representation.

The basic Elliptic curve operations are point addition and point doubling. Elliptic curve cryptographic primitives require scalar point multiplication [7].

Say, given a point P(x,y) on an elliptic curve, one needs to compute kP, where k is a positive integer. This is achieved by a series of doubling and addition of P.

3. PAULI SPIN ½ MATRICES

The basic Pauli spins ½ matrices are used for the encryption of data streams in [8, 9]. In the present work, we provide a novel encryption scheme based on the operation multiplication with Pauli spins ½ matrices.

Definition

The pauli spin matrices are set of three (2x2) complex matrices σ_1, σ_2 and σ_3, which are hermitian and unitary matrices represents the intrinsic angular momentum components of spin ½ particles in quantum mechanics. These matrices are defined as:

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

We denote by $a = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ the identity matrix, $b=\sigma_1$, $c= -i\sigma_2$ and $d=\sigma_3$. Then,

$$b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \; c = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } \; d = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

We braid entangle these (2x2) matrices to form the set B of (4x4) non singular braided matrices [10]. The elements of the set B are formulated as follows:

$B_{01}=\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & -1 \end{bmatrix}$	$B_{02}=\begin{pmatrix} a & b \\ d & c \end{pmatrix}=\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 \end{bmatrix}$	$B_{03}=\begin{pmatrix} a & c \\ d & b \end{pmatrix}=\begin{bmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & -1 & 1 & 0 \end{bmatrix}$
$B_{04}=\begin{pmatrix} b & a \\ c & d \end{pmatrix}=\begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & -1 \end{bmatrix}$	$B_{05}=\begin{pmatrix} b & a \\ d & c \end{pmatrix}=\begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 \end{bmatrix}$	$B_{06}=\begin{pmatrix} b & d \\ c & a \end{pmatrix}=\begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$
$B_{07}=\begin{pmatrix} c & a \\ b & d \end{pmatrix}=\begin{bmatrix} 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & -1 \end{bmatrix}$	$B_{08}=\begin{pmatrix} c & d \\ a & b \end{pmatrix}=\begin{bmatrix} 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$	$B_{09}=\begin{pmatrix} c & d \\ b & a \end{pmatrix}=\begin{bmatrix} 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$
$B_{10}=\begin{pmatrix} d & b \\ a & c \end{pmatrix}=\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$	$B_{11}=\begin{pmatrix} d & c \\ a & b \end{pmatrix}=\begin{bmatrix} 1 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$	$B_{12}=\begin{pmatrix} d & c \\ b & a \end{pmatrix}=\begin{bmatrix} 1 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$

4. ENCODING OF AMAZIGH CHARACTERS

The Amazigh alphabet was officially recognized like belonging to the basic multilingual planned by the International Organization of Standardization (ISO). The table1 below presents the Amazigh alphabet and the associated Unicode allocated by ISO. Tifinagh is encoded in the Unicode range U+2D30 to U+2D7F. With the UTF-8 encoding, Unicode characters can be used in practice. There are 55 defined characters:

Table 1. Encoding of Amazigh Alphabets

Code	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9	+A	+B	+C	+D	+E	+F
U+2D30	ⵀ	ⵁ	ⵂ	ⵃ	ⵄ	ⵅ	ⵆ	ⵇ	ⵈ	ⵉ	ⵊ	ⵋ	ⵌ	ⵍ	ⵎ	ⵏ
U+2D40	ⵐ	ⵑ	ⵒ	ⵓ	ⵔ	ⵕ	ⵖ	ⵗ	ⵘ	ⵙ	ⵚ	ⵛ	ⵜ	ⵝ	ⵞ	ⵟ
U+2D50	ⵠ	ⵡ	ⵢ	ⵣ	ⵤ	ⵥ	ⵦ	ⵧ	⵨	⵩	⵪	⵫	⵬	⵭	⵮	ⵯ
U+2D60	⵰	⵱	⵲	⵳	⵴	⵵										ⵥ
U+2D70																

5. MAIN RESULTS

a. Proposed Scheme

In the proposed scheme, the corresponding code of tifinagh characters is generated as per the step by step procedure given below:

Algorithm (1)

Step 1: Represent a plaintext by hexadecimal code as: 2Dxx.

Step 2: subtracts '2D00' from the corresponding code. The obtained hexadecimal code is shown in Table2.

Step 3. Convert them into decimal form.

Table 2.Synthetic value for Amazigh Alphabets and numbers

										
30	31	32	33	34	35	36	37	38	39	3A
										
3B	3C	3D	3E	3F	40	41	42	43	44	45
										
46	47	48	49	4A	4B	4C	4D	4E	4F	50
										
51	52	53	54	55	56	57	58	59	5A	5B
5C	5D	5E	5F	60	61	62	63	64	65	6F

At last, we encrypt these decimal numbers with selected key matrix based on random point on elliptic curve.

Encryption

The text message is divided into data streams of 4 characters each. These data streams are coded to the equivalent numerals using the code table given below and the message block is obtained.

Algorithm (2)

Step 1: Transform a text message into integer linear blocks as shown in Algorithm 1.

Step 2: Chooses a random integer k and compute: $K=kP_B$.

Step 3: For each number input in binary form, calculate the input in decimal form mod 12. For each number generated, obtain B_i and B_j from the set of matrices (B_{01}, B_{02}, . . ., B_{12}).

Step 4: Make plain text as blocks according to the key matrix. We denote the message block M.

Step 5: Let $K=kP_B$ is a random point which decides which matrix is selected. The choice of code matrix is based on the bits selected (b_t), where t is bit position (LSB→MSB).

Step 6: Multiply Plain text or message block with selected square matrix B_i and B_j. $C=(M* B_i)*B_j$

Repeat (5-6) for the next block not visited.

The cipher text is represented as kP followed by the obtained blocks as: $(kP,C_1,C_2,...,C_n)$

Decryption

Before attempting for decryption of the text, the receiver extracts the coordinate of kP and are stored as P_1.Then, compute $K=n_BP_1$ using his own private key. The coded matrices are selected using the bits of K. The received message is divided into data streams of 4 characters each (linear blocks). To obtain the stream number from encrypted message, the receiver multiplies linear block with inverse of the matrix B_j followed by inverse of B_i. The numerals are converted to hexadecimal. Then, adding this number with "2D00". The result code represents the cooresponding code of Amazigh characters.

b. Implementation of the proposed Method

For demonstration purposes typical Elliptic Curve is represented by:

$$y^2 = x^3 + 4x + 20 \bmod 29;$$

where a = 4, b = 20 and p = 29. The generated points on the curve can be found as shown in Table 3.

Table 3: Set of sample points on EC

(1,5)	(4,19)	(20,3)	(15,27)	(6,12)
(17,19)	(24,22)	(8,10)	(14,23)	(13,23)
(10,25)	(19,13)	(16,27)	(5,22)	(3,1)
(0,22)	(27,2)	(2,23)	(2,6)	(27,27)
(0,7)	(3,8)	(5,7)	(16,2)	(19,16)
(10,4)	(13,6)	(14,6)	(8,19)	(24,7)
(17,10)	(6,17)	(15,2)	(20,26)	(4,10)
(1,24)	O			

The base point P is selected as (1,5). Here the choosing curve contains 37 points with P is the point generator. In the ECC method, we generate a nonce, i.e a random integer k (k < p), which needs to be kept secret. Then kP is evaluated, by a series of additions and doublings, as discussed above. Let us call the source as A and destination as B. Let the private key of the host B be n_B. The public key of user B is evaluated by $P_B = n_B P$.

In our case we have k = 13, n_B = 21, P_B=(0,7), then K= kP_B =(5,22).

Encryption

The Assumed Plain Text is "  " (including alphabets Amazigh). In our case each alphabet is replaced by a by natural number. So the encrypted characters are shown in the following table 4.

Step 1. Assigning Text to Synthetic Data.

Table 4. Encryption of alphabets and numbers

Character												
Synthetic Data	92	48	79	78	73	84	92	73	74	73	79	89

Step 2. Making a Plain text as linear block of size 4.

Table 5.Linear block text

Plain Text	**Blocking the Plain text**				**Synthetic value for Plain Text Block**
					**92, 48, 79, 78**
					**73, 84, 92, 73**
					**74, 73, 79, 89**

Step 3. Select b=bit (K_t), where t is bit position (LSB→MSB), the bit of the binary sequence of K.
Step 4. Selecting (4 x 4) invertible matrices noted B_i and B_j.
Here we choose K= (0010110110).

Input in the binary form	Decimal form mod 12	Message block	Key matrix	Cipher text
00	0	(92, 48, 79, 78)	B_{01}	(171, -30, 126, -13)
10	2		B_{03}	
11	11	(73, 84, 92, 73)	B_{12}	(184, -146, 146, 168)
01	7		B_{08}	
10	3	(74, 73, 79, 89)	B_{04}	(315, -11, -21, 9)
00	9		B_{10}	

The block 1 consist the plaintext value (ⵜ, ⵓ, ⵍ, ⵎ), it's equivalent Synthetic value is (92, 48, 79, 78) as per the table, It is called as a 'M'. Compute the product of this vector with the selected matrices. Our message consists 3 linear blocks. The first block is encrypted with B_{01} and B_{03}. Therefore, (92, 48, 79, 78) encrypted message is (171, -30, 126, -13).
Similarly, block2 (73, 84, 92, 73) encrypted message is (184, -146, 146, 168) and block3 (74, 73, 79, 89) encrypted message is (315, -11, -21, 9).

Decryption

Before attempting for decryption of the text, the receiver extracts the coordinate of kP and are stored as P_1.Then, compute $K=n_BP_1$ using his own private key. The coded matrices are selected using the bits of K.
The received message is divided into data streams of 4 characters each (linear blocks). The linear block is decrypted by using the inverse of the matrix B_j followed by inverse of B_i. The Block 1 (171, -30, 126, -13) decrypted message is (92, 48, 79, 78). Similarly, block2 (184,-146, 146,168) decrypted message is (73, 84, 92, 73) and block3 (315, -11, -21, 9). encrypted message is (74, 73, 79, 89). The obtained numerals are converted to hexadecimal. Then, adding this number with "2D00". The result code represents the cooresponding code of Amazigh characters.

Thus we retrieve the plaintext "ⵜⴰⵎⴰⵣⵉⵖⵜ".

6. SECURITY ANALYSIS

Several types of active and passive attacks are possible on the cipher text [11,12]. There are three basic attacks against the proposed scheme: Cipher text attack, Chosen cipher text attack and Adaptive chosen cipher text attack. In the proposed scheme, it is very difficult, due to the secret key, chosen random point on elliptic curve and the operation matrix multiplication with the linear blocks. Here we have ciphered each Amazigh alphabets and numbers into numbers using private and public key and hence decrypted the keys to obtain the final character and the final message. The proposed encryption technique is very and straight forward. In this algorithm we can make any number of square matrices and blocks. The algorithm is based on the (4 x 4) square matrix. Therefore we can select two square matrices. The reason for selecting linear block cipher for our algorithm, the linear algebra will not produce same kind of result for the repeated text variable. There are a few highlight points about our implementation, First one is we are converting the alphabets Amazigh to synthetic data value, second is we are selecting random point on EC for choosing two code matrices B_i and B_j which announcing as public keys. The bottleneck of our algorithm, we are keeping a random point as a private key. To extract the original information, it is very difficult due to the chosen of point on elliptic curve and the pauli spin ½ matrices.

7. CONCLUSION

The proposed method provides high security level since it involves the encryption at three levels: selection of the random point on EC, selection of the matrices arbitrarily from the set B and the sequence of multiplication of the matrices with linear block cipher.
It is very difficult to obtain secret key from cryptanalysis, because the plaintext is coded using code table, a mod function is used, the random point on EC, and the encoding matrices are changed for each data stream.
Another innovative idea for our algorithm, we are extending characters upto 55 letters of Amazigh. Most of the algorithms are working based on the 33 alphabets, adopted in Morocco, especially hill cipher or linear block cipher. In the proposed algorithm, we are extending the text value upto 55.

REFERENCES

[1] A. Chandra Sekhar, Prasad Reddy P.V.G.D, A.S.N. Murthy, B. Krishna Gandhi "Self Encrypting Data Streams Using Graph Structures" *IETECH Journal of Advanced Computations*, Vol.2 No.1, 2007.
[2] D. Stinson, Cryptography, Theory and Practice, *CRC Press*, Boca Raton Florida, II Edition, 2002.
[3] F.Amounas and E.H. El Kinani, Cryptography with Elliptic Curve Using Tifinagh Characters, *Journal of Mathematics and System Science* Vol.2, No.2, pp.139-144, 2012.
[4] F. Amounas and E.H. El Kinani, Fast Mapping Method based on Matrix Approach For Elliptic Curve Cryptography, *International Journal of Information & Network Security (IJINS)* Vol.1, No.2, pp. 54-59, 2012.
[5] F.Amounas and E.H. El Kinani, Elliptic Curve Digital Signature Algorithm Using Boolean Permutation based ECC, *International Journal of Information & Network Security (IJINS)*, Vol.1, No.3, pp. 216-222, 2012.
[6] F.Amounas and E.H. El Kinani, Construction Efficiency of the Elliptic Curve Cryptosystem using Code Computing for Amazigh Alphabet, *International Journal of Information & Network Security (IJINS)*, vol.2, No.1, pp 43-53, 2013.

[7] J. Lee, H. Kim, Y. Lee, S. M. Hong, and H. Yoon "Parallelized scalar multiplication on elliptic curves defined over optimal extension field," *International Journal of Network Security*, vol. 4, no. 1, pp. 99-106, 2007.
[8] D.Sravana Kumar, CH.Suneetha and A.Chandra Sekhar " Encryption of Data Streams using Pauli spins ½ matrices" *International journal of Engineering Science and Technology* Vol.2(6), 2020-2028, 2010.
[9] Richard Liboff, Introductory Quantum Mechanics, IV Edition, *Addison Wesley*, 2002.
[10] A.Chandra Sekhar, D. Sravana Kumar and CH. Suneetha, Encryption of Data streams using Boolean Matrices, *proceedings of International Conference on Challenges and Applications of Mathematics in Science and Technology*, pp. 524-531, 2010.
[11] B. Zhang, H. Wu, D. Feng, F. Bao, Chosen cipher text attack on a new class of self-synchronizing stream ciphers, *in progress in cryptology-INDOCRYPT 2004*, Lecture Notes in Computer Science, Vol. 3348, pp.73-83, 2004.
[12] Canetti R., Halevi S., and Katz J., Chosen cipher text security from identity-based encryption, *Advances in Cryptography-EUROCRYPT 2004*, Vol. 3027 of LNCS, Springer-Verlag, 2004.

BIOGRAPHY OF AUTHORS

EL HASSAN EL KINANI received the Ph.D in mathematical physics in 1999 from Mohamed V University Rabat Morocco. He is full professor at department of mathematics in Moulay Ismaïl University, Faculty of Sciences and Technics, Errachidia, Morocco. He is interested in classical and quantum cryptography.

E-mail: elkinani_67@yahoo.com

FATIMA AMOUNAS received the DESS (diploma of high special study) degree in informatic in 2002 from Sidi Mohamed Ben Abdellah University, Faculty of Sciences Dhar El Mehrez, Fès Morocco. She is currently a Ph.D student in University Moulay Ismaïl, Faculty of Sciences and Technics, Errachidia, Morocco. Her research interests include elliptic curve and cryptography.

E-mail: F_amounas@yahoo.fr.