ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.9, 6751–6757
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.9.33 Spec. Issue on CAMM-2020

SECURITY OF PREDICTING THE DATA USING RB29 ALGORITHM

R. JAICHANDRAN[1], P.N PUSHPA[2], AMAL NARAYANAN[3], K. MINHAJ ALI[4], AND SYED SHAHAZAD THANGAL[5]

ABSTRACT. Today's world is data world because each and every people survive with data. The data produced from social media because everyone people used media. People's data is very important in the world. This data does not have good security so to overcome this issue we apply the proposed method. The proposed method has four steps; 1. Applying the commutative property of addition in matrix; 2. Applying the associative property of addition in matrix; 3. To swap the prime numbers and non negative integer in given matrix; and final step is multiply the secret key in the matrix. The proposed method provides good security while comparing with Salsa method.

1. INTRODUCTION

Today's world is data world because each and every people survive with data. The data produced from social media because everyone people used media. People's data is very important in the world. This data does not have good security so to overcome this issue we apply the Salsa method. This method has four round processes and each process also four round processes. This process changes the places of the data only. Salsa method provides less security; so the hackers easily hack the data. This author talks the fault attack of the additional rotations XOR for ChaCha [1]. They are introduced the new method name as

[1]*corresponding author*

2010 *Mathematics Subject Classification.* 05C85, 11-04, 15A15, 68W99.

Key words and phrases. Commutative Property, Associative Property, RB29, Salsa, Encryption, Decryption.

Freestyle, and this method has used different cipher texts and also introduced the new concept is hash based halting conditions and key guessing [2]. They are mainly analysis the side channel analysis for ChaCha, and introduced the bricklayer attack [3].There are mainly analyzed the Double A hash function for the security purpose [4]. They are mainly studied the design and implementation of constant time web assembly. This design is fast and flexible to implement the secure algorithms [5]. SRB18 algorithm has discuss about security of twitter analysed data [6]. SRB21phase I studied about prime number with secret key [7]. CBB21 Phase 2 discuss about co-prime numbers [8]. CBB22 algorithm studied about prime number and quadratic form [9]. To overcome this problem introduced the novel method RB29(Rajaprakash ans Bagath Basha) 29.

2. METHODS

Commutative property of addition (CP)

This property must have same design matrix otherwise it cannot be add the matrix, it must be real numbers.

Table 1 and Table 2 are encryption and decryption.

3. ENCRYPTION

A is a data analyzed matrix, B is a secret matrix. [10].

"**Equation (1)**"

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}, \quad B = \begin{bmatrix} 2 & 4 & 3 \\ 5 & 6 & 1 \\ 7 & 9 & 8 \end{bmatrix}$$

$$CP = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix} + \begin{bmatrix} 2 & 4 & 3 \\ 5 & 6 & 1 \\ 7 & 9 & 8 \end{bmatrix} = \begin{bmatrix} 1+2 & 2+4 & 3+3 \\ 4+5 & 5+6 & 6+1 \\ 7+7 & 8+9 & 9+8 \end{bmatrix} = \begin{bmatrix} 3 & 6 & 6 \\ 9 & 11 & 7 \\ 14 & 17 & 17 \end{bmatrix}$$

CP is an input (encrypted) matrix, B and C is s secret matrix.

"**Equation (2)**"

$$CP = \begin{bmatrix} 3 & 6 & 6 \\ 9 & 11 & 7 \\ 14 & 17 & 17 \end{bmatrix}, \quad B = \begin{bmatrix} 2 & 4 & 3 \\ 5 & 6 & 1 \\ 7 & 9 & 8 \end{bmatrix}, \quad C = \begin{bmatrix} 9 & 7 & 8 \\ 6 & 4 & 5 \\ 2 & 3 & 1 \end{bmatrix},$$

$$AP = \begin{bmatrix} 3+2 & 6+4 & 6+3 \\ 9+5 & 11+6 & 7+1 \\ 14+7 & 17+9 & 17+8 \end{bmatrix} + \begin{bmatrix} 9 & 7 & 8 \\ 6 & 4 & 5 \\ 2 & 3 & 1 \end{bmatrix} = \begin{bmatrix} 5 & 10 & 9 \\ 14 & 17 & 8 \\ 21 & 26 & 25 \end{bmatrix} + \begin{bmatrix} 9 & 7 & 8 \\ 6 & 4 & 5 \\ 2 & 3 & 1 \end{bmatrix}$$

$$AP = \begin{bmatrix} 5+9 & 10+7 & 9+8 \\ 14+6 & 17+4 & 8+5 \\ 21+2 & 26+3 & 25+1 \end{bmatrix} = \begin{bmatrix} 14 & 17 & 17 \\ 20 & 21 & 13 \\ 23 & 29 & 26 \end{bmatrix}.$$

TABLE 1. RB29 Encryption

STEPS	RB29 ENCRYPTION
1	Analyzed the prediction data from social media.
2	Convert the prediction data to matrix form.
3	Applying the commutative property (CP) of the matrix CP $CP = A + B = B + A$ **(1)**
4	Applying the associative property (AP) of the matrix AP $AP = A + (B + C) = (A + B) + C$ **(2)**
5	EB = E^n * M **(3)** where EB is encryption matrix B, E is a prime number, n>=0, and M is non negative integer.
6	Identify the possible number of prime numbers multiply by the M for order of matrix.
7	To swap an E and M in a matrix EB.
8	Multiply the secret key S with matrix EB.
9	SKM=AP*S **(4)** where SKM is Secret Key Matrix

"**Equation (3)":** E^n *** M**
EB = 9 => EB=3^1 * 3 =>E=3, n=1, M=3
EB=3^0 * 9=> E=3, n=0, M=9
Pair of numbers (3,3) and (3,9)
Pair-1(3,3)

$$EB = \begin{bmatrix} 14 & 17 & 17 \\ 20 & 21 & 13 \\ 23 & 29 & 26 \end{bmatrix}$$

TABLE 2. RB29 Decryption

STEPS	RB29 DECRYPTION
1	Get the input (encrypted) data matrix.
2	Divide the secret key DS in the matrix SKM. $DM1 = SKM/DS$ **(5)** where DM1 is Decrypted Matrix 1
3	DA = D^n * M **(**6) where DA is decryption matrix A, D is a prime number, n>=0, and M is non negative integer.
4	To swap an D and M in a matrix DA.
3	Minus the secret key matrixes C and B with the matrix DM1. $DM2 = DA - C$ **(7)** where DM2 is Decrypted Matrix 2 $DM3 = DM2 - B$ **(8)** where DM3 is Decrypted Matrix 3
13	Minus the secret key matrix B with the matrix DM3. $DM4 = DM3 - C$ **(9)** where DM4 is Decrypted Matrix 4

Pair-1(3,9)

$$EB = \begin{bmatrix} 14 & 17 & 26 \\ 20 & 21 & 13 \\ 23 & 29 & 17 \end{bmatrix}$$

AP is an input matrix; multiplies with secret key $S = 1/2$ **and "Equation (4)".**

"$SKM = EB * S$, where SKM is Secret Key Multiplication".

$$SKM = \begin{bmatrix} 14 & 17 & 26 \\ 20 & 21 & 13 \\ 23 & 29 & 17 \end{bmatrix} \cdot (1/2) = \begin{bmatrix} 7 & 17/2 & 13 \\ 10 & 21/2 & 13/2 \\ 23/2 & 29/2 & 17/2 \end{bmatrix}$$

Finally, the all matrix should be closure matrix because of all matrixes could be same design, and the original matrix could be encrypted successfully.

4. DECRYPTION

SKM is an input (encrypted) matrix; divide the decryption secret key $DS = 1/2$ **and "Equation (5)."**

"$DM1 = SKM/DS$"

$$DM1 = \begin{bmatrix} 14 & 17 & 26 \\ 20 & 21 & 13 \\ 23 & 29 & 17 \end{bmatrix}$$

"**Equation (6)":** $DA = D^n$ *** M**

DA = 9 => DA=3^1 * 3 =>D=3, n=1, M=3

DA=3^0 * 9=> D=3, n=0, M=9

Pair of numbers (9,3) and (3,3)

Pair-1(9,3)

$$DA = \begin{bmatrix} 14 & 17 & 17 \\ 20 & 21 & 13 \\ 23 & 29 & 26 \end{bmatrix}$$

Pair-1(3,3)

$$EB = \begin{bmatrix} 14 & 17 & 17 \\ 20 & 21 & 13 \\ 23 & 29 & 26 \end{bmatrix}$$

DA is input (decrypted) matrix, B and C is secret matrix and "Equation (7) and (8)".

$$DM1 = \begin{bmatrix} 14 & 17 & 17 \\ 20 & 21 & 13 \\ 23 & 29 & 26 \end{bmatrix}, \quad B = \begin{bmatrix} 2 & 4 & 3 \\ 5 & 6 & 1 \\ 7 & 9 & 8 \end{bmatrix}, \quad C = \begin{bmatrix} 9 & 7 & 8 \\ 6 & 4 & 5 \\ 2 & 3 & 1 \end{bmatrix}$$

"$DM2 = DA - C$, **where** $DM2$ **is decrypted matrix 2".**

$$DM2 = \begin{bmatrix} 14 & 17 & 17 \\ 20 & 21 & 13 \\ 23 & 29 & 26 \end{bmatrix} - \begin{bmatrix} 9 & 7 & 8 \\ 6 & 4 & 5 \\ 2 & 3 & 1 \end{bmatrix} = \begin{bmatrix} 14-9 & 17-7 & 17-8 \\ 20-6 & 21-4 & 13-13 \\ 23-2 & 29-3 & 26-1 \end{bmatrix}$$

$$DM2 = \begin{bmatrix} 5 & 10 & 9 \\ 14 & 17 & 8 \\ 21 & 26 & 25 \end{bmatrix}$$

"$DM3 = DM2 - B$, **where** $DM3$ **is decrypted matrix 3"**

$$DM3 = \begin{bmatrix} 5 & 10 & 9 \\ 14 & 17 & 8 \\ 21 & 26 & 25 \end{bmatrix} - \begin{bmatrix} 2 & 4 & 3 \\ 5 & 6 & 1 \\ 7 & 9 & 8 \end{bmatrix} = \begin{bmatrix} 3 & 6 & 6 \\ 9 & 11 & 7 \\ 14 & 17 & 17 \end{bmatrix}$$

DM3 is input (decrypted) matrix and B is secret key matrix using "Equation (9)".

"$DM4 = DM3 - B$, **where** $DM4$ **is decrypted matrix 4**"

$$DM4 = \begin{bmatrix} 3 & 6 & 6 \\ 9 & 11 & 7 \\ 14 & 17 & 17 \end{bmatrix} - \begin{bmatrix} 2 & 4 & 3 \\ 5 & 6 & 1 \\ 7 & 9 & 8 \end{bmatrix} = \begin{bmatrix} 3-2 & 6-4 & 6-3 \\ 9-5 & 11-6 & 7-1 \\ 14-7 & 17-9 & 17-8 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}$$

5. CONCLUSION

Today's world is data world because each and every people survive with data. The data produced from social media because everyone people used media. People's data is very important in the world. This data does not have good security so to overcome this issue we apply the proposed method. The proposed method has four steps; 1. Applying the commutative property of addition in matrix; 2. Applying the associative property of addition in matrix; 3. To swap the prime numbers and non negative integer in given matrix; and final step is multiply the secret key in the matrix.The RB29 method provide good security while compared with Salsa method. In the future, to add the prime factors operations of the data security.

REFERENCES

[1] P. ARUN BABU, J.J. THOMAS: *Freestyle, a randomized version of ChaCha for resisting offline brute-force and dictionary attacks*, Journal of Information Security and Applications, **49** (2019), art.no.102396. https://doi.org/10.1016/j.jisa.2019.102396

[2] S. V. DILIP KUMAR, S. PATRANABIS, J. BREIER, D. MUKHOPADHYAY, S. BHASIN, A. CHATTOPADHYAY, A. BAKS: *A Practical Fault Attack on ARX-like Ciphers with a Case Study on ChaCha20*, Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), Taipei, 2017, 33-40. doi: 10.1109/FDTC.2017.14

[3] ALEXANDRE ADOMNICAI, JACQUES J. A. FOURNIER, AND LAURENT MASSON: *Bricklayer Attack: A Side-Channel Analysis on the ChaCha Quarter Round*, In: Patra A., Smart N. (eds) Progress in Cryptology - INDOCRYPT 2017. INDOCRYPT 2017. Lecture Notes in Computer Science, vol 10698. Springer, Cham. https://doi.org/10.1007/978-3-319-71667-1_4

[4] B. MAZUMDAR, S.S. ALI, O. SINANOGLU: *Power Analysis Attacks on ARX: An Application to Salsa20*, IEEE 21st International On-Line Testing Symposium (IOLTS), Halkidiki, 2015, 40-43. doi: 10.1109/IOLTS.2015.7229828

[5] C. WATT, J. RENNER, N. POPESCU, S. CAULIGI, D. STEFAN: *CT-Wasm: Type-Driven Secure Cryptography for the Web Ecosystem*, Proceedings of the ACM on Programming LanguagesJanuary, Article No. 77 (2019). https://doi.org/10.1145/3290390

[6] C. BAGATH BASHA, S. RAJAPRAKASH: *Enhancing The Security Using SRB18 Method of Embedding Computing*, Microprocessors and Microsystems, **77** art.id 103125, (2020).

[7] C. BAGATH BASHA, S. RAJAPRAKASH: *Securing Twitter Data Using Srb21 Phase I Methodology*, International Journal of Scientific & Technology Research, **8**(12) (2019), 1952–1955.

[8] C. BAGATH BASHA, S. RAJAPRAKASH: *Applying The CBB21 Phase 2 Method For Securing Twitter Analysed Data*, Advances in Mathematics: Scientific Journal, **9**(3) (2020), 1085-1091.

[9] C. BAGATH BASHA, S. RAJAPRAKASH, V.V.A. HARISH, M.S. KRISHNA, K. PRABHAS: *Securing Twitter Analysed Data Using CBB22 Algorithm*, Advances in Mathematics: Scientific Journal, **9**(3) (2020), 1093-1100.

[10] C. BAGATH BASHA, K. SOMASUNDARAM: *A Comparative Study of Twitter Sentiment Analysis Using Machine Learning Algorithms in Big Data*, International Journal of Recent Technology and Engineering, **8**(1) (2019), 591-599.

[1,2,3,4,5]DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
AARUPADAI VEEDU INSTITUTE OF TECHNOLOGY
VINAYAKA MISSION'S RESEARCH FOUNDATION(DEEMED TO UNIVERSITY)
PAIYANOOR, CHENNAI-603 104,TAMIL NADU, INDIA.
E-mail address: [1]rjaichandran@avit.ac.in

E-mail address: [2]pulseofpushpa@gmail.com

E-mail address: [3]amalnarayanan9@gmail.com

E-mail address: [4]minhajalik@gmail.com

E-mail address: [5]shahzadsidu@gmai.com