ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.9, 6699–6705
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.9.27 Spec. Issue on CAMM-2020

RB26 METHOD FOR SECURING THE SOCIAL MEDIA ANALYZED DATA

R. JAICHANDRAN[1], K. SHANTHA SHALINI[2], SAHEER ANAS[3], SUHAIL AHAMED CP[4], AND MOHAMMED ANAS CH[5]

ABSTRACT. In this paper, we discuss about Salsa and ChaCha methods, and find the disadvantage. To overcome the disadvantage to proposed the RB26 method. The proposed algorithm has four processes. 1. Column operations; 2.Secret key; 3. It has five processes. 1.Prime numbers; 2.Prime numbers applying in quadratic equations; 3.To merge all numbers; 4.To form a pair; 5; Swap the cell values; The fourth process has five processes. 1. Prime number; 2. Perfect numbers; 3. To merge all numbers; 4. To form a pair; 5. Swap the cell values. Finally, the proposed algorithm has compared with ChaCha algorithm.

1. INTRODUCTION

Today's need security of prediction data [8]. Now we discuss and find the various attacks and how this attacks are used. The first method discuss about fault attack of ChaCha, the second method is freestyle method are different texts are key, nonce, and messages. The third method analysed the bricklayer attack. The fourth method attack is fault injection attack. This attack used to counting the block and added the matrix. The fifth method attack is hash function Double A. This function has two processes such as column process and row process. The sixth method attack is ann addition rotation XOR provide the high security. These methods are existing attacks of this paper.This author talks

[1]*corresponding author*

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

Key words and phrases. Salsa, Security, RB26, Prime, ChaCha, Encryption, Decryption.

about ChaCha family, this family talks about the fault attack of the additional rotations XOR [1]. They are introduced the new method of 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 it is used to leakages related to the accesses of memory, and also introduced the bricklayer attack [3]. Ciphers used to initialize the matrix, make a key, counting the block, nonce, and added the matrix [4]. They discussed about the hash function Double A, and this function has two rounds such has column round and row round [5]. There are mainly analyzed the Double A hash function for the security purpose [6]. SRB21 methodology are proposed by Somasundaram Rajaprakash Bagahbasha21 and they mainly discuss the prime numbers of the secret key [7]. Finally, the final method is ChaCha20/4 process, and it is ovolo round process and each process is southeast diagonal process, and provide tiny bit data security. To overcome this drawback, to proposed new algorithm Rajaprakash Bagathbasha26 (RB26) in this current work.

2. METHODS

Table 1 and Table 2 are encryption and decryption.

3. ENCRYPTION

A is analyzed prediction twitter or facebook data matrix [8].

Equation "(1)"

$$CA = \begin{bmatrix} 13 & 12 & 11 \\ 16 & 15 & 14 \\ 19 & 18 & 17 \end{bmatrix}$$

Equation "(2)" [9] , ek=5

$$MA = \begin{bmatrix} 65 & 60 & 55 \\ 80 & 75 & 70 \\ 95 & 90 & 85 \end{bmatrix}$$

Equation "(3)"

Pair-1 (3, 6)

$$ME = \begin{bmatrix} 65 & 60 & 70 \\ 80 & 75 & 55 \\ 95 & 90 & 85 \end{bmatrix}$$

Pair-2 (8, 5)

$$ME = \begin{bmatrix} 65 & 60 & 70 \\ 80 & 90 & 55 \\ 95 & 75 & 85 \end{bmatrix}$$

Pair-3 (5, 6)

$$ME = \begin{bmatrix} 65 & 60 & 70 \\ 80 & 55 & 90 \\ 95 & 75 & 85 \end{bmatrix}$$

Pair-4 (5, 4)

$$ME = \begin{bmatrix} 65 & 60 & 70 \\ 55 & 80 & 90 \\ 95 & 75 & 85 \end{bmatrix}$$

Equation "(4)" [10]

Pair-1 (6, 2)

$$EPN = \begin{bmatrix} 65 & 90 & 70 \\ 55 & 80 & 60 \\ 95 & 75 & 85 \end{bmatrix}$$

Pair-2 (8,4)

$$EPN = \begin{bmatrix} 65 & 90 & 70 \\ 75 & 80 & 60 \\ 95 & 55 & 85 \end{bmatrix}$$

Pair-3 (9, 6)

$$EPN = \begin{bmatrix} 65 & 90 & 70 \\ 75 & 80 & 85 \\ 95 & 55 & 60 \end{bmatrix}$$

Pair-4 (8,1)

$$EPN = \begin{bmatrix} 55 & 90 & 70 \\ 75 & 80 & 85 \\ 95 & 65 & 60 \end{bmatrix}$$

Pair-5 (2,8)

$$EPN = \begin{bmatrix} 55 & 65 & 70 \\ 75 & 80 & 85 \\ 95 & 90 & 60 \end{bmatrix}$$

4. Decryption

Equations "(5)"

$$EPN = \begin{bmatrix} 55 & 65 & 70 \\ 75 & 80 & 85 \\ 95 & 90 & 60 \end{bmatrix}$$

where D is decrypted data matrix.

Pair-1 (8,2)

$$DPN = \begin{bmatrix} 55 & 90 & 70 \\ 75 & 80 & 85 \\ 95 & 65 & 60 \end{bmatrix}$$

Pair-2 (1, 8)

$$DPN = \begin{bmatrix} 65 & 90 & 70 \\ 75 & 80 & 85 \\ 95 & 55 & 60 \end{bmatrix}$$

Pair-3 (6, 9)

$$DPN = \begin{bmatrix} 65 & 90 & 70 \\ 75 & 80 & 60 \\ 95 & 55 & 85 \end{bmatrix}$$

Pair-4 (4, 8)

$$DPN = \begin{bmatrix} 65 & 90 & 70 \\ 55 & 80 & 60 \\ 95 & 75 & 85 \end{bmatrix}$$

Pair-5 (2, 6)

$$DPN = \begin{bmatrix} 65 & 60 & 70 \\ 55 & 80 & 90 \\ 95 & 75 & 85 \end{bmatrix}$$

Equations "(6)" (4, 5), (6, 5), (5, 8), and (6, 3).

Pair-1 (4, 5)

$$MD = \begin{bmatrix} 65 & 60 & 70 \\ 80 & 55 & 90 \\ 95 & 75 & 85 \end{bmatrix}$$

Pair-2 (6, 5)

$$MD = \begin{bmatrix} 65 & 60 & 70 \\ 80 & 90 & 55 \\ 95 & 75 & 85 \end{bmatrix}$$

Pair-3 (5, 8)

$$MD = \begin{bmatrix} 65 & 60 & 70 \\ 80 & 75 & 55 \\ 95 & 90 & 85 \end{bmatrix}$$

Pair-4 (6, 3)

$$MD = \begin{bmatrix} 65 & 60 & 55 \\ 80 & 75 & 70 \\ 95 & 90 & 85 \end{bmatrix}$$

Euations "(7)" and dk=5

$$DA = \begin{bmatrix} 13 & 12 & 11 \\ 16 & 15 & 14 \\ 19 & 18 & 17 \end{bmatrix}$$

Equations "(8)"

$$CA = \begin{bmatrix} 11 & 12 & 13 \\ 14 & 15 & 16 \\ 17 & 18 & 19 \end{bmatrix}$$

5. CONCLUSION

Today's need of prediction data; so apply the ChaCha method. This method done only encryption speed with tiny bit data security. So the proposed algorithm has four processes. 1. Column operations; 2.Secret key; 3. It has five processes. 1.Prime numbers; 2.Prime numbers applying in quadratic equations; 3.To merge all numbers; 4.To form a pair; 5; Swap the cell values; The fourth process has five processes. 1. Prime number; 2. Perfect numbers; 3. To merge all numbers; 4. To form a pair; 5. Swap the cell values. Finally, the RB26 algorithm has compared with ChaCha method and the RB26 algorithm has improved the

TABLE 1. RB26 Encryption

STEPS	RB26 ENCRYPTION
1	$CA = C_i < - > (C_{i+(n-m)})$ **(1)** where CA is Column encrypted matrix, C is a columns, i, n and m is column numbers
2	**MA = ek.A (2) .**
3	$ME = (-b \pm \sqrt{(b^2) - 4ac})/2a.$ where ME is encrypted matrix, a, b, and c are possible prime numbers (3)
4	"Prime numbers in the Matrix MA".
5	"$EPN = (e^{k-1})(e^k) - 1$ **(4).**

TABLE 2. RB26 Decryption

STEPS	RB26 DECRYPTION
1	"Prime numbers in the Matrix A".
2	$DPN = (d^{k-1})(d^k) - 1$ **(5) .**
3	$MD = (-b \pm \sqrt{(b^2) - 4ac})/2a.$ where ME is decrypted matrix, a, b, and c are possible prime numbers (6)
4	**DA = A/dk (7)**
5	"$CA = C_i < - > (C_{i+(n-m)})$ **(8)** where CA is Column encrypted matrix, C is a columns, i, n and m is column numbers"

data security while comparing to ChaCha algorithm. In the future, to add the prime factors operations of the data security in the RB27 method for upcoming journals.

REFERENCES

[1] S. V. DILIP KUMAR, S. PATRANABIS, J. BREIER, D. MUKHOPADHYAY, S. BHASIN, A. CHATTOPADHYAY, A. BAKSI: *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

[2] A.B. PUTHUPARAMBIL, 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

[3] A. ADOMNICAI, J.J.A. FOURNIER, L. 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] K. FUKUSHIMA, R. XU, S. KIYOMOTO, N. HOMMA: *Fault Injection Attack on Salsa20 and ChaCha and a Lightweight Countermeasure*, IEEE Trustcom/BigDataSE/ICESS, Sydney, NSW, 2017, 1032-1037. doi: 10.1109/Trustcom/BigDataSE/ICESS.2017.348

[5] A. ISSA, M.A. AL-AHMAD, A. AL-SALEH: *Double-A - A Salsa20 like the Design*, 4th International Conference on Advanced Computer Science Applications and Technologies (ACSAT), Kuala Lumpur, 2015, 18-23. doi: 10.1109/ACSAT.2015.25

[6] A. AL-SALEH, M. AL-AHMMAD, A. ISSA, A. AL-FOUDERY: *Double-A - A Salsa20 like the Security*, 4th International Conference on Advanced Computer Science Applications and Technologies (ACSAT), Kuala Lumpur, 2015, 24-29. doi: 10.1109/ACSAT.2015.14

[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, 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.

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

[10] K. KARTHIK, C. BAGATH BASHA, U. BHASWANTH THILAK, T. SAI KIRAN, J. RAJ: *Securing Social Media Analyzed Data Using RB20 Method*, Advances in Mathematics: Scientific Journal, **9**(3) (2020), 1157-1163.

[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@gmail.com

E-mail address: [2]shanthashalini@avit.ac.in

E-mail address: [3]saheeranas3@gmail.com

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

E-mail address: [5]naashmuhammed@gmail.com