ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.9, 6679–6685
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.9.25 Spec. Issue on CAMM-2020

SECURING GENERALIZED DATA USING RB23 ALGORITHM

R. JAICHANDRAN[1], K. SHANTHA SHALINI[2], S. LEELAVATHY[3], J. JOHNSON RAJAGURU[4], AND KURUVA PRADEEP[5]

ABSTRACT. The security of ChaCha stream cipher family design from Salsa stream cipher design. The ChaCha design also ovolo round process. ChaCha20 has many versions such as ChaCha20, ChaCha2, ChaCha8, ChaCha7, ChaChca4 are analogue modifications of the round ciphers. These versions are compared with itself, and show the best encryption speed is ChaCha4. This ChaCha4 main drawback is only encryption speed and tiny bit data security. In this work to overcome this drawback and proposed new security algorithm. The proposed algorithm has two processes. The first process is analyze the possible prime number in the given matrix. The second process is apply the possible prime numbers in quadratic equations in the given matrix. Finally, the proposed algorithm has compared with ChaCha algorithm.

1. INTRODUCTION

Today's storage data need more security is very important to all the areas in the world. For example, bank analysed data, social media analysed data, personal storage data, credit and debit card analysed data, and machine learning algorithm prediction data [3]. These data want more security. To overcome these problem to apply the ChaCha design family. ChaCha design from Salsa design. ChaCha family has several variant such as ChaCha20/20 that is 20 round processes, ChaCha20/12 that is 12 round processes, ChaCha20/8 that is

[1]*corresponding author*

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

Key words and phrases. ChaCha, Salsa, Security, RB23, Perfect Number, Prime.

8 round processes, ChaCha20/7 that is 7 round processes, and ChaCha20/4 that is 4 round processes. ChaCha20/4 is ovolo round process and each process is southeast diagonal process. ChaCha rounds are focused about encryption speed and tiny bit data security. To overcome this drawback, to proposed new algorithm Rajaprakash Bagathbasha23 (RB23) in this current work.

Shao et al., studied the Salsa20 independent round process. Almazrooie et al., author discuss the Salsa20/4 diffusion level and speed. Yadav et al., author analyze the Salsa20/9 and ChaCha8, and it is used to improve the reducing of complexity of the previous attack. Ding studied the Salsa20 family stream cipher best attack model is Salsa20/8 and Salsa20/12. Dey et al., they proposed algorithm is Probabilistic Neutral Bits. It is used to improve the current attack. Deepthi et al., they discuss the attack model. This model used key bits is 128 key for Salsa7 and ChaCha6. Maitra also studied the attack model. This model used for the proper choice of IVs by Salsa8 and ChaCha7. Afdhila et al., they discuss the Salsa20 cryptography algorithm. It is used to send the talk data through packets, and performance also good while compared to previous algorithm. Parmar et al., they studied the three types of security like authentication of user, user encrypted the data during transit and user encrypted the data at rest. Bernstein studied the Salsa20 design is the quicker than Advanced Encryption Standard [1]. Bagathbasha et al., proposed the SRB21 methodology. This methodology used to interchanging the prime number secret key and secret key [2]. Bagathbasha etal., SRB18 algorithm has discuss about security of twitter analysed data [4]. Bagathbasha etal., CBB21 Phase 2 discuss about coprime numbers [5]. Bagathbasha etal., CBB22 algorithm studied about prime number and quadratic form [6]. Karthik et al., RB20 method used identify the prime number and perfect number [7]. Rajaprakash et al., RB21 method used to multiply the secret key and identify the perfect numbers [8]. Jaichandran et al., author studied about movies reviews through Twitter data [9].

2. PROPOSED APPROACH

The proposed methodology RB23 with the matrix of order N by N. The proposed algorithm has two processes. The first process is analyze the possible prime numbers in the given matrix. The second process is apply the possible prime number in quadratic equations in the given matrix. The third process is

to merge all numbers into a single row. The fourth process is to form a pair from left to right side from third process. The fifth process is to swap the cell values with the help of pair from the given matrix; and shown in Table 1 and Table 2.

3. Functioning of RB23 Encryption Algorithm

Encryption

The propose RB23 algorithm developing from RB20 method.

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

where A is analyzed twitter or facebook data matrix.

By applying equation "(1)"

a=2,b=3, c=7

$EM = (-3 \pm \sqrt{(3^2) - 4 * 2 * 7})/2 * 2$

$EM = (-3 \pm \sqrt{9 - 56})/4$

$EM = (-3 \pm \sqrt{47})/4$

$EM = (-3 \pm 6.85565)/4$

EM=36855654

Pair of numbers (3, 6), (8, 5), (5, 6) and (5, 4).

Step 1: The 1st pair number (3, 6) should be swapped in the given matrix and this matrix represented start from 0, 1, 2, 3, 4, 5, 6, 7, 8 and 9th cell number is 9-1.

$$FPN = \begin{bmatrix} 1 & 2 & 3 \\ 7 & 5 & 6 \\ 4 & 8 & 9 \end{bmatrix}$$

where FPN is first pair number.

Step 2: The 2nd pair number (8, 5) should be swapped from FPN matrix.

$$SPN = \begin{bmatrix} 1 & 2 & 3 \\ 7 & 5 & 9 \\ 4 & 8 & 6 \end{bmatrix}$$

where SPN is second pair number.

Step 3: The 3rd pair number (5, 6) should be swapped from SPN matrix.

$$TPN = \begin{bmatrix} 1 & 2 & 3 \\ 7 & 5 & 4 \\ 9 & 8 & 6 \end{bmatrix}$$

where TPN is third pair number.

Step 4: The 4th pair number (5, 4) should be swapped from TPN matrix.

$$FOPN = \begin{bmatrix} 1 & 2 & 3 \\ 7 & 4 & 5 \\ 9 & 8 & 6 \end{bmatrix}$$

where FOPN is fourth pair number.

Finally, the original matrix could be encrypted successfully.

4. FUNCTIONING OF RB23 DECRYPTION ALGORITHM

$$DM = \begin{bmatrix} 1 & 2 & 3 \\ 7 & 4 & 5 \\ 9 & 8 & 6 \end{bmatrix}$$

where DM is decrypted matrix.

By applying equations "(2)" a=2,b=3, c=7

$DM = (-3 \pm \sqrt{(3^2) - 4 * 2 * 7})/2 * 2$

$DM = (-3 \pm \sqrt{9 - 56})/4$

$DM = (-3 \pm \sqrt{47})/4$

$DM = (-3 \pm 6.85565)/4$

DM = 36855654.

Pair of numbers (4, 5), (6, 5), (5, 8), and (6, 3).

Step 1: The 1st pair number (4, 5) should be swapped in the given matrix and this matrix represented start from 0, 1, 2, 3, 4, 5, 6, 7, 8 and 9th cell number is 9-1.

$$FPN = \begin{bmatrix} 1 & 2 & 3 \\ 7 & 5 & 4 \\ 9 & 8 & 6 \end{bmatrix}$$

where FPN is first pair number

Step 2: The 2nd pair number (6, 5) should be swapped from FPN matrix.

$$SPN = \begin{bmatrix} 1 & 2 & 3 \\ 7 & 5 & 9 \\ 4 & 8 & 6 \end{bmatrix}$$

where SPN is second pair number

Step 3: The 3rd pair number (5, 8) should be swapped from SPN matrix.

$$TPN = \begin{bmatrix} 1 & 2 & 3 \\ 7 & 5 & 6 \\ 4 & 8 & 9 \end{bmatrix}$$

where TPN is third pair number

Step 4: The 4th pair number (6, 3) should be swapped from TPN matrix.

$$FOPN = \begin{bmatrix} 1 & 2 & 3 \\ 6 & 5 & 6 \\ 3 & 8 & 9 \end{bmatrix}$$

where FOPN is fourth pair number

Finally, the original matrix could be encrypted successfully.

TABLE 1. RB23 Encryption Algorithm

STEPS	RB23 ENCRYPTION ALGORITHM
1	To analyse the possible prime number in the given matrix.
2	$EM = (-b \pm \sqrt{(b^2) - 4ac})/2a.$ where EM is encrypted matrix, a, b, and c are possible prime numbers (1)
3	To merge all the numbers into a single row.
4	To form a pair of numbers from left to right from Step 3.
5	Each and every pair should swapped cell values from given matrix.

TABLE 2. RB23 Decryption Algorithm

STEPS	RB23 DECRYPTION ALGORITHM
1	To analyse the possible prime number in the given matrix.
2	$DM = (-b \pm \sqrt{(b^2) - 4ac})/2a.$ where DM is decrypted matrix, a, b, and c are possible prime numbers (2)
3	To merge all the numbers into a single row.
4	To form a pair of numbers from left to right from Step 3.
5	Each and every pair should swapped cell values from given matrix.

5. DISCUSSION AND CONCLUSION

Today's storage data need more security is very important to all the areas in the world. For example, bank analysed data, social media analysed data, personal storage data, credit and debit card analysed data, and machine learning algorithm prediction data. These data want more security. To overcome these problem to apply the ChaCha design family. ChaCha design from Salsa design and this design done only encryption speed with little bit data security. So we proposed algorithm is RB23, and this algorithm has two processes. The first process is analyze the possible prime number in the given matrix. The second process is apply the possible prime numbers in quadratic equations in the given matrix. Finally, the proposed algorithm has compared with ChaCha algorithm and the RB23 algorithm has increased the data security while comparing to ChaCha algorithm. In the future, to add prime number secret key operations of the data security in the RB24 method for upcoming journals.

REFERENCES

[1] D.J. BERNSTEIN: *The Salsa20 Family of Stream Ciphers*, In: Robshaw M., Billet O. (eds) New Stream Cipher Designs. Lecture Notes in Computer Science, vol 4986. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-68351-3_8

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

[3] 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) (2015), 310-324.

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

[5] 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.

[6] 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.

[7] 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.

[8] S. RAJAPRAKASH, K. KARTHIK, A. MOHAN, S. SARKAR, J. MATHEW: *Design of New Security System Using RB21 Algorithm*, Advances in Mathematics: Scientific Journal, **9**(3) (2020), 1149-1155.

[9] R. JAICHANDRAN, C. BAGATH BASHA, K.L. SHUNMUGANATHAN, S. RAJAPRAKASH, S. KANAGASUBA RAJA: *Sentiment Analysis of Movies on Social Media using R Studio*, International Journal of Engineering and Advanced Technology, **8**(6) (2019), 2171-2175.

[1,2,3,4,5]DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
AARUPADAI VEEDU INSTITUTE OF TECHNOLOGY
VINAYAKA MISSION'S RESEARCH FOUNDATION
CHENNAI, TAMIL NADU, INDIA.
E-mail address: [1]rjaichandran@gmail.com

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

E-mail address: [3]leelavathy@avit.ac.in

E-mail address: [4]rajagurujj@yahoo.com

E-mail address: [5]kuruvapradeep80@gmail.com