ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.9, 6659–6665
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.9.23 Spec. Issue on CAMM-2020

RB22 ALGORITHM FOR NEW SECURITY SYSTEM

R. SHOBANA[1], R. JAICHANDRAN[2], M. SRISATHVIK[3], M. BHANU PRAKASH[4], AND P. BHUVANESH[5]

ABSTRACT. The security of ChaCha family design from Salsa. The ChaCha design also quarter round process like Salsa. ChaCha20 versions are ChaCha 20/20, ChaCha20/12, ChaCha20/8, ChaCha20/7, ChaChca20/4 are analogue modificaLtions of the 20-round cipher, 12-round cipher, 8-round cipher, 7-round cipher, and 4-round cipher. These versions are compared with itself, and best encryption speed is ChaCha20/4. This ChaCha20/4 main drawback is concentrate only encryption speed and little bit data security. To overcome this drawback and proposed novel security algorithm is RB22. RB22 algorithm has 3 processes. In 1st process is column operations; 2nd process is multiplication of secret key; and 3rd process is swap the perfect number. Finally, the RB22 algorithm has compared with ChaCha algorithm.

1. INTRODUCTION

Today's prediction data [7] want more security, so 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 8 round processes, ChaCha20/7 that is 7 round processes, and ChaCha20/4 that is 4 round processes. ChaCha20/4 is quarter round process and each process is southeast diagonal process. ChaCha

[2]*corresponding author*

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

Key words and phrases. ChaCha, Security, RB22, Perfect Number, Prime.

rounds are concentrate about encryption speed and little bit data security. Author used 128 key bits for methods. Salsa20 cryptography algorithm send the talk data through packets. This algorithm performance is good while compared to previous algorithm. Salsa20 design is the quicker than Advanced Encryption Standard. CBB22 method is used to convert the matrix data to quadratic form [2]. CBB21 phase 2 methods is used to swap a co-prime numbers [3]. ChaCha rounds are concentrate about encryption speed and little bit data security. To overcome this drawback, to proposed new algorithm Rajaprakash Bagathbasha22 (RB22) 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 [7].
Equation "(1)"

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

Equation "(2)", ek=5

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

"**Equation "(3)" ([4])**
Pair-1 (3, 0)

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

Pair-2 (1, 0)

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

Pair-3 (4, 0)

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

Pair-4 (2, 0)

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

Pair-5 (4, 5)

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

Pair-6 (3, 0)

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

Pair-7 (4, 0)

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

Pair-8 (5, 1)

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

Pair-9 (0, 4)

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

4. DECRYPTION

"**Equation "(4)" ([4])**

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

where D is decrypted data matrix.

Pair-1 (4, 0)

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

Pair-2 (1, 5)

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

Pair-3 (0, 4)

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

Pair-4 (0, 3)

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

Pair-5 (5, 4)

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

Pair-6 (0, 2)

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

Pair-7 (0, 4)

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

Pair-8 (0, 1)

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

Pair-9 (0, 3)

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

"**Equation "(5)" and dk=5**

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

"**Equation "(6)"**

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

TABLE 1. RB22 Encryption

STEPS	RB22 ENCRYPTION
1st	$CA = C_i <-> (C_{i+(n-m)})$ **(1)** where CA is Column encrypted matrix, C is a columns, i, n and m is column numbers
2nd	**A = ek.A (2)** .
3rd	"Prime numbers in the Matrix A".
4th	"$PN = (e^{k-1})(e^k) - 1$ **(3)**.

5. CONCLUSION

Today's prediction data want more security, so 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 8 round processes, ChaCha20/7 that is 7 round processes, and ChaCha20/4 that is 4 round processes. ChaCha20/4 is quarter round process and each process is southeast diagonal process. ChaCha rounds

TABLE 2. RB22 Decryption

STEPS	RB22 DECRYPTION
1st	"prime numbers in the Matrix A".
2nd	$PN = (d^{k-1})(d^k) - 1$ **(4)** .
3rd	**A = A/dk (5)**
4th	"$CA = C_i < -- > (C_{i+(n-m)})$ **(6)** where CA is Column encrypted matrix, C is a columns, i, n and m is column numbers"

are concentrate about encryption speed and little bit data security. So we proposed novel algorithm is RB22, and this algorithm has 3 processes. In 1st process is column operations; 2nd process ismultiplication of secret key; and 3rd process is swap the perfect number. Finally, the RB22 algorithm has compared with ChaCha algorithm and the RB22 algorithm has increased the security while comparing to ChaCha algorithm. In the future, add more operations of the data security.

REFERENCES

[1] 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.

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

[3] 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.

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

[5] C. BAGATH BASHA, S. RAJAPRAKASH: *Enhancing The Security Using SRB18 Method of Embedding Computing*, Microprocessors and Microsystems, **77** (2020), 103-125.

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

[7] C. BAGATH BASHA, K. SOMASUNDARAM: *A Comparative Study of Twitter Sentiment Analysis Using Machine Learning Algorithms in Big Data*, International Journal of Scientific & Technology Research, **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]shobana@avit.ac.in

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