ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.9, 6707–6713
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.9.28 Spec. Issue on CAMM-2020

SECURING THE PREDICTION DATA USING RB27 ALGORITHM

K. SHANTHA SHALINI[1], S. LEELAVATHY[2], AMAL KRISHNA OTK[3],
RENO THOMAS VARGHESE[4], AND NIVED VISWANATHAN[5]

ABSTRACT. Today people life one of the main part is data in the globe; because without data cannot access anything in the globe. Then automatically data need security in the globe. In default, many data security algorithms are available in the globe. But I take the two previous security methods are Salsa and ChaCha. In this work, it has been discuss the drawbacks of previous methods, and to propose a new method named as the RB27 methodology with the matrix of order N. RB27algorithm has two stages. In the first stage have five processes. 1. Identifying prime numbers; 2. Apply the prime number in quadratic equations; 3. Merge all numbers; 4. Form a pair from left to right side; 5. Swap the cell values using before step. In the second stage have five processes. 1. Identifying the prime number; 2. Find a perfect numbers; 3. Merge all perfect numbers; 4. Form a pairs from left to right side; 5. Swap the cell values using before step. RB27 algorithm has compared with ChaCha algorithm.

1. INTRODUCTION

Today's need security of prediction data [9]. Now we discuss and find the various attacks and how this attacks are used. The first method discuss about fault attack of ChaCha, and it is used to rotate the XOR. The second method discuss about freestyle method, and it is used to different texts are key, nonce, and messages. The third method analysed the bricklayer attack. The fourth

[1]*corresponding author*

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

Key words and phrases. Salsa, Security, RB27, Prime, ChaCha, Encryption, Decryption.

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. They are proposed the fault injection attack on ChaCha and Salsa20 ciphers, and this ciphers used to initialize the matrix, make a key, counting the block, nonce, and added the matrix [1]. They discussed about the hash function Double A rounds, and this round function has two rounds like column round and row round [2]. They are mainly discussed about ann addition rotation XOR (ARX), and this cipher used for high security [3]. There are mainly analyzed the Double A hash function for the security purpose [4]. They studied about the power analysis attack and correlations power analysis (CPA) for the vulnerability of Salsa20. The best attack is power analysis attack [5]. They are mainly studied the design and implementation of constant time web assembly. This design is fast and flexible to implement the secure algorithms [6]. They generalize the notion of probabilistic neutral bits to probabilistic neutral vectors (PNV), and the set of probabilistic neutral vectors is no smaller than that of probabilistic neutral bits. It is used to find and improved the key recovery attacks on reduced the round of Salsa20 and ChaCha [7]. SRB21 methodology are proposed by Somasundaram Rajaprakash Bagahbasha21 and they mainly discuss the prime numbers of the secret key [8]. 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 Bagathbasha27 (RB27) 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 [10].

Equation "(1)"

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

Pair-1 (3, 6)

$$ME = \begin{bmatrix} 1/2 & 1 & 3 \\ 2 & 5/2 & 3/2 \\ 7/2 & 4 & 9/2 \end{bmatrix}$$

Pair-2 (8, 5)

$$ME = \begin{bmatrix} 1/2 & 1 & 3 \\ 2 & 4 & 3/2 \\ 7/2 & 5/2 & 9/2 \end{bmatrix}$$

Pair-3 (5, 6)

$$ME = \begin{bmatrix} 1/2 & 1 & 3 \\ 2 & 3/2 & 4 \\ 7/2 & 5/2 & 9/2 \end{bmatrix}$$

Pair-4 (5, 4)

$$ME = ME = \begin{bmatrix} 1/2 & 1 & 3 \\ 3/2 & 2 & 4 \\ 7/2 & 5/2 & 9/2 \end{bmatrix}$$

"**Equation "(2)" [10]**

Pair-1 (6, 2)

$$EPN = \begin{bmatrix} 1/2 & 4 & 3 \\ 3/2 & 2 & 1 \\ 7/2 & 5/2 & 9/2 \end{bmatrix}$$

Pair-2 (8,4)

$$EPN = \begin{bmatrix} 1/2 & 4 & 3 \\ 5/2 & 2 & 1 \\ 7/2 & 3/2 & 9/2 \end{bmatrix}$$

Pair-3 (9, 6)

$$EPN = \begin{bmatrix} 1/2 & 4 & 3 \\ 5/2 & 2 & 9/2 \\ 7/2 & 3/2 & 1 \end{bmatrix}$$

Pair-4 (8,1)

$$EPN = \begin{bmatrix} 3/2 & 4 & 3 \\ 5/2 & 2 & 9/2 \\ 7/2 & 1/2 & 1 \end{bmatrix}$$

Pair-5 (2,8)

$$EPN = \begin{bmatrix} 3/2 & 1/2 & 3 \\ 5/2 & 2 & 9/2 \\ 7/2 & 4 & 1 \end{bmatrix}$$

4. Decryption

"**Equations "(3)"**

$$D = \begin{bmatrix} 3/2 & 1/2 & 3 \\ 5/2 & 2 & 9/2 \\ 7/2 & 4 & 1 \end{bmatrix}$$

where D is decrypted data matrix.

Pair-1 (8,2)

$$DPN = \begin{bmatrix} 3/2 & 4 & 3 \\ 5/2 & 2 & 9/2 \\ 7/2 & 1/2 & 1 \end{bmatrix}$$

Pair-2 (1, 8)

$$DPN = \begin{bmatrix} 1/2 & 4 & 3 \\ 5/2 & 2 & 9/2 \\ 7/2 & 3/2 & 1 \end{bmatrix}$$

Pair-3 (6, 9)

$$DPN = \begin{bmatrix} 1/2 & 4 & 3 \\ 5/2 & 2 & 1 \\ 7/2 & 3/2 & 9/2 \end{bmatrix}$$

Pair-4 (4, 8)

$$DPN = \begin{bmatrix} 1/2 & 4 & 3 \\ 3/2 & 2 & 1 \\ 7/2 & 5/2 & 9/2 \end{bmatrix}$$

Pair-5 (2, 6)

$$DPN = \begin{bmatrix} 1/2 & 1 & 3 \\ 3/2 & 2 & 4 \\ 7/2 & 5/2 & 9/2 \end{bmatrix}$$

Equations "(4)"

Pair-1 (4, 5)

$$MD = \begin{bmatrix} 1/2 & 1 & 3 \\ 2 & 3/2 & 4 \\ 7/2 & 5/2 & 9/2 \end{bmatrix}$$

Pair-2 (6, 5)

$$MD = \begin{bmatrix} 1/2 & 1 & 3 \\ 2 & 4 & 3/2 \\ 7/2 & 5/2 & 9/2 \end{bmatrix}$$

Pair-3 (5, 8)

$$MD = \begin{bmatrix} 1/2 & 1 & 3 \\ 2 & 5/2 & 3/2 \\ 7/2 & 4 & 9/2 \end{bmatrix}$$

Pair-4 (6, 3)

$$MD = \begin{bmatrix} 1/2 & 1 & 3/2 \\ 2 & 5/2 & 3 \\ 7/2 & 4 & 9/2 \end{bmatrix}$$

TABLE 1. RB27 Encryption

STEPS	RB27 ENCRYPTION
1	Prime number in the given matrix
2	$ME = (-b \pm \sqrt{(b^2) - 4ac})/2a.$ where ME is encrypted matrix, a, b, and c are possible prime numbers **(1)**
3	To form a pair from left to righ
4	All pairs swapped cell values from the given matrix
5	Prime numbers in the Matrix ME".
6	$EPN = (e^{k-1})(e^k) - 1$ **(2)**
7	To form a pair from left to right
8	All pairs swapped cell values from the given matrix

TABLE 2. RB27 Decryption

STEPS	RB27 DECRYPTION
1	Prime numbers in the Matrix A".
2	$DPN = (d^{k-1})(d^k) - 1$ **(3)**
3	To form a pair from right to left.
4	All pairs swapped cell values from the given matrix.
5	Prime numbers in the Matrix DPN".
6	$MD = (-b \pm \sqrt{(b^2) - 4ac})/2a.$ where ME is decrypted matrix, a, b, and c are possible prime numbers (4)
7	To form a pair from right to left.
8	All pairs swapped cell values from the given matrix.

5. CONCLUSION

Today's need security of prediction data. To overcome these problem to apply the ChaCha method. This method done only encryption speed with tiny bit data security. So we proposed novel algorithm is RB27, it has two stages. In the first stage have five processes. 1. Identifying prime numbers; 2. Apply the prime number in quadratic equations; 3. Merge all numbers; 4.Form a pair from left to right side; 5. Swap the cell values using before step. In the second stage have five processes. 1. Identifying the prime number; 2. Find a perfect numbers; 3. Merge all perfect numbers; 4. Form a pairs from left to right side; 5. Swap the cell values using before step. Finally, the proposed algorithm has compared with ChaCha method and the RB27 algorithm has improved the data security while comparing to ChaCha algorithm. In the future, to add the prime factors operations of the data security.

REFERENCES

[1] 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

[2] 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

[3] B. MAZUMDAR, S.S. ALI, O. SINANOGLU: *A Compact Implementation of Salsa20 and Its Power Analysis Vulnerabilities*, ACM Transactions on Design Automation of Electronic Systems, **22** (2006), art.no.11. https://doi.org/10.1145/2934677

[4] 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

[5] 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

[6] C. WATT, J. RENNER, N. POPESCU, S. CAULIGI, D. STEFAN: *CT-Wasm: Type-Driven Secure Cryptography for theWeb Ecosystem*, Proceedings of the ACM on Programming Languages, **3** (2019), Article No.: 77. https://doi.org/10.1145/3290390

[7] Z. SHI, B. ZHANG, D. FENG, W. WU: *Improved Key Recovery Attacks on Reduced-Round Salsa20 and ChaCha*, In: Kwon T., Lee MK., Kwon D. (eds) Information Security and Cryptology, Lecture Notes in Computer Science, **7839** (2012), 337-351. https://doi.org/10.1007/978-3-642-37682-5_24

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

[9] 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.

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

[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]shanthashalini@avit.ac.in

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

E-mail address: [3]amalkrish2255@gmail.com

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

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