ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.3, 1157–1163
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.3.41 Spec. Issue on RDESTM-2020

SECURING SOCIAL MEDIA ANALYZED DATA USING RB20 METHOD

K. KARTHIK[1], C. BAGATH BASHA, U. BHASWANTH THILAK, T. SAI KIRAN, AND J. RAJ

ABSTRACT. Today's world has watched the accumulated of data through social media such has Facebook and Twitter, that are increased enormously day by day. Using these social media, user post or tweet on many topics from anywhere within the world through the web. This social media analysed data need security, and also available more algorithm like AES, DES, Salsa, and etc... In In this paper, discuss two existing algorithm such has AES and Salsa and proposed RB20 method by modifying the Salsa. The proposed method has five processes. The first process is identifying the prime number in the given matrix. The second process is to find a perfect numbers. The third process is to merge all perfect 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 given matrix. The proposed method calculate the time and compared with both AES and Salsa.The proposed method has very good security while compare to both existing algorithms.

1. INTRODUCTION

During the previous years, the global has watched the rise the huge social media information hold on Facebook and Twitter. They are used by multi-user to post on any topic in the social media through the internet. This post used to make the polarity scores. This analysed score has low security. In default, Facebook and Twitter analysed data does not have good security. To overcome this problem. Daniel Bernstein introduces Salsa, a family of stream ciphers, which is

[1]*corresponding author*

Key words and phrases. Encryption, Polarity, Salsa, Security, RB20, Twitter, Tweets, Facebook.

focusses on encryption process. Salsa20 handle the keys of 128 bits and 256 bits, but Daniel Bernstein recommended the 256 bits keys. Salsa20 introduced by Daniel Bernstein, and it has 20 rounds, is faster than the Advanced Encryption Standard (AES) and provide the better security. The Salsa20 reduced versions are Salsa20/12, Salsa20/8, Salsa20/7, Salsa20/6, Salsa20/5, and Salsa20/4. Salsa20/4 process only 3 rounds only because first round has no changed. It is mainly process on encryption speed when compare to other Salsa20 versions, and it does not focuses the data security. To overcome these drawbacks of Salsa20/4 for securing the data, a new method Rajaprakash Bagathbasha20 (RB20) is proposed in this present work. Hongjun introduced the cipher attack in 2002 and apply to the Salsa20. It's used flexible rounds and every round is independent number of rounds [1]. Studied the proposed chaotic Salsa and Salsa20/4. It's wont to compare the diffusion level and speed [2].

Studied and improved the correlation attack between ChaCha8 and Salsa20/9. they're mainly analyze the reducing of complexity of the previous attack [3].

Salsa20 family improved the cipher attack and its best attack model are Salsa20/12 and Salsa20/8 [4]. Studied the ChaCha and Salsa reduced rounds, they proposed new algorithm is Probabilistic Neutral Bits. This algorithm is quicker than the previous attack [5].

Enhanced the attack on 128 key bits of ChaCha6 and Salsa7 [6]. Enhanced the attack of Salsa8 and ChaCha7 with proper choice of IVs [7]. Salsa20 stream cipher cryptography algorithms were apply the talk data. This algorithm is especially wont to study the time interval is silently fast, 1st packet takes a couple of milliseconds and 2nd packet takes one millisecond. The performance of the results show the Salsa20 is best within the data security [8]. This author provides the 3D security like user authentication, encrypted data during transit and encrypted data at rest. This 3D wont to increasing the buffer size, reduces the loop iterations and consequently reduces the general encryption time on ChaCha20 [9]. Proposed Salsa20/20 design which is quicker than AES and Salsa20 family gives more importance for encryption speed [10]. Proposed SRB21 methodology has interchanging the secret key and prime number secret key [11].

2. METHODOLOGY: RB20 METHOD

The proposed RB20 method has five processes. The first process is identifying the prime number in the given matrix. The second process is to find a perfect numbers. The third process is to merge all perfect 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 given matrix as shown in Table 1.

TABLE 1. RB20 METHOD

STEPS	RB20 METHOD
1	Extracting the data from Facebook and Twitter.
2	Analysed twitter or facebook data are stored in the matrix A.
3	Identifying the prime numbers in the Matrix A.
4	$PN = (e^{k-1})(e^k) - 1$ **Equation (1)** where PN is perfect number, e is integer number, e>=2, and k is prime number from given Matrix A.
5	Number of perfect number are derived from step 4.
6	To merge all the perfect numbers into a single row.
7	To form a pair of numbers from left to right from Step 6.
8	Each and every pair should swapped cell values from given matrix.

3. IMPLEMENTATION OF RB20 METHOD

This section explained the RB20 method below

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

where A is analyzed twitter or facebook data matrix [12].

By applying equation "(1)".
Finally, PN = 6284968128.
Pair of perfect numbers (6,2)(8,4)(9,6)(8,1)(2,8) as shown in Table 2.

TABLE 2. PERFECT NUMBERS

STEPS	e value	K value	PN
1	2	2	6
2	2	3	28
1	2	5	496
1	2	7	8128

Step 1: The first pair of perfect number (6, 2) should be swapped in the given matrix.

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

where FPN is first pair of perfect number.

Step 2: The second pair of perfect number (8, 4) should be swapped from FPN matrix.

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

where SPN is second pair of perfect number.

Step 3: The third pair of perfect number (9, 6) should be swapped from SPN matrix.

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

where TPN is third pair of perfect number.

Step 4: The fourth pair of perfect number (8, 1) should be swapped from TPN matrix.

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

where FOPN is fourth pair of perfect number.

Step 5: The fifth pair of perfect number (2, 8) should be swapped from FOPN matrix.

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

where FIPN is fifth pair of perfect number.

Finally, the original matrix could be encrypted successfully.

4. Conclusion

The proposed method RB20 by modifying the Salsa to enhance further security. RB20 algorithm compared with AES and Salsa algorithms; 1) N round in RB20, 16 round in AES, and quarter round in Salsa; 2) Time is high both RB20 and AES, and time is less in Salsa; 3) Security is more high in RB20, Security is good in AES, and Security is less in Salsa; 4) Prime number used in rb20 and no prime numbers both AES and Salsa. The proposed method provides high security because of prime perfecr numbers data while compared to both existing algorithms. In future, to add more operations for data security.

References

[1] Z. Shao, L. Ding: *Related-Cipher Attack on Salsa20*, Proc. Fou. Inter. Conf. on Comp. and Inf. Sci., (2012), 1182–1185.

[2] M. Almazrooie, A. Samsudin, M. M. Singh: *Improving the Diffusion of the Stream Cipher Salsa20 by Employing a Chaotic Logistic Map*, J. of Inf. Pro. Sy., **11**(4) (2015), 310–324.

[3] P. Yadav, I. Gupta, S. K. Murthy: *Study and Analysis of eSTREAM Cipher Salsa And ChaCha*, Proc. Sec. IEEE Int. Con. on Eng. and Tec., 2016.

[4] L. Ding: *Improved Related-Cipher Attack on Salsa20 Stream Cipher*, IEEE Acc., **7** (2019), 30197–30202.

[5] S. Dey, S. Sarkar: *Improved analysis for reduced round Salsa and Chacha*, Dis. App. Mat., **227** (2017), 58–69.

[6] K. K. C. Deepthi, K. Singh: *Cryptanalysis of Salsa and ChaCha: Revisited*, Proc. ICST Ins. for Com. Sci., Soc. Inf. and Tel. Eng., (2018), 324–338.

[7] S. Maitra: *Chosen IV cryptanalysis on reduced round ChaCha and Salsa*, Dis. App. Mat., **208** (2016), 88–97.

[8] D. AFDHILA, S. M. NASUTION, F. AZMI: *Implementation of Stream Cipher Salsa20 Algorithm to Secure Voice on Push to Talk Application*, Proc. IEEE A. Paci. Conf. on Wir. and Mob., (2016), 137–141.

[9] R. R. PARMAR, S. ROY, D. BHATTACHARYYA, S. K. BANDYOPADHYAY, T. KIM: *Large-Scale Encryption in the Hadoop Environment: Challenges and Solutions*, IEEE Acc., **5** (2017), 7156–7163.

[10] D. J. BERNSTEIN: *The Salsa20 Family of Stream Ciphers*, N. St. Ci. Des.: The eST. Fin., Lec. Not. in Com. Sc., M. Robshaw and O. Billet, eds., Berlin: Springer, 2008.

[11] C. BAGATH BASHA, S. RAJAPRAKASH: *Securing Twitter Data Using Srb21 Phase I Methodology*, Inter. J. of Sci. and Tech. Res., **8**(12) (2019), 1952–1955.

[12] C. BAGATH BASHA, K. SOMASUNDARAM: *A Comparative Study of Twitter Sentiment Analysis Using Machine Learning Algorithms in Big Data*, Inter. J. of Rec. Tech. and Eng., **8**(1) (2015), 310–324.

Department of Computer Science and Engineering
Aarupadai Veedu Institute of Technology
Vinayaka Mission's Research Foundation
Chennai, Tamil Nadu, India
E-mail address: karthik@avit.ac.in

Department of Computer Science and Engineering
Aarupadai Veedu Institute of Technology
Vinayaka Mission's Research Foundation
Chennai, Tamil Nadu, India
E-mail address: chan.bagath@gmail.com

Department of Computer Science and Engineering
Aarupadai Veedu Institute of Technology
Vinayaka Mission's Research Foundation
Chennai, Tamil Nadu, India
E-mail address: bhaswanthb1997@gmail.com

Department of Computer Science and Engineering
Aarupadai Veedu Institute of Technology
Vinayaka Mission's Research Foundation
Chennai, Tamil Nadu, India
E-mail address: kiran12171998@gmail.com

Department of Computer Science and Engineering
Aarupadai Veedu Institute of Technology
Vinayaka Mission's Research Foundation
Chennai, Tamil Nadu, India
E-mail address: jithuraj321@gmail.com