ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.3, 1085–1091
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.3.33 Spec. Issue on RDESTM-2020

APPLYING THE CBB21 PHASE 2 METHOD FOR SECURING TWITTER ANALYSED DATA

C. BAGATH BASHA[1] AND S. RAJAPRAKASH

ABSTRACT. Daniel Bernstein has been designed the Salsa20/4. This design has quicker encryption because of the ovolo round with better data security. In the present work, a novel method CBB21 is proposed by altering the Salsa20/4 to increase the data security of the polarity scores, which is essencially required of the current world. The CBB21 method has been swap the co-prime numbers by column wise. The proposed method has calculate the running time and compared with the existing method; and also provide more security of the analyzed data while to comparing to Salsa20/4 method.

1. INTRODUCTION

Today's world people heart is social media like Twitter and Facebook. These social media used to users tweet and re-tweet, and used to make polarity score. This polarity score predict the future trends, so need security of that score, otherwise can be easily hacked, and changing the score result then face the lot of issues, such has company brands, world economic status, and etc...The machine learning algorithm used to predict the movie reviews and performance [1], and also to predict the future with the help of Twitter [2]. Salsa20 handle s the secret key is 256 bits with 20 rounds [3], and it is faster than AES and provides better security [4]. Salsa20/20 round versions are Salsa20/12, Salsa20/8, Salsa20/5, Salsa20/6, Salsa20/7, and finally Salsa20/4 rounds [5]. SRB21 method used to

[1]*corresponding author*

Key words and phrases. Encryption, Salsa, Security, CBB21.

TABLE 1. CBB21 PHASE 2 METHOD

STEPS	CBB22 ENCRYPTION
1	Extracting the data from Twitter.
2	Analyzed twitter data are stored in the matrix A.
3	Swap the Co-prime numbers by column wise of the matrix.

4	if L < N then
	if $gcd(a_{(b+1)j}, a_{(b+2)j} = 1$
	if i < N then
	$swap(a_{(b+1)j}, a_{(b+2)j}$
	L = L+2
	i= i+2
	else
	i = i + 2
	if i = i < N then
	L = L + 2
	else
	j = j + 1
	j=j <= M
	where b = 0,2,4,..N, i = 1,2,3,...N, j= 1,2,3,....M, L is cell numbers, N is order of matrix, N is rows, M is columns

swap the prime number and secret key [6]. The Salsa20/4 focus only encryption speed [7] not data security, so we produce a novel method Chan Bagath Basha21(CBB21) phase 2 in this current work.

2. METHODOLOGY: CBB21 METHOD

This work deals with the data of a particular area collected from Twitter. The data are used to classify the tweets using Rstudio on Twitter. These tweets are used to analyse negative and positive tweets to make polarity scores. The result of the polarity scores could be extracted from Twitter. These data files are converted into a matrix and the files are applied to the proposed methodology CBB21 phase 2 with the matrix of order N by N. CBB21 phase 2 method has to be swap the co-prime numbers by column wise as shown in Table 1.

TABLE 2. CBB21 Phase 2 Method Vs Salsa20/4

Salsa20/4	CBB22 Phase 2 Method
1) Quarter round process. 2) Time less.	1) N round process. 2) Time high.
3) Security more less 4) Focus only time.	3) Security more high. 4) Focus only security

3. IMPLEMENTATION OF CBB21 PHASE 2 METHOD

The proposed CBB21 Phase 2 method is developed from modifying the Salsa20/4.

$$A = \begin{bmatrix} 1 & 2 & 18 & 24 & 5 \\ 6 & 7 & 8 & 9 & 10 \\ 11 & 12 & 13 & 14 & 15 \\ 16 & 17 & 3 & 19 & 20 \\ 21 & 22 & 23 & 4 & 25 \end{bmatrix}.$$

Here, where A is analyzed twitter data matrix.

Step 1: $b = 0$, $i = 1$, $j = 1$, $L = 1$, $N = 5$, $M = 5$; $L < N \Rightarrow 1 < 5$

$$\text{gcd}\ (a_{(b+1)j}, a_{(b+2)j}) = 1 \ \Rightarrow\ \text{gcd}\ (a_{(0+1)1}, a_{(0+2)1}) = 1$$
$$\Rightarrow\ \text{gcd}\ (a_{11}, a_{21}) = 1 \ \Rightarrow\ \text{gcd}\ (1, 6) = 1$$
$$i < N = 1, 2 < 5\ \text{swap}\ (a_{11}, a_{21}) \geq \text{swap}\ (1, 6)$$

$$E = \begin{bmatrix} 6 & 2 & 18 & 24 & 5 \\ 1 & 7 & 8 & 9 & 10 \\ 11 & 12 & 13 & 14 & 15 \\ 16 & 17 & 3 & 19 & 20 \\ 21 & 22 & 23 & 4 & 25 \end{bmatrix}$$

Here where E is encrypted matrix,

$$L = L + 2 \geq 1 + 2 = 3 \quad \text{and} \quad i = i + 2 = 1 + 2 = 3.$$

Step 2: b=2, i=3, j=1, L=3, N = 5, M=5; L<N $\geq$ 3< 5.

$$\Rightarrow\ \text{gcd}\ (a_{(2+1)1}, a_{(2+2)1}) = 1 \ \Rightarrow\ \text{gcd}\ (a_{31}, a_{41}) = 1 \geq\ \text{gcd}\ (11, 16) = 1$$
$$i < N = 3, 4 < 5 \geq \text{swap}\ (a_{31}, a_{41}) \geq \text{swap}\ (11, 16)$$

$$E = \begin{bmatrix} 6 & 2 & 18 & 24 & 5 \\ 1 & 7 & 8 & 9 & 10 \\ 16 & 12 & 13 & 14 & 15 \\ 11 & 17 & 3 & 19 & 20 \\ 21 & 22 & 23 & 4 & 25 \end{bmatrix}$$

$$L = L + 2 \geq 3 + 2 = 5 \quad \text{and} \quad i = i + 2 \geq 3 + 2 = 5$$

Step 3: $b = 4$, $i = 5$, $j = 1$, $L = 5$, $N = 5$, $M = 5$; $L < N \geq 5 \leq 5$ and $j = j + 1 \geq 1 + 1 = 2$.

Step 4: $b = 0$, $i = 1$, $j = 2$, $L = 1$, $N = 5$, $M = 5$.

$$\Rightarrow \text{gcd } (a_{(0+1)2}, a_{(0+2)2}) = 1 \Rightarrow \text{gcd } (a_{12}, a_{22}) = 1 \Rightarrow \text{gcd } (2, 7) = 1$$

$$i < N = 1, 2 < 5 \geq \text{swap } (a_{12}, a_{22}) \geq \text{swap } (2, 7)$$

$$E = \begin{bmatrix} 6 & 7 & 18 & 24 & 5 \\ 1 & 2 & 8 & 9 & 10 \\ 16 & 12 & 13 & 14 & 15 \\ 11 & 17 & 3 & 19 & 20 \\ 21 & 22 & 23 & 4 & 25 \end{bmatrix}$$

$$L = L + 2 \geq 1 + 2 \geq 3 \text{ and } i = i + 2 \geq 1 + 2 \geq 3$$

Step 5: $b = 2$, $i = 3$, $j = 2$, $L = 3$, $N = 5$, $M = 5$; $L < N \geq 3 < 5$.

$$\Rightarrow \text{gcd } (a_{(2+1)2}, a_{(2+2)2}) = 1 \Rightarrow \text{gcd } (a_{32}, a_{42}) = 1 \Rightarrow \text{gcd } (12, 17) = 1$$

$$i < N = 3, 4 < 5 \geq \text{swap } (a_{31}, a_{41}) \geq \text{swap } (12, 17)$$

$$E = \begin{bmatrix} 6 & 7 & 18 & 24 & 5 \\ 1 & 2 & 8 & 9 & 10 \\ 16 & 17 & 13 & 14 & 15 \\ 11 & 12 & 3 & 19 & 20 \\ 21 & 22 & 23 & 4 & 25 \end{bmatrix}$$

$$L = L + 2 \geq 3 + 2 \geq 5 \text{ and } i = i + 2 \geq 3 + 2 \geq 5$$

Step 6: $b = 4$, $i = 5$, $j = 2$, $L = 5$, $N = 5$, $M = 5$; $L < N \geq 5 < 5$ and $j = j + 1 \geq 2 + 1 \geq 3$.

Step 7: $b = 0$, $i = 1$, $j = 3$, $L = 1$, $N = 5$, $M = 5$.

$$\Rightarrow \text{gcd } (a_{(0+1)3}, a_{(0+2)3}) = 1 \Rightarrow \text{gcd } (a_{13}, a_{23}) = 1 \Rightarrow \text{gcd (18, 8) =2}$$

Step 8: $i = i + 2 \geq 1 + 2 = 3$; $L = L + 2 \geq 1 + 2 = 3$ and $b = 2$, $j = 3$, $N = 5$, $M = 5$.

$\Rightarrow$ gcd $(a_{(2+1)3}, a_{(2+2)3}) = 1 \Rightarrow$ gcd $(a_{33}, a_{43}) = 1 \Rightarrow$ gcd (13, 3) =1

$i < N = 3, 4 < 5 \geq$ swap (a_{33}, a_{43}) = > swap (13, 3)

$$E = \begin{bmatrix} 6 & 7 & 18 & 24 & 5 \\ 1 & 2 & 8 & 9 & 10 \\ 16 & 17 & 3 & 14 & 15 \\ 11 & 12 & 13 & 19 & 20 \\ 21 & 22 & 23 & 4 & 25 \end{bmatrix}$$

$L = L + 2 \geq 3 + 2 \geq 5$ and $i = i + 2 \geq 3 + 2 \geq 5$

Step 9: $b = 4$, $i = 5$, $j = 3$, $L = 5$, $N = 5$, $M = 5$; $L < N \geq 5 < 5$ and $j = j + 1 \geq 3 + 1 \geq 4$

Step 10: $b = 0$, $i = 1$, $j = 4$, $L = 1$, $N = 5$, $M = 5$

$\Rightarrow$ gcd $(a_{(0+1)4}, a_{(0+2)4}) = 1 \Rightarrow$ gcd $(a_{14}, a_{24}) = 1 \Rightarrow$ gcd (24, 9) =3

Step 11: b=2, j=4, N=5, M=5; i = i+2$\geq$ 1+2=3 and L=L+2 $\geq$ 1+2=3

$\Rightarrow$ gcd $(a_{(2+1)4}, a_{(2+2)4}) = 1 \Rightarrow$ gcd $(a_{34}, a_{44}) = 1 \Rightarrow$ gcd (14, 19) =1

$i < N = 3, 4 < 5 \geq$ swap $(a_{34}, a_{44}) \geq$ swap (14, 19)

$$E = \begin{bmatrix} 6 & 7 & 18 & 24 & 5 \\ 1 & 2 & 8 & 9 & 10 \\ 16 & 17 & 3 & 19 & 15 \\ 11 & 12 & 13 & 14 & 20 \\ 21 & 22 & 23 & 4 & 25 \end{bmatrix}$$

$L = L + 2 \geq 3 + 2 \geq 5$ and $i = i + 2 \geq 3 + 2 \geq 5$

Step 12: $b = 4$, $i = 5$, $j = 4$, $L = 5$, $N = 5$, $M = 5$; $L < N \geq$ 5< 5 and $j = j + 1$ $\geq$ 4+1 $\geq$5

Step 13: $b = 0$, $i = 1$, $j = 5$, $L = 1$, $N = 5$, $M = 5$

$\Rightarrow$ gcd $(a_{(0+1)5}, a_{(0+2)5-}) = 1 \Rightarrow$ gcd $(a_{15}, a_{25}) = 1 \Rightarrow$ gcd (5, 10) =1

$$\text{i<N = 1,2 < 5} \geq \text{swap } (a_{15}, a_{25}) \geq \text{swap (5, 10)}$$

$$E = \begin{bmatrix} 6 & 7 & 18 & 24 & 10 \\ 1 & 2 & 8 & 9 & 5 \\ 16 & 17 & 3 & 19 & 15 \\ 11 & 12 & 13 & 14 & 20 \\ 21 & 22 & 23 & 4 & 25 \end{bmatrix}$$

$$L = L + 2 \geq 1 + 2 \geq 3 \text{ and } i = i + 2 \geq 1 + 2 \geq 3$$

Step 14: $b = 2$, $i = 3$, $j = 5$, $L = 3$, $N = 5$, $M = 5$

$$\Rightarrow \text{ gcd } (a_{(2+1)5}, a_{(2+2)5-}) = 1 \Rightarrow \text{ gcd } (a_{35}, a_{45}) = 1 \Rightarrow \text{ gcd (15, 20) =5}$$

Step 15: $b = 4$, $j = 5$, $N = 5$, $M = 5$; $i = i + 2 \geq 3 + 2 = 5$ and $L = L + 2 \geq 3 + 2 = 5$

$$/E = \begin{bmatrix} 6 & 7 & 18 & 24 & 10 \\ 1 & 2 & 8 & 9 & 5 \\ 16 & 17 & 3 & 19 & 15 \\ 11 & 12 & 13 & 14 & 20 \\ 21 & 22 & 23 & 4 & 25 \end{bmatrix}.$$

4. Conclusion

Salsa20/4 is faster encryption because of the quarter round and focus only speed of encryption by column wise operations. The proposed method CBB21 phase 2 method has N round process; each round has to swapping the co-prime numbers by columns wise in the matrix. The comparison between proposed and existing method are as shown Table 2. The proposed method has provide good security because of co-prime number while compare to existing method.

References

[1] B. Pang, L. Lee, S. Vaithyanathan: *Thumbs up? Sentiment classification using machine learning techniques*, Pro. of the Con. on Emp. Met. in Nat. Lan. Pro., Philadelphia, 2002.

[2] 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.

[3] Z. Shao, L. Ding: *Related-Cipher Attack on Salsa20*, Fou. Inter. Conf. on Comp. and Inf. Sci., Chongqing, China, 2012.

[4] M. ALMAZROOIE, A. SAMSUDIN, M. M. SINGH: *Improving the Diffusion of the Stream Cipher Salsa20 by Employing a Chaotic Logistic Map*, J. of Infor. Proc. Sys., **11**(12) (2019), 1952–1955.

[5] S. FISCHER, W. MEIER, C. BERBAIN, J. BIASSE, M. J. B. ROBSHAW: *Non-Randomness in eSTREAM Candidates Salsa20 and TSC-4*, Ind. Lec. N. in Com. Sci., R. Barua and T. Lange, eds., Springer, Berlin, Heidelberg, 2006.

[6] 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.

[7] 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.

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