ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.9, 6725–6731
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.9.30 Spec. Issue on CAMM-2020

RB28 ALGORITHM FOR SECURING THE PREDICTED DATA

R. SHOBANA [1], S. LEELAVATHY[2], J. MEENA[3], R.S. SANGEETHA[4], AND SANTHOSH ANAND[5]

ABSTRACT. Today's world is data world because each and every people survive with data. The data produced from social media because everyone people used media. People's data is very important in the world. This data does not have good security so to overcome this issue we apply the proposed method. The proposed method has three steps; 1. Applying the commutative property of addition in matrix; 2. Applying the associative property of addition in matrix; and final step is multiply the secret key in the matrix. The proposed method provides good security while comparing with Salsa method.

1. INTRODUCTION

Today's world is data world because each and every people survive with data. The data produced from social media because everyone people used media. People's data is very important in the world. This data does not have good security so to overcome this issue we apply the Salsa method. This method has four round processes and each process also four round processes. This process changes the places of the data only. Salsa method provides less security; so the hackers easily hack the data. SRB18 algorithm has discuss about security of twitter analysed data [1]. SRB21phase I studied about prime number with secret key [2]. CBB21 Phase 2 discuss about co-prime numbers [3]. CBB22 algorithm studied about prime number and quadratic form [4]. RB20 method

[1] *corresponding author*

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

Key words and phrases. Commutative Property, Associative Property, RB28, Salsa, Encryption, Decryption.

used identify the prime number and perfect number [5]. RB21 method used to multiply the secret key and identify the perfect numbers [6]. They discuss about machine learning algorithm and showed which algorithm is good for prediction [7]. Author studied about movies reviews through Twitter data [8] To overcome this problem introduced the novel method RB28(Rajaprakash ans Bagath Basha) 28.

2. Methods

Commutative property of addition (CP)

This property must have same design matrix otherwise it cannot be add the matrix, it must be real numbers.

"For example, $A = B = B + A$." "**A=**a_{ij}**, B=**b_{ij}"

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} B = \begin{bmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{bmatrix}$$

$''CP = A + B = B + A$"

$$CP = \begin{bmatrix} a_{11}+b_{11} & a_{12}+b_{12} & a_{13}+b_{13} \\ a_{21}+b_{21} & a_{22}+b_{22} & a_{23}+b_{23} \\ a_{31}+b_{31} & a_{32}+b_{32} & a_{33}+b_{33} \end{bmatrix} = \begin{bmatrix} b_{11}+a_{11} & b_{12}+a_{12} & b_{13}+a_{13} \\ b_{21}+a_{21} & b_{22}+a_{22} & b_{23}+a_{23} \\ b_{31}+a_{31} & b_{32}+a_{32} & b_{33}+a_{33} \end{bmatrix}$$

Associative property of addition (AP)

This property also have same design and real numbers.

"For example, $A + (B + C) = (A + B) + C$ **A=**a_{ij}**, B=**b_{ij}**, C=**c_{ij}"

$$C = \begin{bmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{bmatrix}$$

$$AP = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} + \begin{bmatrix} b_{11}+c_{11} & b_{12}+c_{12} & b_{13}+c_{13} \\ b_{21}+c_{21} & b_{22}+c_{22} & b_{23}+c_{23} \\ b_{31}+c_{31} & b_{32}+c_{32} & b_{33}+c_{33} \end{bmatrix}$$

$$= \begin{bmatrix} a_{11}+b_{11} & a_{12}+b_{12} & a_{13}+b_{13} \\ a_{21}+b_{21} & a_{22}+b_{22} & a_{23}+b_{23} \\ a_{31}+b_{31} & a_{32}+b_{32} & a_{33}+b_{33} \end{bmatrix} + \begin{bmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{bmatrix}$$

Table 1 and Table 2 are encryption and decryption.

3. Encryption

A is a data analyzed matrix, B is a secret matrix [7].

"Equation (1)"

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

$$CP = \begin{bmatrix} 1+2 & 2+4 & 3+3 \\ 4+5 & 5+6 & 6+1 \\ 7+7 & 8+9 & 9+8 \end{bmatrix}, \quad CP = \begin{bmatrix} 3 & 6 & 6 \\ 9 & 11 & 7 \\ 14 & 17 & 17 \end{bmatrix}.$$

CP is an input (encrypted) matrix, B and C is s secret matrix.

"Equation (2)"

$$CP = \begin{bmatrix} 3 & 6 & 6 \\ 9 & 11 & 7 \\ 14 & 17 & 17 \end{bmatrix}, \quad B = \begin{bmatrix} 2 & 4 & 3 \\ 5 & 6 & 1 \\ 7 & 9 & 8 \end{bmatrix}, \quad C = \begin{bmatrix} 9 & 7 & 8 \\ 6 & 4 & 5 \\ 2 & 3 & 1 \end{bmatrix},$$

$$AP = \begin{bmatrix} 3+2 & 6+4 & 6+3 \\ 9+5 & 11+6 & 7+1 \\ 14+7 & 17+9 & 17+8 \end{bmatrix} + \begin{bmatrix} 9 & 7 & 8 \\ 6 & 4 & 5 \\ 2 & 3 & 1 \end{bmatrix}, \quad AP = \begin{bmatrix} 5 & 10 & 9 \\ 14 & 17 & 8 \\ 21 & 26 & 25 \end{bmatrix} + \begin{bmatrix} 9 & 7 & 8 \\ 6 & 4 & 5 \\ 2 & 3 & 1 \end{bmatrix},$$

$$AP = \begin{bmatrix} 5+9 & 10+7 & 9+8 \\ 14+6 & 17+4 & 8+5 \\ 21+2 & 26+3 & 25+1 \end{bmatrix}, \quad AP = \begin{bmatrix} 14 & 17 & 17 \\ 20 & 21 & 13 \\ 23 & 29 & 26 \end{bmatrix}.$$

AP is an input matrix; multiplies with secret key $S = 1/2$ and "Equation (3)".

"$SKM = AP * S$, where SKM is Secret Key Multiplication".

$$SKM = \begin{bmatrix} 14 & 17 & 17 \\ 20 & 21 & 13 \\ 23 & 29 & 26 \end{bmatrix} \cdot (1/2) = \begin{bmatrix} 7 & 17/2 & 17/2 \\ 10 & 21/2 & 13/2 \\ 23/2 & 29/2 & 13 \end{bmatrix}.$$

Finally, the all matrix should be closure matrix because of all matrixes could be same design, and the original matrix could be encrypted successfully.

4. Decryption

SKM is an input (encrypted) matrix; divide the decryption secret key $DS = 1/2$ **and "Equation (4)."** "$DM1 = SKM/DS$"

$$DM1 = \begin{bmatrix} 14 & 17 & 17 \\ 20 & 21 & 13 \\ 23 & 29 & 26 \end{bmatrix}$$

DM1 is input (decrypted) matrix, B and C is secret matrix and "Equation (5) and (6)".

$$DM1 = \begin{bmatrix} 14 & 17 & 17 \\ 20 & 21 & 13 \\ 23 & 29 & 26 \end{bmatrix} B = \begin{bmatrix} 2 & 4 & 3 \\ 5 & 6 & 1 \\ 7 & 9 & 8 \end{bmatrix} C = \begin{bmatrix} 9 & 7 & 8 \\ 6 & 4 & 5 \\ 2 & 3 & 1 \end{bmatrix}$$

$"DM2 = DM1 - C$, **where** $DM2$ **is decrypted matrix 2".**

$$DM2 = \begin{bmatrix} 14 & 17 & 17 \\ 20 & 21 & 13 \\ 23 & 29 & 26 \end{bmatrix} - \begin{bmatrix} 9 & 7 & 8 \\ 6 & 4 & 5 \\ 2 & 3 & 1 \end{bmatrix}, \quad DM2 = \begin{bmatrix} 5 & 10 & 9 \\ 14 & 17 & 8 \\ 21 & 26 & 25 \end{bmatrix},$$

$"DM3 = DM2 - B$, **where** $DM3$ **is decrypted matrix 3".**

$$DM3 = \begin{bmatrix} 5 & 10 & 9 \\ 14 & 17 & 8 \\ 21 & 26 & 25 \end{bmatrix} - \begin{bmatrix} 2 & 4 & 3 \\ 5 & 6 & 1 \\ 7 & 9 & 8 \end{bmatrix}, \quad DM3 = \begin{bmatrix} 3 & 6 & 6 \\ 9 & 11 & 7 \\ 14 & 17 & 17 \end{bmatrix}.$$

DM3 is input (decrypted) matrix and B is secret key matrix using "Equation (7)".

$"DM4 = DM3 - B$, **where** $DM4$ **is decrypted matrix 4".**

$$DM4 = \begin{bmatrix} 3 & 6 & 6 \\ 9 & 11 & 7 \\ 14 & 17 & 17 \end{bmatrix} - \begin{bmatrix} 2 & 4 & 3 \\ 5 & 6 & 1 \\ 7 & 9 & 8 \end{bmatrix}, \quad DM4 = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}.$$

TABLE 1. RB28 Encryption

STEPS	RB28 ENCRYPTION
1	Analyzed the prediction data from social media.
2	Convert the prediction data to matrix form.
3	Applying the commutative property (CP) of the matrix CP $CP = A + B = B + A$ **(1)**
4	Applying the associative property (AP) of the matrix AP $AP = A + (B + C) = (A + B) + C$ **(2)**
5	Multiply the secret key S with matrix AP.
6	SKM=AP*S **(3)** where SKM is Secret Key Matrix

TABLE 2. RB28 Decryption

STEPS	RB28 DECRYPTION
1	Get the input (encrypted) data matrix.
2	Divide the secret key DS in the matrix SKM. $DM1 = SKM/DS$ **4)** where DM1 is Decrypted Matrix 1
3	Minus the secret key matrixes C and B with the matrix DM1. $DM2 = DM1 - C$ **(5)** where DM2 is Decrypted Matrix 2 $DM3 = DM2 - B$ **(6)** where DM3 is Decrypted Matrix 3
4	Minus the secret key matrix B with the matrix DM3. $DM4 = DM3 - C$ **(7)** where DM4 is Decrypted Matrix 4

5. CONCLUSION

Today's world is data world because each and every people survive with data. The data produced from social media because everyone people used media. People's data is very important in the world. This data does not have good security so to overcome this issue we apply the proposed method. The proposed method has three steps; 1. Applying the commutative property of addition in matrix; 2. Applying the associative property of addition in matrix; and final step is multiply the secret key in the matrix.The RB28 method provide good security while compared with Salsa method. In the future, to add the prime factors operations of the data security.

References

[1] C. Bagath Basha, S. Rajaprakash: *Enhancing The Security Using SRB18 Method of Embedding Computing*, Microprocessors and Microsystems, **77** art.id 103125, (2020).

[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, S. Rajaprakash: *Applying The CBB21 Phase 2 Method For Securing Twitter Analysed Data*, Advances in Mathematics: Scientific Journal, **9**(3) (2020), 1085-1091.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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(DEEMED TO UNIVERSITY), PAIYANOOR, CHENNAI-603 104,TAMIL NADU, INDIA.

E-mail address: shobana@avit.ac.in

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

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

E-mail address: [4]sangeethasasthri98@gmail.com

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