BBRP22 based security technique for data security

C.Bagath Basha[1,4], S. Rajaprakash[2,5] and S.Sankar Ganesh[3,6]

[1]Department of Artificial Intelligence & Machine Learning, Kommuri Pratap Reddy Institute of Technology,Malkajgiri,Telangana, India
[2]Deparment of CSE, Aarupadai Veedu Institute of Technology, Vinayaka Mission's Research Foundation, Salem, Tamilnadu, India
[3]Department of ECE, P.S.R Engineering College, Sivakasi, Tamilnadu, India

[4]chan.bagath@gmail.com
[5]sankar2017vmu@gmail.com
[6]maheshwariselvam2606@gmail.com

Abstract. Nowadays data plays major role in the current internet world. People generate more data through online media. The generated data are not secured properly and can easily get hacked by the hackers. To overcome from this data security issue, we have planned to apply BBRP25 technique to secure the data. BBRP22 technique has 6 phases. To apply this technique, we must follow the given below steps:1. To track down the great key S; 2. To get the Z1 & Z2 values from indivisible numbers; 3. To view as the an and b values in lattice; to find the values with the assistance k; and trade x and y values. 4. To get the T-test values and match those numbers. 5. To find the n esteem by utilizing k. 6. Apply the n values in legitimate condition; and trade x and y values. The data will be fully secured by applying BBRP22 strategy while compared to ChaCha.

Keywords: BBRP22, encryption, ChaCha, security.

1. Introduction

Nowadays data plays major role in the current internet world. People generate more data through online media. The generated data are not secured properly and can easily get hacked by the hackers. To overcome from this data security issue, we have planned to apply BBRP22 technique to secure the data. ChaCha family has introduced the first ChaCha20/20. ChaCha20/4 mainly used for the reduced the encryption time has comparing with ChaCha20. ChaCha20 technique has mainly using for speed of the encryption but "not increasing the security of current data". To "beat this disadvantage of ChaCha20/4"; presented the novel strategy BBRP (Bagath Basha and RajaPrakash) 22. The time complexity has improved by using ChaCha [1]. They studied about the 3Vs [2] ChaCha technique has proposed by "Bernstein D. J." [15]. The attcakked the ChaCha using XOR method [3]. To create new idea using hash method [4]. To produced the novel attack for ChaCha [5] and Double A [6]. To created new calculation method for security [7]. SRB18 system is utilized to give security to data [8]. SRB21-1 and SRB21-2 technique are utilized to provide the data security [9],[10]. CBB21 [11], CBB22 [12], CBB20 [13], and RJB25 methods are used to provide security of data [14-17]. They proposed 7 phases for giving the security of the information [18].

2. Methodology

Nowadays data plays major role in the current internet world. People generate more data through online media. The generated data are not secured properly and can easily get hacked by the hackers. To overcome from this data security issue, we have planned to apply BBRP25 technique to secure the data. BBRP22 technique has 6 phases. To apply this technique, we must follow the given below steps: 1. To track down the great key S; 2. To get the Z1 & Z2 values from indivisible numbers; 3. To view as the an and b values in lattice; to find the values with the assistance k; and trade x and y values. 4. To get the T-test values and match those numbers. 5. To find the n esteem by utilizing k. 6. Apply the n values in legitimate condition; and trade x and y values.

3. BBRP22 encryption technique

1=> Fetch the input matrix (IP) form social media.

2=> To get the key from IP.

3=> Make it two parts using equation (1), (2), and (3).

4=> T-Test Formula =

$$\frac{(\overline{Z_1}-\overline{Z_2})}{\sqrt{\left(\frac{{A_1}^2}{N_1}\right)+\left(\frac{{A_2}^2}{N_2}\right)}} \tag{1}$$

5=> Get the values from using equation (1)

$$6\text{=>} \quad \overline{Z_1}=\sum\frac{Z_1}{N_1} \qquad \overline{Z_2}=\sum\frac{Z_2}{N_2} \tag{2}$$

$$7\text{=>} \quad A_1=\sqrt{\frac{\sum(Z_1-\overline{\overline{Z}_1})^2}{(N_1-1)}} \qquad A_2=\sqrt{\frac{\sum(Z_1-\overline{\overline{Z}_1})^2}{(N_1-1)}} \tag{3}$$

8=> Get pair values from left to right.

9=> Get n and k value.

$$10\text{=>} \; x_n+y_n=(x+y)\,(x_{n-1}-x_{n-2y}+x_{n-3y2}\ldots\ldots\ldots\ldots+x_{n-2x}-y_{n-1}) \tag{4}$$

4. Result and discussion

- The BBRP22 technique is developed from RJB25 technique [20].

$$\text{IP=}\begin{bmatrix} 301/3 & 302/3 & 303/3 & 304/3 & 305/3 \\ 306/3 & 307/3 & 308/3 & 309/3 & 310/3 \\ 311/3 & 312/3 & 313/3 & 314/3 & 315/3 \\ 316/3 & 317/3 & 318/3 & 319/3 & 320/3 \\ 321/3 & 322/3 & 323/3 & 324/3 & 325/3 \end{bmatrix}$$

Where IP (Input of the matrix).

- Prime Numbers – 1, 3, 5, 7, 11, 13, 17, 19, 23
    - X_1= 3, 5, 7, 11
    - X_2 = 13, 17, 19, 23

Table 1. Z1 and Z2 values.

$\mathbf{Z_1}$	$(Z_1-\overline{Z}_1)$	$(\boldsymbol{Z_1}-\overline{\boldsymbol{Z}}_1)^2$	$\mathbf{Z_2}$	$(\boldsymbol{Z_2}-\overline{\boldsymbol{Z}}_2)$	$(\boldsymbol{Z_2}-\overline{\boldsymbol{Z}}_2)^2$
3	-3.5	12.25	13	-5	25
5	-1.5	2.25	17	-1	1

Table 1. (continued).

7	0.5	0.25	19	1	1
11	4.5	20.25	23	5	25
$\sum(X_1-\overline{X}_1)^2$		35	$\sum(X_2-\overline{X}_2)^2$		52

- **<u>Using Equation (2) and (7) and Table 1</u>**
  - $\overline{Z}_1$=6.5
  - $\overline{Z}_2$=18
- **<u>Using Equation (3) and (6)</u>**
- $Z_1=\sqrt{(35/(4-1))}Z_2=\sqrt{(52/(4-1))}$
- $Z_1=\sqrt{(35/3)}$ $Z_2=\sqrt{(52/(3))}$
- $S_1=11.66$ $S_2=17.33$
- **<u>Using Equation (1) and (8)</u>**
- TTF = $(6.5-18)/\sqrt{((11.66^2/4)+(17.33^2/4))}$
- TTF = $11.5/\sqrt{109.06}$

<u>Step 1: (1,1)</u>

$$\text{TTE}=\begin{bmatrix} 301/3 & 302/3 & 303/3 & 304/3 & 305/3 \\ 306/3 & 307/3 & 308/3 & 309/3 & 310/3 \\ 311/3 & 312/3 & 313/3 & 314/3 & 315/3 \\ 316/3 & 317/3 & 318/3 & 319/3 & 320/3 \\ 321/3 & 322/3 & 323/3 & 324/3 & 325/3 \end{bmatrix}$$

Where TTE is T-Test Encryption

<u>Step 2: (5,1)</u>

$$\text{TTE}=\begin{bmatrix} 301/3 & 306/3 & 303/3 & 304/3 & 305/3 \\ 302/3 & 307/3 & 308/3 & 309/3 & 310/3 \\ 311/3 & 312/3 & 313/3 & 314/3 & 315/3 \\ 316/3 & 317/3 & 318/3 & 319/3 & 320/3 \\ 321/3 & 322/3 & 323/3 & 324/3 & 325/3 \end{bmatrix}$$

<u>Step 3: (0,9)</u>

$$\text{TTE}=\begin{bmatrix} 310/3 & 306/3 & 303/3 & 304/3 & 305/3 \\ 302/3 & 307/3 & 308/3 & 309/3 & 301/3 \\ 311/3 & 312/3 & 313/3 & 314/3 & 315/3 \\ 316/3 & 317/3 & 318/3 & 319/3 & 320/3 \\ 321/3 & 322/3 & 323/3 & 324/3 & 325/3 \end{bmatrix}$$

<u>Step 4: (0,6)</u>

$$\text{TTE}=\begin{bmatrix} 307/3 & 306/3 & 303/3 & 304/3 & 305/3 \\ 302/3 & 310/3 & 308/3 & 309/3 & 301/3 \\ 311/3 & 312/3 & 313/3 & 314/3 & 315/3 \\ 316/3 & 317/3 & 318/3 & 319/3 & 320/3 \\ 321/3 & 322/3 & 323/3 & 324/3 & 325/3 \end{bmatrix}$$

- To find the n value; a=2,b=3, k=2,n=5, **n is odd number**
- **<u>Using Equation (4) and (5)</u>**

- $x^2+y^3= (2+3)(2^{5-1}-2^{5-2}3+2^{5-3}3^2-2^{5-4}3^3-2^{5-5}3^4+3^{5-4}2-3^{5-3}2+3^{5-2}2-3^{5-1})$
- $x^2+y^3= (5)\ (2^4-2^3 3+2^2 9-2^1 27-2^0 81+3^1 2-3^2 2+3^3 2-3^4)$
- $x^2+y^3= (5)(16-24+36-54-81+6-18+54-81)$
- $x^2+y^3= (5)(-146)$
- $x^2+y^3= (5,1), (4,6)$

Step 5: (5,1)

$$\text{TTOE}=\begin{bmatrix} 307/3 & 302/3 & 303/3 & 304/3 & 305/3 \\ 306/3 & 310/3 & 308/3 & 309/3 & 301/3 \\ 311/3 & 312/3 & 313/3 & 314/3 & 315/3 \\ 316/3 & 317/3 & 318/3 & 319/3 & 320/3 \\ 321/3 & 322/3 & 323/3 & 324/3 & 325/3 \end{bmatrix}$$

Where TTOE is T-Test Odd Encryption

Step 6: (4, 6)

$$\text{TTOE}=\begin{bmatrix} 307/3 & 302/3 & 303/3 & 304/3 & 310/3 \\ 306/3 & 305/3 & 308/3 & 309/3 & 301/3 \\ 311/3 & 312/3 & 313/3 & 314/3 & 315/3 \\ 316/3 & 317/3 & 318/3 & 319/3 & 320/3 \\ 321/3 & 322/3 & 323/3 & 324/3 & 325/3 \end{bmatrix}$$

Decryption

- Pair the odd value from right left (6, 4) and (1, 5) and swap it those numbers.

Step 1: (6, 4)

$$\text{TTOD}=\begin{bmatrix} 307/3 & 302/3 & 303/3 & 304/3 & 305/3 \\ 306/3 & 310/3 & 308/3 & 309/3 & 301/3 \\ 311/3 & 312/3 & 313/3 & 314/3 & 315/3 \\ 316/3 & 317/3 & 318/3 & 319/3 & 320/3 \\ 321/3 & 322/3 & 323/3 & 324/3 & 325/3 \end{bmatrix}$$

Where TTOD is T-Test Odd Decryption

Step 2: (1, 5)

$$\text{TTE}=\begin{bmatrix} 307/3 & 306/3 & 303/3 & 304/3 & 305/3 \\ 302/3 & 310/3 & 308/3 & 309/3 & 301/3 \\ 311/3 & 312/3 & 313/3 & 314/3 & 315/3 \\ 316/3 & 317/3 & 318/3 & 319/3 & 320/3 \\ 321/3 & 322/3 & 323/3 & 324/3 & 325/3 \end{bmatrix}$$

- Pair “the T-test value from right to left (6,0), (9,0), (1,5), and (1,1) and swap it those numbers”.

Step 3: (6,0)

$$\text{TTD}=\begin{bmatrix} 310/3 & 306/3 & 303/3 & 304/3 & 305/3 \\ 302/3 & 307/3 & 308/3 & 309/3 & 301/3 \\ 311/3 & 312/3 & 313/3 & 314/3 & 315/3 \\ 316/3 & 317/3 & 318/3 & 319/3 & 320/3 \\ 321/3 & 322/3 & 323/3 & 324/3 & 325/3 \end{bmatrix}$$

Where TTE is T-Test Decryption

Step 4: (9,0)

$$\text{TTD=}\begin{bmatrix} 301/3 & 306/3 & 303/3 & 304/3 & 305/3 \\ 302/3 & 307/3 & 308/3 & 309/3 & 310/3 \\ 311/3 & 312/3 & 313/3 & 314/3 & 315/3 \\ 316/3 & 317/3 & 318/3 & 319/3 & 320/3 \\ 321/3 & 322/3 & 323/3 & 324/3 & 325/3 \end{bmatrix}$$

Step 5: (1,5)

$$\text{TTD=}\begin{bmatrix} 301/3 & 302/3 & 303/3 & 304/3 & 305/3 \\ 306/3 & 307/3 & 308/3 & 309/3 & 310/3 \\ 311/3 & 312/3 & 313/3 & 314/3 & 315/3 \\ 316/3 & 317/3 & 318/3 & 319/3 & 320/3 \\ 321/3 & 322/3 & 323/3 & 324/3 & 325/3 \end{bmatrix}$$

Step 6: (1,1)

$$\text{TTD=}\begin{bmatrix} 301/3 & 302/3 & 303/3 & 304/3 & 305/3 \\ 306/3 & 307/3 & 308/3 & 309/3 & 310/3 \\ 311/3 & 312/3 & 313/3 & 314/3 & 315/3 \\ 316/3 & 317/3 & 318/3 & 319/3 & 320/3 \\ 321/3 & 322/3 & 323/3 & 324/3 & 325/3 \end{bmatrix}$$

The proposed algorithm BBRP22 compare the performance with existing method “ChaCha”. The existing method is to do the process for move all diagonal values into the first column. The three by three matrix has (24, 76, 312, 812, 1531, 6580) bytes => (6x6, 10x10, 15x15, 20x20, 40x40) matrix as shown in the Table 2.

Table 2. KRB22 encryption performance.

File Size	*ChaCha*	*BBRP22*
Two-Four	“1.69”	5.115
Seven-Six	“1.29”	5.742
Three-One-Two	“2.73”	8.994
Eight-Two-Two	“2.64”	11.119
One-Five-Three-One	“3.4”	10.939
Six-Five-Eight Zero	“2.27”	12.291

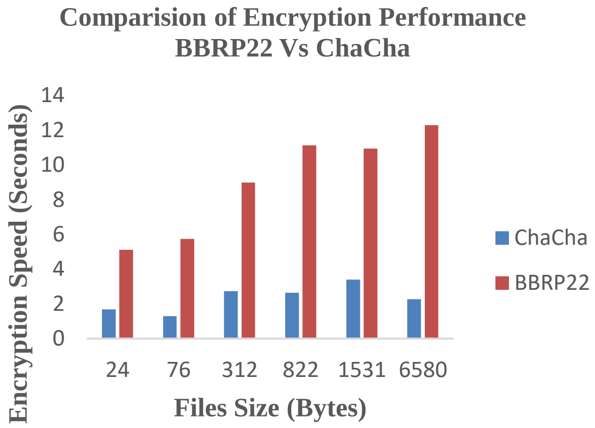

Figure 1. Encryption performance.

From Figure 1, the encryption execution assessment of the proposed calculation BBRP22 encryption execution contrasted and "ChaCha". "ChaCha" idea is the all askew qualities move to the first segment. The BBRP22 procedure has thought about the encryption speed in a moment or two. The encryption performance of the speed 5.115 (s), 5.742 (s), 8.994 (s), 11.119 (s), 10.939 (s) and 12.291 (s) for the" BBRP22. The BBRP22 gives more security of the information; when contrasted with existing procedures.

5. Conclusion

Now the world is fully activated with data alone. This data is produced by using online media; this data is unhindered data; this data does not have incredible security. To beat this issue, we will apply the ChaCha strategy. This method will effectively hack the information from the computer programmers. BBRP22 technique has 6 phases. To apply this technique, we must follow the given below steps: 1. To track down the great key S; 2. To get the Z1 & Z2 values from indivisible numbers; 3. To view as the an and b values in lattice; to find the values with the assistance k; and trade x and y values. 4. To get the T-test values and match those numbers. 5. To find the n esteem by utilizing k. 6. Apply the n values in legitimate condition; and trade x and y values. Hence, BBRP22 technique provides great security while comparing to ChaCha.

References

[1] Fischer S, Meier W, Berbain C, Biasse J F and Robshaw M J B, “Non-Randomness in eSTREAM Candidates Salsa20 and TSC-4”, Indocrypt; LNCS, Springer-Verlag, 2006, pp. 2-16.

[2] Choudhuri A K and Maitra S, “Significantly Improved Multi-bit Differentials for Reduced Round Salsa and ChaCha”, IACR Transactions on Symmetric Cryptology, 2016, pp. 261-287.

[3] Laney D, “3D data management: Controlling data volume, velocity, and variety”, Application Delivery Strategies, META Group, 2001.

[4] Bernstein D J “ChaCha, a variant of Salsa20”, Workshop Record of SASC, 2008, pp. 1-6.

[5] Dilip Kumar S V, Sikhar Patranabis, Jakub Breier, Debdeep Mukhopadhyay, Shivam Bhasin, Anupam Chattopadhyay and Anubhab Baksi, “A Practical Fault Attack on ARX-like Cipherwith a Case Study on ChaCha20”, Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), 2017, pp. 33 40.

[6] Arun Babu P and Jithin Jose Thomas, “Freestyle, a randomized version of ChaCha for resisting offline brute-force and dictionary attacks”, Journal of Information Security and Applications”, 2019, arti. 102396.

[7] Alexandre Adomnicai, Jacques Fournier J A and Laurent Masson, “Bricklayer Attack: A Side-Channel Analysis on the ChaCha Quarter Round”, Progress in Cryptology – INDOCRYPT, Lecture Notes in Computer Science, Springer, 2017, vol 10698, pp. 65 84.

[8] Bagath Basha C and Rajapraksh, “Enhancing The Security Using SRB18 Method of Embedding Computing”, Microprocessor and Microsystems, 2020.

[9] Bagath Basha C and Rajaprakash S, “Securing Twitter Data Using Phase I Methodology”, International Journal of Scientific & Technology Research”, 2019, pp. 1952-1955

[10] Bagath Basha C and Rajaprakash S, “Applying the SRB21 Phase II Methodology for Securing Twitter Analyzed Data”, AIP Conference Proceedings of the International Confererence on Mechanical Electronics and Computer Engineering, 2020.

[11] Bagath Basha C and Rajaprakash S, “Applying The CBB21 Phase 2 Method For Securing Twitter Analyzed Data”, Advances in Mathematics: Scientific Journal”, 2020, pp. 1085-1091.

[12] Bagath Basha C, Rajaprakash S, Harish V V A, Krishna M S, and Prabhas K, “Securing Twitter Analysed Data Using CBB22 Algorithm”, Advances in Mathematics: Scientific Journal, 2020, pp. 1093-1100.

[13] Bagath Basha C, Rajaprakash S, Muthuselvan S, Saisatishsunder P, and Alekhya Rani SVL, “Applying the CBB20 Algorithm for Twitter Analyzed Data”, Journa. of Physic.: Conference Series - First International Conference on Advances in Physical Sciences and Materials, Coimbatore, Tamil Nadu, India, 2020.

[14] Rajaprakash S, Bagath Basha C, Muthuselvan S, Jaisankar N and Ravi Pratap Singh, “RBJ25 Cryptography Algorithm For Securing Big Data”, Journa. of Physic.: Conference Series - First International Conference on Advances in Physical Sciences and Materials, Coimbatore, Tamil Nadu, India, 2020.

[15] Bagath Basha C and Somasundaram K, “A Comparative Study of Twitter Sentiment Analysis Using Machine Learning Algorithms in Big Data”, International Journal of Recent Technology and Engineering, 2019, pp. 591-599.

[16] Bhalaji N, “Efficient and secure data utilization in mobile edge computing by data replication”, Journal of ISMAC 2, 2020, pp. 1-12.

[17] Sungheetha B, Akey, and Rajesh Sharma, “Novel Shared Key Transfer Protocol for Secure Data Transmission in Distributed Wireless Networks”, Journal of trends in Computer Science and Smart technology (TCSST) 2, 2020, pp. 98-108.

[18] C. Bagath Basha, S. Rajaprakash, R. Meenakumari, M. Suresh, P. Hitesh, T. Kokilavani, and R. Ashok Kumar “A novel security algorithm RPBB31 for securing the social media analyzed data using machine learning algorithms” (Wireless Personal Communications) https://doi.org/10.21203/rs.3.rs-1860348/v1