

SC-JBR22 based Method to Secure the Analyzed Data

Dr. R. Jaichandran¹, Dr. S. Muthuselvan², Alok Shree³, Shreya N Gowda⁴ and Thirpula Murali Krishna⁵

¹⁻⁵Department of Computer Science and Engineering, Aarupadai Veedu Institute of Technology, Vinayaka Mission's Research Foundation, Chennai, Tamil Nadu, India

Email: rjaichandran@gmail.com, muthuselvan@avit.ac.in, shree.alok705000@gmail.com, shree.alok705000@gmail.com, muralikrishn124426@gmail.com

Abstract—The current global is very important is internet for each and every people for every work mandatory. With the help of internet every people used many social media, because social media is mandatory for people life. The people decided to do the any new work before analyzed that work in “social media”. This analyzed “data not have good security” in the people systems. In this paper, proposed the new method SC-JBR22-01. This method has 3 stages; 1st stage is to convert the matrix format from analyzed data; 2nd stage is apply the Salsa operations in the matrix; and 3rd stage is apply the ChaCha operations in the matrix. The new SC-JBR22-01 method has provide the good security and performance while compared to ChaCha method.

Index Terms— ChaCha, Encryption, Security, and SC-JBR22.

I. INTRODUCTION

A significant increase in the amount of information being stored, sent, and managed has resulted from the widespread use of the Internet, virtual entertainment, and other applications. for capacity, “transmission” and to handle by the individual and “industry”, in particular. Therefore, new cryptographic computations ought to be made in order to investigate the various “symmetric and asymmetric encryption” decoding methodologies. The productivity of conventional AES calculations has been compared to several chacha [2] calculation types, and it has been examined how much opposition was given and how much time occupied by these computations.

A four layer approach known as SC-JBR22-01 (named after the SalsaChaCha creators JaichandranBagathRajaprakash-01) has been proposed to address the “upcoming new challenges” and to provide compelling insurance to vast amounts of dissected information from “various sources such as the Internet, bank,” interpersonal organisation, PDA, and private facts. with improved defences against many conventional attacks and confirmation. The suggested method is tested against a number of known “cryptographic techniques”

II. RELATED WORK

This creator looks at the “ChaCha family,” which discusses the ineffective assault of more turns [1]. They developed a cunning method called Freestyle that made use of a few code texts and offered a revolutionary idea known as hash-based halting conditions and key speculation [2]. To distinguish releases linked to attacks, AlexandreAdomnicai et al. “suggested chacha side chanel” investigation [3]. In order to attack the “ChaCha and Salsa20” for lacking infusion, “Kazuhide Fukushima et al” are introduced. They create a “key” and “count the blocks” [4]. They discussed “Abdullah Issa et al.”’s A [5]. An expansion turn XOR (ARX) is examined by BodhisatwaMazumdar et al. [6].

A thorough examination of the "Double A" hash computation has been conducted [7]. "BodhisatwaMazumdar et al." examined the power evaluation assault and associations power assessment before proposing Salsa20's flaw. The best investigation attack is "Power" attack [8]. Conrad Watt et al. discovered that "secure" calculations may be carried out quickly [9]. Probabilistic nonpartisan vectors (PNV), which were proposed by "Z. Shi et al.," are an idea of "probabilistic" impartial parts. On "Chacha20 and ChaCha [10]" weakened rounds, it is utilised to discover and "refine" significant recovery attacks.

The SRB21 technique was introduced by "Somasundaram, Rajaprakash, and Bagahbasha21" and it focuses on the indivisible amounts of the mystery key [11]. How social media data was analysed [12]. The author contrasts CBB21[13], CBB20[14], and SRB21-P2[15] with the conventional approach. How to use the SRB18 method to determine runtime efficiency[16]. The RBJ25 approach [17], RB20 method [18], and CBB22 method [19] are contrasted with the AES and ChaCha by the author. How to compare several algorithms to the data from movies [20]. How to store and process the vast amounts of data according to RBJ20 [21] and RPBB31[22].

III. METHODOLOGY

The forecasting analyzed data is used to apply the novel method SC-JBR-22-01 has 3 stages. The first stage has convert the "matrix format". The second stage is apply the Salsa operations. The third stage is apply the ChaCha operations.

Algorithm

- To get the input data from the analyzed matrix data.
- To apply the Salsa operations using Equation(1) in the given matrix S.

$$\begin{aligned} S_{ij} &= S_{ij}, \\ S_{(k+1)j} &= S_{(k+j)j}, \\ \text{if } i > N &\text{ Then} \\ i &= K - N \\ \text{where } k &= 0, 1, 2, \dots N. \quad j = 1, 2, 3 \dots N. \\ N &\text{ is the order of the matrix.} \end{aligned} \quad \text{Equation (1)}$$

- To apply the ChaCha Operations in the converted S matrix.

IV. RESULT AND DISCUSSION

$$\text{IPM} = \begin{bmatrix} TN1 & DL2 & MH3 & PU4 \\ KL5 & AN6 & TE7 & GO8 \\ KA9 & AC10 & OR11 & PY12 \\ GU13 & HP14 & KM15 & AS16 \end{bmatrix}$$

Where IPM is input data matrix

Using Equation (1)

- Process 1: First diagonal value move to the first row in first column.

$$S = \begin{bmatrix} TN1 & DL2 & MH3 & PU4 \\ KL5 & AN6 & TE7 & GO8 \\ KA9 & AC10 & OR11 & PY12 \\ GU13 & HP14 & KM15 & AS16 \end{bmatrix}$$

where S is Salsa matrix

- Process 2: Second diagonal value move to the first row in second column.

$$S = \begin{bmatrix} TN1 & AN6 & MH3 & PU4 \\ KL5 & AC10 & TE7 & GO8 \\ KA9 & HP14 & OR11 & PY12 \\ GU13 & DL2 & KM15 & AS16 \end{bmatrix}$$

- Process 3: Third diagonal value move to the first row in third column.

$$S = \begin{bmatrix} TN1 & AN6 & OR11 & PU4 \\ KL5 & AC10 & KM15 & GO8 \\ KA9 & HP14 & MH3 & PY12 \\ GU13 & DL2 & TE7 & AS16 \end{bmatrix}$$

- Process 4: Fourth diagonal value move to the first row in fourth column.

$$S = \begin{bmatrix} TN1 & AN6 & OR11 & AS16 \\ KL5 & AC10 & KM15 & PU4 \\ KA9 & HP14 & MH3 & GO8 \\ GU13 & DL2 & TE7 & PY12 \end{bmatrix}$$

- Now, apply to the ChaCha operations in the converted S matrix.
- Process 5: First diagonal value move to the first column in the first row.

$$C = \begin{bmatrix} TN1 & AN6 & OR11 & AS16 \\ KL5 & AC10 & KM15 & PU4 \\ KA9 & HP14 & MH3 & GO8 \\ GU13 & DL2 & TE7 & PY12 \end{bmatrix}$$

where C is ChaCha matrix

- Process 6: Second diagonal value move to the first column in the Second row.

$$C = \begin{bmatrix} TN1 & AN6 & OR11 & AS16 \\ AC10 & KM15 & PU4 & KL5 \\ KA9 & HP14 & MH3 & GO8 \\ GU13 & DL2 & TE7 & PY12 \end{bmatrix}$$

- Process 7: Third diagonal value move to the first column in the third row.

$$C = \begin{bmatrix} TN1 & AN6 & OR11 & AS16 \\ AC10 & KM15 & PU4 & KL5 \\ MH3 & GO8 & KA9 & HP14 \\ GU13 & DL2 & TE7 & PY12 \end{bmatrix}$$

- Process 8: Fourth diagonal value move to the first column in the fourth row.

$$C = \begin{bmatrix} TN1 & AN6 & OR11 & AS16 \\ AC10 & KM15 & PU4 & KL5 \\ MH3 & GO8 & KA9 & HP14 \\ PY12 & GU13 & DL2 & TE7 \end{bmatrix}$$

The proposed algorithm SC-JBR22-01 compares ChaCha's encryption performance. All diagonal values migrate to the first column in the ChaCha concept. According to Table 1, The 3x3=>24 bytes , 6x6=>76 bytes, 10x10=> 312 bytes, 15x15=> 812 bytes, 20x20=> 1531 bytes, 40x40=> 6580 bytes.

TABLE I. SC-JBR22-01 ENCRYPTION PERFORMANCE

File Size	ChaCha	SC-JBR22-01
24	1.69	2.6
76	1.29	2.8
312	2.73	4.2
822	2.64	4.6
1531	3.4	6.2
6580	2.27	6.7

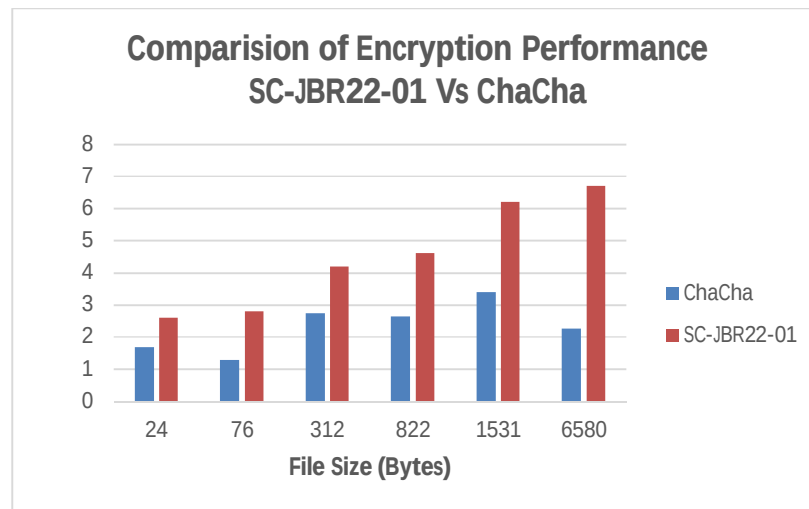


Figure 1. Performance comparison for SC-JBR22-01 and ChaCha

The SC-JBR22-01 method has “compared the encryption speed” in seconds based on Figure 1. The SC-JBR22-encryption 01's performance was 2.6 (s), 2.8 (s), 4.2 (s), 4.6 (s), 6.2 (s), and 6.7 (s). When compared to current methods, the SC-JBR22-01 offers more data protection.

IV. CONCLUSION

In today's world, the internet plays a crucial role in people's daily lives. Every person's work requires access to the internet, particularly several social media sites. Before beginning any new company task, the individuals desire to undertake a "social media" analysis of that work. This analysis found that the systems used by users lacked adequate data security. We suggested the new approach SC-JBR22-01 to address this security problem. This method consists of three stages: the first stage involves converting studied data into a matrix format; the second stage involves applying Salsa operations to the matrix; and the third stage involves applying ChaCha operations to the matrix. Comparing the new SC-JBR22-01 approach to the "ChaCha" method, it offers better security and performance.

REFERENCES

- [1] Dilip Kumar, S. V., SikharPatranabis, JakubBreier, DebdeepMukhopadhyay, ShivamBhasin, AnupamChattopadhyay, AnubhabBaksi, “A Practical Fault Attack on ARX-like Ciphers with a Case Study on ChaCha20”, Works. On Fault Diagnosis and Tolerance in Cryptography, 33-40, 2017.

- [2] ArunBabu, P., Jithin Jose Thomas, "Freestyle, a randomized version of ChaCha for resisting offline brute-force and dictionary attacks", IEEE Transaction on Information Forensics and Security, 2018.
- [3] Alexandre Adomnicai, Jacques J. A. Fournier, Laurent Masson, "Bricklayer Attack: A Side-Channel Analysis on the ChaCha Quarter Round", Lecture Notes in Computer Science, Springer, 65-84.
- [4] Kazuhide Fukushima, RuiXu, ShinsakuKiyomoto, Naofumi Homma, " Fault Injection Attack on Salsa20 and ChaCha and a Lightweight Countermeasure" IEEE Trustcom/BigDataSE/ICSS, 1032-1037, (2017).
- [5] Abdullah Issa, Mohammad A. Al-Ahmad, Abdullah Al-Saleh, " Double-A – A Salsa20 like the Design", In: 4th International Conference on Advanced Computer Science Applications and Technologies, IEEE, 18-23, 2015.
- [6] Bodhisatwa Mazumdar, Sk. Subidh Ali, OzgurSinanoglu, "A Compact Implementation of Salsa20 and Its Power Analysis Vulnerabilities", ACM Transaction on Design Automation of Electronic Systems, 22, 11:1-11:26.
- [7] Abdullah Al-Saleh, Mohammed Al-Ahmmad, Abdullah Issa, Adel Al-Foudery, "DOUBLE-A – A Salsa20 like the Security", In: 4th International Conference on Advanced Computer Science Applications and Technologies, IEEE, 24-29, 2015.
- [8] Bodhisatwa Mazumdar, Sk Subidh Ali, OzgurSinanoglu, "Power Analysis Attacks on ARX: An Application to Salsa20", In: 21st International On-Line Testing Symposium, IEEE, 40-43, 2015.
- [9] Conrad Watt, John Renner, Natalie Popescu, SunjayCauligi, Deian Stefan, "CT-Wasm: Type-Driven Secure Cryptography for theWeb Ecosystem", ACM Programming Language 3, POPL, 77:1-77:29, 2019.
- [10] Shi, Z., Zhang, B., Feng, D., Wu, W., " Improved Key Recovery Attacks on Reduced-Round Salsa20 and ChaCha", Springer, ICISC 2012, LNCS 7839, 337-351, 2012.
- [11] Bagath Basha, C., Rajaprakash, S., "Securing Twitter Data Using SRB21 Phase I Methodology", International Journal of Scientific & Technology Research, 8, 1952 – 1955.
- [12] Bagath Basha, C., Somasundaram, K., "A Comparative Study of Twitter Sentiment Analysis Using Machine Learning Algorithms in Big Data", International Journal of Recent Technology and Engineering, 8, 591-599, 2019.
- [13] Bagath Basha, C., Rajaprakash, S., "Applying The CBB21 Phase 2 Method For Securing Twitter Analyzed Data", Advances in Mathematics: Scientific Journal, 1085-1091, 2020.
- [14] Bagath Basha, C., Rajaprakash, S., Muthuselvan, P., Saisatishsunder, Alekhyia Rani, SVL, "Applying the CBB20 Algorithm for Twitter Analyzed Data", In: First International Conference on Advances in Physical Sciences and Materials, Coimbatore, Tamil Nadu, India, 2020.
- [15] Bagath Basha, C., Rajaprakash, S., "Applying the SRB21 Phase II Methodology for Securing Twitter Analyzed Data", In: International Conference on Mechanical Electronics and Computer Engineering, 2020.
- [16] Bagath Basha, C., Rajaprakash, S., "Enhancing The Security Using SRB18 Method of Embedding Computing". Microprocessor and Microsystems, 2020.
- [17] Rajaprakash, S., Bagath Basha, C., Muthuselvan, S., Jaisankar, N., Ravi Pratap Singh, "RBJ25 Cryptography Algorithm For Securing Big Data", In: First International Conference on Advances in Physical Sciences and Materials, Coimbatore, Tamil Nadu, India, 2020.
- [18] Karthik, K., Bagath Basha, C., Bhaswanth Thilak, U., Sai Kiran, T., Raj J., "Securing Social Media Analyzed Data Using RB20 Method", Advances in Mathematics: Scientific Journal, 3, 2020.
- [19] Bagath Basha, C., Rajaprakash, S., Harish, V.V.A., Krishna, M.S., Prabhas, K., "Securing Twitter Analysed Data Using CBB22 Algorithm". Advances in Mathematics: Scientific Journal, 1093-1100, 2020.
- [20] Jaichandran, R., Bagath Basha, C., Shunmuganathan, K. L., Rajaprakash, S., Kanagasuba Raja, S., "Sentiment Analysis of Movies on Social Media using R Studio", International Journal of Engineering and Advanced Technology, 8, 2019.
- [21] Rajaprakash, S., Jaisankar, N., Bagath Basha, C., Jayan, A., Sebastian, G., "RBJ20 Cryptography Algorithm for Securing Big Data Communication using Wireless Networks", WorldS4, Springer, LNNS Book Series (ISSN: 237 – 3370, London, 499-507, 2022.
- [22] 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>.