VIII. Analysis of SAFER S-Box Algorithm

This algorithm is covering both sides which an algorithm requires for IoT devices, it is lightweight and also more secure. This encryption algorithm involves SAFFER with S-Box. SAFER is the most outstanding algorithm for low power devices and Bluetooth devices [10]. So that's why we chose SAFER on the confusion layer, which has simple and fast operations. On the diffusion layer, Musaria K. et al .in [10] are using a 16x16 matrix which makes this system complex because for decryption we have to find t he i nverse o f the matrix which is not a suitable option for low computational devices. XIAXIA GUO et al in [14] are also using SAFER for the confusion layer but at the diffusion layer, FNTT [13] is used which also requires very computation. So we need some simple method for the diffusion layer and we chose S-Boxes for that. But like DES and other algorithms, we are not using new S-box for each round which consumes more memory to store S-Boxes. Vijay Dahiphale et al .in [12] are just using one S-Box which is also not a good option because it compromises the security of the encryption. As if we use only one S-Box its very easy for an attacker to compromise your security because he only needs one S-Box to encrypt the whole encrypted text into plain text and if we use a new S-Box for each round we need more number of S-Boxes which is not good for low memory devices, so that's why we chose 4 S-Boxes. They require less memory as compared to use a new S-Box for each round like we were doing in DES and it's also good that we are using multiple S-Boxes not relying on a single S-Box. As I already mention that if you follow this encryption algorithm the attacker needs S-Boxes and also the sequence S-Boxes because they don't know at which position which S-Box is used. Low cost and the lightweight algorithm is presented bySeddiq Q. Abd Al-Rahman et al in [18] which is involved the bitwise XOR and MixCoLayer type of complex functions which are not much suitable. After understanding these issues we used 4 S-Boxes which are half than the number of rounds and we are not changing S-Box for each round. We using all the boxes for each round by just manipulation its positions. By using fewer S-Boxes, we are saving device memory and required less storage capacity for S-Boxes and by manipulating the positions of S-Boxes we can achieve high security at the diffusion layer. This is the main advantage of our scheme on other schemes that were previously presented. A comparison with the already proposed algorithm is also presented in Table I.

TABLE I. Comparison with already proposed Algorithms

Algorithm	Complexity	Time	Cost	Security
ANU-II [12]	Less	Less	Low	Low
XTEA with AES [18]	Less	High	High	High
SAFER+ 128-Key [10]	High	High	High	High
SAFER-Fermat [14]	Less	High	High	High
SAFER With S-BOX (Proposed)	Less	Less	Less	High

IX. Conclusion

This paper presents an improved form of the SAFER++ encryption algorithm by using the S-Boxes. which involved less complex mathematical implementations and make this encryption algorithm more simple and secure. We design an encryption algorithm that gives us more security, less cost and less complex. This scheme is developed by keeping in mind the three key parameters of IoT devices. Encryption has divided into two-part confusion and diffusion layer, at confusion layer SAFER++ block cipher has used for encryption, which has simple and very less complex operations which a device can handle very easily.At the diffusion layer, we have used less number of S-Boxes and manipulate the positions so that each byte is processed with the help of different Box at different round. This scheme requires low memory to store S-Boxes because of fewer S-Boxes and we are not using different S-Box for each round of encryption, in this way we are saving our resources of IoT devices. This encryption algorithm is suitable for low memory devices. As we know IoT devices have low memory and cannot handle complex computations. So, this encryption technique fulfills all the requirements for the encryption of data for IoT devices.

References

[1] G. T. anthoshš Krishna B V, "Optimum information transmission through a channel with unknown parameters," pp. 107–111, 2017.

[2] P. P. Marioš Frustaci, "Evaluating critical security issues of the iot world: Present and future challenges," *IEEE INTERNET OF THINGS JOURNAL*, vol. 5, pp. 2483–24 958, 2018.

[3] D. S. S. s. Sridharš, "Intelligent security framework for iot devices," pp. 1–5, 2017.

[4] S. Y. J. H. P. s. Singhš, P. K. Sharma, "Advanced lightweight encryption algorithms for iot devices: Survey challenges and solutions," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–18, 2017.

[5] N. M. R. K. J. Patelš, "Secure end to end data aggregation using public key encryption in wireless sensor network," *Int. J. Comput. Appl.*, vol. 122.

[6] williamš, "Cryptography and network security principle and practices, chapter 3, block cipher and the data encryption standard."

[7] D. Coppersmithš, "The data encryption standard (des) and its strength against attacks," 1992.

[8] R. V. Daemenš J., "The design of rijndael. "aes - the advanced encryption standard," p. 238.

[9] J. L. Masseyš, "Safer k-64: A byte-oriented block-ciphering algorithm," *Proc. Fast Softw. Encryption*, pp. 1–17, 1993.

[10] M. K. M. et al., "Matlab implementation of 128-key length safer+ cipher system," *Int. Journal of Engineering Research and Application*, vol. 7.

[11] A. A. et al., "A novel symmetric cryptography algorithm for fast and secure encryption," pp. 1–6, 2015.

[12] G. B. Vijayš Dahiphale, "Anu–ii: A fast and efficient lightweight encryption design for security in iot," pp. 131–137, 2017.

[13] M. F. A.-G. S. Boussakta and J. A. Neasham, "Fermat number transform diffusion's analysis," pp. 237–240, 2011.

[14] J. H. IAXIAš GUO, "A complexity-reduced block encryption algorithm suitable for internet of things," *IEEE Access*, pp. 54 760–54 769, 2019.

[15] C. E. Shannonš, "Communication theory of secrecy systems," *Bell Labs Tech. J.*

[16] A. B. D. Cannière and G. Dellkrantz, "Crypt analysis of safer++," pp. 195–211, 2003.

[17] M. J. A. Amjadš Hussain Zahid, "A novel construction of efficient substitution-boxes using cubic fractional transformation," vol. 21.

[18] A. M. S. Seddiqš Q, Abd Al-Rahman, "Nvlc: New variant lightweight cryptography algorithm for internet of things," pp. 176–181, 2019.