An Effective S-box Construction Based on Linear Recurrences with Constant Co-Efficient

Nasir Siddiqui1 · Wajeeha Iftikhar1 · Muhammad Ehatisham Ul Haq2

Accepted: 14 November 2021 / Published online: 5 January 2022
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2021

Abstract

In this paper, we propose an algorithm for the construction of substitution-box (S-box) through a linear recurrence relation. S-box is considered as the building block of block ciphers; here, we present a technique to construct S-boxes by using linear recurrence relation to comply with the standards of cryptographically secure S-box. We have witnessed that the latest research relies more on improving already existing techniques, rather than developing wholly new methods. We use linear recurrence for the design of S-box in an entirely new way. Real values, including initial and obtained values, are concealed by converting it into new numbers to avoid any pattern to follow. The obtained S-boxes are analyzed through benchmark performance tests to check the strength and quality of our proposed S-boxes. Later, we used the S-boxes to encrypt an image and also performed encryption and decryption of data in noisy channels to make it more applicable in low-profile applications.

Keywords Substitution-box · Symmetric cryptography · Linear recurrence formula · Image encryption

1 Introduction

The security of data has become a major necessity of our life in the present era. Fast and modern communication channels are being used around the globe, which demands the security of transmitted data to avoid privacy hazards. In order to prevent the misuse of data by unauthorized people, many researchers are developing techniques to create confusion in the original data. As time progresses, the need to develop strong cryptographic algorithms...
is becoming crucial. Cryptographically secure systems are becoming very important nowadays as we are using them not only in military and defense applications, but also in our daily life in our mobile phones, social media accounts, and banks [1].

To secure the communication through mobile phone and wireless sensor networks, the data transmitted is encrypted using symmetric or asymmetric algorithms to avoid the leakage of information. Substitution-box (S-box) plays a significant role in ensuring the security of the system and is considered to be a major component of a symmetric block cipher in cryptography. S-box creates confusion in data by establishing a unique relationship between plaintext and cipher text. Most secure block ciphers include both substitution and permutation [2]. The purpose of this paper is to construct S-box that satisfies all the necessary conditions for developing a secure system. It is a known fact that in the last two decades, the academic study of construction of S-boxes for securing our data has been an attractive area of study for many researchers. Advanced Encryption Standard (AES) is considered as the strongest system for data security and is widely used, but due to the high computational complexities, comparatively easy applicable algorithms are developed these days[3].

The proposed technique of S-box construction is based on linearly recurrence relation. The idea of using linear recurrence may be perceived as outdated in this era. However, we use it in a unique way along with the latest methods to get efficient results.

This paper is organized as follows. In Section 2, the preliminaries are discussed. In Section 3, the method for the construction of our substitution-box is explained. In Section 4, the comparison with already existing techniques for S-box design is presented and discussed. The strength of our constructed S-boxes is tested on the basis of Non-Linearity, Bit Independence Criterion, Strict Avalanche Criterion, Linear Probability, and Differential Probability [4, 5].

2 Preliminaries

2.1 Linear Recurrence Formula

In order to incorporate linear recurrence in this research, we delve into its prior history, which can be classified as finite history and full history [6]. Finite history emphasizes on the dependence of fixed number of earlier values, while an equation that depends on all the preceding terms has a full history. Similar to differential equation, it can be classified into homogeneous and non-homogenous. Homogenous linear recurrence relations are easily distinguishable from non-homogenous relations due to the presence of an extra term $g(x)$. The formula of linear recurrence is defined in Eq. (1).

$$c_0x_n + c_1x_{n-1} + \ldots + c_{m}x_{n-m} = g(x), \quad n \geq m$$

If $g(x) = 0$, equation is homogenous, but when it is not equal to zero, then equation is non-homogenous. Here, we considered a homogenous equation with all coefficients zero except $c_0$, $c_1$ and $c_2$. Here we take the values as $c_0 = 1$, $c_1 = -1$ and $c_2 = -1$. 

 Springer
3 Scheme of Proposed S-box Generation

3.1 Step 1

First, we consider the Fibonacci number calculation formula [6], as given in the following equation.

\[ x_n = x_{n-1} + x_{n-2} \]  

(2)

Consider, two initial values (i.e., integers) at random.

3.2 Step 2

In our experiments, the initial random values, i.e., 150 and 130, are used to calculate further values. But, after many iterations, maximum of 168 distinct integer values are calculated. To calculate more values, we apply the same formula with slight change in initial conditions. The process repeats until we get all required values from 0 to 255. We get all values by using a formula three to four times with the change in initial conditions and using different variables. For example, we use Eq. (3) with different initial values for generating more values.

\[ y_n = y_{n-1} + y_{n-2} \]  

(3)

We can also change the formula as a product of preceding terms instead of summation to create more confusion. Table 1 shows the set of a few initial values used for generating the further values.

3.3 Step 3

The numbers are arranged in specific way that calculated values are picked in iterations in a respective manner. For example, the first value from \( x \) is used, then the first value of \( y \) and so on. This step makes all values more random. The program is designed using MATLAB software.

The S-box obtained by following these steps is shown in Table 2. All the values are obtained with \( x, y \) and \( z \) variables. But to create more confusion, in the last step, we use the formula presented in Eq. (4)

\[ t_n = t_{n-1} \times t_{n-2} \]  

(4)

It can be observed from Table 2 that the all our initial values are appearing in the first row. So, to overcome this problem, we apply another the next step.

Table 1 Set of initial values for S-box generation

| \( x_0 \) | \( x_1 \) | \( y_0 \) | \( y_1 \) | \( z_0 \) | \( z_1 \) | \( t_0 \) | \( t_1 \) |
|---|---|---|---|---|---|---|---|
| 150 | 130 | 185 | 146 | 180 | 165 | 95 | 240 |
3.4 Step 4

The S-box obtained after third step is transformed by converting the values from decimal to binary and permuted in reverse order to get the new decimal numbers. This step does not affect the non-linearity of the S-box; rather it helps in hiding the initial values. Figs. 1 and 2 show the steps for the proposed S-box construction method.

The process of number flipping is applied to every value in the S-box to transform our S-box into a new S-box. The finalized S-box generated using this transformation is shown in Table 3.

4 Analysis Criterion of S-boxes

In order to investigate the strength of our constructed S-box, we test our S-box according to the following criteria: Non-Linearity (NL), Strict Avalanche Criterion (SAC), Linear Probability (LP), Differential Probability (DP), and Bit Independence Criterion (BIC), as explained in [7, 8]. The values obtained for the proposed S-box are presented in Table 4, which are compared with the existing S-boxes in Table 5 and Figs. 4, 5, 6, and 7.

4.1 Non-Linearity

S-box is designed in such a way that the relation between plaintext and cipher text is non-linear in terms of mapping, otherwise it would be susceptible to linear cryptanalysis. Non-linearity is actually the distance between a Boolean function and the set of all the affine functions. The importance of non-linearity for the encryption process cannot be denied as mentioned in [8]..
Fig. 1 Flowchart representation for the proposed method

Fig. 2 Flipping of numbers to generate the proposed S-box
The calculated non-linearity of our proposed S-box is 106, with minimum non-linearity as 104 and maximum non-linearity as 108. The comparison with the non-linearity of the known S-boxes is presented in Table 6 and Fig. 3.

### 4.2 Strict Avalanche Criterion

According to the SAC, if in the function that is forming the substitution box, we change the single bit of input, it is necessary that there is probability of 50% change in the output bits sequence. If the SAC value is closer to that of AES, it becomes more reliable. The obtained strict avalanche value for our constructed S-box is better than skipjack S-box and residue prime, as shown in Table 5 and Fig. 4.
| S-boxes                  | Non-linearity | SAC  | LP   | DP   | BIC  |
|-------------------------|---------------|------|------|------|------|
|                         | Maximum       | Minimum | Average Value |      |      |      |
| Proposed S-box          | 108           | 104  | 106  | 0.4970 | 160 | 0.039 | 103.57 |
| AES S-box[9]            | 112           | 112  | 112  | 0.504 | 144 | 0.0156 | 112 |
| APA S-box[10]           | 112           | 112  | 112  | 0.5   | 144 | 0.0156 | 112 |
| Gray S-box[11]          | 112           | 112  | 112  | 0.499 | 144 | 0.0156 | 112 |
| $S_4$ AES S-box[12]     | 112           | 112  | 112  | 0.504 | 144 | 0.0156 | 112 |
| Skipjack S-box[13]      | 108           | 104  | 105.75 | 0.503 | 156 | 0.0468 | 104.14 |
| Xyi S-box[14]           | 106           | 104  | 105  | 0.502 | 168 | 0.0468 | 103.78 |
| Residue prime[15, 16]   | 104           | 94   | 99.5 | 0.516 | 162 | 0.281 | 101.71 |
| [17]                    | 108           | 102  | 104.5 | 0.4980 | 160 | 0.0469 | 104.64 |
4.3 Bit Independence Criterion

The independent behavior of the pair of variables and the changes in input bits are considered as significant factors of BIC. According to this criterion, the input bits are transformed completely, and then output bits are checked for their independence. Bit independence is one of the most important criterions of S-box strength. The proposed S-box produces good results for the BIC, as shown in Table 5 and Fig. 5.

4.4 Differential Probability and Linear Probability

To access the imbalance of an event, the linear probability of the constructed S-box is calculated. It is represented by the formula given in Eq. (5)
An Effective S-box Construction Based on Linear Recurrences…

\[ LP = \max_{\beta p, \beta q \neq 0} \left| \frac{\# \{ x \in GF(2^8) / x. \beta p = s(x). \beta q \} - \frac{1}{2}}{2^q} \right| \]  

(5)

| Table 7 | Image encryption results using proposed algorithm |
|---------|-----------------------------------------------|
| Image   | Entropy | Correlation coefficient | Energy | Contrast | Homogeneity |
| Pepper image | 7.5846 | 0.1013 | 0.0178 | 9.2410 | 0.4663 |

| Table 8 | Error rate values for noise removal (with SNR=5) using the proposed S-box |
|---------|----------------------------------------------------------------------------|
| Proposed box | 0.48836 | 0.52672 | 0.51432 | 0.49176 | 0.50002 | 0.51988 |
| AES     | 0.51024 | 0.49726 | 0.50752 | 0.48836 | 0.50478 | 0.50342 |
| Gray    | 0.50068 | 0.4726  | 0.49452 | 0.52324 | 0.49314 | 0.48764 |
| Skipjack | 0.487  | 0.4997  | 0.4910  | 0.5232  | 0.4917  | 0.4883  |
| Residue Prime | 0.50134 | 0.50684 | 0.51574 | 0.4863  | 0.51988 | 0.51438 |

| Table 9 | Error rate values for noise removal (with SNR=10) using the proposed S-box |
|---------|----------------------------------------------------------------------------|
| Proposed box | 0.41966 | 0.4175 | 0.42868 | 0.4328 | 0.40998 | 0.44062 |
| AES     | 0.42626 | 0.41104 | 0.42532 | 0.42826 | 0.41532 | 0.42396 |
| Gray    | 0.41404 | 0.42832 | 0.4167  | 0.42144 | 0.41014 | 0.43382 |
| Skipjack | 0.4184  | 0.4085  | 0.4079  | 0.429   | 0.4137  | 0.4226  |
| Residue Prime | 0.43694 | 0.4143 | 0.42026 | 0.41984 | 0.41216 | 0.43372 |
In the given formula, \( p \) represents the input values of S-box. The input and output masks are expressed in the form of \( \beta p, \beta q \) respectively. We compared our results with the standard S-box results. Our obtained value is 0.125, which is not too susceptible in terms of linear attacks [18].

To measure the differential uniformity of the constructed S-box, we check the DP value of the constructed S-box. The formula for the calculation of DP is expressed in the following form in Eq. (6)

![Fig. 4 Strict avalanche criterion (SAC) values comparison for different S-boxes](image)

![Fig. 5 Bit independence criterion (BIC) values comparison for different S-boxes](image)

| Proposed box   | 0.00668 | 0.01052 | 0.01866 | 0.02438 | 0.03308 | 0.04632 |
|----------------|---------|---------|---------|---------|---------|---------|
| AES            | 0.00618 | 0.01294 | 0.02292 | 0.02988 | 0.03636 | 0.04592 |
| Gray           | 0.00606 | 0.0125  | 0.0164  | 0.02808 | 0.03486 | 0.05184 |
| Skipjack       | 0.0183  | 0.0306  | 0.0389  | 0.0540  | 0.0562  | 0.0635  |
| Residue Prime  | 0.0060  | 0.01578 | 0.02082 | 0.0273  | 0.03064 | 0.0379  |

Table 10 Error rate values for noise removal (with SNR=15) using the proposed S-box
To represent the differentials, we use $\Delta x$ and $\Delta y$. On the basis of comparative analysis shown in Figs. 6 and 7, we can say that our results are better than Skipjack, Xyi, and Residue Prime [18].

$DP = \left[ \frac{\# \{ x \in X / S(x) \oplus S(y \oplus \Delta x = \Delta y) \}}{2^n} \right]$ (6)

Fig. 6 Comparison of linear probability values for different S-boxes

Fig. 7 Comparison of differential probability values for different S-boxes

5 Image Encryption

We also performed image encryption in order to test the strength of the constructed S-box. We use Capsicum image for the encryption process. The image with pixel values of 0 to 255 is considered for encryption and the S-box ranging from 0 to 255 is applied on the image, which will replace pixel values of the image. The algorithm is applied twice to get the best results for the encrypted image as shown in Table 7 and Fig 8.

 Springer
6 Noise Resistant Property of the Proposed S-box

As we know, that the intruder can add noise to any communication channel intentionally. This makes it necessary to develop an algorithm, which is noise resistant. The noise must be removed to reduce the effect of channel noise caused by unauthorized person [20, 21]. The next step is followed by the analysis of our constructed S-box based on bit error rate (BER), which is actually a function of length of burst errors for multiple values of Signal to Noise Ratio (SNR) in aggregation with the single error correction code.

N . We also compare the performance of our constructed S-box for noise removal with conventional S-boxes. The data is taken in the form of 100 random blocks with the block size N=256. To encode our data, we use linear hamming code. The length of the code word is taken as (7, 4), whereas the minimum value of the hamming distance is kept equal to 3 . We then introduce the burst errors of different lengths in the data using Additive White Gaussian Noise (AWGN). The noise is then XORed it with the modular data for analyzing the performance of our S-box against the burst errors. Error rates are calculated at different values of SNR and compared with the results of standard S-boxes, i.e., AES, Gray, Skipjack, and Residue Prime S-boxes, as shown in Tables 8, 9, and 10. These results show that the proposed S-box can provide strong resistance against the noise. The error rate values for known S-boxes are taken from the existing study [22].

7 Conclusion

In this work, we proposed a new scheme for the construction of S-boxes. We established that linear recurrence relation can be used to construct efficient S-boxes in a simpler way. The technique presented for S-box construction has better results than some known algorithms. The strength of constructed S-boxes is analyzed by performance tests in order to cope up to the standards of well-known S-boxes. Furthermore, the constructed S-box is used for the encryption of an image as well as for noise removal, and it showed effective results.
References

1. Paar, C., & Pelzl, J. (2009). Understanding cryptography: A textbook for students and practitioners. NewYork: Springer.
2. Greene, D. H., & Knuth, D. E. (2007). Mathematics for the analysis of algorithms. NewYork: Springer.
3. Sarfraz, M., Hussain, I., Ali, F., & Rasheed, A. (2016). A mobius transformation based algorithm for the construction of cryptographically strong 131028 S-boxes having highly nonlinear. International Journal of Computer Science and Information Security, 14(5), 611.
4. Ahmad, M., Haleem, H., & Khan, P. M. (2014). A new chaotic substitution box design for block ciphers. In 2014 International Conference on Signal Processing and Integrated Networks (SPIN) (pp. 255–258). IEEE.
5. Han, J. S., Kim, H. S., & Neggers, J. (2012). On Fibonacci functions with Fibonacci numbers. Advances in Difference Equations, 2012(1), 126.
6. Wilf, H. S. (2005). generatingfunctionology. CRC Press.
7. Zahid, A. H., & Arshad, M. J. (2019). An innovative design of substitution-boxes using cubic polynomial mapping. Symmetry, 11(3), 437.
8. Farwa, S., Muhammad, N., Shah, T., & Ahmad, S. (2017). A novel image encryption based on algebraic S-box and Arnold transform. 3D Research, 8(3), 26.
9. Daemen, J., & Rijmen, V. (2013). The design of Rijndael: AES-the advanced encryption standard. NewYork: Springer.
10. Cui, L., & Cao, Y. (2007). A new S-box structure named affine-power-affine. International Journal of Innovative Computing, Information and Control, 3(3), 751–759.
11. Tran, M. T., Bui, D. K., & Duong, A. D. (2008). Gray S-box for advanced encryption standard. In 2008 International Conference on Computational Intelligence and Security (Vol. 1, pp. 253–258). IEEE.
12. Hussain, I., Shah, T., & Mahmood, H. (2010). A new algorithm to construct secure keys for AES. International Journal of Contemporary Mathematical Sciences, 5(26), 1263–1270.
13. Hussain, I., Shah, T., Gondal, M. A., & Wang, Y. (2011). Analyses of SKIPJACK S-box. World Applied Sciences Journal, 13(11), 2385–2388.
14. Hussain, I., Shah, T., Gondal, M. A., Khan, W. A., & Mahmood, H. (2013). A group theoretic approach to construct cryptographically strong substitution boxes. Neural Computing and Applications, 23(1), 97–104.
15. Abuelyamam, E. S. (2013). Residues of prime numbers as entries for the S-Box. In 2013 International Conference On Computing, Electrical And Electronic Engineering (ICCEEE) (pp. 584–588). IEEE.
16. Hussain, I., Shah, T., Mahmood, H., Gondal, M. A., & Bhatti, U. Y. (2011). Some analysis of S-box based on residue of prime number. Proc Pak Acad Sci, 48(2), 111–115.
17. Liu, L., Zhang, Y., & Wang, X. (2018). A novel method for constructing the S-box based on spatiotemporal chaotic dynamics. Applied Sciences, 8(12), 2650.
18. Khan, M., & Shah, T. (2015). An efficient construction of substitution box with fractional chaotic system. Signal, Image and Video Processing, 9(6), 1335–1338.
19. Cheung, J. M. (2010). The design of S-boxes (Doctoral dissertation, Sciences).
20. Hussain, I., Anees, A., Aslam, M., Ahmed, R., & Siddiqui, N. (2018). A noise resistant symmetric key cryptosystem based on S 8 S-boxes and chaotic maps. The European Physical Journal Plus, 133(4), 167.
21. Hussain, I., Shah, T., Gondal, M. A., & Khan, W. A. (2011). Construction of cryptographically strong 8x8 S-boxes. World Applied Sciences Journal, 13(11), 2389–2395.
22. Siddiqui, N., Naseer, A., & Ehatisham-ul-Haq, M. (2020). A novel scheme of substitution-box design based on modified Pascal’s triangle and elliptic curve. Wireless Personal Communications, 1, 1–16.

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.
Dr. Nasir Siddiqui received his Ph.D. degree in Mathematics from the Quaid-i-Azam University, Islamabad, Pakistan in 2010. Currently he is working as Associate Professor at University of Engineering and Technology (UET), Taxila, since February 2011. His research interests and experiences lie within the areas of Algebra, Fuzzy Algebra, Cryptography, Information Security, and Group Theory (Permutation Groups).

Wajeeha Iftikhar received her BS (Hons) degree in Mathematics from the University of Wah, Wah Cantt, Pakistan, in 2016. She is currently pursuing her MS degree in Mathematics from University of Engineering and Technology (UET), Taxila, Pakistan. Her research area is mainly focused on information security and cryptography.

Muhammad Ehatisham-ul-Haq received his B.Sc. and M.Sc. degrees in Computer Engineering from the University of Engineering and Technology (UET), Taxila, Pakistan, in 2014 and 2017, respectively, and won Gold Medals. He acquired his Ph.D. degree in Computer Engineering (with specialization in Pervasive and Ubiquitous Computing) from UET Taxila, Pakistan, in 2021. He is currently working as an Assistant Professor at the Department of Creative Technologies, Air University, Islamabad, Pakistan. His research interests lie in the areas of signal, image, and video processing, biomedical signal processing, mobile sensing, machine learning, human activity and emotion recognition, human behavior analysis, and information security.