VOL. 18, NO. 6, MARCH 2023 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

DETERMINISTIC APPROACH TO CLASSIFY THE POWER-EFFICIENT S-BOX USING MACHINE LEARNING

G. Sowmiya and S. Malarvizhi
Department of Electronics and Communication Engineering, SRM Institute of Science and Technology, Kattankulathur, Chennai, India
E-Mail: sg8182@srmist.edu.in

ABSTRACT

The substitution box (s-box) serves as one of the key elements of cryptography responsible for uncertainty and nonlinear properties. These boxes must have a variety of security qualities in order to protect a cipher against various attacks, including side-channel attacks. Designing a 16*16 s-box that is both cryptographically secure and energy efficient is a difficult task. Thus, in order to automate the process of determination and verification of dynamic power efficiency of s-boxes, a method of supervised machine learning approach has been used here. Additionally, utilizing the outcomes of supervised learning, in order to construct s-boxes that are both cryptographically secure and low-power, we propose a deterministic model that may be used in an optimization strategy to estimate the dynamic strength of an s-box. A machine learning- approach has been integrated to automate and categorize the power efficiency. It is evident that there is a 4% increase in the accuracy of power prediction of s-box.

Keywords: S-box, power efficiency, AES, dynamic power, machine learning (ML), lookup table (LUT).

1. INTRODUCTION

The term "Internet of Things" (IoT) items refers to situations where physical objects link to and exchange information with several other systems or equipment over a portal or other communication networks. These physical items typically incorporate sensors, computing power, software, and other technologies. The term "Internet - of-Things" has been criticised for being misleading since devices must be connected to a system and separately addressed rather than the broad internet. The combination of different systems, including cloud computing, reasonably priced sensors, Machine Learning and extremely powerful embedded devices have altered the industry. The Internet of Things is made possible with the help of conventional fields namely embedded devices, wireless sensors, control systems, and automation (which includes home-based automation). These domains may be accessed and controlled by ecosystem-based devices like smart speakers and smartphones. The Internet of Things is used in the healthcare industry as well. The Internet is often known as the globally connected computer network with identities managed by IANA (Internet Address and Naming Authority).

From safe transactions and payments to private communications and authentication methods, security offers a number of features and applications. Cryptography is a key element of safe communication. The AES is currently the most popular and substantially employed symmetric encryption method. It is found six times more quickly than triple DES. A replacement was necessary because the DES (Data Encryption Standard) key size was too tiny. It was considered to be unsafe to an intensive key search attack as the power of the processing increased. S-box implementation usually makes use of Look Up Tables (LUTs), which store 256 predefined s-box and inverse s-box values in a ROM. In terms of gate count, it appears to have a smaller critical depth and is appropriate for Field Programmable Gate Array implementation. In high-speed pipelined architectures, the LUT's insurmountable delay becomes a disadvantage. The architecture of AES hardware implementation determines its efficiency of size, speed power consumption, and security. Diverse parameters in terms of size for mobile applications and high-speed computing for rapid responses are required by different applications of society. The s-box transform in Advanced Encryption Standard implementation is a nonlinear transformation that contributes significantly to obtaining high security by providing confusion in data processing encryption. For VLSI or FPGA designs of small-footprint mobile applications, CFA-based optimization is utilised to reduce the size, and data security is assured using various masking techniques. The reliability, scalability, and power consumption for AES hardware implementation are all influenced by its architecture whether it is to lessen the chip size, and power utilization or to maximise security, efficiency, and throughput, researchers have done everything possible to optimise one or more attributes for a given application [1]. Varying applications in society need different size parameters for portable applications and high-speed processing for a quick response. Considerable cost parameters, including essential route delay, silicon area and energy usage of different performances were examined on a synthesis run of a 0.25 m CMOS conventional CMOS library [2].

The simulation results reveal unequivocally that each of the 8 s-box implementations has distinctive properties. For instance, different S-boxes' power usage varies by at most an order of magnitude, highlighting the significance of choosing the right S-box according to the needs of the application. The S-Box comprises two transformations: inverting the multiplication component in the Galois Field and using a modified affine transformation [3]. The drawback of S- Box is that it consumes excess time and energy. This constraint must be circumvented by making minor changes to the affine and inverse affine transforms. The issue of network security has grown in importance. A crucial component of the

system for information security is encryption, which has become a viable solution. Several measures are required to secure the shared data. We built three encryption approaches, AES, RSA, and DES algorithms and differentiate their encryption performance based on an examination of the stimulated time during encryption and decryption [4]. The issue of network security has grown in importance. A crucial component of the system of information security is encryption, which has become a viable solution. The S-Box, being based on the composite field arithmetic method, is a combinational logic with minimal power and delay. It is implemented using the pipelining methodology [5]. XOR, AND, NOT, and OR logic gates are used in the S-Box design's four-stage pipelining.

The pipelined-based S-Box consumes less power and operates at a faster rate than the traditional structure. Complex parallelism is utilised to execute Shift Row, Substitution Byte, Add Round Keys and Mix Column in order to boost efficiency [6]. The original text is changed into cipher text using S-Box complex parallelism. The S-Box is the part of the AES algorithm that uses the most time and energy [7, 8]. It is possible to alter the affine transformation in an effort to speed up AES. A framework for reporting on the effectiveness of cryptographically robust S-boxes that uses supervised machine learning. On two subsets of a large collection of power-efficient S-boxes, a) 4*4 optimal and b) 4*4 optimal along with involutive S-boxes, the validity and efficacy of our technique are documented [9,10].

1.2 Related Work

Dynamic power usage has a significant the way that the dynamic power is used has a big impact on how much power the cryptography chip uses. To count all bit toggles, also known as bit flips, that take place during the encryption of a single block using a particular algorithm [11]. Compare the size and power needs of four lightweight block ciphers-PRESENT, SIMON, SPECK, and KHUDRA-on ASIC and FPGA-based platforms [12]. These lightweight block ciphers are compared to the Advanced Encryption Standard (AES) that acts as a benchmark and exemplifies the resource conservation that particular lightweight block cyphers can achieve. S-boxes are chosen using a process that prioritises power/area efficiency. Since power/area efficiency plays an influential role in lightweight ciphers, and also intensify only on the s-box dimension usually found in such constructs, we experiment with 4×4 and 5×5 S-box sizes [13]. An incidentals-boxes are created as permutations of weights between 0 and 2^{n-1} and check the results regarding dimensions and power. The pattern dependence problem has recently been addressed by a number of probabilistic power estimation algorithms [14]. In reality, all these are only applied to combinational circuits and demand that the user describe the usual behaviour at the inputs of the combinational circuit. The DPA resistivity of the S-boxes in the suggested class is higher than that of the AES Rijndael s-box, according to the results of the correlation analysis. Boolean function features for S-boxes are designed to minimize transparency order, boost defense against DPA attacks, and guarantee coordinating function with greater nonlinearity and favourable global avalanche characteristics. [15]. To get the desired S-box by manipulating the fitness function since the optimization algorithm uses the fitness function to regulate the level of optimization [16]. In order to attain the features of compact dimensions, the S-box is developed primarily using a dual basis, and the circuit is made simplifier by AND-XOR array structure [17]. This article is organised in tails for the remainder of it. The Section II provides a basic overview of the cryptographic properties of S-boxes and the criteria for the Machine Learning model's quality. We go over the machine learning framework which can be used to arrange a group of S-boxes based on their power efficiency in Section III. In this section, every feature can be used for the feature set for modelling. For a set of 16*16 optimum S-boxes and we present experimental findings in Sections IV and V demonstrating the effectiveness and high performance of our tool.

2. DETERMINING THE POWER EFFICIENCY OF S-BOX

In this section, we go through two general techniques for figuring out how efficient S-boxes are at using power. The first method is based on simulation, and the second is probabilistic.

a) Using a simulation-based approach: The average power dissipation of the circuit is calculated by tallying and averaging the event data after compiling the signal occurrences throughout time.

b) Using a probabilistic-based approach: A signal is considered as a random variable with some statistical properties in the likelihood power estimation approach (static probability, transition density, etc.). In contrast to the simulation-based approach, whereby estimates the exact delay, this methodology uses a shorten delay model, sometimes referred to as the zero-delay model, where the same delay is retained at all the gates. Each input signal also receives a static probability, generally 0.5, which is illogical. In this approach, a logic extractor is utilised to convert the substitution box specification into a logic form using the Binary Decision Diagram (BDD) model or signal probability.

2.1 Proposed Work

This research focused on the power effectiveness of S-boxes. As was previously said, the present approaches to calculating power performances are inaccurate or sluggish. As a result, our main objective is to create a novel methodology that evaluates the performance and efficiency of a set of substitution boxes in a short amount of time while keeping high accuracy. In this article, we present an automated method that employs Supervised Machine Learning (SML) to categorise a set of n* n substitution boxes into two groups (Good and Bad) according to their power efficacy. The article focuses on the Look Up Table -based design for substitution -boxes with AND, OR, and inverter (or A-O-I) gates. We discover that the inherent Boolean functions (also referred

to as the component functions) corresponding to the S-box literal computations [in Sum-Of-Products (SOP), factor, and kernel function -extracted forms] and AND-OR-NOT gate counts are the key elements in the switching activity of the associated functions of an s-box. However, it can be difficult to mathematically define such a relationship. The switching activity of a collection of substitution boxes' component functions impacts the system's dynamic power efficiency, which encourages us to use an ML-based method to anticipate it.

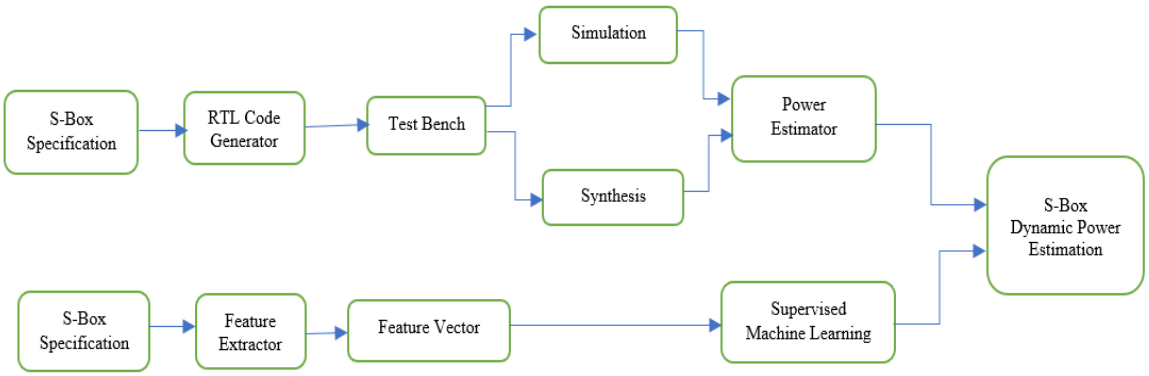

Figure-1. Design Flow for Power Efficiency of S-Box Using ML Approach.

Figure-1 shows the flow diagram for the findings on power-efficient s-boxes that were produced using this methodology. The gate-level-netlist and latency file is created by first synthesising a look-up table-based substitution box design utilising a technology repository through a commercially accessible synthesis tool. The switching activity file, which records the toggle count of each signal, is produced using the test-bench file, delay model, and gate-level-netlist. Commercial simulation tools are a viable option for this. The activity file also includes details on each node's time characteristics, which define the lengths of time for all nodes and signals at different levels. Every potential combination of signal transitions that could be input is included in the test-bench file. Using the gate-level-netlist, any commercial power calculation application may calculate the precise power and produce the corresponding switching activity file. Using a commercially accessible synthesis tool, a LUT- dependent s-box design utilising a technology library will be first synthesized to build the gate-level-netlist and delay file. The switching activity file, which records the toggle count of each signal, is produced using the test-bench file, delay model, and gate-level-netlist. Commercial simulation tools are a good choice in this case. The activity file also contains details on every node's characteristics, which include the time periods for all nodes including signals at various levels. Every combination of signal transitions from the input is included in the test-bench file. Any commercial power estimation application uses the gate-level-netlist and this originated switching activity file to decide the precise power. The work presents a set of powerful-efficient s-boxes from a huge set of 16*16 optimal s-box to show the efficiency of our methodology. According to the trial findings, our method is roughly 97% and 87.5% accurate for both classifiers. The simulation-based method uses Cadence Virtuoso to calculate power efficiency.

2.2 Sources of Power Dissipation

When the logic gate is in the active state, it dissipates power, which is known as the CMOS dynamic power. It is mostly caused by the input signal's switching activity or by the charging and discharging of internal node capacitances.

$$P_{dynamic} = C_L * (V_{dd})^2 * f.$$

Where $V_{dd}$is the voltage supplied, $C_L$is the node capacitance, and f is the signal frequency. The charging and discharging of the load capacitances when the gate shifts from one logic to another logic is the fundamental cause of the CMOS dynamic power dissipation ($P_{dynamic}$) the leakage current or short circuit current while neither the PMOS nor the NMOS stacks are fully ON.

3. S-BOX POWER ESTIMATION USING MACHINE LEARNING

3.1 S-Box

This byte uses non-linear substitution. Another byte is used to replace each byte. S-Box is used by this substitution byte to produce the encryption text. The s-box uses two processes. The multiplicative inverse of the matrix's finite field is taken using the first one (input data). Second, the output of the multiplicative inverse is subjected to the affine transformation. This finite field allows for area reduction, and it is this finite field that is used to implement the compact field AES. In modern technology, the s-box can be found by employing two different level logic, such as the sum of products and the product of sum, to deduce its truth table. Using a synthesis tool, it is possible to reduce the number of primitive logic cells while also optimising cell size. The multiplicative inverse and affine transform operations are based on the operations of the finite Galois Field in the development of the s-box (2^8). Combinational logic can be used to calculate this function and its inverse quickly. In

comparison to a straightforward solution using read-only memories for lookup table, this method provides advantages.

3.2 Feature Extractor

The goal of feature extraction is to lessen the total number of resources required to explain a large amount of information. The enormous range of variables that are included in sophisticated data analysis is one of the key challenges. When an investigation with a large number of variables uses a significant amount of memory and computation resources, a classification model may increase the precision to training samples and perform badly on new samples. By integrating the variables, feature extraction is a method for avoiding these issues even while effectively characterizing the data. Many machine learning experts think that effective model creation depends on correctly tuned feature extraction.

3.3 Feature Vector

"In machine learning, extracted features are used to mathematically and simply express numerical or symbolic properties of an object, known as features. For many applications involving machine learning and pattern recognition, they are essential. Machine learning algorithms frequently require a quantitative evaluation of the objects in order to analyse them and do statistical analysis. A vector is a sequence of integers, similar to a matrix with one column but several rows that can frequently be represented geographically. They are employed in statistical methods like linear regression. Feature vectors are the equivalent of vectors of independent variables. A feature is a metric or figurative attribute of a feature of an object.

3.4 Machine Learning Model

The frameworks for supervised machine learning can be divided into two groups, one is the classification approach and the other is the regression approach. In regression, a continuous value is a forecast, whereas, in classification, a class label is anticipated. Some well-known measures are used to assess how well an ML predicts. We quickly review the popular metrics for evaluating ML-based models in this section. We start by taking into account that the confusion matrix is one of the most understandable yet simple metrics for determining the accuracy and correctness of classification ML-based models. The following entries make up the 2 by 2 matrix's "actual" and "predicted" dimensions.

a) **True Positive (TP):** The Predicted and actual values both fall into 1. (True).

b) **False Positive (FP):** Here the predicted value is 1(True), but the actual data is 0 (False).

c) **False Negative (FN):** In this case, the data point actually, belongs to class 1 (True), whereas the forecast belongs to class 0 (False).

d) True Negative (TN): In this scenario, the data point's actual class and anticipated class are both 0 (False).

The work fully describes our Machine Learning (ML)-based methodology in this section, which is used to estimate and categorise s-boxes according to their dynamic power usage. As previously stated, when we talk about dynamic power, we mostly refer to the AND-OR-INVERTER Implementation of an s-box.

3.4.1 Support vector machine algorithm

Feature extraction aims to reduce the volume of resources required to describe ample of data. The enormous range of variables that are included in sophisticated data analysis is one of the key challenges. When an investigation with a large number of variables uses a significant amount of memory and computation resources, a classification model may increase the precision of training samples and perform badly on new samples. Feature extraction is a technique for combining the variables to get around these problems and still accurately characterising the data set. Many specialists working under machine learning believe that properly adjusted feature extraction is the key to effective model construction.

3.4.2 Naive bayes classifier

Based on the Bayes theorem, the Naive Bayes algorithm is essentially a learning technique for classification problems. We mainly employ a large training set for text categorization. Making efficient algorithms that can generate precise predictions is made simpler by this. Being a probabilistic classifier, it makes a prediction based on the probability that even an object will occur. Spam filtration, topic detection, and article classification are a few uses for Naive Bayes algorithms.

3.4.3 Kernel functions in Support Vector Machine (SVM)

Using a kernel function, data can be input and then transformed into the format needed for processing. The term "kernel" is employed because the window for manipulating the data in a Support Vector Machine is provided by a set of mathematical operations. The kernel function frequently changes the training set of data to cause a non-linear selection surface to transform into a linear equation in the greater number of dimension spaces. The inner product between two points in a common feature dimension is what it basically returns.

When the data can be split using a single line, or when it is linearly separable, a linear kernel is utilized. It is one of the most often utilized kernels. It is frequently used when a particular data collection contains a large number of features. Text Classification is one of the instances where there are numerous features because each letter of the alphabet is a separate feature. Therefore, Linear Kernel is primarily used in Text Classification.

4. PERFORMANCE METRICS

The estimation of leakage power and dynamic power (total power) has been carried out in the Cadence EDA tool which is given in Table-1 along with the total area report in Table-2.

Table-1. Total power dissipation report.

Component	Number of Cells	Leakage Power Dissipation (nW)	Dynamic Power Dissipation (nW)	Total Power Dissipation (nW)
S-Box Encoder	474	6143.049	43501.879	49644.928

Table-2. Total area report.

Component	Number of Cells	Cell Area occupied	Total Area
S-Box Encoder	474	2159	2159

4.1 Preparation of the dataset

By simulating the Verilog code of an S-Box to obtain the dataset values, the.csv file of the dataset containing data from the s-box, such as power, area, and delay, is produced. The columns contain the S-Box's power, area, and delay values in cumulative form.

4.4.1 Mean Absolute Error (MAE) vs Root-Mean Square Error (RMSE)

A few common and familiar metrics of error calculation for ML based regression issues are MAE and RMSE. There are significant variations between the two, despite the fact that they are employed for the same objective (understanding the flaws in your forecasts). Selecting the appropriate metrics for your model can have a significant impact on your capacity to resolve issues. The error metric is used by the algorithms you'll employ to build models to carry out optimizations. It's critical to comprehend the differences between error measures because the decision on an error metric will have an impact on the bottommost model and how to estimate its performance. For the data set obtain from the work, the Mean Absolute Error and Root Mean Square Error is 0.125 and 0.35.

4.2 Data pre-processing

We must designate the columns in this section just as the dependent variable column (Y) and the independent variable column (X), scale its collected data using the Standard Scalar function, fit the model using Sklearn, and then save the trained and tested variables. By standardising the variables, the data is scaled and can be used for classification. Table-3 displays the quite accurately, also plotting the ROC (Receiver Operating Characteristics) curve for both Naive Bayes and SVM classifier, and they are shown in Figures 2 and 3 respectively. Comparing diagnostic tests is done using ROC curves, or receiver accuracy that were acquired in our experiment. The results show that our classifier models predict a set of Substitution box power efficiency operating characteristic curve-plot. The absolute true positive rates and the false positive rates are plotted in this graph.

Table-3. Performance result for 16 ×16 optimal S-Boxes.

Classifier	TN	FP	FN	TP	Accuracy %
Naive Bayes	20	1	0	19	97.5
SVM	15	5	0	20	87.5

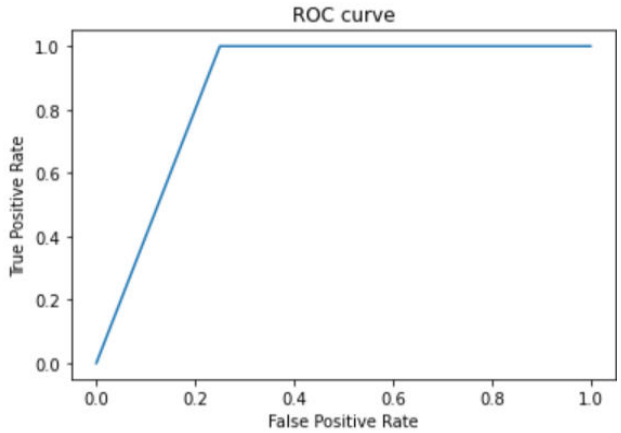

Figure-2. ROC plot for 16 ×16 optimal S-Box for Naïve Bayes Model.

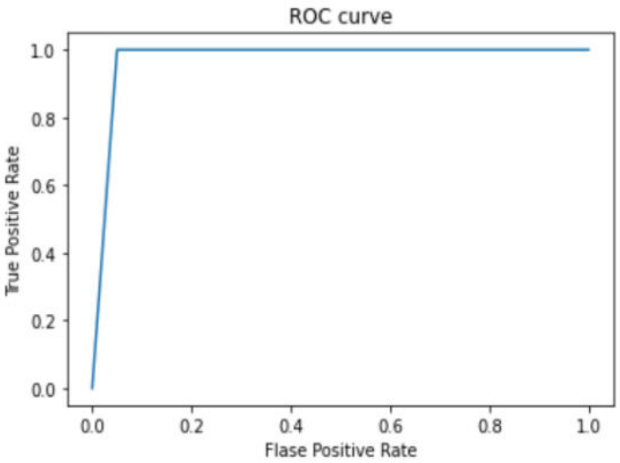

Figure-3. ROC plot for optimal 16 ×16 S-box for SVM model.

5. CONCLUSIONS

In this paper, we provide an automated framework with supervised machine learning support for the power effectiveness report of cryptographically robust S-boxes. The selection of the most power-efficient S-boxes from a large set of 16 ×16 optimal substitution boxes has been done with the help of ML-based algorithms. We have proven the usefulness of our methodology for power efficiency calculation. The experimental outcomes demonstrate that our strategy (using AND-OR-NOT gates) outperforms the conventional way by about 84% for 16 ×16 s-boxes. The performance of the s-box is also validated in the Cadence EDA tool to find the area and power report of 16 ×16 s-boxes.

REFERENCES

[1] Singh, A., Prasad, A., Talwar, Y. Compact and Secure S-Box Implementations of AES-A Review. In: Somani, A. K., Shekhawat, R. S., Mundra, A., Srivastava, S., Verma, V.K. (eds). 2020. Smart Systems and IoT: Innovations in Computing. Smart Innovation. Systems and Technologies, Springer, Singapore, Vol. 141. https://doi.org/10.1007/978-981-13-8406-6_80.

[2] Tillich, S., Feldhofer, M., Popp, T. et al. 2008. Area, Delay, and Power Characteristics of Standard-Cell Implementations of the AES S-Box. Journal of Signal Processing Systems 50, 251-261. https://doi.org/10.1007/s11265-007-0158-2.

[3] V. Nandan, R. Gowri Shankar Rao. 2020. Low-power and area-efficient design of AES S-Box using enhanced transformation method for security application. International Journal of Communication Systems. https://doi.org/10.1002/dac.4308.

[4] Mahajan, Prerna and Abhishek Sachdeva. 2013. A study of encryption algorithms AES, DES and RSA for security. Global Journal of Computer Science and Technology.

[5] Shanthini, M., P. Rajasekar and H. Mangalam. 2014. Design of low power S-box in Architecture Level using GF. International journal of engineering research and general science (IJERG). pp. 1-9.

[6] Baby, Anusuya and Christo Ananth. 2014. S-Box Using AES Technique. International Journal of Engineering Research & Technology (IJERT) 3.3: 285-290.

[7] O. B. Sahoo, D. K. Kole and H. Rahaman. 2012. An Optimized S-Box for Advanced Encryption Standard (AES) Design. International Conference on Advances in Computing and Communications, 2012, pp. 154-157. http://doi.org/10.1109/ICACC.2012.35.

[8] Johannes Wolkerstorfer, Elisabeth Oswald and Mario Lamberger. 2002. An ASIC Implementation of the AES SBoxes. Institute for Applied Information Processing and Communication, Graz University of Technology, Springer-Verlag Berlin Heidelberg.

[9] Sadhukhan, Rajat, Nilanjan Datta and Debdeep Mukhopadhyay. 2019. Power efficiency of s-boxes: From a machine-learning-based tool to a deterministic model. IEEE Transactions on Very Large-Scale Integration (VLSI) Systems. 27.12: 2829-2841.

[10] R. Sadhukhan, N. Datta and D. Mukhopadhyay. 2019. A machine learning based approach to predict power efficiency of S-boxes. in Proc.32nd Int. Conf. VLSI Design, Jan. pp. 531-532. doi: 10.1109/VLSID.2019.00121.

[11] L. Batina et al. 2013. Dietary recommendations for lightweight block ciphers:Power, energy and area analysis of recently developed architectures. Cryptol. ePrint Archive, Tech. Rep. 2013/753, [Online]. Available: https://eprint.iacr.org/2013/753.

[12] R. Sadhukhan, S. Patranabis, A. Ghoshal, D. Mukhopadhyay, V. Saraswat and S. Ghosh. 2017. An evaluation of lightweight block ciphers for resource-constrained applications: Area, performance, and security. J. Hardw. Syst. Security, 1(3): 203-218, http://doi: 10.1007/s41635-017-0021-2.

[13] S. Picek, B. Yang, V. Rozic and N. Mentens. 2016. On the construction of hardware-friendly 4×4 and 5×5 S-boxes. in Selected Areas in Cryptography. Cham, Switzerland: Springer.

[14] F. N. Najm. 1994. A survey of power estimation techniques in VLSI circuits. IEEE Trans. Very Large Scale Integr. (VLSI) Syst. 1(4): 446-455.

[15] B. Mazumdar, D. Mukhopadhyay and I. Sengupta. 2013. Constrained search for a class of good bijective S-boxes with improved DPA resistivity. IEEE Trans. Inf. Forensics Security. 8(12): 2154-2163.

[16] Zhu D., Tong X., Zhang M., Wang Z. 2020. A New S-Box Generation Method and Advanced Design Based on Combined Chaotic System. Symmetry, 12: 2087. https://doi.org/10.3390/sym12122087.

[17] P. Qin, F. Zhou, N. Wu and F. Xian. 2021. A Compact Implementation of AES S-BOX Based on Dual Basis. 2021 IEEE 4th International Conference on Electronics Technology (ICET), pp. 118-122, doi: 10.1109/ICET51757.2021.9451103, 2021.