Lightweight Design Choices for LED-like Block Ciphers

Sumanta Sarkar[1], Habeeb Syed[1], and Rajat Sadhukhan[2] and Debdeep Mukhopadhyay[2]

[1] TCS Innovation Labs, Hyderabad, INDIA
sumanta.sarkar1@tcs.com, habeeb.syed@tcs.com
[2] Indian Institute of Technology, Kharagpur, INDIA
rajatssr835@gmail.com, debdeep.mukhopadhyay@gmail.com

Abstract. Serial matrices are a preferred choice for building diffusion layers of lightweight block ciphers as one just needs to implement the last row of such a matrix. In this work we analyze a new class of serial matrices which are the lightest possible 4×4 serial matrix that can be used to build diffusion layers. With this new matrix we show that block ciphers like LED can be implemented with a reduced area in hardware designs, though it has to be cycled for more iterations. Further, we suggest the usage of an alternative S-box to the standard S-box used in LED with similar cryptographic robustness, albeit having lesser area footprint. Finally, we combine these ideas in an end-end FPGA based prototype of LED. We show that with these optimizations, there is a reduction of 16% in area footprint of one round implementation of LED.

Keywords: MDS matrix, Serial matrix, Recursive Diffusion Layer, Lightweight, S-box, LED.

1 Introduction

Lightweight Cryptography is an area that is focused on research and development of cryptographic algorithms suitable for resource constrained devices like RFID tags, wireless sensors, etc. These kind of devices have very low resource, and as such the usual cryptographic algorithms like AES, RSA etc. are not suitable therein. Internet of Things (IoT) is a network of devices like RFIDs/sensors. Therefore, lightweight cryptography plays a crucial role in securing the data that flows in IoT network. IoT has wide applications, for example, health monitoring, supply chain, defense, etc. Thus low area footprint and high throughput are two key areas of focus in lightweight cryptography. Some known lightweight block ciphers include PRESENT [3], PRINCE [4], CLEFIA [20].

Maximum Distance Separable (MDS) matrices are popular choice to build diffusion layers of block ciphers as they have maximal branch number. Block ciphers such as AES, Twofish, SHARK are some of the well known block cipher using MDS matrices for diffusion. For a square matrix to be MDS it needs to satisfy the condition that its every possible square sub matrix has to be non singular. This requirement makes it challenging to find MDS matrices having efficient implementation in hardware.

In [11] the metric XOR count that measures the implementation cost of a diffusion matrix is introduced. Using this metric one can find MDS matrices which can be efficiently implemented in resource constrained environment. In the recent document produced by NIST [14], the requirement of simpler rounds as a lightweight design principle was emphasized wherein a simple round is iterated over multiple cycles to achieve the desired security. This idea popularized by the lightweight hash function, PHOTON [6] and block cipher, LED [7]. However, it is an open research problem of striving to find further lightweight constructions which can be iterated multiple times to obtain the desired security levels. This method provides an effective mechanism of obtaining lightweight implementations, while not compromising on security, albeit at the cost of extra clock cycles. While for lightweight applications, the gate count of the design is of utmost priority, which can be achieved at the penalty of extra clock cycles, in some applications it may be also a constraint to ensure that the latency does not blow up significantly. This may be important specifically in those environments where energy is also of utmost importance. Hence, it is an interesting research problem of finding lightweight primitives, like linear layers, S-boxes, which can be iterated or cascaded to obtain the same security. On the other hand, the architecture should also amortize the extra latency by employing suitable techniques, which we also strive to find in this work.

In this paper we first explore lightweight recursive MDS layers and show that these diffusion layers can be constructed in terms of serial matrices which have very low XOR count. Known use of 4×4 serial matrices like [6, 7] involve matrices S such that S^4 is MDS. We extend this idea by finding new lightweight serial matrices S for which S^i are MDS for $i > 4$. First we characterize the MDS property of 4×4 serial matrices, where the last row has three 1's (Theorem 1 and Theorem 2). We show specific constructions of these lightweight serial matrices (Theorem 2), and show that there exist a matrix with XOR count of 13 (Corollary 1), which is lesser than that of the lightest serial matrix (used for LED), where the XOR count is 16. However, this new matrix needs to be iterated 8 times, while that for LED needs to be repeated for 4 times. In the subsequent part of the paper, we strive to develop a lightweight design of a LED round in hardware, wherein the twice increase in cycles is amortized by a multiple-clock design. In this design, the linear layer which has much lesser critical path compared to the overall critical path (which also includes the S-box), can be operated by a faster clock compared to the overall cipher. Furthermore, we show that ensuring the same cryptographic strength as that of the LED S-box, one can replace with compositions of smaller non-linear S-boxes which have similar robustness, though at a lesser hardware cost. Finally, we combine these ideas and show that the area can be saved by 16% as compared to the original design. However, our design has 30% higher latency. Note that a major application of lightweight encryption is to secure data in IoT network, where low area footprint is always a key factor. requirement of the other lightweight features like throughput, energy, etc, depends on the applications. For example, if we consider environment monitoring as an IoT application, then we can afford some latency in the encryption algorithm, as this application does not require immediate action upon receiving the data from the environment. However, as the devices are low resourced, it becomes important to decrease the area footprint as low as possible.

Rest of the paper is organized as follows: in Section 2 we recall some introductory results on serial matrices, XOR counts followed by Section 3 in which we present some new recursive MDS matrices defined by extremely lightweight serial matrices. In Section 4 we describe details of implementation of or new primitives in `LED` block cipher and the resulting optimizations.

2 Preliminaries

Here we briefly recall some basic facts about linear diffusion layers and MDS matrices. Denote by $\mathbb{F}_{2^m}$ finite field of size 2^m. For any $x = (x_0, \ldots, x_{n-1}) \in \mathbb{F}_{2^m}^n$ its m-weight $wt_m(x)$ (or simply $wt(x)$ when there no ambiguity) is the count of non zero elements in x. An $n \times n$ linear diffusion layer over m-bit words is a linear map $T : \mathbb{F}_{2^m}^n \longrightarrow \mathbb{F}_{2^m}^n$. Diffusion property of T is measured in terms of *differential branch number* , which is defined as

$$\mathtt{BN}(T) = \min_{x \in \mathbb{F}_{2^m}^n, x \neq 0} \{wt(x) + wt(T\,x)\}.$$

It is well known [5, Ch 9] that $\mathtt{BN}(T) \leq n + 1$ and a diffusion layer that attains the maximum is known as *perfect diffusion layer*[⋆]. Linear diffusion layers are closely connected with MDS codes. Let $\mathcal{C} = [2n, n]$ be a linear code defined over $\mathbb{F}_{2^m}$. Suppose that $[I|C]$ is a generator matrix of $\mathcal{C}$, where I is $n \times n$ identity matrix and C is a non singular matrix of the same size. Such a code is MDS if the minimum distance of the code attains Singleton bound [13], i.e., if the minimum distance is $2n - n + 1 = n + 1$. Note that the matrix C can be used to define an $n \times n$ linear diffusion layer over $\mathbb{F}_{2^m}$ and the code $\mathcal{C}$ is MDS if and only if $\mathtt{BN}(C) = n + 1$. Extending the notion of MDS codes to matrices, we say that the matrix C is MDS if the code $\mathcal{C}$ is MDS. Another independent way of characterizing an MDS matrix is given below which we will be using to check if a given square matrix is MDS:

Fact 1 [13, Ch.4] An $n \times n$ matrix M over $\mathbb{F}_{2^m}$ is MDS if and only if every square submatrix of M is nonsingular.

2.1 XOR Counts

The finite field $\mathbb{F}_{2^m}$ is also a m dimensional vector space over $\mathbb{F}_2$. This vector space has several bases but we use only the polynomial basis given by

[⋆] The term "perfect diffusion layer" was coined by Vaudenay in [22] wherein he suggested for the first time that MDS matrices can be used to design linear diffusion layers.

$\{\alpha, \alpha^2, \ldots, \alpha^{m-1}\}$ where α is the root of the irreducible polynomial that defines $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$. The notion of XOR count defined below, was introduced in [11] to measure the cost of field multiplication in $\mathbb{F}_{2^m}$.

Definition 1. *Let $\mathcal{B}$ be a vector space basis of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$. For any $a \in \mathbb{F}_{2^m}$ the* XOR *count of a with respect to $\mathcal{B}$ is denoted by* $\mathrm{XOR}\,(a)$ *and is defined as the number of* XOR*s needed to implement the field multiplication of a with an arbitrary element $b \in \mathbb{F}_{2^m}$*

Though the XOR count of a depends on basis of $\mathbb{F}_{2^m}$, we simply denote it by $\mathrm{XOR}\,(a)$ whenever there is no ambiguity. Using this metric one can find diffusion matrices which can be efficiently implemented.

The linear diffusion layers in block ciphers are defined by MDS matrices. In [11] the notion of XOR count of an element was extended to XOR count of a row of a matrix. Suppose R_i is a row $R_i = (\beta_{i,0}, \ldots, \beta_{i,n-1}) \in \mathbb{F}_{2^m}^n$ of a matrix. Denote by ρ_i the number of non zero entries in R_i, then the XORs needed to implement row R_i is given by

$$\sum_{j=0}^{n-1} \mathrm{XOR}\,(\beta_{i,j}) + (\rho_i - 1) \cdot m. \tag{1}$$

This notion of XOR count was further extended to the full matrix in [18] as

$$\mathrm{XOR}\,(M) = \sum_{i=0}^{n} \sum_{j=0}^{n-1} \mathrm{XOR}\,(\beta_{i,j}) + \sum_{i=0}^{n} (\rho_i - 1) \cdot m, \tag{2}$$

where M is an $n \times n$ matrix over $\mathbb{F}_{2^m}$. In this paper we are mainly focused on Serial matrices, in which we only need to know the cost of the last row (1).

Based on the notion of XOR count several works followed [12,17,21] in order to obtain MDS matrices with low XOR counts. For instance, [18] showed the minimum value of XOR count that 4×4 MDS matrices can have over $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$. Recently [19] presented 8×8 MDS MDS matrices with the lowest known XOR counts over $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$.

3 Recursive MDS Matrices

A serial matrix of order $n \times n$ over $\mathbb{F}_{2^m}$ is a matrix of the form

$$\mathrm{S} = \begin{bmatrix} 0 & 1 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & \ldots & 1 \\ a_0 & a_1 & \ldots & a_{n-1} \end{bmatrix}, \tag{3}$$

which is usually denoted by $\mathrm{S} = \mathrm{Serial}\,(a_0, \ldots, a_{n-1})$. The matrix S is companion matrix of the monic polynomial $a_0 + a_1X + \ldots + a_{n-1}X^{n-1} + X^n \in \mathbb{F}_{2^m}[X]$ with $a_0 \neq 0$. One can easily see that inverse of S is

$$\mathrm{S}^{-1} = \begin{bmatrix} \frac{a_1}{a_0} & \frac{a_2}{a_0} & \ldots & \frac{a_{n-1}}{a_0} & \frac{1}{a_0} \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ldots & \vdots & \\ 0 & 0 & \ldots & 1 & 0 \end{bmatrix}. \tag{4}$$

By a recursive MDS matrix we mean a MDS matrix M such that $M = \mathrm{S}^i$ for some serial matrix S and positive integer i. Recursive MDS matrices are a preferred choice for diffusion layers in lightweight cryptography as only the last row of such a matrix needs to be implemented. However, the downside is that it causes latency since the output of diffusion layer is obtained by applying S recursively as

$$(y_0, \ldots, y_{n-1}) = \underbrace{\mathrm{S} \ldots (\mathrm{S}}_{i \text{ times}}\,(x_0, \ldots, x_{n-1}))\ldots). \tag{5}$$

An additional advantage of using recursive MDS matrix in block cipher is that its inverse also has simple form (as in (4)) and can be implemented efficiently.

Several techniques have been proposed to construct recursive diffusion layers. In [1, 16, 23] authors presented construction of recursive diffusion layers using binary linear maps instead of matrices defined over $\mathbb{F}_{2^m}$. Later Augot and Finiasz constructed recursive MDS matrices from shortened BCH codes [2] following which more general characterization of Recursive MDS matrices is presented in [8,9]. In [10] authors discussed construction of 4×4 MDS matrices from serial matrices defined over sets of the form $\{1, \alpha, \alpha^2, \alpha + 1\} \subset \mathbb{F}_{2^m}$.

3.1 Lightweight Recursive MDS Matrices

If $\mathrm{S} = \mathrm{Serial}\,(a_0, \ldots, a_{n-1})$ is an $n \times n$ serial matrix defined over $\mathbb{F}_{2^m}$ then it is easy to see that the least possible value of i for which S^i is MDS is $i = n$. Consequently while constructing such MDS matrices the usual practice is to find an $n \times n$ serial matrices S for which S^n is MDS. This is done mainly to minimize throughput latency: If S^i is MDS then we need i iterations to compute the output $y = (\mathrm{S}^i) \cdot x$ (see (5)) and hence optimal throughput is achieved when $i = n$. However, it is possible to find new lightweight serial matrices S such that S^i is MDS if we assume $i \geq n$.

In this section we present some new lightweight recursive MDS matrices which have not been analyzed so far. To begin we briefly recall some terminology from [2] which will be useful in presenting new results. Suppose $\mathrm{S} = \mathrm{Serial}\,(a_0, \ldots, a_{n-1})$ be the companion matrix of the polynomial $f(X) = a_0 + a_1X + \ldots + a_{n-1}X^{n-1} + X^n$ defined over $\mathbb{F}_{2^m}$. We can interpret the matrix S as

$$\mathrm{S} = \begin{bmatrix} 0 & 1 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & 1 \\ a_0 & a_1 & \dots & a_{n-1} \end{bmatrix} = \underbrace{\begin{bmatrix} X \\ X^2 \\ \vdots \\ X^{n-1} \\ X^n \bmod f(X) \end{bmatrix}}_{(*)} \tag{6}$$

where elements of each row in the matrix $(*)$ consists of coefficients of the polynomial given in that row. With these notations it is easy to see that for any $i \geq 1$ the matrix S^i is given by

$$\mathrm{S}^i = \begin{bmatrix} X^i \bmod f(X) \\ X^{i+1} \bmod f(X) \\ \vdots \\ X^{i+(n-1)} \bmod f(X) \end{bmatrix}. \tag{7}$$

Recall that in general one is interested in $n \times n$ serial matrices S for which S^n is MDS in order to optimize the throughput. However in many cases it is not possible to obtain such MDS matrices. In the following we identify two such classes.

Lemma 1. *Let $n \geq 4$ and $\mathrm{S} = \mathrm{Serial}\,(a_0, \dots, a_{n-1})$, be defined over $\mathbb{F}_{2^m}$. Then S^n is not* MDS *if $a_{n-1} = a_{n-2} = 1$ or $a_{n-1} = a_{n-3} = 1$.*

Proof. Suppose $f(X) = a_0 + \ldots + a_{n-1}X^{n-1} + X^n$ be the the polynomial associated with the matrix S. We define c, c_i as follows. Let $c = a_{n-1}^2 + a_{n-2}$ and for $i = 0, \dots, n-3$,

$$c_i = a_i \cdot a_{n-1} + a_{i-1}, \tag{8}$$

where we use the convention that $a_i = 0$ for $i < 0$. Using these notations one can check that

$$X^{n+2} \bmod f(X) = a_0 \cdot c + \sum_{i=1}^{n-2} (a_i\, c + c_{i-1})X^i + (a_{n-1}^3 + a_{n-3})X^{n-1}. \tag{9}$$

From (7) it follows that the coefficients occurring in above polynomial form third row in the matrix S^n. If $a_{n-1} = a_{n-2} = 1$ then we get that $c = 0$ and consequently the matrix S^n is not MDS. Similarly if $a_{n-1} = a_{n-3} = 1$ then the coefficient of X^{n-1} in (9) becomes zero and the matrix S^n is not MDS. □

Lemma 2. *Let $\mathrm{S} = \mathrm{Serial}\,(a_0, \dots, a_{n-1})$ be a matrix defined over $\mathbb{F}_{2^m}$. Then S^n is not* MDS *if $a_{i-1} = a_i = a_{n-1} = 1$ for any $i = 1, \dots, n-2$*

Proof. Using c_i as in (8) we have

$$X^{n+1} \bmod f(X) = a_0 a_{n-1} + \sum_{i=1}^{n-2} c_i X^i + (a_{n-1}^2 + a_{n-2})X^{n-1} \tag{10}$$

coefficients of which occur as second row in the matrix S^n. Here we have defined c_{n-2} precisely as in (8). If $a_{i-1} = a_i = a_{n-1} = 1$ for any $i = 1, \ldots, n-2$ then $c_i = 0$ and hence the matrix S^n is not MDS. □

While searching for lightweight recursive MDS matrices one would like to consider the lightest possible serial matrix, $\mathrm{S} = \mathrm{Serial}\,(1, \ldots, 1)$ which consists of only '1' as entries. However, one can easily check that in this case S^i is not MDS for any $i \geq 1$. We state this observation as a fact:

Fact 2. Let $\mathrm{S} = \mathrm{Serial}\,(1, \ldots, 1)$ be an $n \times n$ be defined over $\mathbb{F}_{2^m}$. Then S^i is not MDS for any $i \geq 1$.

Following Fact 2, the lightest possible recursive matrix could be of the form $\mathrm{S} = \mathrm{Serial}\,(a_0, \ldots, a_{n-1})$ where $a_i \neq 1$ for some $0 \leq i \leq n-1$ and $a_j = 1$ for every $0 \leq j \neq i \leq n-1$. Our objective is to find the lightest possible such matrix for which S^i is MDS with the minimum $i \geq n$.

In practice size of the diffusion matrix used in a lightweight block cipher is 4×4. Keeping this in mind we fix $n = 4$ in the remaining part of this Section. In [10] authors show that if $\mathrm{S} = \mathrm{Serial}\,(a_0, a_1, a_2, a_3)$ is such that $a_i = 1$ for more than 2 values of i then S^4 is never MDS over $\mathbb{F}_{2^m}$. If we relax the condition that S^4 need to be MDS and consider matrices such that S^i is MDS for $i > 4$, then we get new serial matrices which are the lightest possible. In the following we analyze MDS property of S^i, where $S = \mathrm{Serial}\,(a_0, a_1, a_2, a_3)$ such that $a_i = 1$ for 3 values of i

Theorem 1. *Let* $\mathrm{S} = \mathrm{Serial}\,(a_0, a_1, a_2, a_3)$ *be a serial matrix defined over* $\mathbb{F}_{2^m}$ *in which* $a_i = 1$ *for precisely* 3 *values of* i*. For* $1 \leq i \leq 8$ *the matrices* S^i *are not* MDS *if*

(i) $\mathrm{S} = \mathrm{Serial}\,(a, 1, 1, 1)$
(ii) $\mathrm{S} = \mathrm{Serial}\,(1, a, 1, 1)$
(iii) $\mathrm{S} = \mathrm{Serial}\,(1, 1, 1, a)$,

where $a \notin \{0, 1\}$.

Proof. Let $\mathrm{S} = \mathrm{Serial}\,(a_0, a_1, a_2, a_3)$ be a serial matrix defined over $\mathbb{F}_{2^m}$. From (7) it follows directly that for $i = 1, 2, 3$ the matrix S^i has 0 entries and hence cannot be MDS. Remains to show that S^i is not MDS for $4 \leq i \leq 8$ whenever S is in any of the form (i),(ii),(iii) as given in theorem. We do this by considering each form separately. In the following we denote the polynomial associated with the serial matrix S by $f(X)$

Case 1. $\mathrm{S} = \mathrm{Serial}\,(a, 1, 1, 1),\ a \notin \{0, 1\}$.
The polynomial corresponding to the serial matrix S is $f(X) = a + X + X^2 + X^3 + X^4$ from which it follows that

$$X^7 \bmod f(X) = 0 + 0 \cdot X + a\,X^2 + (a+1)\,X^3.$$

Note that this polynomial has zero coefficients and that these coefficients form a row in the matrices S^i for $4 \leq i \leq 7$ as can be seen from (7). Consequently none of these matrices can be MDS. Using same argument we see that the matrix S^8 cannot be MDS because the coefficients of

$$X^{10} \bmod f(X) = a^2 + 0 \cdot T + (a^2+1) \cdot T^2 + 0 \cdot T^3.$$

form a row in this matrix.
Case 2. $\mathrm{S} = \mathrm{Serial}\,(1, a, 1, 1),\ a \notin \{0, 1\}$.
In this case we see that

$$X^7 \bmod f(X) = (a+1) + (a^2+a) \cdot X + a \cdot X^2 + 0 \cdot X^3, \quad \text{and} \tag{11a}$$
$$X^8 \bmod f(X) = 0 + (a+1) \cdot X + (a^2+a) \cdot X^2 + a \cdot X^3. \tag{11b}$$

Using the argument as in Case 1 we see that the matrices S^i cannot be MDS for $4 \le i \le 7$ because of zero coefficients in (11a) and the matrix S^8 cannot be MDS because of zero coefficients in (11b).
Case 3. $\mathrm{S} = \mathrm{Serial}\,(1, 1, 1, a),\ a \notin \{0, 1\}$.
Unlike previous cases, here all the matrices S^i contain non zero entries for $4 \le i \le 8$. However each of this matrix has a 2×2 singular submatrix. To prove this first note that

$$X^7 \bmod f(X) = a^3 + 1 + (a^3+a^2)X + (a^3+a^2+a)X^2 + (a^4+a^2)X^3 \tag{12a}$$
$$\begin{aligned} X^8 \bmod f(X) = a^4 + a^2 + (a^4+a^3+a^2+1)X + \\ (a^4+a^3)X^2 + (a^5+a^2+a)X^3 \end{aligned} \tag{12b}$$

For $i \ge 1$ let $R_i = (r_{i,0}, r_{i,1}, r_{i,2}, r_{i,3})$ where $r_{i,j}$ is the Coefficient of X^j in the polynomial $(X^i \bmod f(X))$. Using (7) we know that R_7, R_8 occur as two consecutive rows in the matrices S^i for $i = 5, 6, 7$. From (12a) and (12b) it is easy to see that $r_{7,0}r_{8,2} + r_{8,0}r_{7,2} = 0$ which implies that the matrices S^i have a 2×2 singular submatrix for $i = 5, 6, 7$ and hence are not MDS matrices. Finally it remains to show that S^8 is also not MDS. We have

$$\begin{aligned} X^{10} \bmod f(X) = (a^6+a^4+a^2) + (a^6+a^5+a^4+a)X + \\ (a^6+a^5+a^2+a)X^2 + (a^7+a^4+a+1)X^3 \end{aligned} \tag{13}$$

and

$$\begin{aligned} X^{11} \bmod f(X) = a^7 + a^4 + a + 1 + (a^7+a^6+a^2+a+1)X + \\ (a^7+a^6+a^5+1)X^2 + (a^8+a^6)X^3 \end{aligned} \tag{14}$$

The rows R_{10}, R_{11} occur in the matrix S^8 and from (13) and (14) we see that the sub matrix

$$\begin{bmatrix} r_{10,1}, & r_{10,2} \\ r_{11,1}, & r_{11,2} \end{bmatrix} \tag{15}$$

is a singular submatrix of S^8 making it non MDS. □

Theorem 2. *Let* $\mathrm{S} = \mathrm{Serial}\,(1, 1, a, 1)$ *be defined over* $\mathbb{F}_{2^m}$*, then* S^i *is not* MDS *for* $1 \le i \le 7$*. Further,* S^8 *is* MDS *precisely in either the following two cases:*

(1) *If the minimal polynomial of a over $\mathbb{F}_2$ is $X^4 + X + 1$*
(2) *If the degree of the minimal polynomial of a over $\mathbb{F}_2$ is ≥ 5 and the minimal polynomial is not in the set $\{\, X^5 + X^4 + X^2 + X + 1,\ X^5 + X^3 + X^2 + X + 1,\ X^5 + X^4 + X^3 + X^2 + 1\}$*

Proof. Let $f(x) = 1 + x + a\,x^2 + x^3 + x^4$ be the associated polynomial of the serial matrix $\mathrm{S} = \mathrm{Serial}\,(1, 1, a, 1)$ from which we can easily see that

$$x^7 \bmod f(x) = 0 + (a+1)\,x + a\,x^2 + (a^2 + a)\,x^3.$$

Using the argument as in Case 1 of Theorem 1 we conclude that S^i is not MDS for $1 \leq i \leq 7$.

To prove the remaining part of the theorem denote by $\mathrm{S}(x)$ the matrix of the form $\mathrm{Serial}\,(1, 1, x, 1)$ where x is an indeterminate. Let Δ_i be the set of determinants of all of the $i \times i$ submatrices of $\mathrm{S}^8(x)$. We have

$$\begin{aligned}
\Delta_1 = \{&x^3 + x^2 + x, x^3 + x^2 + x + 1, x^4 + 1, x^2, x^2 + 1, x,\\
&x^4 + x^2, x^2 + x, x^3 + x + 1\}\\
\Delta_2 = \{&x^6 + x^5 + x + 1, x^5 + x^4 + x, x^5 + x^3 + x^2 + 1, x^5 + x^3 + x,\\
&x^6 + x^4 + 1, x^6 + x^2, x^4 + x^2, x^4 + x^3, x^7 + x^6 + x^5 + x^3 + x + 1,\\
&x^5 + x, x^6 + x^4 + x^3 + x^2 + x, x^6, x^4 + 1, x^6 + x^5 + x^4 + x,\\
&x^7 + x^5 + x^3 + x, x^5 + x^4 + x^3 + x, x^8 + x^6 + x^2 + 1, x^7 + x^6 + x^3 + 1\}\\
\Delta_3 = \{&x^3 + x^2 + x, x^3 + x^2 + x + 1, x^4 + 1, x^2, x^2 + 1, x, x^4 + x^2, x^2 + x, x^3 + x + 1\}\\
&\text{and } \Delta_4 = \{1\}.
\end{aligned}$$

Denote by Δ the set of irreducible factors of polynomials in $\Delta_1 \cup \Delta_2 \cup \Delta_3$. It is easy to see that,

$$\begin{aligned}
\Delta = \{&x, x + 1, x^2 + x + 1, x^3 + x + 1, x^3 + x^2 + 1,\\
&x^4 + x^3 + 1, x^4 + x^3 + x^2 + x + 1,\\
&x^5 + x^4 + x^2 + x + 1, x^5 + x^3 + x^2 + x + 1, x^5 + x^4 + x^3 + x^2 + 1\}
\end{aligned}$$

Now, if we consider the matrix $\mathrm{S}(a)$ for some $a \in \mathbb{F}_{2^m}$ then $\mathrm{S}(a)^8$ is MDS if and only if $\delta(a) \neq 0$ for every $\delta(x) \in \Delta$. One can check that this happens precisely in either the two cases (1), (2) stated in statement of theorem. □

Corollary 1. *The matrix* $\mathrm{S} = \mathrm{Serial}\,(1, 1, \alpha, 1)$ *defined over $\mathbb{F}_{2^4}$, where α is a root of irreducible polynomial $X^4 + X + 1$ is the lightest serial matrix such that* S^8 *is* MDS*, and* $\mathrm{XOR}\,(\mathrm{S}) = 13$.

Proof. As $\mathrm{Serial}\,(1, 1, 1, 1)$ can never be MDS for any $(\mathrm{Serial}\,(1, 1, 1, 1))^i$, thus the next possibility that $(\mathrm{Serial}\,(a_0, a_1, a_2, a_3))^8$ is MDS when it is of the form $\mathrm{Serial}\,(1, 1, a, 1)$ for some $a \notin \{0, 1\}$. The element α which is a root of $X^4 + X + 1 = 0$ has the lowest nonzero XOR count which is 1. This results in that S is the lightest serial matrix such that S^8 is MDS, and $\mathrm{XOR}\,(\mathrm{S}) = 13$. □

4 Lightweight Architecture for Block Ciphers: A case study on `LED`

In this section, we will describe the hardware implementation of datapath of typical AES-like block ciphers. We consider the particular instance of `LED`, though the idea can be generalized for a larger class of block ciphers having an MDS block as diffusion layer. Along with implementing the above discussed lightweight linear layer, we focus on two other important aspects: 1) the design of the non-linear S-box, and 2) the overall composition of the layers to ensure that the two-fold increase in the iteration requirement of the modified linear layer does not lead to a double increase in the latency. We start with discussion on the the non-linear S-box.

We have implemented the datapath of `LED`, using an ASIC design flow. We have used *Synopsys Design Compiler(version: vI-2013.12-SP5-4)* for synthesis and *Synopsys VCS(version: I-2014.03-SP1-1)* for simulation. Standard cell library*(TSL18FS120)* on 180nm technology from *TowerSemiconductor Ltd.* is used during synthesis, which is characterized using *SiliconSmart Software (version: 2008.02-SP1p1)* under *Fast-Fast process(P)*, *1.98V voltage(V)* and *-40 degree C temperature(T)*.

4.1 Choosing an efficient 4 × 4 S-box

The 4×4 S-box that is used in `LED` has nonlinearity 4, differential uniformity 4, and algebraic degree 3. The polynomial expression over $\mathbb{F}_{2^4}$ of this S-box is

$$(\alpha^3+\alpha^2+1)x^{14}+(\alpha^3+\alpha^2+1)x^{13}+(\alpha^3+\alpha^2)x^{12}+(\alpha^3+\alpha^2+\alpha)x^{11}$$

$$+(\alpha^3+1)x^{10}+(\alpha^3+1)x^9+(\alpha^2+\alpha+1)x^8+\alpha^2x^7+(\alpha^3+\alpha^2)x^6$$

$$+(\alpha^3+\alpha)x^5+(\alpha^3+\alpha^2+\alpha)x^4+(\alpha^2+\alpha+1)x^3+(\alpha^2+\alpha+1)x^2+\alpha^3+\alpha^2,$$

where α is a primitive root of $X^4+X+1=0$. Instead an S-box which is monomial would have low hardware footprint. The monomials $X \mapsto X^i$ for $i = 7, 11, 13, 14$, are such that the associated 4×4 S-box has nonlinearity 4, differential uniformity 4, and algebraic degree 3. We consider such monomial with the least i, i.e., $X \mapsto X^7$. As this S-box has fixed points: $0 \mapsto 0$, $1 \mapsto 1$, etc., we consider $X \mapsto X^7+1$. The associated S-box will thus not have any fixed points, while the other cryptographic properties like nonliearity, differential uniformity, degree remain invariant. The proposed S-box values are shown in Table 4.1.

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(x)	1	0	A	C	8	F	7	6	D	4	9	2	E	3	5	B

Table 1. S-box defined by $X \mapsto X^7+1$

We also evaluate that the implementation cost of this S-box is lesser than that of LED. We implement the proposed S-box function as $X^7 = X^4 \times X^2 \times X$, which requires 2 nibble wise multiplication operation, 1 square and 1 fourth power calculation followed by one bit XOR . We did not not choose $X^7 = X^4 \times X^3$, as X^3 is heavier than the 2 multiplication operations in case of the former decomposition. Our proposed 4×4 S-box occupies $359um^2$ area, which is 28.6 GE. Here 1 GE is the area required for one 2-input NAND gate. A 2-input lowest drive NAND gate of our library occupies 12.544 um^2 area. This design may be compared with the standard look-up table based LED S-box implementation occupies $391um^2$, which is 31.2 GE, which is 9% more than the proposed S-box. We compare the two designs with respect to both cryptographic strengths and area requirement using the S-Box Evaluation Tool (SET) [15] tool in Table 4.1. It may be observed that we have reduced the hardware overhead of the non-linear layer using our proposed method without compromising on security parameters like non-linearity, differential uniformity and degree of a typical 4×4 S-box as used in LED.

Property	**Proposed S-box**	LED **S-box**
Nonlinearity	4	4
Algebraic Degree	3	3
Algebraic Immunity	2	2
Differential Uniformity	4	4
Robustness to Differential Cryptanalysis	0.750	0.750
Silicon Area	359 um^2	391 um^2

Table 2. S-box Properties as Evaluated by S-Box Evaluation Tool

4.2 Implementing Lightweight Serial Matrix

In this section we describe the implementation strategy of our new lightweight MDS matrix and compare it with existing MDS matrix used in LED. Denote by S_1 the serial matrix Serial $(\alpha^2, 1, \alpha, \alpha)$ which is the existing diffusion matrix of LED block cipher. This matrix is considered to be lightest which has XOR $(\mathrm{S}_1) = 16$ with S_1^4 being MDS. We implemented $\mathrm{S}_1 \times X$, where $X = [x_1, x_2, x_3, x_4]^t$ is a column vector, each element x_i of the vector is a nibble. This implementation has hardware footprint $387.5um^2$ (31 GE) comprising of six 3-input XOR gates and two 2-input XOR gates.

Next consider the serial matrix $\mathrm{S}_2 = $ Serial $(1, 1, \alpha, 1)$ as given in Corollary 1. This serial matrix is lighter than S_1 with XOR cost 13, using which MDS matrix is calculated as S_2^8. Similar to the implementation of S_1, we implemented $\mathrm{S}_2 \times X$, and hardware footprint reported by the synthesis tool is $365.4um^2$ (29 GE) comprising of five 3-input XOR gates and three 2-input XOR gates.

We design the entire data-path of LED using proposed transformation and the overall design results show compaction. The critical path length and the overall area of the linear layer and the entire data-path is shown in Table 3 below. From the table it can be seen that there is saving of 16% area in the proposed datapath (1044.6 GE) compared to the original LED datapath (1244.2 GE). However, one may argue that in the proposed linear layer result obtained by computing $S_2^8 \times X$, (X is the state matrix) requiring 8 clock cycles, whereas in the original LED design the linear layer result is obtained from $S_1^4 \times X$ which requires only 4 clock cycles. So it may seem that the new design incurs twice latency compared to the original design for one round implementation. Our proposed S-box takes lesser time to execute, notably, delay for the S-box and shift row combined is 2.47 ns for LED, whereas for the new design it is just 1.63 ns. This helps reduce the overall delay in our design not reaching the double the delay of LED. Then overall latency of the LED is $0.61 \times 4 + 2.47 = 4.91$ ns, while that for the new design it is $0.61 \times 8 + 1.63 = 6.51$ ns. Thanks to lower latency incurred by the S-box, the overall increase in latency of the new design is capped at 30%.

In IoT applications low area footprints is always a factor, whereas in some applications like environment monitoring some latency is affordable. So, for these class of applications our design has very high impact.

Design	$\mathbf{Cr}_{\text{datapath}}$(ns)[**]	$\mathbf{Cr}_{\text{linearlayer}}$(ns)	$\mathbf{A}_{\text{datapath}}$ (GE)	$\mathbf{A}_{\text{linearlayer}}$ (GE)
LED	3.08	0.61	1244.2	123.56
Our Design	2.24	0.61	1044.6	116.5

Table 3. Area and Critical Path Time Comparison for one round implementation of our design and LED

4.3 Restraining Latency by Double Clock Architecture

The new lightweight MDS matrix S_2 requires 8 iterations to compute the full effect of diffusion layer since S_2^8 is MDS. Compared to original matrix S_1 which needs 4 iterations the matrix S_2 increases latency. We now describe a solution for reducing the latency caused by our serial matrix implementation. If the user wants to have very low area footprint like our design, and also wants to have low latency, then following is our suggestion. One can use double clock architecture to check the latency of the new design. We present this in Figure 1. The figure shows the operation of the serial matrix is done at a clock clk2 which is faster than clk1, rests of the operations are done at clk1. With this architecture we can curb the latency and at the same time can benefit from the low area cost.

[**] This latency is due to one iteration of serial matrix along with S-box implementation and shift row operation.

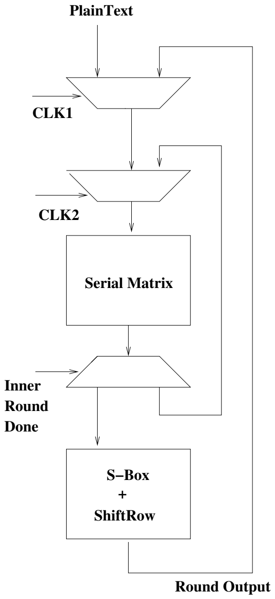

Fig. 1. Datapath Design of our Proposed Method

5 Conclusions

Latency is inherent to the block ciphers whose diffusion layer is based on serial matrices. In this work we have shown that if we relax latency slightly, then we can further reduce the implementation cost of the diffusion layer. We have applied our newly discovered matrix in the diffusion layer of LED, and on top of that we also have proposed a lighter S-box. The combining effect of these two is that we have obtained a variant of LED which is lighter than the original one. We also have proposed a multi-clock design of the LED data-path which can be used to restrain increase in the latency.

Our diffusion matrix opens up the applicability of an $n \times n$ serial matrix S in lightweight block ciphers, such that S^i is MDS for $i > n$. On the other hand, the proposed multi-clock architecture is also interesting to explore further.

References

1. D. Augot and M. Finiasz. Exhaustive Search for Small Dimension Recursive MDS Diffusion Layers for Block Ciphers and Hash Functions. In *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on*, pages 1551–1555. IEEE, 2013.
2. D. Augot and M. Finiasz. Direct Construction of Recursive MDS Diffusion Layers using Shortened BCH Codes. In *International Workshop on Fast Software Encryption*, pages 3–17. Springer, 2014.
3. A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe. PRESENT: An Ultra-Lightweight Block Cipher. In P. Paillier and I. Verbauwhede, editors, *Cryptographic Hardware and Embedded Systems - CHES 2007*, volume 4727 of *LNCS*, pages 450–466. Springer, 2007.
4. J. Borghoff, A. Canteaut, T. Güneysu, E. B. Kavun, M. Kneževic, L. R. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechberger, P. Rombouts, S. ren S. Thomsen, and T. Y. in. PRINCE - A Low-latency Block Cipher for Pervasive Computing Applications (Full version). Cryptology ePrint Archive, Report 2012/529, 2012. `http://eprint.iacr.org/`.
5. J. Daemen and V. Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Information Security and Cryptography. Springer, 2002.
6. J. Guo, T. Peyrin, and A. Poschmann. The PHOTON Family of Lightweight Hash Functions. In P. Rogaway, editor, *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*, volume 6841 of *Lecture Notes in Computer Science*, pages 222–239. Springer, 2011.
7. J. Guo, T. Peyrin, A. Poschmann, and M. J. B. Robshaw. The LED Block Cipher. In B. Preneel and T. Takagi, editors, *Cryptographic Hardware and Embedded Systems - CHES 2011*, volume 6917 of *LNCS*, pages 326–341. Springer, 2011.
8. K. C. Gupta, S. K. Pandey, and A. Venkateswarlu. On the Direct Construction of Recursive MDS Matrices. *Designs, Codes and Cryptography*, 82(1-2):77–94, 2017.
9. K. C. Gupta, S. K. Pandey, and A. Venkateswarlu. Towards a General Construction of Recursive MDS Diffusion Layers. *Designs, Codes and Cryptography*, 82(1-2):179–195, 2017.
10. K. C. Gupta and I. G. Ray. On Constructions of MDS Matrices from Companion Matrices for Lightweight Cryptography. In *International Conference on Availability, Reliability, and Security*, pages 29–43. Springer, 2013.
11. K. Khoo, T. Peyrin, A. Y. Poschmann, and H. Yap. FOAM: Searching for Hardware-Optimal SPN Structures and Components with a Fair Comparison. In L. Batina and M. Robshaw, editors, *Cryptographic Hardware and Embedded Systems - CHES 2014*, volume 8731 of *Lecture Notes in Computer Science*, pages 433–450. Springer Berlin Heidelberg, 2014.
12. M. Liu and S. M. Sim. Lightweight MDS Generalized Circulant Matrices. In T. Peyrin, editor, *Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers*, volume 9783 of *Lecture Notes in Computer Science*, pages 101–120. Springer, 2016.
13. F. J. Macwilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes (North-Holland Mathematical Library)*. North Holland, January 1983.
14. K. A. McKay, L. Bassham, M. S. Turan, and N. Mouha. `NISTIR 8114`, 2017. Report on Lightweight Cryptography, `http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8114.pdf`.

15. S. Picek, L. Batina, D. Jakobović, B. Ege, and M. Golub. S-box, SET, Match: A Toolbox for S-box Analysis. In D. Naccache and D. Sauveron, editors, *8th IFIP International Workshop on Information Security Theory and Practice (WISTP)*, volume LNCS-8501 of *Information Security Theory and Practice. Securing the Internet of Things*, pages 140–149, Heraklion, Crete, Greece, June 2014. Springer. Part 5: Short Papers.
16. M. Sajadieh, M. Dakhilalian, H. Mala, and P. Sepehrdad. Recursive Diffusion Layers for Block Ciphers and Hash Functions. In *Fast Software Encryption*, pages 385–401. Springer, 2012.
17. S. Sarkar and S. M. Sim. A Deeper Understanding of the XOR Count Distribution in the Context of Lightweight Cryptography. In D. Pointcheval, A. Nitaj, and T. Rachidi, editors, *Progress in Cryptology - AFRICACRYPT 2016 - 8th International Conference on Cryptology in Africa, Fes, Morocco, April 13-15, 2016, Proceedings*, volume 9646 of *Lecture Notes in Computer Science*, pages 167–182. Springer, 2016.
18. S. Sarkar and H. Syed. Lightweight Diffusion Layer: Importance of Toeplitz Matrices. *IACR Trans. Symmetric Cryptol.*, 2016(1):95–113, 2016.
19. S. Sarkar and H. Syed. Analysis of Toeplitz MDS Matrices. Cryptology ePrint Archive, Report 2017/368, 2017. `http://eprint.iacr.org/2017/368`.
20. T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata. The 128-Bit Blockcipher CLEFIA (Extended Abstract). In A. Biryukov, editor, *Fast Software Encryption, 14th International Workshop, FSE 2007, Luxembourg, Luxembourg, March 26-28, 2007, Revised Selected Papers*, volume 4593 of *Lecture Notes in Computer Science*, pages 181–195. Springer, 2007.
21. S. M. Sim, K. Khoo, F. Oggier, and T. Peyrin. Lightweight MDS Involution Matrices. In G. Leander, editor, *Fast Software Encryption*, volume 9054 of *Lecture Notes in Computer Science*, pages 471–493. Springer Berlin Heidelberg, 2015.
22. S. Vaudenay. On the Need for Multipermutations: Cryptanalysis of MD4 and SAFER. In *Fast Software Encryption*, pages 286–297. Springer, 1995.
23. S. Wu, M. Wang, and W. Wu. Recursive Diffusion Layers for (lightweight) Block Ciphers and Hash Functions. In L. R. Knudsen and H. Wu, editors, *Selected Areas in Cryptography: 19th International Conference, SAC 2012, Windsor, ON, Canada, August 15-16, 2012, Revised Selected Papers*, pages 355–371, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.