A deeper understanding of the XOR count distribution in the context of lightweight cryptography

Sumanta Sarkar[1] and Siang Meng Sim[2]

[1] TCS Innovation Labs, Hyderabad, INDIA
[2] Nanyang Technological University, SINGAPORE
sumanta.sarkar1@tcs.com, ssim011@e.ntu.edu.sg

Abstract. In this paper, we study the behavior of the XOR count distributions under different bases of finite field. XOR count of a field element is a simplified metric to estimate the hardware implementation cost to compute the finite field multiplication of an element. It is an important criterion in the design of lightweight cryptographic primitives, typically to estimate the efficiency of the diffusion layer in a block cipher. Although several works have been done to find lightweight MDS diffusion matrices, to the best of our knowledge, none has considered finding lightweight diffusion matrices under other bases of finite field apart from the conventional polynomial basis. The main challenge for considering different bases for lightweight diffusion matrix is that the number of bases grows exponentially as the dimension of a finite field increases, causing it to be infeasible to check all possible bases. Through analyzing the XOR count distributions and the relationship between the XOR count distributions under different bases, we find that when all possible bases for a finite field are considered, the collection of the XOR count distribution is invariant to the choice of the irreducible polynomial of the same degree. In addition, we can partition the set of bases into equivalence classes, where the XOR count distribution is invariant in an equivalence class, thus when changing bases within an equivalence class, the XOR count of a diffusion matrix will be the same. This significantly reduces the number of bases to check as we only need to check one representative from each equivalence class for lightweight diffusion matrices. The empirical evidence from our investigation says that the bases which are in the equivalence class of the polynomial basis are the recommended choices for constructing lightweight MDS diffusion matrices.

Key words: lightweight cryptography, finite field multiplication, basis of finite field, XOR count, MDS matrices, diffusion layer.

1 Introduction

In today's world *Internet of Things (IoT)* is a buzzword. The devices that are involved in IoT are equipped with very limited power and memory. The standard cryptographic primitives often do not suit in these devices. Thus to cater the security requirement of IoT, the so-called topic *lightweight cryptography* has emerged.

Lightweight cryptography is mostly based on symmetric-key cryptography. Examples of lightweight ciphers include eSTREAM finalists `Grain` v1 [7], `MICKEY` 2.0 [1], and `Trivium` [11]. On the other hand, the block ciphers `CLEFIA` [9], `PRESENT` [2] have already been included in the ISO standardization project of lightweight cryptography ISO/IEC 29192. The block cipher `PRINCE` [3] is another block cipher that is lightweight, and after its arrival in 2012, it has generated a lot of interest in the community.

There are two important cryptographic criteria of a block cipher, and other cryptographic primitives such as hash functions that are based on block ciphers—confusion and diffusion. The confusion layer makes the relation between key and ciphertext as complex as possible, and on the other hand the diffusion layer spreads the plaintext statistics through the ciphertext. A popular choice for constructing the diffusion layer is to use maximum distance separable (MDS) matrices, for instance `AES` [4] and `LED` [6] use MDS matrix to achieve the maximum diffusion power. However, having MDS matrix in a lightweight cipher is a real challenge for the designers as MDS matrices tend to have high implementation cost. To quantify the hardware cost of the diffusion layer, a metric to estimate the cost for implementing the coefficients of the diffusion matrix is required.

Before [8], a common belief was that field elements with low Hamming weight tends to be lightweight. For instance, one of the rationales for the choice of `AES` diffusion matrix coefficients was its simplicity and low Hamming weight. However, there was no clear implication of how low Hamming weight elements would result in lightweight implementation. In 2014, the authors of [8] proposed to look at the number of XORs required to compute the multiplication of a fixed field elements. As a result, they found MDS diffusion matrices that required lesser XORs to implement than the `AES` diffusion matrix and yet with higher total Hamming weight. In 2015, the authors of [10] extended the search for lightweight diffusion matrices, with special focus on involutory (self-inverse) MDS matrices, over other finite fields defined by other irreducible polynomials besides the irreducible polynomial used for `AES` diffusion matrix. Besides finding new lightweight diffusion matrices, the authors proposed that the choice of irreducible polynomial to construct lightweight matrices should not be dependent on the Hamming weight of the polynomial, but the high standard deviation of the XOR count distribution. Although all possible irreducible polynomials for generating finite fields have been studied, the choice of the basis has not been considered.

In symmetric-key cryptography, the conventional choice of basis is the polynomial basis. However, there are many other choices of basis, for instance a normal basis, which is commonly used in elliptic curve cryptography. These new choices of basis give rise to new sets of XOR count distributions. Hence a natural question is whether there exist even lighter MDS diffusion matrices when we consider different bases besides the polynomial basis, which is the main motivation of this work. However, extending the search for lightweight matrices to other bases brings about a new challenge—the number of bases grows exponentially as the dimension of the finite field increases. Perhaps this is one reason that little work in any aspect of cryptography has looked into the different choices of bases.

Contributions. In this paper we deeply study the distribution of XOR count of field elements and characterize how sensitive they are to the change of basis. Prior to this work, little work has been done on analyzing different finite field bases in the cryptographical aspect. In Section 2, after giving a brief introduction to finite field and its bases, we describe how to compute the XOR count of a field element and the XOR count of a diffusion matrix. In Section 3.2, we analyze the distribution of XOR counts and show that the mean of the XOR count distribution is invariant of the irreducible polynomial and basis. In addition, we prove that the collection of XOR count distributions is the same for any irreducible polynomial of the same degree. This implies that we only need to consider XOR count distributions under one irreducible polynomial. In Section 3.3, we show that there are bases that generate similar XOR count distributions, which means that there are "redundant bases", and we can reduce the number of bases to consider when we search for lightweight diffusion matrices. In Section 4, we formally define the equivalence relation between bases whose XOR count distributions are invariant, and propose the concept of equivalence classes of bases. Since it is sufficient to search for lightweight MDS diffusion matrices under one representative basis from each equivalence class, this significantly reduces the number of bases to consider. In Section 5, we describe the algorithms for finding all equivalence classes of bases, and searching lightweight MDS and involutory MDS diffusion matrices under the representative bases. Although we do not find new lighter (involutory) MDS diffusion matrices, our empirical evidence shows that the polynomial basis, and its equivalent bases, are the recommended choice of bases for constructing lightweight MDS diffusion matrices.

2 Preliminary

In this section, first we give a short recap on finite field and its bases. Next, we describe how the XOR count of a field element and XOR count of a diffusion matrix under some irreducible polynomial are computed.

2.1 Finite field

We denote by $\mathrm{GF}(2^n)$ the finite field with 2^n elements, $n \geq 1$. The addition $+$ over $\mathrm{GF}(2^n)$ will be used in this paper with ambiguity, however implication will be clear from the context. The exclusive-or (XOR) sign $\oplus$ will sometimes be used to mean addition modulo 2.

The extension field $\mathrm{GF}(2^n)$ of $\mathrm{GF}(2)$ is constructed using an irreducible polynomial of degree n. Let $\mathrm{GF}(2^n)/p(X)$ denote the field having the underlying irreducible polynomial $p(X)$ of degree n[3]. Note that for any other irreducible polynomial $q(X)$ of degree n, the two fields $\mathrm{GF}(2^n)/p(X)$ and $\mathrm{GF}(2^n)/q(X)$ are isomorphic. Throughout the paper we will be using the notation $\mathrm{GF}(2^n)/p(X)$ only when we need to mention $p(X)$ explicitly.

The number of irreducible polynomial of degree n over GF(2), denoted as $M_n(2)$, is given by the following formula,

$$M_n(2) = \frac{1}{n}\sum_{d|n} \mu(d) 2^{\frac{n}{d}}, \tag{1}$$

where $\mu(d)$ is the Möbius function [5].

2.2 Bases of a finite field

Let α denote a primitive element of $\mathrm{GF}(2^n)$, then any nonzero element in the finite field can be expressed as α^i. Given $\mathrm{GF}(2^n)$, consider a set of elements in the field $\mathcal{B} = \{\alpha^{r_0}, \alpha^{r_1}, ..., \alpha^{r_{n-1}}\}$, where r_i's are non-negative integers. If the GF(2)-linear combinations of elements of $\mathcal{B}$ span the entire field, we call this as a basis, that is through the basis, we identify $\mathrm{GF}(2^n)$ with the vector space $\mathrm{GF}(2)^n$. Sometimes we denote the basis as $\{\alpha^{r_i}\}_{i=0}^{n-1} = \{\alpha^{r_0}, \alpha^{r_1}, ..., \alpha^{r_{n-1}}\}$.

The number of bases for a given finite field $\mathrm{GF}(2^n)$ is given as

$$\frac{1}{n!}\prod_{s=0}^{n-1}(2^n - 2^s). \tag{2}$$

Conventionally, we use the polynomial basis $\{\alpha^0, \alpha^1, ..., \alpha^{n-1}\}$, but there are many other bases such as a normal basis, which is of the form $\{\alpha^i, \alpha^{2i}, ..., \alpha^{2^{n-1}i}\}$[4], where integer $i > 0$.

2.3 XOR count of finite field elements and diffusion matrices

MDS matrices are popular choice for building the diffusion layer of a block cipher. Towards the construction of lightweight diffusion layer, it is required that the total operations needed to execute the diffusion layer on an input vector (the product of the matrix and a vector) should also be low. In this paper, we consider XOR count as the metric for lightweightness of matrices as done in [8, 10].

In practice, a finite field element is represented by its corresponding vector space element by choosing some basis. Then to realize a product of two finite field elements we need to express the product in terms of the basis elements, where the coefficients are linear functions of coordinates of the two elements.

[3] This notation should not be confused with the finite field notation $\mathrm{GF}(2)[X]/(P)$, where (P) is an ideal generated by irreducible polynomial P. Nevertheless, both notations refer to the same thing. i.e., $\mathrm{GF}(2^n)/p(X) = \mathrm{GF}(2)[X]/(P)$

[4] This is a necessary condition for a normal basis, not every i forms a basis.

Definition 1. *The XOR count of an element θ in the field* $\mathrm{GF}(2^n)$ *is the number of XORs required to implement the multiplication of θ with an arbitrary element β. We name the set of XOR counts of all the elements of* $\mathrm{GF}(2^n)$ *as the XOR count distribution.*

For example, consider $\mathrm{GF}(2^3)/(X^3+X+1)$ and a basis $\{1, \alpha, \alpha^2\}$. Consider the multiplication of $\alpha^4 = \alpha + \alpha^2$ with an arbitrary element $\beta = b_0 + b_1\alpha + b_2\alpha^2$, where $b_i \in \{0, 1\}$

$$(b_0 + b_1\alpha + b_2\alpha^2)(\alpha + \alpha^2) = (b_1 + b_2) + (b_0 + b_1)\alpha + (b_0 + b_1 + b_2)\alpha^2.$$

In other words, the product of the α^4 and β is of the form

$$(b_1 \oplus b_2, b_0 \oplus b_1, b_0 \oplus b_1 \oplus b_2),$$

in which there are 4 XORs[5]. Therefore, the XOR count of the element α^4 is 4. It is trivial to check that the zero element will have XOR count 0. Since the coefficients of MDS diffusion matrices must be nonzero, in the XOR count distribution we will not mention the XOR count of the zero element. One may also check that for this basis, identity element also has XOR count 0.

We observe that the XOR count distribution of a field may differ as per the choice of basis. For example, consider $\mathrm{GF}(2^3)/(X^3 + X + 1)$ and enumerate the nonzero field elements as $\{\alpha^i\}_{i=0}^{6}$. For the basis $\{1, \alpha, \alpha^2\}$, the XOR count distribution is $\{0, 1, 2, 4, 4, 3, 1\}$. However, if we consider the normal basis $\{\alpha^3, \alpha^6, \alpha^{12}\}$[6], then the XOR count distribution is $\{0, 3, 3, 2, 3, 2, 2\}$.

The XOR count of one row of a diffusion matrix can be computed using the following formula given in [8]:

$$\text{XOR count of one row} = \sum_{i=1}^{k} \gamma_i + (\ell - 1) \cdot n,$$

where γ_i is the XOR count of the i-th entry in the row of the matrix, k being the order of the diffusion matrix, ℓ is the number of nonzero coefficients in the row and n is the dimension of the finite field. For example, the first row of the `AES` diffusion matrix being $(1, 1, 2, 3)$ over the field $\mathrm{GF}(2^8)/(X^8+X^4+X^3+X+1)$, so the XOR count for the first row is $(0+0+3+11)+3\times 8 = 38$. Note that for MDS matrices, all coefficients are nonzero thus we can assume $\ell = k$. Since the latter term of the formula is dependent of the dimension of the finite field and order of the MDS matrix, it will be a fixed constant for a given finite field and order of the MDS matrix. Hence, we are only interested in the sum of the XOR count of the coefficients.

In this paper, sometime we describe a diffusion matrix with relatively lower XOR counts as a lightweight matrices.

[5] We acknowledge that common terms in the expression could be computed just once and reused to save some XOR count. However, that would require additional cycle and extra memory cost which would very likely to outweigh the cost saved for the XOR count.

[6] Note that the element α^{12} can also be written as α^5 as the finite field multiplication of primitive element has a cycle of length 7.

3 XOR Count Distribution

In this section, we first give a special property of the XOR count distribution under normal bases. Next in Section 3.2, we analyze the XOR count distribution and its relation between different irreducible polynomials. We show that any choice of the irreducible polynomial generates the same collection of XOR count distributions when all bases are considered. Lastly in Section 3.3, we study the similarity of the XOR count distribution under different bases. This is the building block for constructing the equivalence classes of bases in Section 4.

3.1 XOR count distribution under normal bases

We give an interesting property of the XOR count regarding normal bases. First, it is known that the binary representation of an element α^{2i} is a shift rotation of the binary representation for α^i under a normal basis. This is a nice feature in the context of hardware implementation.

Proposition 1. *Under a normal basis, α^i of $\mathrm{GF}(2^n)$ has the same XOR count as α^{2i}.*

Proof. Without loss of generality, let the normal basis be $\{\alpha, \alpha^2, ..., \alpha^{2^{n-1}}\}$, an element α^i can be expressed as a polynomial $\alpha^i = a_0\alpha + a_1\alpha^2 + ... + a_{n-1}\alpha^{2^{n-1}}$, while the square of the element has a shift in the coefficient, $\alpha^{2i} = a_{n-1}\alpha + a_0\alpha^2 + ... + a_{n-2}\alpha^{2^{n-1}}$.

For any arbitrary element $b_0\alpha + b_1\alpha^2 + ... + b_{n-1}\alpha^{2^{n-1}}$, the XOR count of α^{2i} can be computed as

$$\begin{aligned}&(a_{n-1}\alpha + a_0\alpha^2 + ... + a_{n-2}\alpha^{2^{n-1}})(b_0\alpha + b_1\alpha^2 + ... + b_{n-1}\alpha^{2^{n-1}})\\ =&\Big((a_0\alpha + a_1\alpha^2 + ... + a_{n-1}\alpha^{2^{n-1}})(b_1\alpha + b_2\alpha^2 + ... + b_0\alpha^{2^{n-1}})\Big)^2.\end{aligned}$$

Since squaring is simply a shift in the binary representation, the number of XORs in $\Big(\alpha^i(b_1\alpha + b_2\alpha^2 + ... + b_0\alpha^{2^{n-1}})\Big)^2$ is the same as that of $\alpha^{2i}(b_1\alpha + b_2\alpha^2 + ... + b_0\alpha^{2^{n-1}})$. Furthermore, the number of XORs in $\alpha^{2i}(b_1\alpha + b_2\alpha^2 + ... + b_0\alpha^{2^{n-1}})$ is the same as that of $\alpha^{2i}(b_0\alpha + b_1\alpha^2 + ... + b_{n-1}\alpha^{2^{n-1}})$ as $\{b_0, \dots, b_{n-1}\}$ is simply a permutation of $\{b_1, \dots, b_0\}$. Hence, the XOR count of α^{2i} is the same as the XOR count of α^i. □

Thus there will be several repetitions in the XOR count distributions when normal basis is considered. As one can see from the example in the previous section that the elements α, α^2 and α^4 have the same XOR count 3 while α^3, α^6 and α^5 have the same XOR count 2.

3.2 XOR count spectrum

For a field element θ, we can define a matrix such that the XOR count of the product with an arbitrary element b can be computed directly from that matrix.

Let $\{1, \alpha\}$ be a basis of $\mathrm{GF}(2^2)$. For a fixed element $a_0 + a_1\alpha$ of $\mathrm{GF}(2^2)$ the multiplication with an arbitrary element $b_0 + b_1\alpha$ will give

$$(b_0 + b_1\alpha)(a_0 + a_1\alpha) = b_0a_0 + b_1a_1 + (b_0a_1 + (a_0 + a_1)b_1)\alpha.$$

In vector notation, this product is actually $(b_0a_0 \oplus b_1a_1, b_0a_1 \oplus (a_0 \oplus a_1)b_1$, which can be written as a matrix product

$$\begin{pmatrix} a_0 & a_1 \\ a_1 & a_0 \oplus a_1 \end{pmatrix} \times \begin{pmatrix} b_0 \\ b_1 \end{pmatrix}.$$

Clearly if there are k_i 1's in the i-th row, then there will be $k_i - 1$ XORs of b_i's in the i-th coordinate of the product.

In general if $\{\alpha^{r_1}, \ldots, \alpha^{r_n}\}$ is a basis of $\mathrm{GF}(2^n)/p(X)$, the product of a fixed element $\theta = a_0\alpha^{r_1} + \ldots + a_{n-1}\alpha^{r_n}$ and an arbitrary element $b = b_0\alpha^{r_1} + \ldots + b_{n-1}\alpha^{r_n}$ can be expressed as a multiplication matrix M_θ and $(b_0, \ldots, b_{n-1})$, where

$$M_\theta = \begin{bmatrix} L_{0,0}(a_0, \ldots, a_{n-1}) & \ldots & L_{0,n-1}(a_0, \ldots, a_{n-1}) \\ L_{1,0}(a_0, \ldots, a_{n-1}) & \ldots & L_{1,n-1}(a_0, \ldots, a_{n-1}) \\ \vdots & \ddots & \vdots \\ L_{n-1,0}(a_0, \ldots, a_{n-1}) & \ldots & L_{n-1,n-1}(a_0, \ldots, a_{n-1}) \end{bmatrix},$$

note that each $L_{i,j}(a_0, \ldots, a_{n-1})$ is some GF(2)-linear combination of $\{a_0, \ldots, a_{n-1}\}$. As said before if there are k_i 1's in row i, the total number of XORs needed is $\sum_{i=1}^{n}(k_i - 1)$.

It is to be noted that the matrix M_θ is invertible, since $\theta^{-1}\theta b = b$, equivalently $M_\theta^{-1}M_\theta \times [b_0, \ldots, b_{n-1}]^T$ should give $[b_0, \ldots, b_{n-1}]^T$. This fact is used to determine the following property of the matrix M_θ.

We call an n-tuple binary vector nonzero if at least one coordinate of it is nonzero.

Lemma 1. *The collection of the row vectors taken from any fixed row of all the matrices M_θ for all nonzero θ, is in bijection with the set of nonzero n-tuple binary vectors.*

Proof. It is clear that every row of the matrix M_θ of a nonzero element θ is nonzero n-tuple binary vectors, else M_θ is not invertible. Consequently, for each row i, row vectors are pairwise distinct for all such matrices. Suppose not, let θ_1 and θ_2 be distinct elements with the same binary vector in row i. Then $\theta_1 + \theta_2$ is another nonzero element with zeroes in row i which contradicts that nonzero elements are invertible. □

Proposition 2. *The total XOR count of the elements in* $\mathrm{GF}(2^n)$ *is* $n\sum_{i=2}^{n}\binom{n}{i}(i-1)$*, and it is invariant of the choice of irreducible polynomial and basis.*

Proof. By Lemma 1, the row i of nonzero multiplication matrices is in bijection with the set of nonzero n-tuple binary vectors over GF(2). Hence, summing the number of XORs for the row i of all elements is $\sum_{i=2}^{n}\binom{n}{i}(i-1)$. Since there are n rows, we have $n\sum_{i=2}^{n}\binom{n}{i}(i-1)$. □

This proposition shows that there is no clear advantage in choosing some particular irreducible polynomial and basis over another.

As the example in Section 2.3 shows that XOR count distribution may change under different basis, therefore, one may think that varying over all possible bases, the set of XOR count distributions might be different for $\mathrm{GF}(2^n)/p(X)$ and $\mathrm{GF}(2^n)/q(X)$. However, our analysis shows that for a basis $\mathcal{B}$ in $\mathrm{GF}(2^n)/p(X)$ there will be a basis $\mathcal{B}'$ in $\mathrm{GF}(2^n)/q(X)$ such that XOR count distribution of $\mathrm{GF}(2^n)/p(X)$ under $\mathcal{B}$ will be equal to that of $\mathrm{GF}(2^n)/q(X)$ under $\mathcal{B}'$. The proof is as follows.

For brevity, we call the set of all XOR count distributions for all possible bases as the *XOR count spectrum.*

Lemma 2. *Let $\psi : \mathrm{GF}(2^n)/p(X) \to \mathrm{GF}(2^n)/q(X)$ an isomorphism between these two finite fields. If $\{\alpha_0, \ldots, \alpha_{n-1}\}$ is a basis of $\mathrm{GF}(2^n)/p(X)$, then the set $\{\psi(\alpha_0), \ldots, \psi(\alpha_{n-1})\}$ is a basis of $\mathrm{GF}(2^n)/q(X)$.*

Theorem 1. *The XOR count spectrum of $\mathrm{GF}(2^n)/p(X)$ and $\mathrm{GF}(2^n)/q(X)$ are the same.*

Proof. We show that for a basis of $\mathrm{GF}(2^n)/p(X)$, there is a basis of $\mathrm{GF}(2^n)/q(X)$, where XOR count distribution will be the same. Let α and β be the primitive elements of $\mathrm{GF}(2^n)/p(X)$ and $\mathrm{GF}(2^n)/q(X)$ respectively. Suppose $\{\alpha_0, \ldots, \alpha_{n-1}\}$ is a basis of $\mathrm{GF}(2^n)/p(X)$. Consider an arbitrary element of $\mathrm{GF}(2^n)/p(X)$ as $b_0\alpha_0 + \ldots + b_{n-1}\alpha_{n-1}$ and multiply with the element α^i

$$\alpha^i(b_0\alpha_0 + \ldots + b_{n-1}\alpha_{n-1}) = L_0\alpha_0 + \ldots + L_{n-1}\alpha_{n-1}, \tag{3}$$

where L_i's are some linear combinations of $\{b_0, \ldots, b_{n-1}\}$. If in the linear combination L_i there are c_i XORs, then XOR count is $\sum_{i=0}^{n-1} c_i$. Notice that the value of each $L_i \in \{0, 1\}$.

Apply ψ on both sides of (3), and we get

$$\psi(\alpha)^i(b_0\psi(\alpha_0) + \ldots + b_{n-1}\psi(\alpha_{n-1})) = L_0\psi(\alpha_0) + \ldots + L_{n-1}\psi(\alpha_{n-1}).$$

From Lemma 2, we know that $\{\psi(\alpha_0), \ldots, \psi(\alpha_{n-1})\}$ is a basis of $\mathrm{GF}(2^n)/q(X)$, and from the above we get that there is $\psi(\alpha)^i$ in $\mathrm{GF}(2^n)/q(X)$ such that its XOR count under $\{\psi(\alpha_0), \ldots, \psi(\alpha_{n-1})\}$ is $\sum_{i=0}^{n-1} c_i$.

Thus the XOR count spectrum obtained for $\mathrm{GF}(2^n)/p(X)$ will be the same for $\mathrm{GF}(2^n)/q(X)$. □

Therefore, we see that there is no gain in considering $\mathrm{GF}(2^n)$ under different irreducible polynomials, as this will not generate any new XOR count spectrum. Hence for the rest of the paper, we omit the irreducible polynomial of the corresponding field unless necessary.

3.3 Bases with similar XOR count distributions

Let us now check if there is any similar XOR count distribution within the XOR count spectrum, more precisely saying that we would like to see if a given finite field $\mathrm{GF}(2^n)/p(X)$, there are bases whose corresponding XOR count distributions are equal (up to a permutation). In the following we present the results.

Lemma 3. *If $\{\alpha^{r_0}, \ldots, \alpha^{r_{n-1}}\}$ is a basis of $\mathrm{GF}(2^n)$, then $\{\alpha^{r_0+1}, \ldots, \alpha^{r_{n-1}+1}\}$ is also a basis of $\mathrm{GF}(2^n)$.*

Proposition 3. *Given a finite field $\mathrm{GF}(2^n)$ and bases $\mathcal{B} = \{\alpha^{r_0}, \ldots, \alpha^{r_{n-1}}\}$ and $\mathcal{B}^{+t} = \{\alpha^{r_0+t}, \ldots, \alpha^{r_{n-1}+t}\}$, for integer $t > 0$, the XOR count distribution of $\mathrm{GF}(2^n)$ under these bases are exactly the same.*

Proof. For simplicity we prove it for $t = 1$, the rest follows by induction. For an arbitrary element $b = b_0\alpha^{r_0} + \ldots + b_{n-1}\alpha^{r_{n-1}}$, we can express the multiplication with α^j under $\mathcal{B}$ as

$$\alpha^j(b_0\alpha^{r_0} + \ldots + b_{n-1}\alpha^{r_{n-1}}) = L_0\alpha^{r_0} + \ldots + L_{n-1}\alpha^{r_{n-1}},$$

where L_i's are some linear combinations of $\{b_0, \ldots, b_{n-1}\}$. Suppose c_i is the number of XORs in L_i, then XOR count of α^j under $\mathcal{B}$ is $\sum_{i=0}^{n-1} c_i$.

On the other hand, the multiplication with α^j under $\mathcal{B}^{+1}$ can be expressed as

$$\begin{aligned}\alpha^j(b_0\alpha^{r_0+1} + \ldots + b_{n-1}\alpha^{r_{n-1}+1}) &= \alpha^j(b_0\alpha^{r_0} + \ldots + b_{n-1}\alpha^{r_{n-1}})\alpha \\ &= (L_0\alpha^{r_0} + \ldots + L_{n-1}\alpha^{r_{n-1}})\alpha \\ &= L_0\alpha^{r_0+1} + \ldots + L_{n-1}\alpha^{r_{n-1}+1}.\end{aligned}$$

Clearly the XOR count in this case is $\sum_{i=0}^{n-1} c_i$ too.

Therefore, the XOR count distribution of $\mathrm{GF}(2^n)$ under $\{\alpha^{r_0}, \ldots, \alpha^{r_{n-1}}\}$ and $\{\alpha^{r_0+1}, \ldots, \alpha^{r_{n-1}+1}\}$ are exactly the same. □

Next we find that there is another set of bases where the corresponding XOR count distributions are the same up to a permutation.

Lemma 4. *If $\{\alpha^{r_0}, \ldots, \alpha^{r_{n-1}}\}$ is a basis of $\mathrm{GF}(2^n)$, then $\{\alpha^{2r_0}, \ldots, \alpha^{2r_{n-1}}\}$ is also a basis of $\mathrm{GF}(2^n)$.*

Proposition 4. *Given a finite field $\mathrm{GF}(2^n)$, the XOR count distribution under the bases $\mathcal{B} = \{\alpha^{r_0}, \ldots, \alpha^{r_{n-1}}\}$ and $\mathcal{B}^{\times 2^s} = \{\alpha^{2^s r_0}, \ldots, \alpha^{2^s r_{n-1}}\}$, for integer $s > 0$, are the same up to a permutation.*

Proof. For simplicity, we prove for $s = 1$, the rest will follow by induction.

For an arbitrary element $b = b_0\alpha^{r_0}, \ldots, b_{n-1}\alpha^{r_{n-1}}$, we can express the multiplication with α^j under $\mathcal{B}$ as

$$\alpha^j(b_0\alpha^{r_0} + \ldots + b_{n-1}\alpha^{r_{n-1}}) = L_0\alpha^{r_0} + \ldots + L_{n-1}\alpha^{r_{n-1}}, \tag{4}$$

where L_i's are linear combinations of $\{b_0, \dots, b_{n-1}\}$. If c_i is the number of XORs in L_i, then the XOR count of α^j under $\mathcal{B}$ is $\sum_{i=0}^{n-1} c_i$.

To compute the XOR count for α^{2i} under $\mathcal{B}^{\times 2}$, we square (4) to obtain

$$\alpha^{2j}(b_0\alpha^{2r_0} + \ldots + b_{n-1}\alpha^{2r_{n-1}}) = L_0\alpha^{2r_0} + \ldots + L_{n-1}\alpha^{2r_{n-1}}. \tag{5}$$

Clearly the XOR count obtained from (5) is also $\sum_{i=0}^{n-1} c_i$. Since $\gcd(2, 2^n - 1) = 1$, the mapping from α^j under $\mathcal{B}$ to α^{2i} under $\mathcal{B}^{\times 2}$ is bijection. Therefore, XOR count distribution under $\mathcal{B}$ and $\mathcal{B}^{\times 2}$ are just permutation of each other. □

4 Equivalence Classes of Bases

In the previous section, we have seen the similarities in some of the XOR count distributions generated by different bases. In this section, we formally introduce the equivalence relation between bases whose XOR count distributions produce the lightest MDS matrix with the same XOR count. Using this equivalence relation, we construct the equivalence classes of bases.

From Proposition 3, it is clear that for any MDS diffusion matrix $M = [\beta_{i,j}]_{k\times k}$ has the same XOR count both under $\mathcal{B}$ and $\mathcal{B}^{+t}$. As for the other type of basis $\mathcal{B}^{\times 2^s}$, by Proposition 4, we know that the XOR count of M under $\mathcal{B}$ will match with that of another matrix $M' = [\beta_{i,j}^2]_{k\times k}$ under $\mathcal{B}^{\times 2}$, however, it is unclear if M' is also an MDS matrix. Thus, we need the following lemma.

Lemma 5. *Suppose $M = [\beta_{i,j}]_{k\times k}$ is an MDS matrix over $\mathrm{GF}(2^n)$, then $M' = [\beta_{i,j}^2]_{k\times k}$ is also an MDS matrix.*

Proof. It is known that all square submatrices of an MDS matrix have nonzero determinants. Since $\mathrm{GF}(2^n)$ has characteristic 2, the determinants of the submatrices of M' are square of the determinants of the corresponding submatrices of M, which are also nonzero. □

With Lemma 5, it is now clear that M' is also MDS. Therefore, we can say that by Proposition 3 and 4, the XOR count distributions of $\mathrm{GF}(2^n)$ under $\mathcal{B}$, $\mathcal{B}^{+t}$ and $\mathcal{B}^{\times 2^s}$ are invariant for the MDS matrices over finite fields under these bases. Because for every MDS matrix with some XOR count found under $\mathcal{B}$, there will be another MDS matrix having the same XOR count under $\mathcal{B}^{+t}$ and $\mathcal{B}^{\times 2^s}$, and vice versa. With that said, we can partition the set of all bases of $\mathrm{GF}(2^n)$ into distinct equivalence classes.

Definition 2. *The bases $\mathcal{B} = \{\alpha^{r_i}\}_{i=0}^{n-1}$ and $\mathcal{B}' = \{\alpha^{u_i}\}_{i=0}^{n-1}$ of $\mathrm{GF}(2^n)$ are equivalent if $u_i = (2^s r_i + t)$ mod $2^n - 1$ for some $s \geq 0$ and $t \geq 0$. The collection of these equivalent bases forms an equivalence class of bases.*

With these equivalence classes of bases, it is sufficient to consider one basis representative from each equivalence class in order to find one of the lightest MDS matrices over all possible bases.

Next, we analyze the cardinality of the equivalence classes. Interestingly, the bases are not uniformly partitioned into equivalence classes. For instance, for $\mathrm{GF}(2^3)$, there are 28 bases and only 2 equivalence classes, where one consists of 21 bases while the other has 7. This complicates the counting of the number of equivalence classes for a given field dimension. Therefore, instead of finding the exact cardinality of the equivalence class, we give a bound to it.

Lemma 6. *The cardinality of any equivalence classes of bases of* $\mathrm{GF}(2^n)$ *is a multiple of* $2^n - 1$.

Proof. Consider basis of the form $\mathcal{B}^{+t} = \{\alpha^{r_i+t}\}_{i=0}^{n-1}$, for positive integer t, which is in the equivalence class of $\mathcal{B} = \{\alpha^{r_i}\}_{i=0}^{n-1}$. Then the proof is immediate if we can show that the smallest positive integer t that satisfies $\mathcal{B}^{+t} = \mathcal{B}$ is $t = 2^n - 1$.

Since $\alpha^{2^n-1} = 1$, it is clear that $\mathcal{B}^{+t} = \mathcal{B}$ when $t = 2^n - 1$. Suppose there exists $t_0 < 2^n - 1$ such that $\mathcal{B}^{+t_0} = \mathcal{B}$, taking the summation of the elements in the basis, we have

$$\alpha^{r_0+t_0} + \ldots + \alpha^{r_{n-1}+t_0} = \alpha^{r_0} + \ldots + \alpha^{r_{n-1}}.$$

Since $\{\alpha^{r_i}\}_{i=0}^{n-1}$ is a basis, the summation, $\sum_{i=0}^{n-1} \alpha^{r_i}$, is nonzero and invertible. Hence we can simplify the equation and obtain $\alpha^{t_0} = 1$, which is a contradiction that α is a primitive element of the finite field. □

Theorem 2. *A lower bound and upper bound of the cardinality of any equivalence classes of bases of* $\mathrm{GF}(2^n)$ *is* $2^n - 1$ *and* $n \cdot 2^n - 1$ *respectively.*

Proof. From Lemma 6, we know that the lower bound of the cardinality of equivalence class is $2^n - 1$. Since $\alpha^{2^n} = \alpha$, it is clear that $\mathcal{B}^{\times 2^s} = \mathcal{B}$ when $s = n$. Therefore, the largest possible cardinality is $n \cdot 2^n - 1$, when these n sets of bases, $\{\mathcal{B}^{+t}\}_{t=0}^{2^n-1}$, $\{(\mathcal{B}^{\times 2})^{+t}\}_{t=0}^{2^n-1}$, $\{(\mathcal{B}^{\times 2^2})^{+t}\}_{t=0}^{2^n-1}$,...,$\{(\mathcal{B}^{\times 2^{n-1}})^{+t}\}_{t=0}^{2^n-1}$, belong to the same equivalence class and are pairwise distinct. □

Lastly, we show that every equivalence class contains one certain kind of basis. This allows us to find a representative basis from each equivalence classes more efficiently.

Proposition 5. *Every equivalence class always contains a basis of the form* $\{1, \alpha^{u_1} \ldots, \alpha^{u_{n-1}}\}$.

Proof. Given a basis $\{\alpha^{r_0}, \alpha^{r_1} \ldots, \alpha^{r_{n-1}}\}$ from an equivalence class, consider $t = 2^n - 1 - r_0$, then the equivalent basis $\{\alpha^{r_i+t}\}_{i=0}^{n-1} = \{1, \ldots, \alpha^{2^n-1-r_0+r_{n-1}}\}$ also belongs to the same equivalence class. □

5 Search Algorithms and Results

In this section, we first present our strategy to find all the equivalence classes of bases, then it is sufficient for us to apply our search on one representative of each equivalence classes for lightweight (in terms of low XOR count) MDS diffusion matrices. Next, we adopt the similar strategy as described in [10, Sect5.2] and extend the search to different bases for lightweight (involutory) MDS Hadamard matrices of order 4.

5.1 Enumerating equivalence classes

Search algorithm. By Proposition 5, we know that the representative of an equivalence class is of the form $\{1, \alpha^{u_1}, \ldots, \alpha^{u_{n-1}}\}$. Therefore, all we need is to start from $\{1, \alpha^{u_1}, \ldots, \alpha^{u_{n-1}}\}$, if it is a basis then we can generate the equivalence class by

$$\{1, \alpha^{u_1}, \ldots, \alpha^{u_{n-1}}\} \rightarrow \{1, \alpha^{2^s u_1 + t}, \ldots, \alpha^{2^s u_{n-1} + t}\}, s \geq 0, t \geq 0.$$

This way we need to test $\binom{2^n-2}{n-1}$ possible basis representatives in the worst case. The pseudocode for enumerating the equivalence class is presented in Appendix A.

Results. Due to memory issue, we are unable to compute the exact number of equivalence classes of bases for $n \geq 6$. However, by Theorem 2, we are able to estimate the number of equivalence classes as we know the lower bound and upper bound of the cardinality of an equivalence class to be $2^n - 1$ and $n \cdot 2^n - 1$ respectively.

In Table 1, the second column shows the number of irreducible polynomials for each dimension which can be computed from (1). By Theorem 1, we only need to consider one arbitrary irreducible polynomial. The total number of bases which can be computed using (2) is given in the third column, while the number of equivalence classes of bases for each dimension is given in the last column.

Table 1. Number of equivalence classes of bases

dimension of finite field	**number of irreducible polynomial**	**number of bases**	**number of equivalence classes**
$n = 3$	2	28	2
$n = 4$	3	840	16
$n = 5$	6	83328	540
$n = 6$	7	$2^{24.74}$	$2^{16.18} \sim 2^{18.76}$
$n = 7$	18	$2^{34.92}$	$2^{25.12} \sim 2^{27.93}$
$n = 8$	30	$2^{46.91}$	$2^{35.92} \sim 2^{38.92}$

5.2 Finding lightweight (involutory) MDS matrices under different bases

Search algorithm. The authors of [10] analyzed the structure of Hadamard matrices and presented the equivalence classes of Hadamard matrices and a simplified check for MDS property on Hadamard matrices. In this paper, we focus on Hadamard matrices of order 4 as 4 × 4 matrices are commonly used in diffusion layer of a block cipher, for instance in AES. In addition, involutory MDS Hadamard matrices can be easily constructed, as a Hadamard matrix is involution iff the XOR-sum of the first row is 1. Based on these results, we only need to choose a set of lightweight coefficients and test for MDS, the arrangement of the entries is invariant as there is only one equivalence class of Hadamard matrices for order 4 [10].

From Section 4, we see that bases within an equivalence class of bases have the same (w.r.t. XOR count) collection of MDS matrices. Hence, it is sufficient to check one representative from each equivalence class. To search for lightweight MDS matrices over a given basis, we set some threshold value as the upper bound for the total XOR count of the coefficients. If the sum of the XOR count of the candidate is lower than the threshold, then we check if it forms an MDS Hadamard matrix. In order to search for lightweight involutory MDS Hadamard matrices, an additional condition that the XOR-sum of the candidates equals to 1 is required. For $\mathrm{GF}(2^4)$ and $\mathrm{GF}(2^8)$, we set the threshold value to be the XOR count of the lightest MDS matrices found in [10]. For other order of finite fields, we set the threshold value to some arbitrary large value. The threshold value will be updated whenever we find a new (involutory) MDS Hadamard matrix with lesser total XOR count. The pseudocode for finding lightweight (involutory) MDS Hadamard matrices is presented in Appendix B.

Results. For $n = 3, 4, 5$, we search through all the equivalence classes of bases. For $n = 8$, we consider the polynomial and normal bases because these are the two most commonly used bases. The outcome is that the lightest MDS and involutory MDS Hadamard matrices are found for the bases that belong to the equivalence class containing the polynomial basis. And naturally for $n = 4, 8$, the XOR count of the lightest MDS and involutory MDS Hadamard matrices match with the results from [10].

5.3 Recommended choice of basis

Although we do not find MDS diffusion matrices with XOR count lesser than the existing ones, it is interesting to see that the lightest diffusion matrices are found under the polynomial basis. From Proposition 2, it seems that there is no clear implication that one basis is strictly better than another, as the mean XOR count is the same for any basis. However, the XOR count distribution may vary for different bases, that is quantified by the standard deviation. A high standard deviation implies that the distribution of XOR count is far apart from the mean, thus there will be more elements with relatively lower/higher XOR count. As pointed out in [10], in general the order of the finite field is much larger than the order of the diffusion matrix, since only a few elements of the finite field are used, there is a better chance of finding lightweight diffusion matrix under XOR distributions with higher standard deviation.

To illustrate this concept, consider taking the two XOR count distributions, $D_1 = \{0, 1, 2, 4, 4, 3, 1\}$ and $D_2 = \{0, 3, 3, 2, 3, 2, 2\}$, from Section 2.3 as an example. One can observe that the standard deviations of D_1 and D_2 are 1.57

and 1.07 respectively. Suppose we want to construct an MDS matrix of order 2, we need to pick 2 distinct nonzero elements. Under D_1, we can pick 2 elements corresponding to XOR count 0 and 1, which is lower than any choice that we make under D_2. The main reason being that the XOR counts in D_2 are much closer to the mean, while under D_1 we are able to pick elements with relatively lower XOR count and check if they form an MDS matrix. Therefore, we look into the standard deviation of the XOR count distribution of the bases.

By computing the standard deviation for all representation bases of the equivalence classes of bases, we observe that the standard deviation of the polynomial bases are significantly larger than the highest standard deviation of the non-polynomial bases. The results are summarized in Table 2.

Table 2. Highest standard deviation of various bases

dimension of finite field	**polynomial basis**	**other basis**
$n = 3$	1.46	0.99
$n = 4$	2.68	1.71
$n = 5$	4.09	3.55

dimension of finite field	**polynomial basis**	**normal basis**
$n = 8$	7.53	4.48

For any finite field GF(2^n), we conjecture that the XOR distribution under a polynomial basis tends to have a higher standard deviation as compared to other bases. Therefore, we think that considering the polynomial basis, or its equivalent bases, is the preferable choice for finding lightweight diffusion matrices.

5.4 Conclusion

In this paper, we study the behavior of the XOR count distribution under different bases and irreducible polynomials. We show that for all irreducible polynomials, the XOR count spectrum is the same. Hence, we only need to consider one irreducible polynomial when all bases are considered. Under a fixed irreducible polynomial, the bases can be partitioned into equivalence classes, where the XOR count distribution is invariant under these bases. In addition, we provide a search algorithm for finding all the equivalence classes of bases. Using these equivalence classes of bases, we complete the search for lightweight MDS and involutory MDS Hadamard matrix of order 4 for finite field dimension $n = 3, 4, 5$. Our result suggests that the bases from the equivalence class of polynomial basis are the recommended choice for constructing lightweight MDS diffusion matrices.

Acknowledgements

The authors would like to thank Thomas Peyrin for his valuable comments.

References

1. Steve Babbage and Matthew Dodd. The stream cipher MICKEY 2.0, 2006. http://www.ecrypt.eu.org/stream/mickeypf.html.
2. Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. PRESENT: An Ultra-Lightweight Block Cipher. In Pascal Paillier and Ingrid Verbauwhede, editors, *Cryptographic Hardware and Embedded Systems - CHES 2007*, volume 4727 of *LNCS*, pages 450–466. Springer, 2007.
3. Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Kneževic, Lars R. Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, Peter Rombouts, Søren S. Thomsen, and Tolga Yalçin. PRINCE - A Low-latency Block Cipher for Pervasive Computing Applications (Full version). Cryptology ePrint Archive, Report 2012/529, 2012. http://eprint.iacr.org/.
4. Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Information Security and Cryptography. Springer, 2002.
5. F.W. Gehring and P. R. Halmos, editors. *Introduction to analytic number theory, Undergraduate Texts in Mathematics*. New York-Heidelberg: Springer-Verlag, 1976.
6. Jian Guo, Thomas Peyrin, Axel Poschmann, and Matthew J. B. Robshaw. The LED Block Cipher. In Bart Preneel and Tsuyoshi Takagi, editors, *Cryptographic Hardware and Embedded Systems - CHES 2011*, volume 6917 of *LNCS*, pages 326–341. Springer, 2011.
7. Martin Hell, Thomas Johansson, and Willi Meier. Grain : a Stream Cipher for Constrained Environments. *Int. J. Wire. Mob. Comput.*, 2(1):86–93, May 2007.
8. Khoongming Khoo, Thomas Peyrin, Axel Y. Poschmann, and Huihui Yap. FOAM: Searching for Hardware-Optimal SPN Structures and Components with a Fair Comparison. In Lejla Batina and Matthew Robshaw, editors, *Cryptographic Hardware and Embedded Systems - CHES 2014*, volume 8731 of *Lecture Notes in Computer Science*, pages 433–450. Springer Berlin Heidelberg, 2014.
9. Taizo Shirai, Kyoji Shibutani, Toru Akishita, Shiho Moriai, and Tetsu Iwata. The 128-Bit Blockcipher CLEFIA (Extended Abstract). In Alex 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.
10. Siang Meng Sim, Khoongming Khoo, Frédérique Oggier, and Thomas Peyrin. Lightweight MDS Involution Matrices. In Gregor Leander, editor, *Fast Software Encryption*, volume 9054 of *Lecture Notes in Computer Science*, pages 471–493. Springer Berlin Heidelberg, 2015.
11. Yun Tian, Gongliang Chen, and Jianhua Li. On the Design of Trivium. Cryptology ePrint Archive, Report 2009/431, 2009. http://eprint.iacr.org/.

A Pseudocode for finding equivalent bases of GF(2^n)

Algorithm 1 Finding equivalent bases for GF(2^n).

```
INPUT: GF($2^n$) generated by a primitive element $\alpha$, $\mathbf{S} = \emptyset$.
OUTPUT: $\mathbf{B}$ the set of basis representatives of distinct equivalence classes of bases.
  set $\mathbf{B} = \emptyset$ and counter $= 0$
  for each set $\{(0, i_1, \ldots, i_{n-1}) : i_j \in [1, 2^n - 2]\}$ chosen from $\binom{2^n-2}{n-1}$ possible combinations do
      generate $E = \{\alpha^{2^s i_1 + t \mod 2^n - 1}, \ldots, \alpha^{2^s i_n + t \mod 2^n - 1} : s \in [0, n-1], t \in [0, 2^n - 2]\}$
      store every member of $E$ in $\mathbf{S}$ that has 1 and is new to $\mathbf{S}$, and update counter++
      if $\{1, \alpha^{i_1}, \ldots, \alpha^{i_{n-1}}\}$ is a basis then
          store $\{1, \alpha^{i_1}, \ldots, \alpha^{i_{n-1}}\}$ in $\mathbf{B}$
          if counter= $\binom{2^n-2}{n-1}$ then
              return $\mathbf{B}$ as the set of bases that are representatives to all distinct equivalence classes
          end if
      end if
  end for
```

B Pseudocode for finding lightweight (involutory) MDS Hadamard matrices over GF(2^n)

Algorithm 2 Finding lightweight (involutory) MDS Hadamard matrices for GF(2^n).

```
INPUT: MDS_threshold, IMDS_threshold, nonzero elements of $GF(2^n)$, XOR count
  of the field elements.
OUTPUT: XOR count of the lightest MDS and involutory MDS Hadamard matrices
  of order 4.
  sort the elements in ascending order according to their XOR counts
  for each set $S$ of 4 elements chosen from $\binom{2^n-1}{4}$ possible combinations do
      if XOR-sum of elements = 1 then
          if sum of XOR count $<$ IMDS_threshold then
              construct Hadamard matrix $H$ from $S$
              if $H$ is MDS then
                  update IMDS_threshold = sum of XOR count
              end if
          end if
      else if sum of XOR count $<$ MDS_threshold then
          construct Hadamard matrix $H$ from $S$
          if $H$ is MDS then
              update MDS_threshold = sum of XOR count
          end if
      end if
  end for
  return MDS_threshold and IMDS_threshold
```