IACR Transactions on Cryptographic Hardware and Embedded Systems
ISSN 2569-2925, Vol. 2024, No. 4, pp. 763–794. DOI:10.46586/tches.v2024.i4.763-794

Know-Thy-Basis: Decomposing $\mathbb{F}_{2^6}$ for Lightweight S-box Implementation

Dilip Sau[1], Sumanta Sarkar[2], Dhiman Saha[3] and Kalikinkar Mandal[4]

[1] Center for Computational & Data Sciences, Indian Institute of Technology Kharagpur, India
dilipsau1996@gmail.com
[2] University of Warwick, Coventry, UK
sumanta.sarkar@warwick.ac.uk
[3] de.ci.phe.red Lab, Department of Computer Science and Engineering,
Indian Institute of Technology Bhilai, India
dhiman@iitbhilai.ac.in
[4] University of New Brunswick, Fredericton, NB, Canada
kmandal@unb.ca

Abstract. A recent trend has shown constructions of 6-bit S-boxes that are mostly focused on their cryptographic elegance, while their lightweight aspects have not really been addressed well. This paper attempts to plug-in this existing research gap where we show how the composite structure of the extension field $\mathbb{F}_{2^6}$ could be leveraged. An earlier well-known example is an efficient implementation of `AES` S-box using the tower field extension of $\mathbb{F}_{2^8}$. The case of $\mathbb{F}_{2^{ab}}$ is completely different from any tower field as the implementation varies as per the choice of extension – for instance, $\mathbb{F}_{(2^a)^b}$ or $\mathbb{F}_{(2^b)^a}$, where a and b are prime. Thus, it makes the implementation of S-boxes over $\mathbb{F}_{2^6} = \mathbb{F}_{2^{(2\times 3)}}$ very interesting. In this work, we systematically study the composite field structure of $\mathbb{F}_{2^6}$ from a hardware standpoint for a class of S-boxes that are power mapping or their affine equivalents. We analyze the hardware efficiency with respect to different representations of the field extension, i.e., $\mathbb{F}_{(2^2)^3}$ or $\mathbb{F}_{(2^3)^2}$. Furthermore, for each extension, we investigate the impact of various choices of bases – for instance, we present the evidence of the effect that normal or polynomial bases have on the implementation. This gives us further insight on the choice of basis with respect to the field extension. In the process, we present a *special normal basis*, when used in conjunction with $\mathbb{F}_{(2^3)^2}$ results in the least (or very close to least) area in terms of GE for the 18 (6 quadratic and 12 cubic) S-boxes studied in this work. The special normal basis reported here has some algebraic properties which make it inherently hardware friendly and allow us to predict the area reduction, without running a tool. Overall, this work constitutes an extensive hardware characterization of a class of cryptographically significant 6-bit S-boxes giving us interesting insights into the systematic lightweight implementation of S-boxes without relying on an automated tool.

Keywords: Lightweight · S-box · Composite Field · Hardware Implementation

1 Introduction

There are two sides of cryptography, the first one is the theory that we use to come up with a secure design, and the second is the implementation aspect. Once a secure design is available, it becomes important to find an optimal implementation of it in hardware and software. For symmetric primitives such as block ciphers and cryptographic permutations, S-boxes play an important role as they introduce the nonlinearity/confusion into these designs. Apart from a high nonlinearity, S-boxes should have good cryptographic

Received: 2024-04-15 Accepted: 2024-06-15 Published: 2024-08-31

properties such as low differential uniformity, and high degree to resist powerful well-known attacks. At one end, we have `AES` [DBN+01] standard `Rijndael` [DR02] block cipher that uses an 8-bit S-box, and on the other end, we have designs like `PRESENT` [BKL+07] and `GIFT` [BPP+17] which use 4-bit S-boxes with the goal of minimizing the hardware cost. A further push to lightweight designs was given when the NIST initiated the standardization of lightweight cryptography algorithms [NIS19]. Finally, in 2022, `ASCON` [DEMS21] authenticated encryption with associated data (AEAD) was selected as the new lightweight cryptography standard. One interesting design choice of `ASCON` is that it used 5-bit S-boxes. Although the application of a 5-bit S-box was not new (as `KECCAK` [PA11] had already used it), `ASCON` was the first to apply a 5-bit S-box with non-trivial branch numbers (both differential and linear branch numbers are equal to 3) that helped in reducing the number of rounds. Later, `SYCON` [MSST22] AEAD was proposed that aimed to further reduced the hardware cost of `ASCON`, and it used a different 5-bit S-box with similar properties, but having a lighter cost in hardware than `ASCON`'s S-box. There have been applications of 6-bit S-boxes too; for example, block ciphers like `SC2000` [SYY+02], `FIDES` [BBK+13], `BipBip` [BDD+23], `SPEEDY` [LMMR21] have used 6-bit S-boxes. Most notably, the only known APN permutations on even dimensions were discovered in the class of 6-bit S-boxes, that we call `APN6` [BDMW10]. From the advancement of symmetric-key cryptography, it is now visible that the study of 6-bit S-boxes has started getting a momentum.

Broadly, there are two approaches to construct an S-box with desirable properties. One approach to construct an n-bit S-box is by selecting n component Boolean functions in n variables so that the S-box is a permutation and has a lighter implementation. Another approach is the finite field based constructions of S-boxes over $\mathbb{F}_{2^n}$.

In practice, the representation of S-boxes has a great impact on its implementation. For example, if we consider implementing an S-box defined over an extension field, one needs to define the finite field at the first place, as an extension can be defined in several ways. There are different types of bases and irreducible polynomials to choose from. Therefore, before implementing an S-box defined over a finite field, one needs a careful consideration regarding the implementation of the field. The case of composite fields is interesting as there are different subfields that can have the bases of extension. For instance, an efficient implementation of the AES S-box was presented by studying the composite structure of the field $\mathbb{F}_{2^8}$ [Rij00]. The class of 4-bit S-boxes is well-analyzed, and there are several tools (e.g., LIGHTER [JPST17], PEIGEN [BGLS19]) that can find efficient implementations. However, for 5-bit S-boxes, there is no scope of exploiting the composite field structure, so one has to depend on synthesis tools to find an efficient implementation.

The case of 6-bit S-boxes is interesting as $\mathbb{F}_{2^6}$ is a composite field. However, to the best of our knowledge, the implementation aspect of 6-bit S-boxes exploiting the composite field structure of $\mathbb{F}_{2^6}$ has not been studied yet. In this paper, we aim to fill this gap, and show field decompositions to find efficient S-box implementations in hardware.

1.1 Our Contribution

In this paper, we address a topic which has not received any attention from the hardware community of cryptography: efficient implementation of 6-bit S-boxes exploiting the decomposition of $\mathbb{F}_{2^6}$. Below we summarize our contributions.

A detailed analysis of the decomposition of $\mathbb{F}_{2^6}$. Earlier decomposition of $\mathbb{F}_{2^8}$ was done by [Rij00] for an efficient implementation of AES S-box. Our study is more comprehensive as we look at the decomposition of $\mathbb{F}_{2^6}$ covering the different extensions of different subfields and also considering several bases. We focus on the S-boxes of the form $\mathcal{S}(x) = \lambda x^d + \ell(x)$, where $\ell(x)$ is a linearized polynomial over $\mathbb{F}_{2^6}$ and our decomposition method is shifted a little from the general approach to better support this form of S-boxes. The optimal

decomposition of $\mathbb{F}_{2^6}$ is achieved through the first three degree followed by two degree ('three-two') extension, particularly when dealing with higher-degree ($d \geq 3$) S-boxes. The exponentiation operation is based on the binomial expansion. As a result, the first two degree followed by three degree ('two-three') extension involves a large number of constant multiplications and additions on $\mathbb{F}_{2^2}$.

Composite field analysis with respect to a special basis. In the binomial expansion pertaining to the exponentiation, the constant multiplication operation on the lower field depends on the type of basis and polynomial chosen. In the case of the second extension for the 'three-two' extension, we identified a specific normal basis that eliminates the need for any constant multiplication operation in the lower field. Our optimized implementation results are given in Table 1.

Table 1: Summary of the best results in terms of area with respect to the best decomposition of $\mathbb{F}_{2^6}$ reported in this work. Here, $\mathcal{LBN}$, $\mathcal{DBN}$, $\mathcal{LIN}$, $\mathcal{DU}$ and deg denote the linear branch number, differential branch number, linearity, differential uniformity and degree of the S-box, respectively.

S-box	Cryptographic Properties					LUT			ANF			Field Decomposition		
	$\mathcal{LBN}$	$\mathcal{DBN}$	$\mathcal{LIN}$	$\mathcal{DU}$	deg	Area (GE)	Latency (ns)	Power (μW)	Area (GE)	Latency (ns)	Power (μW)	Area (GE)	Latency (ns)	Power (μW)
SMS5	3	3	16	4	2	121.50	0.71	6.58	79.50	0.82	4.96	74.50	1.16	6.18
SMS10	3	3	16	4	2	118.75	0.74	6.31	79.50	0.82	4.96	74.50	1.16	5.90
SMS17	3	3	16	4	2	115.50	0.70	6.44	79.75	0.78	4.93	74.75	1.16	5.93
SMS20	3	3	16	4	2	116.25	0.77	6.62	79.50	0.82	4.96	74.75	1.16	5.93
SMS34	3	3	16	4	2	121.00	0.77	6.61	80.25	0.78	5.05	74.50	1.16	5.90
SMS40	3	3	16	4	2	115.50	0.70	6.44	79.75	0.78	4.93	74.75	1.16	5.93
SMS13	3	3	16	4	3	150.25	0.92	7.84	140.75	0.94	7.91	128.00	1.98	13.76
SMS19	3	3	16	4	3	150.25	0.92	7.84	145.00	0.90	8.20	124.75	2.19	14.00
SMS26	3	3	16	4	3	150.25	0.92	7.84	142.75	0.88	8.06	124.75	2.19	14.00
SMS38	3	3	16	4	3	156.25	1.01	7.77	143.50	0.88	8.14	133.50	2.36	17.02
SMS41	3	3	16	4	3	150.25	0.92	7.84	150.00	0.84	8.08	132.00	1.83	11.96
SMS52	3	3	16	4	3	158.00	0.98	8.16	147.75	1.00	7.74	131.25	2.32	16.05
SMSL13	3	3	64	8	3	126.00	0.79	7.20	136.50	0.78	7.12	120.75	2.25	12.98
SMSL19	3	3	64	8	3	124.75	0.84	7.18	134.25	0.72	7.32	118.75	2.02	11.93
SMSL26	3	3	64	8	3	126.00	0.79	7.20	141.25	0.90	7.52	119.75	2.40	13.46
SMSL38	3	3	64	8	3	126.00	0.79	7.20	137.75	0.86	7.30	116.50	2.24	13.36
SMSL41	3	3	64	8	3	126.00	0.79	7.20	136.00	0.88	7.68	116.50	2.22	13.44
SMSL52	3	3	64	8	3	126.00	0.79	7.20	137.50	0.88	7.28	117.75	2.28	13.59
x^{23}	2	2	24	10	4	133.50	1.16	7.82	129.00	0.78	7.32	127.75	0.98	7.14
x^{62}	2	2	16	4	5	139.50	0.86	7.68	128.50	0.76	6.66	137.75	2.90	22.92

Application in lightweight implementation of S-boxes. Once we have the best possible decomposition of $\mathbb{F}_{2^6}$, we apply this to implement 6-bit S-boxes. Although our method is general enough to consider S-boxes of the form $\mathcal{S}(x) = \lambda x^d + \ell(x)$, however, for the sake of lightweightness, we stick to degree 2 and 3. Further we choose $\ell(x) = 0$ or $\ell(x) = \mu x$. We do not restrict to the S-boxes of the form x^d only, we intentionally include the form $\lambda x^d + \ell(x)$ as this class contains S-boxes with good cryptographic properties and notably S-boxes with linear and differential branch number 3. Seeing that 6-bit S-boxes are getting attention, we provide lightweight implementations of these S-boxes which serves as the stepping stone for efficient and cryptographically significant 6-bit S-boxes that could be used in cipher designs.

2 Preliminaries

2.1 Notations

Let $\mathbb{F}_{2^n}$ be a finite field with 2^n elements and $\mathbb{F}_2^n$ be an n-dimensional vector space over $\mathbb{F}_2$. Let $wt(x)$ be the Hamming weight of $x \in \mathbb{F}_2^n$. The symbol $\oplus$ is the bitwise XOR operation and $x \cdot y$ is $x_0y_0 \oplus \cdots \oplus x_{n-1}y_{n-1}$, where $x = (x_0, \ldots, x_{n-1})\mathbb{F}_2^n$ and $y = (y_0, \ldots, y_{n-1})\mathbb{F}_2^n$.

An n-bit S-box is a permutation $\mathcal{S} : \mathbb{F}_2^n \to \mathbb{F}_2^n$. The S-box $\mathcal{S}$ can also be viewed as an n-tuple of Boolean functions in n-variable, i.e., $\mathcal{S} = (f_1, \ldots, f_n)$, where $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$, where f_i is called a *coordinate* function of $\mathcal{S}$ and any linear combination of coordinate functions is called a *component* function of $\mathcal{S}$.

Equivalently, an S-box can also be defined over the finite field $\mathbb{F}_{2^n}$ as an univariate permutation polynomial $F(x)$.

We denote by $\mathbb{GL}(n, \mathbb{F}_2)$, the set of all linear permutations of $\mathbb{F}_2^n$. Clearly $\mathbb{GL}(n, \mathbb{F}_2)$ is a proper subset of the set of all permutations over $\mathbb{F}_2^n$.

2.2 Composite Field and Isomorphisms

In this subsection, we recall the notion of composite fields which is central to the understanding of the current work. Moreover we add some basic concepts pertaining to the field isomorphisms which will aid the reader to grasp the rest of the work. We start by stating the following well-known definition.

Definition 1 (Composite Field)**.** Let a and b be two positive integers such that $q = a \times b$. Then the field $\mathbb{F}_{(2^a)^b}$ is called a *composite field*, which is isomorphic to $\mathbb{F}_{2^q}$, if there exist irreducible polynomials, $f(x)$ of degree a and $g(y)$ of degree b, which are used to extend $\mathbb{F}_2$ to $\mathbb{F}_{2^a}$, and $\mathbb{F}_{2^a}$ to $\mathbb{F}_{(2^a)^b}$ respectively.

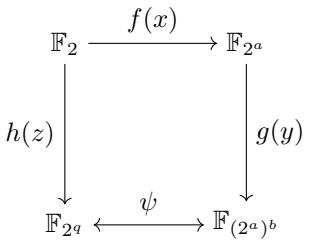

Figure 1: Composite field structure for $\mathbb{F}_{(2^a)^b}$ with $q = a \times b$.

Finite fields of the same order are *isomorphic*. Hence, the fields $\mathbb{F}_{2^q}$ and $\mathbb{F}_{(2^a)^b}$ are isomorphic since $q = a \times b$. Let ω, α and β be the primitive elements in the fields $\mathbb{F}_{2^q}$, $\mathbb{F}_{2^a}$, and $\mathbb{F}_{(2^a)^b}$, respectively, with multiplication modulo polynomials $h(z)$, $f(x)$ and $g(y)$. The map $\psi : \mathbb{F}_{2^q} \to \mathbb{F}_{(2^a)^b}$ is defined as: $\psi(0) = 0$, $\psi(\omega^i) = (\beta^\xi)^i$, $0 \leq i \leq 2^q - 2$, for $\xi \in \mathbb{Z}^+$ such that β^ξ is a primitive element in $\mathbb{F}_{(2^a)^b}$. This mapping is an isomorphism between $\mathbb{F}_{2^q}$ and $\mathbb{F}_{(2^a)^b}$ if $h(\beta^\xi) \equiv 0 \bmod g(\beta)$. The number of field isomorphisms between these two fields is q, that is there are q different values of ξ to form an isomorphism map. The composite field structure of $\mathbb{F}_{(2^a)^b}$ induced by its isomorphism with $\mathbb{F}_{2^q}$ is illustrated in Figure 1.

2.3 Cryptographic Properties of S-boxes

We first briefly describe the cryptographic properties of an S-box such as nonlinearity, differential uniformity, and algebraic degree [Car10]. The nonlinearity of an n-variable Boolean function f is the measure of the distance of f from the set of all n-variable affine Boolean functions. The nonlinearity of the S-box $\mathcal{S}$ is the minimum nonlinearity among all the component function of $\mathcal{S}$. The algebraic degree of $\mathcal{S}$ is the maximum degree of its coordinate functions.

Let $\mathcal{S}(\delta, \Delta) = \#\{x \in \mathbb{F}_2^n : \mathcal{S}(x) \oplus \mathcal{S}(x \oplus \delta) = \Delta\}$, where δ is the input difference and Δ is the output difference. Differential uniformity of $\mathcal{S}$ is defined as $\mathcal{DU}_\mathcal{S} = \max_{\delta \neq 0, \Delta}\{\mathcal{S}(\delta, \Delta)\}$.

Lower $\mathcal{DU}_{\mathcal{S}}$ has higher resistance against the differential attack [BS91]. S-boxes having the least possible $\mathcal{DU}$ which is 2, are called Almost Perfect Nonlinear (APN) functions. The differential distribution table (DDT) of an S-box is the matrix representation of all possible input-output differences for the S-box where the (δ, Δ)-th element of DDT is $\mathcal{S}(\delta, \Delta)$.

The correlation coefficient of $\mathcal{S}$ with respect to an input mask $\alpha \in \mathbb{F}_2^n$ and an output mask $\beta \in \mathbb{F}_2^n$ is given by

$$\mathtt{C}_{\mathcal{S}}(\alpha, \beta) = \sum_{x \in \mathbb{F}_2^n} (-1)^{\beta \cdot \mathcal{S}(x) + \alpha \cdot x}. \tag{1}$$

If $\mathcal{S}(x) = (f_1(x), \ldots, f_n(x))$, then $\beta \cdot \mathcal{S}(x)$ is a Boolean function that is a linear combination of $\{f_1(x), \ldots, f_n(x)\}$, and $\alpha \cdot x$ is a linear Boolean function of the form $\ell_1 x_1 \oplus \ldots \oplus \ell_n x_n$. Nonlinearity of $\mathcal{S}$ is $2^{n-1} - \frac{1}{2} \max |\mathtt{C}_{\mathcal{S}}(\alpha, \beta)|$. The correlation matrix $\mathtt{C}_{\mathcal{S}}$ of $\mathcal{S}$ is a $2^n \times 2^n$ matrix indexed by $\alpha, \beta \in \mathbb{F}_2^n$ in which the entry in the cell (α, β) is given by $\mathtt{C}_{\mathcal{S}}(\alpha, \beta)$.

Differential and linear properties are related to differential and linear branch numbers, as described below.

Definition 2. The differential branch number of $\mathcal{S}$, denoted by $\mathcal{DBN}(\mathcal{S})$, and the linear branch number of $\mathcal{S}$, denoted by $\mathcal{LBN}(\mathcal{S})$, are defined as

$$\mathcal{DBN}(\mathcal{S}) = \min_{x, x' \in \mathbb{F}_2^n, x \neq x'} \{wt(x \oplus x') + wt(\mathcal{S}(x) \oplus \mathcal{S}(x'))\},$$

$$\mathcal{LBN}(\mathcal{S}) = \min_{\alpha, \beta \in \mathbb{F}_2^n, \mathtt{C}_{\mathcal{S}}(\alpha, \beta) \neq 0} \{wt(\alpha) + wt(\beta)\},$$

where $\mathtt{C}_{\mathcal{S}}(\alpha, \beta)$ is the correlation coefficient as in Eq. (1).

Partitioning the class of S-boxes according to an *affine equivalence* relation is important to study cryptographic properties of S-boxes.

Definition 3 (Affine Equivalence)**.** Let $\mathcal{S}, \mathcal{S}'$ be two permutations of $\mathbb{F}_2^n$. We say that $\mathcal{S}$ is affine equivalent to $\mathcal{S}'$ if there exist matrices A, $B \in \mathbb{GL}(n, \mathbb{F}_2)$, and $c, d \in \mathbb{F}_2^n$ such that

$$\mathcal{S}'(x) = B \cdot \mathcal{S}[A\,x \oplus c] \oplus d, \qquad \text{for all } x \in \mathbb{F}_2^n. \tag{2}$$

Affine equivalence preserves some cryptographic properties of S-boxes, such as differential uniformity, nonlinearity, degree (greater than 1). However, it does not preserve branch numbers in general. In some special cases such as when A and B are permutation matrices (matrix obtained by permuting rows (or columns) of an identity matrix), then we have $\mathcal{DBN}(\mathcal{S}) = \mathcal{DBN}(\mathcal{S}_1)$ and $\mathcal{LBN}(\mathcal{S}) = \mathcal{LBN}(\mathcal{S}_1)$.

3 Revisiting the SMS Construction of S-boxes

3.1 The SMS Construction [SMS19]

In this section, we discuss how cryptographically significant 6-bit S-boxes are generated. We consider lightweight 6-bit S-boxes that have non-trivial branch numbers, meaning S-boxes with differential branch number 3 and linear branch number 3. We focus on the S-boxes having the form $\mathcal{S}(x) = \lambda x^d + \ell(x)$ for $x \in \mathbb{F}_{2^6}$, where $\ell(x)$ is a linearized polynomial. This form of S-boxes is chosen as our implementation of $\mathbb{F}_{2^6}$ is arranged keeping this type of form in mind.

The study of 6-bit S-boxes with differential and linear branch number 3 was initiated in [SMS19]. They used the link between the resilient Boolean functions and the linear branch number, and proposed algorithms to obtain 5-bit and 6-bit S-boxes with differential and linear branch number 3. In the following, we propose an improvement of their algorithms for finding such functions efficiently.

We first give the definition of a resilient Boolean function.

Definition 4. A Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is called r-resilient if

$$\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \alpha \cdot x} = 0,$$

for all $\alpha \in \mathbb{F}_2^n$ such that $0 \leq wt(\alpha) \leq r$.

The relation between resilient Boolean functions and a linear branch number was first mentioned in [SS18] which is as follows.

Lemma 1. *All the coordinate Boolean functions of the S-box $\mathcal{S}$ are $(\mathcal{LBN}(\mathcal{S}) - 2)$-resilient and the algebraic degree $deg(\mathcal{S}) \leq n - \mathcal{LBN}(\mathcal{S}) + 1$.*

Therefore, for an n-bit S-box with linear branch number 3, all its coordinate Boolean functions must be 1-resilient and the degree is bounded by $n - 2$.

A brief description of the method for finding S-boxes with differential and linear branch number 3 that was followed in [SMS19] is as follows. First, a collection of 1-resilient n-variable Boolean functions is chosen. Among them, n-subsets are checked if they form an S-box (permutation). If so, then the S-box has linear branch number 3. Next, an affine equivalence class of the S-box is searched. As mentioned earlier, an affine equivalence class does not preserve branch number, so the search ends when an S-box with linear and differential branch number 3 is found.

One drawback of this algorithm is that when an S-box, say $\mathcal{S}$ with linear branch number 3 is obtained, then it has to search for all possible A, $B \in \mathbb{GL}(n, \mathbb{F}_2)$ such that the new S-box obtained as $\mathcal{S}'(x) = B \cdot \mathcal{S}[A\,x]$ has both linear and differential branch numbers equal to 3. For quadratic S-boxes, [SMS19] chose A and B to be binary Toeplitz matrices.

In our search, for quadratic and cubic S-boxes with linear and differential branch number 3, we take the basic algorithm from [SMS19], however we make a significantly different choices for A and $B \in \mathbb{GL}(n, \mathbb{F}_2)$.

We take a 'minimal' approach for upgrading an S-box with linear branch number 3 to the one with linear and differential branch number 3. For instance, we take $B = \mathcal{I}$, where $\mathcal{I}$ is the identity matrix. This will add no cost for B. So we expect $\mathcal{S}'$ such that $\mathcal{S}'(x) = \mathcal{S}(Ax)$ to have linear and differential branch number 3. The first choice for A would have been permutation matrices as they would incur no cost over $\mathcal{S}$. However, applying a transformation by a permutation matrix does not alter the branch numbers, thus this option is ruled out. So we move to the next choice which are matrices of the form $T_{i,j} = \mathcal{I} + E_{i,j}$, where $E_{i,j}$ is the binary matrix having only 1 as the (i, j)-th entry. This type of matrices are well known in matrix theory and they are called Type III elementary matrices. These matrices are quite hardware friendly as there is only one row that has two 1's incurring only one XOR for that. Based on the above discussions, we now describe the steps that we take for generating lightweight S-boxes with linear and differential branch number 3.

Construction 1. *1. We apply Algorithm 1 of [SMS19] to obtain an 6-bit S-box with linear branch number 3 of degree 2 of the form*

$$\mathcal{S}(x) = \lambda x^d + \mu x,$$

for $x \in \mathbb{F}_{2^6}$, where $\lambda (\neq 0), \mu \in \mathbb{F}_{2^6}$.

2. We check S-boxes $\mathcal{S}'$ given by $\mathcal{S}'(x) = \mathcal{S}(Ax)$, where A comes from the class of Type III matrices of dimension 6×6.

3. After running for all such Type III matrices, we check if any S-box with linear and differential branch number equal to 3 is found.

Note that we are not interested in much general form of linearized polynomial $\ell(x)$ and consider μx instead as we strictly maintaining the lightweight approach.

In Appendix C, we provide 6 quadratic S-boxes and 12 cubic S-boxes which we derive from Construction 1. The notation for the S-boxes which are generated from the function x^d is denoted by SMSd and for the S-boxes having nonzero linear term denoted by SMSLd.

3.2 Implementation of S-box in $\mathbb{F}_{2^6}$

An S-box over $\mathbb{F}_{2^6}$ can be viewed as a mapping from $\mathbb{F}_{2^6}$ to $\mathbb{F}_{2^6}$. The S-boxes in [SMS19] are constructed using a special class of functions of the form $F(x) = \lambda x^d + \mu x$, where λ, μ is a constant in $\mathbb{F}_{2^6}$ and $0 < d < 64$. For example, if $wt(d) = 2$, it is called the quadratic class and if $wt(d) = 3$, it is called the cubic class. Given a power mapping $F(x) = x^d$, in the SMS construction, an S-box that has a linear branch number 3 is constructed as follows:

$$\mathcal{S}(x) = (Tr(\lambda_0 F(x)), Tr(\lambda_1 F(x)), \cdots, Tr(\lambda_5 F(x))) \tag{3}$$

where $Tr(\lambda_i F(x)), 0 \leq i \leq 5$ are component functions and $\lambda_0, \lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5 \in \mathbb{F}_{2^6}$ are chosen so that $Tr(\lambda_i F(x))$ is a 1-resilient function. Equation (3) can be written as $\mathcal{S}(x) = M \cdot F(x)$, where M is an invertible matrix defined by $\lambda_0, \lambda_1, \lambda_2, \lambda_3, \lambda_4$, and λ_5. Applying affine transformations A and B on the input and output of $\mathcal{S}(x)$, we may get an S-box, $\mathcal{S}'(x) = B\mathcal{S}(Ax)$, with $\mathcal{DBN} = 3$ and $\mathcal{LBN} = 3$. The details of computing $S'(x)$ is shown in Figure 2. Implementing S' requires computing three matrix multiplications and

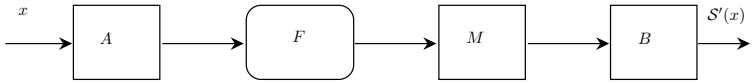

Figure 2: A high-level overview of computing S' on an input x

$F(x) = \lambda x^d + \mu x$. To reduce the matrix multiplication cost, the authors used a low-cost Toeplitz matrix A and the identity matrix B. Our hardware optimization in this work mainly focused on an optimized implementation of $F(x) = x^d$ in an isomorphic composite field as λ and μ constant values which may need some extra hardware cost.

4 Characterizing Composite Field Structure of $\mathbb{F}_{2^6}$

In this section, we furnish a comprehensive characterization of the finite field $\mathbb{F}_{2^6}$ with respect to its composite field structure. This is vital to our overall aim of coming up with lightweight implementations of 6-bit S-boxes which are cryptographically significant. We start by outlining the representations of $\mathbb{F}_{2^6}$ as extensions of $\mathbb{F}_{2^2}$ and $\mathbb{F}_{2^3}$. We then explore the problem of choosing a basis (polynomial or normal) while exploring its implication on the *lightweightness* of the resulting implementation. We conclude the section by formulating the expression for a general power function in the composite field of $\mathbb{F}_{2^6}$, as we are focusing on the implementation of the S-boxes of the form $\mathcal{S}(x) = \lambda x^d + \mu x$.

4.1 Decomposition of $\mathbb{F}_{2^6}$

The field $\mathbb{F}_{2^6}$ can be generated by employing any primitive polynomial $h(z)$ of degree 6 over $\mathbb{F}_2$. The structural characteristics of field elements vary based on the chosen primitive polynomial, leading to distinct representations in isomorphic fields. Without loss of generality, we choose the primitive polynomial $h(z) = z^6 + z^4 + z^3 + z + 1$ as a defining polynomial for the field $\mathbb{F}_{2^6}$. Assuming ω as a primitive element in $\mathbb{F}_{2^6}$ over $\mathbb{F}_2$ multiplication modulo primitive polynomial $h(z)$, then any element in $\mathbb{F}_{2^6}$ can be expressed

as $\theta = \vartheta_0 + \vartheta_1\omega + \vartheta_2\omega^2 + \vartheta_3\omega^3 + \vartheta_4\omega^4 + \vartheta_5\omega^5$, where ϑ_i's belong to $\mathbb{F}_2$. Equivalently we can say the elements in $\mathbb{F}_{2^6}$ are nothing but just binary strings $(\vartheta_5, \vartheta_4, \vartheta_3, \vartheta_2, \vartheta_1, \vartheta_0) \in \mathbb{F}_2^6$.

Furthermore, the representation of elements in $\mathbb{F}_{2^6}$ takes two distinct forms, depending upon the chosen composite field structure. The composite field for $\mathbb{F}_{2^6}$ can be constructed in two ways, illustrated in Figure 3. One approach involves a 3-degree extension followed by a 2-degree extension, while the alternative method consists of a 2-degree extension followed by a 3-degree extension. Both composite constructions and element representations will be elaborated below.

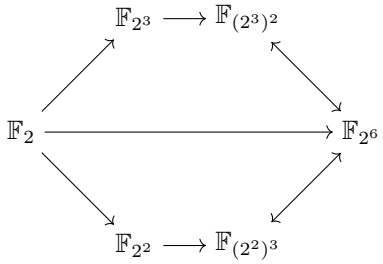

Figure 3: Composite Field Structure for $\mathbb{F}_{2^6}$.

Structure of $\mathbb{F}_{2^6}$ as an extension of $\mathbb{F}_{2^2}$. The only primitive polynomial of degree 2 in $\mathbb{F}_2[x]$ is $f_2(x) = x^2 + x + 1$. Consequently, for the first extension, by default, we have to choose $f_2(x)$. To form an isomorphic composite field of $\mathbb{F}_{2^6}$ it is necessary to fix the degree of extension to 3 in the next extension. The polynomial choices for constructing $\mathbb{F}_{2^6}$ are given by,

$$\mathbb{F}_2 \xrightarrow{x^2+x+1} \mathbb{F}_{2^2} \xrightarrow{y^3+\Delta_0 y^2+\Delta_1 y+\Delta_2} \mathbb{F}_{2^6}.$$

There are 12 primitive polynomials of degree 3 in $\mathbb{F}_{2^2}[y]$, which are of the form $g_3(y) = y^3 + \Delta_0 y^2 + \Delta_1 y + \Delta_2$ for the second extension with $\Delta_i \in \mathbb{F}_{2^2}$. Combining these two polynomials yields the composite field $\mathbb{F}_{(2^2)^3}$.

The field $\mathbb{F}_{(2^2)^3}$ is also a vector space over $\mathbb{F}_{2^2}$ with a dimension of three. Therefore, any element in $\mathbb{F}_{(2^2)^3}$ can be expressed as a linear combination of its basis vectors. Let us assume β is a primitive element in $\mathbb{F}_{(2^2)^3} = \mathbb{F}_{2^2}[y]/\langle g_3(y)\rangle$. Therefore, every basis is of the form $\mathcal{B} = \{\beta^{\mathcal{L}_0}, \beta^{\mathcal{L}_1}, \beta^{\mathcal{L}_2}\}$, for some values of $0 \leq \mathcal{L}_0, \mathcal{L}_1, \mathcal{L}_2 \leq 62$. Consequently, any element in $\mathbb{F}_{(2^2)^3}$ is expressed as $\theta = \theta_0\beta^{\mathcal{L}_0} + \theta_1\beta^{\mathcal{L}_1} + \theta_2\beta^{\mathcal{L}_2}$, where $\theta_i \in \mathbb{F}_{2^2}$.

Moreover, the field $\mathbb{F}_{2^2}$ is a vector space of dimension 2 over $\mathbb{F}_2$. Therefore, θ_i's can similarly be expressed in terms of the basis vectors of $\mathbb{F}_{2^2}$. Suppose α is a primitive element in $\mathbb{F}_{2^2} = \mathbb{F}_2[x]/\langle f_2(x)\rangle$. Then every element in $\mathbb{F}_{2^2}$ is represented by $\theta_i = \theta_{i_0}\alpha^{l_0} + \theta_{i_1}\alpha^{l_1}$, with respect to the basis $\mathcal{C} = \{\alpha^{l_0}, \alpha^{l_1}\}$, for some $0 \leq l_0, l_1 \leq 2$. Different choices of primitive polynomials in each step of the extension will result in distinct representations of elements in $\mathbb{F}_{(2^2)^3}$.

Structure of $\mathbb{F}_{2^6}$ as an extension of $\mathbb{F}_{2^3}$. There exist two primitive polynomials of degree 3 in $\mathbb{F}_2[x]$: $f_3(x) = x^3 + x^2 + 1$ and $f_3(x) = x^3 + x + 1$. This gives us two potential choices to construct the isomorphic composite field of $\mathbb{F}_{2^6}$ during the initial extension. We have considered the polynomial $f_3(x) = x^3 + x^2 + 1$ for the rest of our work.

For the second extension, there are 18 primitive polynomials of the form $g_2(y) = y^2 + \Gamma_0 y + \Gamma_1$, where Γ_0 and Γ_1 belong to $\mathbb{F}_{2^3}$. Consequently, the selection of primitive polynomials for each extension step is outlined as follows.

$$\mathbb{F}_2 \xrightarrow{x^3+x^2+1} \mathbb{F}_{2^3} \xrightarrow{y^2+\Gamma_0 y+\Gamma_1} \mathbb{F}_{2^6}.$$

Likewise, the composite field $\mathbb{F}_{(2^3)^2}$ is also a vector space over $\mathbb{F}_{2^3}$ with a dimension of two. Let γ be a primitive element in $\mathbb{F}_{(2^3)^2} = \mathbb{F}_{2^3}[x]/\langle g_2(y)\rangle$. Consequently, any basis of $\mathbb{F}_{(2^3)^2}$ would be the form $\mathcal{B}^* = \{\gamma^{\mathcal{M}_0}, \gamma^{\mathcal{M}_1}\}$ for some $0 \leq \mathcal{M}_0, \mathcal{M}_1 \leq 62$. Thus, an element in $\mathbb{F}_{(2^3)^2}$ can be expressed as $\theta = \theta_0\gamma^{\mathcal{M}_0} + \theta_1\gamma^{\mathcal{M}_1}$, where $\theta_0, \theta_1 \in \mathbb{F}_{2^3}$.

Furthermore, $\mathbb{F}_{2^3}$ acts as a vector space of dimension three over $\mathbb{F}_2$. Let δ be a primitive element in $\mathbb{F}_{2^3} = \mathbb{F}_2[x]/\langle f_3(x)\rangle$, then every element in $\mathbb{F}_{2^3}$ can be represented by $\theta_i = \theta_{i_0}\delta^{m_0} + \theta_{i_1}\delta^{m_1} + \theta_{i_2}\delta^{m_2}$ with respect to the basis $\mathcal{C}^* = \{\delta^{m_0}, \delta^{m_1}, \delta^{m_2}\}$ for some $0 \leq m_0, m_1, m_2 \leq 6$.

Based on the choice of the primitive polynomials, a total of 12 for $\mathbb{F}_{(2^2)^3}$ and 18 for $\mathbb{F}_{(2^3)^2}$ different composite field structures are possible. Now we can choose any particular isomorphism map to represent any element in the composite field. The representation is also dependent on various combinations of bases in each step of extension. This implies that one could have different implementations of the same function based on their choice of field extension as well as the associated bases. However, which ones of these choices *would lead to a lightweight implementation* of the function under consideration is *not known a priori*. This is a fundamental problem that we aim to address in this work for a particular class of functions over $\mathbb{F}_{2^6}$ giving S-boxes.

In the following subsection we will discuss how to get the transformation matrix of $\mathbb{F}_{2^6}$ and its composite field according to the choice of different bases.

4.2 Transformation Matrix for Different Choices of Bases

The transformation matrix is important for representing elements under any chosen basis. The elements in the field $\mathbb{F}_{2^6}$ are represented with respect to a polynomial basis; therefore, it is necessary to transform these elements to a composite field basis.

Transformation matrix between $\mathbb{F}_{2^6}$ and $\mathbb{F}_{(2^2)^3}$. Let ω is a primitive element in $\mathbb{F}_{2^6} = \mathbb{F}_2[z]/\langle h(z)\rangle$ and ψ be an isomorphism between $\mathbb{F}_{2^6}$ and $\mathbb{F}_{(2^2)^3}$. Thus there exits κ and τ such that $\alpha = \psi(\omega^\kappa)$ and $\beta = \psi(\omega^\tau)$, since ω generates the multiplicative group of $\mathbb{F}_{2^6}$. Therefore one can easily obtain the values of κ and τ from the composite field isomorphisms, which depend on the values of ξ. How to find the value of ξ is discussed in Subsection 2.2.

Let us consider the following bases.

- $\mathcal{P} = \{1, \omega, \omega^2, \omega^3, \omega^4, \omega^5\}$ be a polynomial basis of $\mathbb{F}_{2^6}/\mathbb{F}_2$.
- $\mathcal{B} = \{\beta^{\mathcal{L}_0}, \beta^{\mathcal{L}_1}, \beta^{\mathcal{L}_2}\}$ be a basis of $\mathbb{F}_{(2^2)^3}/\mathbb{F}_{2^2}$
- $\mathcal{C} = \{\alpha^{l_0}, \alpha^{l_1}\}$ be a basis of $\mathbb{F}_{2^2}/\mathbb{F}_2$.

This implies that the following.

- $\mathcal{BC} = \{\beta^{\mathcal{L}_0}\alpha^{l_0}, \beta^{\mathcal{L}_0}\alpha^{l_1}, \beta^{\mathcal{L}_1}\alpha^{l_0}, \beta^{\mathcal{L}_1}\alpha^{l_1}, \beta^{\mathcal{L}_2}\alpha^{l_0}, \beta^{\mathcal{L}_2}\alpha^{l_1}\}$ is a basis of $\mathbb{F}_{(2^2)^3}/\mathbb{F}_2$,
- Each $\beta^{\mathcal{L}_j}\alpha^{l_i}$ has a pre-image in $\mathbb{F}_{2^6}$ which is $\omega^{l_i\kappa+\mathcal{L}_j\tau} = \psi^{-1}(\alpha^{l_i}\beta^{\mathcal{L}_j})$

Thus the transition matrix between the basis

$$\{\omega^{l_0\kappa+\mathcal{L}_0\tau}, \omega^{l_1\kappa+\mathcal{L}_0}, \omega^{l_0\kappa+\tau\mathcal{L}_1}, \omega^{l_1\kappa+\mathcal{L}_1\tau}, \omega^{l_0\kappa+\mathcal{L}_2\tau}, \omega^{l_1\kappa+\mathcal{L}_2\tau}\}$$

and the polynomial basis $\mathcal{P}$ is the inverse isomorphism between $\mathbb{F}_{2^6}$ and $\mathbb{F}_{(2^2)^3}$. Therefore, the inverse transition matrix gives us the required transformation matrix.

Transformation matrix between $\mathbb{F}_{2^6}$ and $\mathbb{F}_{(2^3)^2}$. Similarly for the isomorphism map ϕ between $\mathbb{F}_{2^6}$ and $\mathbb{F}_{(2^3)^2}$ there are κ and τ such that $\gamma = \phi(\omega^\kappa)$ and $\delta = \phi(\omega^\tau)$. Suppose $\mathcal{B}^* = \{\gamma^{\mathcal{M}_0}, \gamma^{\mathcal{M}_1}\}$ is a basis for $\mathbb{F}_{(2^3)^2}/\mathbb{F}_{2^3}$ and $\mathcal{C}^* = \{\delta^{m_0}, \delta^{m_1}, \delta^{m_2}\}$ is a basis for $\mathbb{F}_{2^3}/\mathbb{F}_2$ then again the inverse transition matrix between the bases $\{\omega^{\kappa m_0+\tau\mathcal{M}_0}, \omega^{\kappa m_1+\tau\mathcal{M}_0}, \omega^{\kappa m_2+\tau\mathcal{M}_0}, \omega^{\kappa m_0+\tau\mathcal{M}_1}, \omega^{\kappa m_1+\tau\mathcal{M}_1}, \omega^{\kappa m_2+\tau\mathcal{M}_1}\}$ and the polynomial basis $\mathcal{P}$ provides the transformation matrix according to chosen bases.

Enumerating different possible representations. The transformation matrix varies depending upon different values for κ, τ, and the diverse choice of the primitive polynomial in each extension. The number of field isomorphisms between the fields $\mathbb{F}_{2^6}$ and $\mathbb{F}_{(2^2)^3}$ or $\mathbb{F}_{(2^3)^2}$ is precisely 6. That is for a fixed choice of basis in each level of extension we encounter 6 different transition matrices. Thus, for 12 different primitive polynomials of $g_3(y)$ and 18 different primitive polynomials of $g_2(y)$ (as discussed in the previous sub-section) total number of different possible representations is given below. Each of the representations leads to different implementation of the SMS S-boxes under consideration.

		# Field Isomorphisms		# Primitive Polynomials		
$\mathbb{F}_{2^6} \leftrightarrow \mathbb{F}_{(2^3)^2}$: #Representations	=	$\overbrace{6}$	×	$\overbrace{12}$	=	72
$\mathbb{F}_{2^6} \leftrightarrow \mathbb{F}_{(2^2)^3}$: #Representations	=	6	×	18	=	180

4.3 Choice of Bases

Choosing a different basis for the extension field results in a distinct representation of a field element influencing the implementation of functions defined over the field. Hence, the selection of the underlying basis is crucial for the hardware implementation. As mentioned earlier, we consider extensions $\mathbb{F}_{(2^2)^3}$ and $\mathbb{F}_{(2^3)^2}$, where we opted for combinations of polynomial and normal bases at every level of these extension to reduce the circuit complexity. While other basis types are viable and there are too many such options to exhaust. Therefore, we only concentrate on the polynomial normal basis types. One particular reason for choosing a normal basis is that the squaring of a linear combination of these basis elements is free.

Let us recall the general form of bases from Subsection 4.1.

$$\overbrace{\mathcal{B} = \{\beta^{\mathcal{L}_0}, \beta^{\mathcal{L}_1}, \beta^{\mathcal{L}_2}\}}^{\mathbb{F}_{(2^2)^3}/\mathbb{F}_{2^2}} \qquad \overbrace{\mathcal{C} = \{\alpha^{l_0}, \alpha^{l_1}\}}^{\mathbb{F}_{2^2}/\mathbb{F}_2}$$

$$\overbrace{\mathcal{B}^* = \{\gamma^{\mathcal{M}_0}, \gamma^{\mathcal{M}_1}\}}^{\mathbb{F}_{(2^3)^2}/\mathbb{F}_{2^3}} \qquad \overbrace{\mathcal{C}^* = \{\delta^{m_0}, \delta^{m_1}, \delta^{m_2}\}}^{\mathbb{F}_{2^3}/\mathbb{F}_2}$$

So, for some $1 \leq \mathcal{J} \leq 2$, the polynomial basis and normal basis of $\mathbb{F}_{2^2}$ are respectively given below.

- $\{1, \alpha\}$ $(l_0 = 0, l_1 = 1)$
- $\{\alpha^{\mathcal{J}}, (\alpha^{\mathcal{J}})^2\}$ $(l_0 = \mathcal{J}, l_1 = 2\mathcal{J})$

Similarly, for some $1 \leq \mathcal{K} \leq 62$, the polynomial basis and normal basis of $\mathbb{F}_{(2^2)^3}$ are respectively given below.

- $\{1, \beta, \beta^2\}$ $(\mathcal{L}_0 = 0, \mathcal{L}_1 = 1, \mathcal{L}_2 = 2)$
- $\{\beta^{\mathcal{K}}, (\beta^{\mathcal{K}})^4, (\beta^{\mathcal{K}})^{16}\}$ $(\mathcal{L}_0 = \mathcal{K}, \mathcal{L}_1 = 4\mathcal{K}, \mathcal{L}_2 = 16\mathcal{K})$

For the first extension, we consider the normal basis $\{\alpha, \alpha^2\}$. For the second extension we find that $\{\beta^{\mathcal{K}}, (\beta^{\mathcal{K}})^4, (\beta^{\mathcal{K}})^{16}\}$ forms a basis for $\mathcal{K} = 1$ only with respect to 6 primitive

polynomials $g_3(y)$ out of 12. For the remaining 6 primitive polynomials, we find that $\{\beta^{\mathcal{K}}, (\beta^{\mathcal{K}})^4, (\beta^{\mathcal{K}})^{16}\}$ forms a basis for $\mathcal{K} = 3$.

We denote the combination of the polynomial and normal basis of the field $\mathbb{F}_{(2^2)^3}$ as follows.

- $\mathsf{P}\text{-}\mathsf{P}_2^3 = \{1, \alpha, \beta, \alpha\beta, \beta^2, \alpha\beta^2\}$.
- $\mathsf{P}\text{-}\mathsf{N}_2^3 = \{\alpha, \alpha^2, \alpha\beta, \alpha^2\beta, \alpha\beta^2, \alpha^2\beta^2\}$.
- $\mathsf{N}\text{-}\mathsf{P}_2^3 = \{\{\beta, \alpha\beta, \beta^4, \alpha\beta^4, \beta^{16}, \alpha\beta^{16}\}\ , \{\beta^3, \alpha\beta^3, \beta^{12}, \alpha\beta^{12}, \beta^{48}, \alpha\beta^{48}\}\}$.
- $\mathsf{N}\text{-}\mathsf{N}_2^3 = \{\{\alpha\beta, \alpha^2\beta, \alpha\beta^4, \alpha^2\beta^4, \alpha\beta^{16}, \alpha^2\beta^{16}\}\ , \{\alpha\beta^3, \alpha^2\beta^3, \alpha\beta^{12}, \alpha^2\beta^{12}, \alpha\beta^{48}, \alpha^2\beta^{48}\}\}$.

Next, we describe the choice of bases for $\mathbb{F}_{(2^3)^2}$. For some $1 \leq \mathcal{J} \leq 6$, the polynomial basis and normal basis for $\mathbb{F}_{2^3}$ are given by

- $\{1, \delta, \delta^2\}$ $(m_0 = 0, m_1 = 1, m_2 = 2)$
- $\{\delta^{\mathcal{J}}, (\delta^{\mathcal{J}})^2, (\delta^{\mathcal{J}})^4\}$ $(m_0 = \mathcal{J}, m_1 = 2\mathcal{J}, m_2 = 4\mathcal{J})$.

For some $1 \leq \mathcal{K} \leq 62$, the polynomial basis and normal basis of $\mathbb{F}_{(2^3)^2}$ are respectively,

- $\{1, \gamma\}$ $(\mathcal{M}_0 = 0, \mathcal{M}_1 = 1)$
- $\{\gamma^{\mathcal{K}}, (\gamma^{\mathcal{K}})^8\}$ $(\mathcal{M}_0 = \mathcal{K}, \mathcal{M}_1 = 8\mathcal{K})$.

For the first extension, we utilize the conventional normal basis $\{\delta, \delta^2, \delta^4\}$, and for the second extension, we employ $\{\gamma, \gamma^8\}$.

The combination of the polynomial and normal basis for the field $\mathbb{F}_{(2^3)^2}$ is denoted as follows.

- $\mathsf{P}\text{-}\mathsf{P}_3^2 = \{1, \delta, \delta^2, \gamma, \gamma\delta, \gamma\delta^2\}$.
- $\mathsf{P}\text{-}\mathsf{N}_3^2 = \{\delta, \delta^2, \delta^4, \gamma\delta, \gamma\delta^2, \gamma\delta^4\}$.
- $\mathsf{N}\text{-}\mathsf{P}_3^2 = \{\gamma, \delta\gamma, \delta^2\gamma, \gamma^8, \delta\gamma^8, \delta^2\gamma^8\}$.
- $\mathsf{N}\text{-}\mathsf{N}_3^2 = \{\delta\gamma, \delta^2\gamma, \delta^4\gamma, \delta\gamma^8, \delta^2\gamma^8, \delta^4\gamma^8\}$.

Therefore, we have considered in total $72 \times 4 = 288$ representations of the field $\mathbb{F}_{(2^2)^3}$, and $108 \times 4 = 432$ representations of the field $\mathbb{F}_{(2^3)^2}$ according to the above choice of bases. We have considered in total 720 representations of the field $\mathbb{F}_{2^6}$. Moreover, we introduce a special kind of normal basis in the second extension for each composite field, which we will discuss in Section 5. In the following subsection, our primary focus shifts to discussing the implementation of the exponentiation function for a fixed-choice of basis.

4.4 Exponentiation Operation in the Composite Field

We are concentrating on the lightweight implementation of the cryptographically significant S-box of the form $\mathcal{S}(x) = \lambda x^d + \mu x$; therefore, efficient implementation of the exponentiation function leads to efficient implementation for these functions. We can choose either the field $\mathbb{F}_{(2^2)^3}$ or $\mathbb{F}_{(2^3)^2}$ for the implementation. We will discuss the exponentiation concerning different composite fields one by one and show how the implementation results differ. Suppose d is any positive integer, then d can be represented using its binary representation, and the number of ones in its binary representation is the hamming weight of d. Let the hamming weight of d be t then $d = 2^{d_1} + 2^{d_2} + \cdots + 2^{d_t}$, where $0 \leq d_i \leq \lfloor \log_2 d \rfloor + 1$, $1 \leq i \leq t$.

Exponentiation in the field $\mathbb{F}_{(2^2)^3}$. Recall $\mathcal{B} = \{\beta^{\mathcal{L}_0}, \beta^{\mathcal{L}_1}, \beta^{\mathcal{L}_2}\}$ is a basis of $\mathbb{F}_{(2^2)^3}$, so the representation of an element $\theta \in \mathbb{F}_{(2^2)^3}$ can be expressed as $\theta = \theta_0\beta^{\mathcal{L}_0} + \theta_1\beta^{\mathcal{L}_1} + \theta_2\beta^{\mathcal{L}_2}$, where $\theta_0, \theta_1, \theta_2 \in \mathbb{F}_{2^2}$. Therefore, the exponentiation of θ is given by,

$$\begin{aligned}
\theta^d &= \left(\theta_0\beta^{\mathcal{L}_0} + \theta_1\beta^{\mathcal{L}_1} + \theta_2\beta^{\mathcal{L}_2}\right)^d \\
&= \left(\theta_0\beta^{\mathcal{L}_0} + \theta_1\beta^{\mathcal{L}_1} + \theta_2\beta^{\mathcal{L}_2}\right)^{\sum_{i=1}^{t} 2^{d_i}} \\
&= \prod_{i=1}^{t} (\theta_0\beta^{\mathcal{L}_0} + \theta_1\beta^{\mathcal{L}_1} + \theta_2\beta^{\mathcal{L}_2})^{2^{d_i}} \\
&= \prod_{i=1}^{t} (\theta_0^{2^{d_i}}\beta^{\mathcal{L}_0 2^{d_i}} + \theta_1^{2^{d_i}}\beta^{\mathcal{L}_1 2^{d_i}} + \theta_2^{2^{d_i}}\beta^{\mathcal{L}_2 2^{d_i}}) \\
&= \sum_{i_1,\cdots,i_t \in \{0,1,2\}} \theta_{i_1}^{2^{d_1}} \cdots \theta_{i_t}^{2^{d_t}} \beta^{(\mathcal{L}_{i_1} 2^{d_1} + \mathcal{L}_{i_2} 2^{d_2} + \cdots + \mathcal{L}_{i_t} 2^{d_t})} \\
&= \sum_{i_1,\cdots,i_t \in \{0,1,2\}} \alpha^0_{i_1\cdots i_t} \theta_{i_1}^{2^{d_1}} \cdots \theta_{i_t}^{2^{d_t}} \beta^{\mathcal{L}_0} + \sum_{i_1,\cdots,i_t \in \{0,1,2\}} \alpha^1_{i_1\cdots i_t} \theta_{i_1}^{2^{d_1}} \cdots \theta_{i_t}^{2^{d_t}} \beta^{\mathcal{L}_1} + \\
&\quad \sum_{i_1,\cdots,i_t \in \{0,1,2\}} \alpha^2_{i_1\cdots i_t} \theta_{i_1}^{2^{d_1}} \cdots \theta_{i_t}^{2^{d_t}} \beta^{\mathcal{L}_2} \qquad (4)
\end{aligned}$$

The coefficients $\alpha^0_{i_1\cdots i_t}$, $\alpha^1_{i_1\cdots i_t}$, $\alpha^2_{i_1\cdots i_t}$ are elements of the field $\mathbb{F}_{2^2}$, as each exponent of β can be represented by the basis $\mathcal{B}$ over $\mathbb{F}_{2^2}$. These coefficients indicate which scalar multiplication is required in the lower field. However, the scalar multiplication varies depending on the chosen primitive polynomial. Thus, the exponentiation in $\mathbb{F}_{2^6}$ is reduced to the field operations such as exponentiation, addition, multiplication, and scalar multiplication in $\mathbb{F}_{2^2}$, which is the main advantage using the composite field. Appendix A provides all the subfield operations in $\mathbb{F}_{2^2}$, corresponding to the polynomial and normal bases.

Exponentiation in the field $\mathbb{F}_{(2^3)^2}$. Any element in $\mathbb{F}_{(2^3)^2}$ also be expressed as a linear combination of its basis $\mathcal{B}^* = \{\gamma^{\mathcal{M}_0}, \gamma^{\mathcal{M}_1}\}$. So, the element in $\mathbb{F}_{(2^3)^2}$ is expressed as $\theta = \theta_0\gamma^{\mathcal{M}_0} + \theta_1\gamma^{\mathcal{M}_1}$. Therefore, the exponentiation is given by,

$$\begin{aligned}
\theta^d &= (\theta_0\gamma^{\mathcal{M}_0} + \theta_1\gamma^{\mathcal{M}_1})^d \\
&= (\theta_0\gamma^{\mathcal{M}_0} + \theta_1\gamma^{\mathcal{M}_1})^{\sum_{i=1}^{t} 2^{d_i}} \\
&= \prod_{i=1}^{t} (\theta_0\gamma^{\mathcal{M}_0} + \theta_1\gamma^{\mathcal{M}_1})^{2^{d_i}} \\
&= \prod_{i=1}^{t} (\theta_0^{2^{d_i}}\gamma^{\mathcal{M}_0 2^{d_i}} + \theta_1^{2^{d_i}}\gamma^{\mathcal{M}_1 2^{d_i}}) \\
&= \sum_{i_1,\cdots,i_t \in \{0,1\}} \theta_{i_1}^{2^{d_1}} \cdots \theta_{i_t}^{2^{d_t}} \gamma^{(\mathcal{M}_{i_1} 2^{d_1} + \cdots + \mathcal{M}_{i_t} 2^{d_t})} \\
&= \sum_{i_1,\cdots,i_t \in \{0,1\}} \alpha^0_{i_1\cdots i_t} \theta_{i_1}^{2^{d_1}} \cdots \theta_{i_t}^{2^{d_t}} \gamma^{\mathcal{M}_0} + \sum_{i_1\cdots i_t \in \{0,1\}} \alpha^1_{i_1\cdots i_t} \theta_{i_1}^{2^{d_1}} \cdots \theta_{i_t}^{2^{d_t}} \gamma^{\mathcal{M}_1} \qquad (5)
\end{aligned}$$

The coefficients $\alpha^0_{i_1\cdots i_t}$, $\alpha^1_{i_1\cdots i_t}$ are the scalars in $\mathbb{F}_{2^3}$. In this case, the exponentiation operation in $\mathbb{F}_{2^6}$ is reduced to some exponentiation, addition, multiplication, and scalar multiplication in the lower field $\mathbb{F}_{2^3}$. The subfield operations in $\mathbb{F}_{2^3}$ with respect to polynomial and normal bases are provided in Appendix B.

The subfield operations in the field $\mathbb{F}_{2^3}$ are more costly compared to $\mathbb{F}_{2^2}$. However, utilizing $\mathbb{F}_{2^3}$ provides the advantage, especially when implementing higher-algebraic-degree

exponential functions like $\mathcal{S}(x) = x^d$, where the Hamming weight of d is greater than or equal to 3. The combination of polynomial and normal bases facilitates an efficient implementation of the SMS S-boxes. The implementation cost of these S-boxes is provided in Table 4, Table 5 and Table 6. The next question arises: can we reduce the subfield operation? Yes, we can reduce the scalar multiplication operation by choosing a special kind of basis. We will discuss the basis in the following section.

5 Introducing a Special Normal Basis

Suppose we opt for either a polynomial basis or a normal basis in the second extension. Then, the implementation of the exponentiation requires scalar multiplications in the intermediate field ($\mathbb{F}_{2^2}$ or $\mathbb{F}_{2^3}$), adding an additional cost to the implementation. In this section, we introduce a *special normal basis* that possesses inherent algebraic properties, eliminating the need for scalar multiplication operations. Furthermore, this basis provides a more closed form for each coordinate while calculating the exponent. In Theorem 1 and Theorem 2, we discuss how to find such *special normal basis*.

Theorem 1. *Let $\mathcal{SN}^* = \{\gamma_1, \gamma_2\}$ be a basis of $\mathbb{F}_{(2^3)^2}/\mathbb{F}_{2^3}$ such that γ_1, γ_2 are the roots of $f(x) = x^2 + x + 1$ over $\mathbb{F}_2$. Then, $\mathcal{SN}^*$ is a normal basis over $\mathbb{F}_{2^3}$, and any power of γ_1 is a linear span of $\mathcal{SN}^*$ over $\mathbb{F}_2$.*

Proof. Since γ_1, γ_2 are the roots of $f(x) = x^2 + x + 1$, then $\gamma_1 + \gamma_2 = 1$ and $\gamma_1 \cdot \gamma_2 = 1$. Again, we have $\gamma_1^2 + \gamma_1 + 1 = 0$, which implies $\gamma_1^2 = 1 + \gamma_1 = \gamma_2$ and $\gamma_1^3 = 1$. Combining these two, we get $\gamma_2 = \gamma_1^8$, that is, $\mathcal{SN}^* = \{\gamma_1, \gamma_1^8\}$ is a normal basis. Let k be a positive integer. Then $k \equiv 0, 1, 2 \bmod 3$, which implies, γ_1^k is equivalent to $\gamma_1 + \gamma_2, \gamma_1, \gamma_2$.

Corollary 1. *If $\theta = (\theta_0, \theta_1)$ is an element with respect to this basis $\mathcal{SN}^*$, then for any positive integer k, $\theta^{2^k} = (\theta_0^{2^k}, \theta_1^{2^k})$ if k is even, otherwise $(\theta_1^{2^k}, \theta_0^{2^k})$.*

Since γ_1 is an element of $\mathbb{F}_{(2^3)^2}$, there is a value $\mathcal{K}$ such that $\gamma_1 = \gamma^{\mathcal{K}}$. If $\mathcal{SN}^* = \{\gamma^{\mathcal{K}}, \gamma^{8\mathcal{K}}\}$ is a basis, then it serves as a normal basis for $\mathbb{F}_{(2^3)^2}$. We found that the only possible values for which $\mathcal{SN}^*$ forms a basis are $\mathcal{K} = 21$ and 42 for all choices of the polynomials on the second extension.

If $\chi = \gamma^{21}$, then $\mathcal{SN}^* = \{\chi, \chi^8\}$ is the normal basis over $\mathbb{F}_{2^3}$. Hence, from Equation 5, the exponentiation in $\mathbb{F}_{(2^3)^2}$ can be expressed as:

$$\begin{aligned} \theta^d &= (\theta_0\chi + \theta_1\chi^8)^d \\ &= \prod_{i=1}^{t} \{\theta_0^{2^{d_i}} \chi^{2^{d_i}} + \theta_1^{2^{d_i}} (\chi^8)^{2^{d_i}}\} \\ &= \sum_{i_1,\cdots,i_t \in \{0,1\}} \alpha^0_{i_1\cdots i_t} \theta_{i_1}^{2^{d_1}} \cdots \theta_{i_t}^{2^{d_t}} \chi + \sum_{i_1,\cdots,i_t \in \{0,1\}} \alpha^1_{i_1\cdots i_t} \theta_{i_1}^{2^{d_1}} \cdots \theta_{i_t}^{2^{d_t}} \chi^8 \end{aligned} \tag{6}$$

where $\alpha^0_{i_1\cdots i_t}$ and $\alpha^1_{i_1\cdots i_t}$ are in $\mathbb{F}_2$, as χ^k can be represented as a linear combination of χ and χ^8 over $\mathbb{F}_2$ for a positive integer k. This basis eliminates the need for scalar multiplications in $\mathbb{F}_{2^3}$, which makes it advantageous for an efficient hardware implementation.

For example, consider the function $F(x) = x^d$, with $d = 5 = 2^{d_1} + 2^{d_2}$ and $d_1 = 0, d_2 = 2$ and $t = 2$. For the basis $\mathcal{SN}^* = \{\chi, \chi^8\}$, we have $\mathcal{M}_0 = 21, \mathcal{M}_1 = 42$. Then the

Table 2: Some useful function implementation respect to special normal basis $\mathcal{SN}^*$.

Values of d	Coordinates
5	$[(\theta_0+\theta_1)^5+\theta_0^5,(\theta_0+\theta_1)^5+\theta_1^5]$
10	$[(\theta_0+\theta_1)^3+\theta_1^3,(\theta_0+\theta_1)^3+\theta_0^3]$
20	$[(\theta_0+\theta_1)^6+\theta_0^6,(\theta_0+\theta_1)^6+\theta_1^6]$
13	$\{(\theta_0+\theta_1)^2+\theta_0\theta_1)\}[\theta_0^4,\theta_1^4]$
19	$\{(\theta_0+\theta_1)^4+(\theta_0\theta_1)^2)\}[\theta_0,\theta_1]$
38	$\{(\theta_0+\theta_1)+(\theta_0\theta_1)^4)\}[\theta_1^2,\theta_0^2]$
23	$\{\theta_0^2\theta_1^2(\theta_0^2+\theta_1^2)(\theta_0\theta_1+\theta_0^2+\theta_1^2)\}[\theta_1,\theta_0]+[\theta_1^2,\theta_0^2]$
62	$(\theta_0^2+\theta_1^2+\theta_0\theta_1)^6[\theta_1,\theta_0]$

exponentiation computation can be written as

$$\begin{aligned}
\theta^5 &= (\theta_0\gamma^{\mathcal{M}_0}+\theta_1\gamma^{\mathcal{M}_1})^5\\
&= \sum_{i_1,i_2\in\{0,1\}} \theta_{i_1}^{2^{d_1}}\theta_{i_2}^{2^{d_2}}\gamma^{(\mathcal{M}_{i_1}2^{d_1}+\mathcal{M}_{i_2}2^{d_2})}\\
&= \sum_{i_1,i_2\in\{0,1\}} \theta_{i_1}\theta_{i_2}^{4}\gamma^{(\mathcal{M}_{i_1}+4\mathcal{M}_{i_2})}\\
&= \theta_0\theta_0^4\gamma^{42}+\theta_0\theta_1^4\gamma^{0}+\theta_1\theta_0^4\gamma^{0}+\theta_1\theta_1^4\gamma^{21}\\
&= \theta_0^5\chi^8+\theta_0\theta_1^4(\chi+\chi^8)+\theta_1\theta_0^4(\chi+\chi^8)+\theta_1^5\chi\\
&= (\theta_1^5+\theta_0\theta_1^4+\theta_0\theta_1^4)\chi+(\theta_0^5+\theta_0\theta_1^4+\theta_0\theta_1^4)\chi^8\\
&= \{(\theta_0+\theta_1)^5+\theta_0^5\}\chi+\{(\theta_0+\theta_1)^5+\theta_1^5\}\chi^8 \qquad (7)
\end{aligned}$$

Therefore, to efficiently compute $F(x)=x^5$ in $\mathbb{F}_{2^6}$, we need only three additions and three fifth power operations in $\mathbb{F}_{2^3}$. Similarly, one can write an expression like above for $\mathcal{K}=42$. We summarize the S-boxes of the form $\mathcal{S}(x)=x^d$ in Table 2, which are useful for designing S-boxes discussed in Section 3 with respect to the basis $\{\chi,\chi^8\}$. Note that the implementations of x^d with $d=40,17,34,41,26,52$ directly follow the implementation of x^d for $d=5,10,20,13,19,38$ respectively, with a rotation on inputs as the exponents are in the same coset.

For the combination of the polynomial and normal basis in the first extension, the special normal basis of $\mathbb{F}_{(2^3)^2}$ is denoted as follows.

- $\mathsf{SN\text{-}P}_3^2=\{\gamma^{21},\delta\gamma^{21},\delta^2\gamma^{21},\gamma^{42},\delta\gamma^{42},\delta^2\gamma^{42}\}$.
- $\mathsf{SN\text{-}N}_3^2=\{\delta\gamma^{21},\delta^2\gamma^{21},\delta^4\gamma^{21},\delta\gamma^{42},\delta^2\gamma^{42},\delta^4\gamma^{42}\}$.

Theorem 2. *Let $\mathcal{SN}=\{\beta_1,\beta_2,\beta_3\}$ be a basis of $\mathbb{F}_{(2^2)^3}/\mathbb{F}_{2^2}$ such that β_0, β_1, β_3 are the roots of the equation $f(x)=x^3+x^2+1$ in $\mathbb{F}_2[x]$. Then, $\mathcal{SN}$ is a normal basis over $\mathbb{F}_{2^2}$, and any power of β_1 is a linear span of $\mathcal{SN}$ in $\mathbb{F}_2$.*

Proof. Since β_1 is a root of $x^3+x^2+1=0$, $\beta_1^3+\beta_1^2+1=0$ and $\beta_1^7=1$. This implies $\beta_1^{16}=\beta_1^2$. Now, $(\beta_1^4)^3+(\beta_1^4)^2+1=\beta_1^5+\beta_1+1=0$ and $(\beta_1^{16})^3+(\beta_1^{16})^2+1=\beta_1^6+\beta_1^4+1=0$. Therefore, $\beta_2=\beta_1^4$ and $\beta_3=\beta_1^{16}$, that means if $\mathcal{SN}=\{\beta_1,\beta_2,\beta_3\}$ forms a basis, it must be a normal basis. For any positive integer k with $k\equiv 0,1,2,3,4,5,6 \bmod 7$, β_1^k is equivalent to $\beta_1+\beta_2+\beta_3,\beta_1,\beta_3,\beta_1+\beta_2,\beta_2,\beta_2+\beta_3,\beta_1+\beta_3$, that is, any power of β_1 is a linear span of $\mathcal{B}$ over $\mathbb{F}_2$.

Corollary 2. *If $\theta = (\theta_0, \theta_1, \theta_2)$ be any element with respect to this basis $\mathcal{SN}$, then for any positive integer k, $\theta^{2^k} = (\theta_0^{2^k}, \theta_1^{2^k}, \theta_2^{2^k})$ if $k = 3n$ or $(\theta_2^{2^k}, \theta_0^{2^k}, \theta_1^{2^k})$ if $k = 3n+1$ or $(\theta_1^{2^k}, \theta_2^{2^k}, \theta_0^{2^k})$ if $k = 3n+2$ for a positive integer n.*

Since β_1 is an element of $\mathbb{F}_{(2^2)^3}$ there is a $\mathcal{K}$ such that $\beta_1 = \beta^{\mathcal{K}}$. If $\mathcal{SN} = \{\beta^{\mathcal{K}}, \beta^{4\mathcal{K}}, \beta^{16\mathcal{K}}\}$ is a basis, then it is a normal basis for $\mathbb{F}_{(2^2)^3}$. We found that the only possible values for which $\mathcal{SN}$ forms a basis are $\mathcal{K} = 9, 18, 27, 36, 45$, and 54 for the choice of the polynomials for the second extension.

If $\chi = \beta^9$, then $\mathcal{SN} = \{\chi, \chi^4, \chi^{16}\}$ is a normal basis over $\mathbb{F}_{2^3}$, and from Equation 4, the exponentiation computation in $\mathbb{F}_{(2^2)^3}$ can be written as:

$$\begin{aligned}\theta^d &= (\theta_0\chi + \theta_1\chi^4 + \theta_1\chi^{16})^d \\ &= \sum_{i_1,,\cdots,i_t \in \{0,1,2\}} \alpha^0_{i_1\cdots i_t} \theta_{i_1}^{2^{d_1}} \cdots \theta_{i_t}^{2^{d_t}} \chi + \sum_{i_1,\cdots,i_t \in \{0,1,2\}} \alpha^1_{i_1\cdots i_t} \theta_{i_1}^{2^{d_1}} \cdots \theta_{i_t}^{2^{d_t}} \chi^4 + \\ &\quad \sum_{i_1,\cdots,i_t \in \{0,1,2\}} \alpha^2_{i_1\cdots i_t} \theta_{i_1}^{2^{d_1}} \cdots \theta_{i_t}^{2^{d_t}} \chi^{16} \end{aligned} \tag{8}$$

where $\alpha^0_{i_1\cdots i_t}$, $\alpha^1_{i_1\cdots i_t}$, $\alpha^2_{i_1\cdots i_t}$ belong to $\mathbb{F}_2$. Therefore, we do not need any scalar multiplication in $\mathbb{F}_{2^3}$, which gives an efficient hardware implementation. The addition, multiplication, and square operations are sufficient to perform an exponentiation operation. We summarize a compact form of the functions $\mathcal{S}(x) = x^d$, for $d = 5, 10, 13, 38$, with respect to the special normal basis on Table 3. The implementations for $d = \{\{20, 17\}, \{34, 41\}, \{52, 19\}, \{26, 41\}\}$ directly follow the implementation of $d = 5, 10, 13, 38$ with a rotation on inputs, respectively, as these power functions are in the same coset.

For the choice of the polynomial and normal basis in the first extension, our special normal basis of $\mathbb{F}_{(2^2)^3}$ is denoted as follows.

- $\mathsf{SN\text{-}P}_2^3 = \left\{ \begin{array}{c} \{\beta^9, \alpha\beta^9, \beta^{36}, \alpha\beta^{36}, \beta^{18}, \alpha\beta^{18}\}, \\ \{\beta^{27}, \alpha\beta^{27}, \beta^{45}, \alpha\beta^{45}, \beta^{54}, \alpha\beta^{54}\} \end{array} \right\}$
- $\mathsf{SN\text{-}N}_2^3 = \left\{ \begin{array}{c} \{\alpha\beta^9, \alpha^2\beta^9, \alpha\beta^{36}, \alpha^2\beta^{36}, \alpha\beta^{18}, \alpha^2\beta^{18}\}, \\ \{\alpha\beta^{27}, \alpha^2\beta^{27}, \alpha\beta^{45}, \alpha^2\beta^{45}, \alpha\beta^{54}, \alpha^2\beta^{54}\} \end{array} \right\}$

Table 3: Some 2-degree and 3-degree function implementation respect to special normal basis $\mathcal{SN}$.

Values of d	Coefficients
5	$[(\theta_1^2 + \theta_2^2 + \theta_0\theta_2), (\theta_0^2 + \theta_2^2 + \theta_0\theta_1), (\theta_0^2 + \theta_1^2 + \theta_1\theta_2)]$
10	$[(\theta_0 + \theta_2 + \theta_0^2\theta_1^2), (\theta_0 + \theta_1 + \theta_1^2\theta_2^2), (\theta_1 + \theta_2 + \theta_0^2\theta_2^2)]$
13	$[\theta_0 + \theta_1 + \theta_2^3\theta_0 + \theta_1^2(\theta_0\theta_1 + \theta_0\theta_2 + \theta_1\theta_2) + \theta_0^2(\theta_1^2 + \theta_2^2 + \theta_1\theta_2),$ $\theta_1 + \theta_2 + \theta_0^3\theta_1 + \theta_2^2(\theta_0\theta_1 + \theta_0\theta_2 + \theta_1\theta_2) + \theta_1^2(\theta_0^2 + \theta_2^2 + \theta_0\theta_2),$ $\theta_0 + \theta_2 + \theta_1^3\theta_2 + \theta_0^2(\theta_0\theta_1 + \theta_0\theta_2 + \theta_1\theta_2) + \theta_2^2(\theta_0^2 + \theta_1^2 + \theta_0\theta_1)]$
38	$[\theta_0^2 + \theta_0(\theta_1^2\theta_2^2 + \theta_0^2\theta_1^2) + (\theta_0 + \theta_1)^3\theta_2^2 + \theta_2(\theta_0 + \theta_1 + \theta_2 + \theta_0^2\theta_1^2),$ $\theta_1^2 + \theta_1(\theta_2^2\theta_0^2 + \theta_1^2\theta_2^2) + (\theta_1 + \theta_2)^3\theta_0^2 + \theta_0(\theta_0 + \theta_1 + \theta_2 + \theta_1^2\theta_2^2),$ $\theta_2^2 + \theta_2(\theta_0^2\theta_1^2 + \theta_2^2\theta_0^2) + (\theta_2 + \theta_0)^3\theta_1^2 + \theta_1(\theta_0 + \theta_1 + \theta_2 + \theta_2^2\theta_0^2)]$

Like other exponents in Table 3, one can derive the coefficients for the exponents $d = 23$ and 63, but we omit it here as the expression for these two functions is quite large. That

implies the hardware implementation cost of them is significantly high in the composite field $\mathbb{F}_{(2^2)^3}$.

We observed that the implementation on $\mathbb{F}_{(2^2)^3}$ of $\mathcal{S}(x) = x^d$ with an algebraic degree greater than two incurs a low cost of finite field operations in the intermediate field but leads to an increase in the number of base field additions. Conversely, in the case of the field $\mathbb{F}_{(2^3)^2}$, the base field operation is more expensive, yet the number of base field additions is reduced, resulting in significant hardware savings.

6 Hardware Implementation Results and Comparisons

With all the theory in place, we now share the results of the hardware implementation of the all different S-boxes that have been studied in this work. It is worth recalling that one single SMS S-box can be implemented in multiple ways based on the different representations discussed earlier as well the choice of the conventional basis and the special normal basis introduced in this work. Our results validate the claims of the special normal basis to be the natural choice for a better lightweight implementation *almost* across all implementation attempts. Before we proceed to delve deeper into the research insights derived and validated from the hardware implementation, we outline the comprehensiveness of the current work by enumerating the full spectrum of the implementations carried out.

	#Representations for a fixed basis		# Bases	
# $\mathbb{F}_{(2^2)^3}$ implementations/S-box =	72	×	6	= 432
# $\mathbb{F}_{(2^3)^2}$ implementations/S-box =	108	×	6	= 648
# S-boxes studied =	18			
# S-box implementations =	$(432 + 648) \times 18 = 19,440$			

In addition to these, we also implement two more functions $\mathcal{S}(x) = x^d$ with $d = 23$ and $d = 62$ using our special normal basis for the decompositions of $\mathbb{F}_{(2^3)^2}$. The function for $d = 23$ is a degree 4 function and the function for $d = 62$ is the inverse function, which has degree 5. That means we have considered all possible classes of power function in this implementation. We choose only the special normal bases ($\mathsf{SN\text{-}N}_3^2, \mathsf{SN\text{-}P}_3^2$) in this case as for the other cases the implementation contains a huge number of subfield operations. Finally, for the $(18 + 2)$ functions we have also synthesized their ANF and LUT logics to have a global comparison. So in total, we have implemented $19440 + (108 \times 2) \times 2 + 20 \times 2 = 19,912$ representations. All the implementation source codes and related scripts are available at https://github.com/de-ci-phe-red-LABS/KnowThyBasis.

Hardware implementation flow. All implementations were done using Verilog HDL. As regards register-transfer-level (RTL) synthesis for ASICs, the Cadence Genus Synthesis Solution tool was used with the 65 *nm* UMC Mixed-Mode Low Leakage Low-K cell library. The Genus tool configuration was set to `-effort high` for maximum area optimization. In order to compare area across implementations, gate-equivalent (GE) was used which is a standard parameter used for this purpose. The server configuration was 64 bit - Intel Xeon Processor (Skylake, IBRS) @ 2 GHz.

Implementation knockout and comparison strategy. As enumerated above, there were a close 20K implementations that had to be analyzed across 18 S-boxes. In order to come up with a fair comparison we sorted the results for each S-box across each basis for each of two decompositions of $\mathbb{F}_{2^6}$. The implementation with the least area for a particular choice of basis for a specific S-box made it to the comparison tables furnished in the subsections below. The comparisons were done locally among the SMS S-boxes with degrees 2 and 3 and degree 3 with linear terms. Within the local comparisons, segregation has been made

based on the conventional bases and the special normal bases on top of the decompositions. For more holistic data interpretation, best results from each segregated group are also compare. Here, by *abuse* of notation, we use the following to highlight most area efficient bases among conventional and specials bases as concluded from the implementation results.

- Special Normal Bases $\begin{cases} \mathsf{SB}_2^3 = \mathrm{Min}_{\mathrm{Area}}(\mathsf{SN\text{-}N}_2^3, \mathsf{SN\text{-}P}_2^3) \\ \mathsf{SB}_3^2 = \mathrm{Min}_{\mathrm{Area}}(\mathsf{SN\text{-}N}_3^2, \mathsf{SN\text{-}P}_3^2) \end{cases}$
- Conventional Bases $\begin{cases} \mathsf{CB}_2^3 = \mathrm{Min}_{\mathrm{Area}}(\mathsf{N\text{-}N}_2^3, \mathsf{N\text{-}P}_2^3, \mathsf{P\text{-}N}_2^3, \mathsf{P\text{-}P}_2^3) \\ \mathsf{CB}_3^2 = \mathrm{Min}_{\mathrm{Area}}(\mathsf{N\text{-}N}_3^2, \mathsf{N\text{-}P}_3^2, \mathsf{P\text{-}N}_3^2, \mathsf{P\text{-}P}_3^2) \end{cases}$

Finally, for a global comparison, the best basis-decomposition combination was pitted against the traditional LUT and ANF based implementations across all the 20 functions studied here. In the next subsections, the detailed results are furnished.

6.1 Results for 2-Degree SMS S-box

Here, we look at the area footprint of 2-degree SMS S-boxes which is captured by Table 4. The basis which registers the lowest area across the 6 choices is $\mathsf{N\text{-}P}_2^3$. However, what is interesting is that the clear second choice is our special normal basis $\mathsf{SN\text{-}N}_3^2$ and the difference between areas registered by $\mathsf{SN\text{-}N}_3^2$ and $\mathsf{N\text{-}P}_2^3$ is *only* ≤ 0.75 GE. This validates our claim on the special normal basis with regard to its inherent hardware friendliness. Figure 4 shows a comparative view of the conventional and special bases with respect to two decompositions of $\mathbb{F}_{2^6}$.

Table 4: Comparing all 2-degree SMS S-boxes across different bases. The best result is from basis $\mathsf{N\text{-}P}_2^3$ (highlighted in blue bold) while the second best is from basis $\mathsf{SN\text{-}N}_3^2$ (highlighted in black bold). The difference is upper bounded by 0.75 GE signifying how close they are.

S-box	$\mathsf{N\text{-}N}_2^3$	$\mathsf{N\text{-}P}_2^3$	$\mathsf{P\text{-}N}_2^3$	$\mathsf{P\text{-}P}_2^3$	$\mathsf{SN\text{-}N}_2^3$	$\mathsf{SN\text{-}P}_2^3$	$\mathsf{N\text{-}N}_3^2$	$\mathsf{N\text{-}P}_3^2$	$\mathsf{P\text{-}N}_3^2$	$\mathsf{P\text{-}P}_3^2$	$\mathsf{SN\text{-}N}_3^2$	$\mathsf{SN\text{-}P}_3^2$
SMS5	78.00	**74.25**	81.75	77.25	75.00	77.50	79.50	76.00	84.00	120.25	**74.50**	75.25
SMS10	79.50	**74.25**	80.50	77.75	75.25	77.50	94.00	123.00	81.75	125.25	**74.50**	76.50
SMS17	78.50	**74.25**	80.75	78.25	75.25	77.00	94.50	125.50	87.00	125.50	**74.75**	76.50
SMS20	78.50	**74.25**	78.25	78.25	75.00	78.25	80.00	77.50	76.75	77.50	**74.75**	75.50
SMS34	78.75	**73.75**	78.50	76.00	75.00	76.50	75.50	75.75	77.00	77.75	**74.50**	75.25
SMS40	79.50	**74.25**	78.00	77.75	75.25	77.00	78.00	79.25	83.50	118.50	**74.75**	75.50

6.2 Results for 3-Degree SMS S-box

The degree 3 functions are obviously more complex than degree 2 and would have higher area foot-print. The decomposition of $\mathbb{F}_{2^6}$ with respect to our special normal basis fares well here is able to lead to the minimum area. There is only one out-lier which, to our surprise seemed anomalous since its area was strikingly less than all of the bases considered for SMS41 S-box. The details of area are reported in Table 5. The basis $\mathsf{SN\text{-}N}_3^2$ gives the best result for two cases: $\mathsf{SN\text{-}P}_3^2$ provides the best area for three cases, and for the remaining one S-box, $\mathsf{P\text{-}P}_3^2$ gives the best result. However, what is interesting is that the special normal basis registers the best results on the maximum cases. This again validates our claim on this class of functions. Figure 5 shows a comparative view of the conventional and special bases with respect to the two decompositions of $\mathbb{F}_{2^6}$.

6.3 Results for 3-Degree SMS S-box with Linear Terms

Here again, the presence of additional linear terms increases the circuit complexity which the proposed special normal basis handles better. The results are furnished in captured by

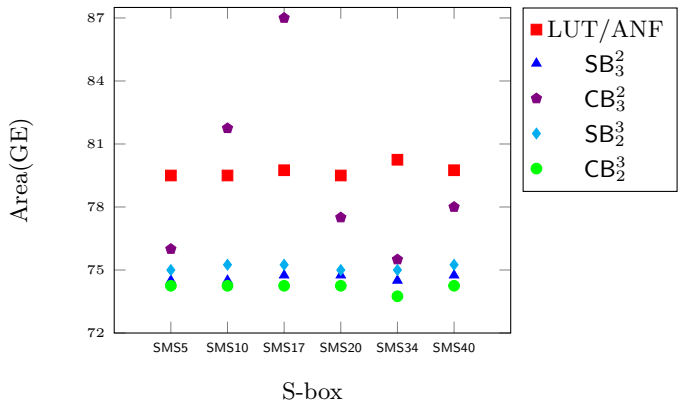

Figure 4: The area of all 2-degree S-boxes with respect to different basis choices. Here, SB_3^2 is the special basis and the extension order is "three-two", and CB_3^2 is the conventional basis and extension order is "two-three". The plotted points are minimum area with respect to each basis that we have achieved, as described above. From the proximity of the points $\in SB_3^2$ and CB_2^3, one can appreciate that the area achieved by using the special normal basis introduced here is very close to the minimum.

Table 5: Comparing all 3-degree SMS S-boxes having no linear term across different bases. The best result is from basis SN-P_3^2 and SN-N_3^2 (highlighted in blue bold) except for the S-box SMS41. In this case we got almost all the best results from SB_3^2.

S-box	N-N_2^3	N-P_2^3	P-N_2^3	P-P_2^3	SN-N_2^3	SN-P_2^3	N-N_3^2	N-P_3^2	P-N_3^2	P-P_3^2	SN-N_3^2	SN-P_3^2
SMS13	137.25	137.25	136.50	136.00	153.25	182.50	136.25	137.00	136.50	135.25	132.25	**128.00**
SMS19	137.75	140.25	136.50	136.50	152.75	181.00	135.75	137.00	137.00	137.50	132.75	**124.75**
SMS26	135.75	135.75	136.75	137.25	150.75	185.75	135.00	137.00	138.00	136.75	132.75	**124.75**
SMS38	137.50	140.25	137.00	139.75	152.25	145.25	137.00	137.25	138.25	137.00	**133.50**	133.75
SMS41	135.75	137.75	138.00	136.50	151.50	185.50	138.25	138.50	138.50	**117.00**	132.00	132.00
SMS52	137.50	137.50	136.25	137.50	153.25	182.50	137.50	137.75	137.50	139.00	**131.25**	133.75

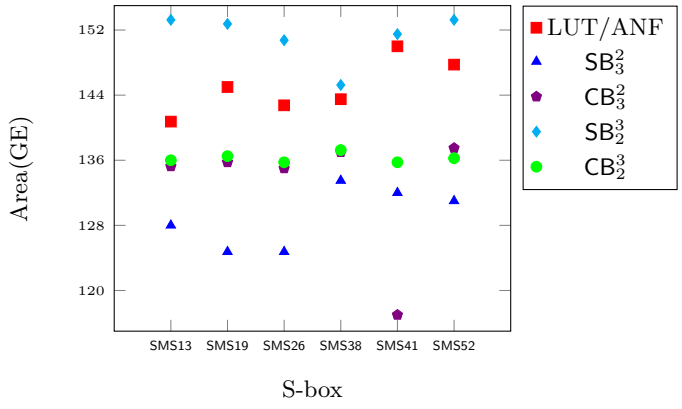

Figure 5: The area of all 3-degree S-boxes with respect to different basis choices. Like above, the plotted points represent the are minimum area with respect to each basis that we have achieved. With the exception of SMS41 implemented using conventional basis CB_3^2, in all other cases the special normal basis registers the minimum area with considerable margin.

Table 6. The basis SN-N_3^2 provides the best result for four S-boxes and the basis SN-P_3^2 registers the lowest area for the remaining two S-boxes. This validates our claim on the special normal basis with regard to its inherent hardware friendliness. Like above, a more holistic view is depicted in Figure 6 plotting the best results across conventional and special basis groups.

Table 6: Comparing all 3-degree SMS S-boxes having non zero linear term across different bases. The best result is from basis SN-P_3^2 and SN-N_3^2 (highlighted in blue bold). In this case we got all the best results from SB_3^2.

S-box	N-N_2^3	N-P_2^3	P-N_2^3	P-P_2^3	SN-N_2^3	SN-P_2^3	N-N_3^2	N-P_3^2	P-N_3^2	P-P_3^2	SN-N_3^2	SN-P_3^2
SMSL13	127.00	127.25	126.00	125.50	133.00	134.00	120.75	126.75	123.50	122.25	**120.75**	125.50
SMSL19	125.25	129.75	127.25	125.00	139.50	134.50	128.00	124.50	128.00	122.75	119.25	**118.75**
SMSL26	128.75	128.75	124.25	124.25	138.75	133.75	123.00	121.50	124.00	123.75	120.75	**119.75**
SMSL38	127.75	127.75	126.75	126.75	136.25	135.50	125.00	127.50	125.25	123.00	**116.50**	130.25
SMSL41	130.00	130.25	124.50	126.25	136.00	132.75	125.50	126.00	123.00	119.75	**116.50**	126.75
SMSL52	130.75	130.75	122.75	124.50	133.00	136.50	124.00	125.00	123.00	123.50	**117.75**	130.25

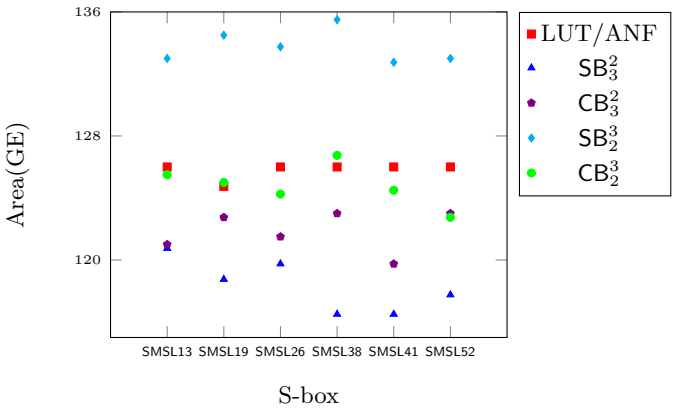

Figure 6: The area of all 3-degree S-boxes having non-zero linearize term with respect to different basis choices. In this case, the special normal basis emerges as a clear winner leading to minimum area for all 6 S-boxes.

7 Discussion

The primary motivation of this work was the design space exploration pertaining to the decompositions of $\mathbb{F}_{2^6}$ that would particularly suit a lightweight implementation of S-boxes. In doing so, we not only covered the conventional polynomial and normal bases, but also introduced a special normal basis that, by theory, seemed to better exploit the decomposition. One could, by looking at the way the decomposition affects the subfield operations, predict that the hardware area would be better thereby fulfilling the primary goal. The discovery of this basis stands out as an important contribution of this work since it paves the way for a better understanding of basis choice while dealing with the composite field decomposition, without actually implementing the S-box.

The extensiveness of this work is evident from the fact that close to *20,000* implementations were analyzed in this work before coming to the conclusion that for all practical purposes, the new basis delivers a better lightweight design and in most cases, with a considerable margin. The results are particularly better for higher degree foundations where the number of operations grow and hence, there is more scope of optimization.

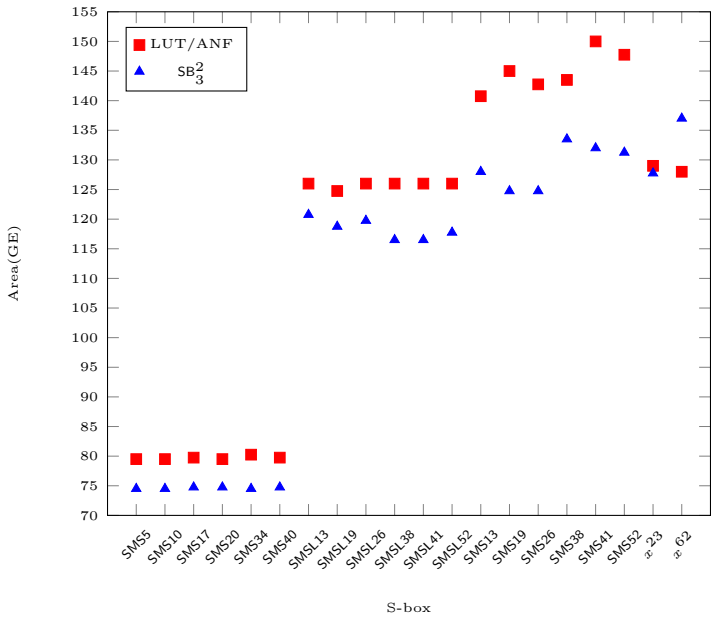

Figure 7: Area comparison between ANF/LUT vs the minimum area with respect to composite field.

Figure 7 gives a final overview of the best results for the new basis in comparison with traditional implementations such as LUT and ANF. With the exception of the x^{62} function, the special normal basis beats the LUT and ANF implementations emerging as a better choice highlighting the importance of composite field decomposition as a viable path for lightweight design.

In Table 7, we compare the implementation costs of the power mappings or their affine equivalent S-boxes, namely SMS34, SMS26, SMSL41, x^{23} and x^{62}, with other known 6-bit S-boxes such as SC2000, APN6, FIDES, SPEEDY and BipBip. We measure the area based on their LUT and ANF (as available in the literature) as opposed to univariate polynomial representation over a finite field as done in case of SMS34, SMS26, SMSL41, x^{23} and x^{62} S-boxes. From this comparison, we see that, except for SPEEDY and BipBip, S-boxes based on the power mappings or their affine equivalents have lower area requirements. We emphasize that SMS34, SMS26 and SMSL41 have stronger cryptographic properties among all these listed S-boxes, most notably, they have linear and differential branch numbers equal to 3. This indicates that these S-boxes are interesting candidates for lightweight cipher designs. It is intriguing to find out whether SC2000, APN6, FIDES, SPEEDY, and BipBip S-boxes will have lower implementation costs based on our method. In that case, we need univariate representations of these S-boxes from their truth tables through Lagrange interpolation, which generally results in a large number of terms. For instance, SPEEDY and BipBip S-boxes have 62 and 41 terms, respectively, in their univariate representations. Our method, in particular, works well when the S-box has a low number of terms. Thus, we believe that evaluating the area of these S-boxes using our method will not be effective.

Our primary motivation, while studying the decomposition of $\mathbb{F}_{2^6}$ for lightweight S-boxes was centered around area which is a standard practice in literature. However, as lightweightness is a multidimensional property, it is interesting to see how the S-boxes fared in terms of other important metrics like latency and power. To find this out, we employed the Cadence Genus tool to report these metrics for the area optimized implementations that we have considered in this work. It must be noted that the tool was not instructed to

Table 7: A detailed comparison of the best SMS S-boxes, namely SMS34, SMS26, SMSL41 along with x^{23} and x^{62} with respect to SB_3^2 and the existing 6-bit S-boxes.

S-box	Cryptographic Properties					LUT			ANF			SB_3^2		
	$\mathcal{LBN}$	$\mathcal{DBN}$	$\mathcal{LIN}$	$\mathcal{DU}$	deg	Area (GE)	Latency (ns)	Power (μW)	Area (GE)	Latency (ns)	Power (μW)	Area (GE)	Latency (ns)	Power (μW)
SC2000 [SYY+02]	2	2	16	4	5	202.68	0.78	7.70	201.24	0.82	7.70	-	-	-
APN6 [BDMW10]	2	2	16	2	4	194.40	0.73	7.22	207.00	1.00	7.99	-	-	-
FIDES [BBK+13]	2	2	16	2	4	191.88	0.94	7.42	190.00	0.74	7.21	-	-	-
SPEEDY [LMMR21]	2	2	24	8	5	55.80	0.28	2.20	54.27	0.31	2.18	-	-	-
BipBip [BDD+23]	2	2	16	4	3	54.72	0.30	2.30	54.36	0.31	2.22	-	-	-
SMS34	3	3	16	4	2	121.00	0.77	6.61	80.25	0.78	5.05	74.50	1.16	5.90
SMS26	3	3	16	4	3	150.25	0.92	7.84	142.75	0.88	8.06	124.75	2.19	14.00
SMSL41	3	3	64	8	3	126.00	0.79	7.20	136.00	0.88	7.68	116.50	2.22	13.44
x^{23}	2	2	24	10	4	133.50	1.16	7.82	129.00	0.78	7.32	127.75	0.98	7.14
x^{62}	2	2	16	4	5	139.50	0.86	7.68	128.50	0.76	6.66	137.75	2.90	22.92

optimize these metrics and as stated before, the main objective was to lower the area. So, along with area, in Table 1, we also report the results for latency and power for the S-boxes belonging to SMSd, SMSLd groups and x^{23}, x^{62} with respect to field decomposition the *special normal basis* SB_3^2 (a more comprehensive analysis is furnished in Appendix D). It is intuitive to note that low area, in most of the cases, leads to low power as evident from Table 1. The interplay with latency is, however, more subtle as it relies on the depth of the critical path. Table 7, which gives an overview of the best results for 6-bits S-boxes, allows us to study this interplay more closely. SMS34 and x^{23} vary largely in their area (74.5 GE and 127.75 GE respectively) while their corresponding power consumptions (5.9 μW and 7.14 μW respectively) are comparatively closer. Now, if we turn to latency, we see that their latencies are also close which is due to the lower depth of the critical path. In this case, the lower depth leads to less switching, thereby reducing the power consumption. The critical path schematics obtained from the synthesized net-lists of the S-boxes SMS34, SMS26, SMSL41, x^{23} and x^{62} are given in Appendix E. Figure 11 clearly shows that the SMS34 S-box, which has the lowest area, also has the shortest critical path.

In this work, all reported costs are based on the 65 *nm* UMC Mixed-Mode Low Leakage Low-K cell library. It is important to emphasize that our special normal basis has advantageous algebraic properties, as presented through Theorem 1 and Theorem 2, and subsequently in Corollary 1 and Corollary 2. These properties result in a highly compact final expression of x^d with respect to the field decomposition (see Table 2, Table 3), suggesting that the implementation cost of x^d could be lower. This hypothesis has been validated by experiments for most S-boxes using the aforementioned library. Therefore, it appears that the algebraic properties of the special normal basis are responsible for reducing implementation costs. We believe this will lead to lower costs across different libraries as well. Exploring this further with other libraries would be intriguing, and we leave this for future study.

8 Conclusions and Future Works

We have addressed the efficient implementation of S-boxes over $\mathbb{F}_{2^6}$ by exploiting the composite field structure. We present this paper as a foundation stone for studying the efficient implementation of S-boxes over $\mathbb{F}_{2^6}$ or other composite fields. We have analyzed how the choice of extension as well as the choice of bases impact in the implementation. There are so many combinations of bases and field extensions that we could not exhaust. Interestingly, we have found a method that gives us a normal basis which we call a special normal basis that has been effective in reducing the hardware cost. All our study is based on the S-boxes which are power mapping or their affine equivalents. Therefore, it will be interesting to analyze other classes of S-boxes with respect to field decomposition of $\mathbb{F}_{2^6}$. In particular, we are curious to know the effect of the special normal basis on the S-boxes that have not been considered in this paper. Furthermore, we leave it to the future

research to consider other bases if more efficient implementation could be found. Our implementation results have considered 2-degree and 3-degree S-boxes with the best known linear and differential branch number (both being 3) along with other good cryptographic properties that have been generated through Construction 1. It will be a nice research direction to consider the improvement of Construction 1 that will be able to generate degree 4 S-boxes over $\mathbb{F}_{2^6}$ with linear and differential branch number 3.

Acknowledgments.

The authors are grateful to the reviewers of TCHES for their valuable comments, which have substantially improved this paper. Furthermore, Sumanta Sarkar acknowledges the research grants from Engineering and Physical Sciences Research Council, EP/T014784/1 and EP/X036669/1.

References

[BBK+13] Begül Bilgin, Andrey Bogdanov, Miroslav Knežević, Florian Mendel, and Qingju Wang. Fides: Lightweight authenticated cipher with side-channel resistance for constrained hardware. In *Cryptographic Hardware and Embedded Systems-CHES 2013: 15th International Workshop, Santa Barbara, CA, USA, August 20-23, 2013. Proceedings 15*, pages 142–158. Springer, 2013.

[BDD+23] Yanis Belkheyar, Joan Daemen, Christoph Dobraunig, Santosh Ghosh, and Shahram Rasoolzadeh. Bipbip: A low-latency tweakable block cipher with small dimensions. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 326–368, 2023.

[BDMW10] Keith A Browning, John F Dillon, MT McQuistan, and Alan J Wolfe. An APN permutation in dimension six. *Finite Fields: theory and applications*, 518:33–42, 2010.

[BGLS19] Zhenzhen Bao, Jian Guo, San Ling, and Yu Sasaki. PEIGEN – a Platform for Evaluation, Implementation, and Generation of S-boxes. *IACR Transactions on Symmetric Cryptology*, 2019(1):330–394, Mar. 2019.

[BKL+07] 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.

[BPP+17] Subhadeep Banik, Sumit Kumar Pandey, Thomas Peyrin, Siang Meng Sim, Yosuke Todo, and Yu Sasaki. GIFT: A small present. *IACR Cryptology ePrint Archive*, 2017:622, 2017.

[BS91] Eli Biham and Adi Shamir. Differential Cryptanalysis of DES-like Cryptosystems. In *Proceedings of the 10th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '90, pages 2–21, London, UK, UK, 1991. Springer-Verlag.

[Car10] Claude Carlet. Vectorial Boolean Functions for Cryptography. In P. Hammer Y. Crama, editor, *Boolean Methods and Models*. Cambridge University Press, 2010.

[DBN+01] Morris J Dworkin, Elaine B Barker, James R Nechvatal, James Foti, Lawrence E Bassham, E Roback, and James F Dray Jr. Advanced encryption standard (AES). 2001.

[DEMS21] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. Ascon v1.2: Lightweight Authenticated Encryption and Hashing. *J. Cryptol.*, 34(3):33, 2021.

[DR02] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Information Security and Cryptography. Springer, 2002.

[JPST17] Jérémy Jean, Thomas Peyrin, Siang Meng Sim, and Jade Tourteaux. Optimizing Implementations of Lightweight Building Blocks. *IACR Transactions on Symmetric Cryptology*, 2017(4):130–168, Dec. 2017.

[LMMR21] Gregor Leander, Thorben Moos, Amir Moradi, and Shahram Rasoolzadeh. The speedy family of block ciphers-engineering an ultra low-latency cipher from gate level for secure processor architectures. *Cryptology ePrint Archive*, 2021.

[MSST22] Kalikinkar Mandal, Dhiman Saha, Sumanta Sarkar, and Yosuke Todo. Sycon: a new milestone in designing ASCON-like permutations. *J. Cryptogr. Eng.*, 12(3):305–327, 2022.

[NIS19] NIST. NIST Lightweight Cryptography project, 2019.

[PA11] G. Bertoni, J. Daemen, M. Peeters and G. Van Assche. The Keccak reference. Round 3 submission to NIST SHA-3, 2011.

[Rij00] Vincent Rijmen. Efficient Implementation of the Rijndael S-box. *Katholieke Universiteit Leuven, Dept. ESAT. Belgium*, 2000.

[SMS19] Sumanta Sarkar, Kalikinkar Mandal, and Dhiman Saha. On the Relationship Between Resilient Boolean Functions and Linear Branch Number of S-Boxes. In Feng Hao, Sushmita Ruj, and Sourav Sen Gupta, editors, *Progress in Cryptology - INDOCRYPT 2019 - 20th International Conference on Cryptology in India, Hyderabad, India, December 15-18, 2019, Proceedings*, volume 11898 of *Lecture Notes in Computer Science*, pages 361–374. Springer, 2019.

[SS18] Sumanta Sarkar and Habeeb Syed. Bounds on Differential and Linear Branch Number of Permutations. In Willy Susilo and Guomin Yang, editors, *Information Security and Privacy*, pages 207–224, Cham, 2018. Springer International Publishing.

[SYY+02] Takeshi Shimoyama, Hitoshi Yanami, Kazuhiro Yokoyama, Masahiko Takenaka, Kouichi Itoh, Jun Yajima, Naoya Torii, and Hidema Tanaka. The Block Cipher SC2000. In *Revised Papers from the 8th International Workshop on Fast Software Encryption*, FSE '01, pages 312–327, Berlin, Heidelberg, 2002. Springer-Verlag.

A Field Arithmetic Over $\mathbb{F}_{2^2}$

The field $\mathbb{F}_{2^2}$ is formed using the primitive polynomial $f_2(x) = x^2 + x + 1$. Consequently, operations within $\mathbb{F}_{2^2}$ are conducted modulo $f_2(\alpha)$, where α denotes a primitive root of $f_2(x)$. Since our exponentiation depends on addition, scalar multiplication, multiplication,

and some other operations over $\mathbb{F}_{2^2}$, we examine the representation of each operation in both polynomial and normal bases in Table 8.

Table 8: Operation over $\mathbb{F}_{2^2}$ with respect to polynomial and normal basis.

Operation	Notation	Polynomial Basis $(1, \alpha)$	Normal Basis (α, α^2)
Addition	$x \oplus y$	$[x_0 \oplus y_0, x_1 \oplus y_1]$	$[x_0 \oplus y_0, x_1 \oplus y_1]$
Square	x^2	$[x_0 \oplus x_1, x_1]$	$[x_1, x_0]$
Cube Multiplication	x^3y	$(x_0 \oplus x_1 \oplus x_0x_1)[y_0, y_1]$	$(x_0 \oplus x_1 \oplus x_0x_1)[y_0, y_1]$
Multiplication	xy	$[x_0y_0 \oplus x_1y_1, x_0y_1 \oplus x_1y_0 \oplus x_1y_1]$	$(x_0y_1 \oplus x_1y_0)[1, 1] \oplus [x_1y_1, x_0y_0]$
Scalar Multiplication	αx	$[x_1, x_0 \oplus x_1]$	$[x_1, x_0 \oplus x_1]$
	$\alpha^2 x$	$[x_0 \oplus x_1, x_0]$	$[x_0 \oplus x_1, x_0]$

B Field Arithmetic Over $\mathbb{F}_{2^3}$

As we have chosen the primitive polynomial $f_3(x) = x^3 + x^2 + 1$ over $\mathbb{F}_2$ to form the field $\mathbb{F}_{2^3}$, the field operations in $\mathbb{F}_{2^3}$ are performed modulo $f_3(\alpha)$, where α denotes a primitive root of $f_3(x)$. As discussed in Section 4, the exponentiation depends on addition, scalar multiplication, multiplication, cube, fourth power, fifth power, sixth power over $\mathbb{F}_{2^3}$. Table 9 and Table 10 provide the representation of each operation in polynomial and normal bases, respectively.

Table 9: Operation over $\mathbb{F}_{2^3}$ with respect to polynomial basis.

Operation	Notation	Polynomial Basis $(1, \alpha, \alpha^2)$
Addition	$x \oplus y$	$[x_0 \oplus y_0, x_1 \oplus y_1, x_2 \oplus y_2]$
Square	x^2	$[x_0 \oplus x_2, x_2, x_1 \oplus x_2]$
Cube	x^3	$[x_0 \oplus x_1 \oplus x_0x_2, x_2 \oplus x_0x_1 \oplus x_0x_2, x_1 \oplus x_2 \oplus x_0x_1 \oplus x_1x_2]$
Fourth Power	x^4	$[x_0 \oplus x_1, x_1 \oplus x_2, x_1]$
Fifth Power	x^5	$[x_0x_1 \oplus x_0 \oplus x_1 \oplus x_2, x_0x_2 \oplus x_1x_2 \oplus x_1, x_0x_1 \oplus x_0x_2 \oplus x_2]$
Sixth Power	x^6	$[x_0x_1 \oplus x_0x_2 \oplus x_1x_2 \oplus x_0 \oplus x_2, x_0x_1 \oplus x_1x_2 \oplus x_1 \oplus x_2, x_0x_2 \oplus x_1x_2 \oplus x_1]$
Multiplication	xy	$[x_0y_0 \oplus x_2y_1 \oplus x_1y_2 \oplus x_2y_2, x_1y_0 \oplus x_0y_1 \oplus x_2y_2, x_2y_0 \oplus x_1y_1 \oplus x_2y_1 \oplus x_0y_2 \oplus x_1y_2 \oplus x_2y_2]$
Scalar Multiplication	αx	$[x_2, x_0, x_1 \oplus x_2]$
	$\alpha^2 x$	$[x_1 \oplus x_2, x_2, x_0 \oplus x_1 \oplus x_2]$
	$\alpha^3 x$	$[x_0 \oplus x_1 \oplus x_2, x_1 \oplus x_2, x_0 \oplus x_1]$
	$\alpha^4 x$	$[x_0 \oplus x_1, x_0 \oplus x_1 \oplus x_2, x_0 \oplus x_2]$
	$\alpha^5 x$	$[x_0 \oplus x_2, x_0 \oplus x_1, x_1]$
	$\alpha^6 x$	$[x_1, x_0 \oplus x_2, x_0]$

C Look Up Table of All SMS S-boxes

We have generated 6 2-degree S-boxes and 12 3-degree S-boxes using Construction 1. The look up table for each S-box with additional parameters are given in Table 11, Table 12 and Table 13.

Table 10: Operation over $\mathbb{F}_{2^3}$ with respect to normal basis.

Operation	Notation	Normal Basis $(\alpha, \alpha^2, \alpha^4)$
Addition	$x \oplus y$	$[x_0 \oplus y_0, x_1 \oplus y_1, x_2 \oplus y_2]$
Square	x^2	$[x_2, x_0, x_1]$
Cube	x^3	$[x_0 \oplus x_1 \oplus x_0x_2, x_1 \oplus x_2 \oplus x_1x_0, x_2 \oplus x_0 \oplus x_2x_1]$
Fourth Power	x^4	$[x_1, x_2, x_0]$
Fifth Power	x^5	$[x_1 \oplus x_2 \oplus x_1x_0, x_2 \oplus x_0 \oplus x_2x_1, x_0 \oplus x_1 \oplus x_0x_2]$
Sixth Power	x^6	$[x_2 \oplus x_0 \oplus x_2x_1, x_0 \oplus x_1 \oplus x_0x_2, x_1 \oplus x_2 \oplus x_1x_0]$
Multiplication	xy	$[x_1y_0 \oplus x_0y_1 \oplus x_2y_1 \oplus x_1y_2 \oplus x_2y_2, x_0y_0 \oplus x_2y_0 \oplus x_2y_1 \oplus x_0y_2 \oplus x_1y_2, x_1y_0 \oplus x_2y_0 \oplus x_0y_1 \oplus x_1y_1 \oplus x_0y_2]$
Scalar Multiplication	αx	$[x_1, x_0 \oplus x_2, x_1 \oplus x_2]$
	$\alpha^2 x$	$[x_0 \oplus x_2, x_2, x_0 \oplus x_1]$
	$\alpha^3 x$	$[x_2, x_1 \oplus x_2, x_0 \oplus x_1 \oplus x_2]$
	$\alpha^4 x$	$[x_1 \oplus x_2, x_0 \oplus x_1, x_0]$
	$\alpha^5 x$	$[x_0 \oplus x_1, x_0 \oplus x_1 \oplus x_2, x_1]$
	$\alpha^6 x$	$[x_0 \oplus x_1 \oplus x_2, x_0, x_0 \oplus x_2]$

Table 11: Listing all 2-degree SMS S-boxes with $(\mu_0, \cdots, \mu_5) = (0, \cdots, 0)$ and $A = \mathcal{I} + E_{6,1}$.

S-Box	$F(x)$	$\lambda_0, \cdots, \lambda_5$	LUT
SMS5	x^5	27,38,28,43,50,31	(0, 46, 59, 7, 48, 23, 6, 51, 53, 29, 8, 50, 43, 10, 27, 40, 31, 56, 47, 26, 4, 42, 57, 5, 16, 49, 38, 21, 37, 13, 30, 36, 39, 45, 20, 12, 18, 17, 44, 61, 2, 14, 55, 41, 25, 28, 33, 54, 32, 35, 24, 9, 62, 52, 11, 19, 63, 58, 1, 22, 15, 3, 60, 34).
SMS10	x^{10}	2,57,41,37,60,47	(0, 58, 47, 28, 3, 29, 24, 15, 23, 53, 32, 11, 46, 40, 45, 34, 61, 35, 62, 41, 16, 42, 39, 20, 1, 7, 26, 21, 22, 52, 57, 18, 30, 54, 17, 48, 9, 5, 50, 55, 8, 56, 31, 38, 37, 49, 6, 27, 2, 14, 33, 36, 59, 19, 44, 13, 63, 43, 4, 25, 60, 12, 51, 10).
SMS17	x^{17}	27,55,7,13,63,31	(0, 45, 31, 52, 10, 54, 36, 30, 58, 51, 1, 14, 29, 5, 23, 9, 55, 11, 61, 7, 32, 13, 27, 48, 2, 26, 44, 50, 56, 49, 39, 40, 60, 57, 34, 33, 6, 18, 41, 59, 4, 37, 62, 25, 19, 35, 24, 46, 8, 28, 3, 17, 47, 42, 21, 22, 63, 15, 16, 38, 53, 20, 43, 12)
SMS20	x^{20}	4,32,28,43,13,63	(0, 54, 47, 26, 5, 27, 18, 15, 29, 57, 32, 7, 46, 34, 43, 36, 59, 37, 62, 35, 16, 38, 45, 24, 1, 13, 22, 25, 28, 56, 51, 20, 30, 60, 17, 48, 3, 9, 52, 61, 2, 50, 31, 44, 41, 49, 12, 23, 4, 14, 33, 40, 55, 21, 42, 11, 63, 39, 8, 19, 58, 10, 53, 6)
SMS34	x^{34}	8,57,41,19,21,10	(0, 54, 61, 19, 40, 27, 18, 57, 43, 15, 4, 56, 53, 20, 29, 36, 31, 44, 55, 28, 2, 52, 45, 3, 8, 41, 50, 11, 35, 7, 30, 34, 51, 39, 10, 6, 24, 9, 38, 47, 16, 22, 59, 37, 13, 14, 33, 58, 32, 49, 12, 5, 62, 42, 21, 25, 63, 60, 1, 26, 23, 17, 46, 48)
SMS40	x^{40}	8,16,49,60,47,10	(0, 45, 31, 52, 10, 54, 36, 30, 58, 51, 1, 14, 29, 5, 23, 9, 55, 11, 61, 7, 32, 13, 27, 48, 2, 26, 44, 50, 56, 49, 39, 40, 60, 57, 34, 33, 6, 18, 41, 59, 4, 37, 62, 25, 19, 35, 24, 46, 8, 28, 3, 17, 47, 42, 21, 22, 63, 15, 16, 38, 53, 20, 43, 12)

Table 12: Listing all 3-degree SMS S-boxes with $(\mu_0, \cdots, \mu_5) = (0, \cdots, 0)$ and $A = \mathcal{I} + E_{1,3}$.

S-Box	$F(x)$	$\lambda_0, \cdots, \lambda_5$	LUT
SMS13	x^{13}	36,31,39,5,10,44	(0, 50, 14, 29, 39, 25, 21, 6, 58, 13, 44, 19, 11, 61, 16, 34, 42, 37, 56, 52, 23, 41, 46, 31, 55, 26, 5, 2, 33, 48, 9, 62, 20, 24, 45, 3, 10, 43, 60, 51, 53, 36, 35, 57, 54, 7, 30, 40, 18, 47, 27, 38, 49, 28, 32, 1, 15, 8, 17, 63, 12, 22, 59, 4).
SMS19	x^{19}	13,51,60,20,6,59	(0, 37, 19, 30, 57, 14, 28, 17, 39, 26, 50, 13, 11, 62, 4, 33, 35, 56, 38, 52, 29, 42, 51, 31, 61, 7, 24, 1, 40, 36, 10, 55, 20, 6, 58, 9, 3, 43, 54, 45, 60, 48, 41, 46, 53, 25, 23, 34, 5, 59, 15, 49, 44, 22, 32, 8, 27, 2, 12, 63, 18, 21, 47, 16).
SMS26	x^{26}	57,36,33,17,31,58	(0, 49, 11, 30, 39, 28, 22, 3, 57, 14, 42, 21, 13, 62, 16, 33, 41, 38, 56, 50, 23, 44, 43, 31, 55, 25, 6, 1, 36, 48, 12, 59, 18, 24, 46, 5, 9, 45, 58, 53, 54, 34, 37, 60, 51, 7, 27, 40, 17, 47, 29, 35, 52, 26, 32, 4, 15, 8, 20, 63, 10, 19, 61, 2)
SMS38	x^{38}	13,39,10,20,3,24	(0, 37, 28, 27, 46, 19, 11, 12, 53, 26, 56, 7, 22, 59, 1, 36, 52, 42, 49, 41, 15, 50, 60, 31, 47, 21, 10, 4, 34, 33, 18, 61, 9, 17, 58, 6, 20, 54, 57, 39, 43, 40, 38, 51, 45, 14, 29, 48, 5, 62, 23, 44, 35, 25, 32, 2, 30, 16, 3, 63, 24, 13, 55, 8)
SMS41	x^{41}	18,28,60,6,48,45	(0, 38, 21, 27, 60, 11, 26, 20, 39, 25, 49, 14, 13, 59, 2, 36, 37, 56, 35, 50, 30, 41, 53, 31, 62, 7, 24, 4, 40, 34, 9, 55, 18, 3, 57, 12, 5, 45, 51, 46, 58, 48, 44, 43, 54, 28, 23, 33, 6, 61, 15, 52, 42, 19, 32, 8, 29, 1, 10, 63, 17, 22, 47, 16)
SMS52	x^{52}	54,57,28,33,25,48	(0, 22, 13, 43, 60, 35, 42, 12, 23, 41, 25, 38, 37, 59, 2, 20, 21, 56, 19, 26, 46, 49, 29, 47, 62, 7, 40, 4, 48, 18, 33, 31, 10, 3, 57, 36, 5, 53, 27, 54, 58, 24, 52, 51, 30, 44, 15, 17, 6, 61, 39, 28, 50, 11, 16, 32, 45, 1, 34, 63, 9, 14, 55, 8)

Table 13: Listing all 3-degree SMS S-boxes with $(\mu_0, \cdots, \mu_5) = (36, \cdots, 36)$ and $A = \mathcal{I} + E_{5,3}$.

S-Box	$F(x)$	$\lambda_0, \cdots, \lambda_5$	LUT
SMSL13	x^{13}	36,7,43,13,39,5	(0, 12, 62, 55, 20, 38, 8, 11, 34, 49, 52, 9, 51, 58, 13, 30, 27, 42, 29, 35, 39, 21, 16, 25, 44, 23, 32, 63, 61, 33, 10, 6, 22, 40, 59, 15, 7, 60, 48, 53, 19, 26, 5, 45, 41, 1, 47, 18, 57, 4, 24, 37, 43, 46, 3, 50, 14, 17, 54, 2, 31, 28, 36, 56).
SMSL19	x^{19}	32,27,28,51,20,6	(0, 6, 47, 59, 34, 11, 4, 21, 9, 56, 42, 20, 57, 45, 22, 39, 53, 13, 54, 25, 27, 50, 32, 52, 14, 51, 8, 63, 62, 24, 5, 3, 35, 12, 61, 23, 19, 46, 40, 58, 49, 37, 18, 30, 28, 16, 31, 33, 60, 2, 36, 26, 29, 15, 17, 41, 7, 48, 43, 1, 55, 38, 10, 44).
SMSL26	x^{26}	36,33,17,21,47,10	(0, 48, 61, 31, 17, 28, 32, 42, 12, 7, 21, 34, 15, 45, 50, 57, 43, 44, 51, 14, 30, 19, 1, 35, 52, 27, 4, 63, 55, 6, 40, 24, 25, 36, 47, 58, 26, 53, 5, 23, 11, 41, 18, 54, 38, 2, 62, 9, 39, 16, 33, 22, 46, 60, 10, 13, 56, 3, 29, 8, 59, 49, 20, 37).
SMSL38	x^{38}	49,41,39,60,20,3	(0, 10, 59, 55, 18, 35, 8, 13, 33, 52, 50, 12, 53, 57, 14, 27, 29, 41, 30, 37, 39, 22, 16, 28, 42, 23, 32, 63, 62, 36, 9, 3, 19, 40, 61, 15, 7, 58, 48, 54, 21, 25, 6, 46, 44, 4, 47, 17, 60, 2, 24, 38, 45, 43, 5, 49, 11, 20, 51, 1, 31, 26, 34, 56).
SMSL41	x^{41}	8,57,18,37,6,48	(0, 3, 47, 61, 33, 13, 2, 26, 12, 52, 37, 18, 60, 46, 19, 43, 58, 14, 51, 28, 29, 49, 32, 50, 7, 57, 4, 63, 55, 20, 10, 9, 41, 6, 62, 27, 25, 39, 36, 53, 56, 42, 17, 23, 22, 16, 31, 40, 54, 1, 34, 21, 30, 15, 24, 44, 11, 48, 45, 8, 59, 35, 5, 38).
SMSL52	x^{52}	54,38,33,63,31,48	(0, 24, 31, 47, 12, 11, 16, 50, 3, 37, 13, 48, 39, 23, 56, 30, 54, 19, 60, 35, 43, 44, 4, 52, 25, 46, 1, 63, 61, 33, 18, 10, 14, 17, 55, 58, 42, 29, 5, 45, 38, 22, 40, 57, 49, 32, 59, 6, 53, 8, 20, 41, 51, 27, 34, 7, 26, 36, 15, 2, 62, 28, 9, 21).

D Implementation details of S-boxes belonging to SMSd, SMSLd groups and x^{23}, x^{62}

We provide the area, latency and power consumptions of all the S-boxes belonging to SMSd, SMSLd groups and x^{23}, x^{62} with respect to different choices of bases and field decompositions in Table 14, Table 15 and Table 16. In these tables, the symbol `S:E` denotes the starting and ending point of the critical path, considering $x_0, x_1, \cdots, x_5$ as the inputs and $y_0, y_1, \cdots, y_5$ as the outputs.

Table 14: Implementation details of SMS5, SMS10, SMS17, SMS20, SMS34, SMS40 with respect to different bases and field decompositons.

S-box	Basis	Composite Field				S-box	Basis	Composite Field			
		Area (GE)	Latency (ns)	S:E	Power(μW)			Area (GE)	Latency (ns)	S:E	Power(μW)
SMS5	N-N$_2^3$	78.00	1.18	$x_1 : y_1$	6.47	SMS20	N-N$_2^3$	78.50	1.16	$x_1 : y_1$	6.48
	N-P$_3^3$	74.25	0.96	$x_4 : y_1$	5.82		N-P$_2^3$	74.25	1.09	$x_4 : y_2$	5.92
	P-N$_2^3$	81.75	1.36	$x_0 : y_3$	6.69		P-N$_2^3$	78.25	1.04	$x_0 : y_3$	6.14
	P-P$_2^3$	77.25	1.20	$x_2 : y_3$	6.26		P-P$_2^3$	78.25	1.42	$x_0 : y_3$	6.70
	SN-N$_2^3$	75.00	1.01	$x_4 : y_1$	5.65		SN-N$_2^3$	75.00	1.01	$x_4 : y_1$	5.65
	SN-P$_2^3$	77.50	1.20	$x_1 : y_1$	6.56		SN-P$_2^3$	78.25	1.20	$x_1 : y_1$	6.62
	N-N$_3^2$	79.50	0.58	$x_1 : y_3$	4.73		N-N$_3^2$	80.00	0.64	$x_2 : y_5$	4.88
	N-P$_3^2$	76.00	0.76	$x_1 : y_2$	4.72		N-P$_3^2$	77.50	0.66	$x_4 : y_3$	4.79
	P-N$_3^2$	84.00	1.26	$x_1 : y_2$	6.82		P-N$_3^2$	76.75	0.70	$x_2 : y_1$	4.57
	P-P$_3^2$	120.25	1.51	$x_0 : y_2$	10.24		P-P$_3^2$	77.50	0.71	$x_1 : y_1$	4.64
	SN-N$_3^2$	74.50	1.16	$x_1 : y_5$	6.18		SN-N$_3^2$	74.75	1.16	$x_1 : y_2$	5.93
	SN-P$_3^2$	75.25	1.38	$x_5 : y_2$	6.76		SN-P$_3^2$	75.50	1.28	$x_4 : y_4$	6.54
SMS10	N-N$_2^3$	79.50	1.16	$x_1 : y_3$	6.58	SMS34	N-N$_2^3$	78.75	1.22	$x_1 : y_4$	6.54
	N-P$_2^3$	74.25	0.96	$x_4 : y_3$	5.82		N-P$_2^3$	73.75	1.13	$x_4 : y_5$	5.76
	P-N$_2^3$	80.50	1.03	$x_0 : y_2$	6.18		P-N$_2^3$	78.50	1.03	$x_0 : y_0$	5.88
	P-P$_2^3$	77.75	1.20	$x_3 : y_5$	6.32		P-P$_2^3$	76.00	1.04	$x_3 : y_0$	5.40
	SN-N$_2^3$	75.25	1.06	$x_4 : y_3$	5.83		SN-N$_2^3$	75.00	0.98	$x_4 : y_5$	5.92
	SN-P$_2^3$	77.50	1.30	$x_1 : y_3$	6.57		SN-P$_2^3$	76.50	1.21	$x_1 : y_4$	6.61
	N-N$_3^2$	94.00	1.14	$x_0 : y_2$	6.74		N-N$_3^2$	75.50	0.66	$x_2 : y_0$	4.71
	N-P$_3^2$	123.00	1.46	$x_1 : y_1$	10.46		N-P$_3^2$	75.75	0.76	$x_3 : y_1$	4.66
	P-N$_3^2$	81.75	1.26	$x_1 : y_4$	7.04		P-N$_3^2$	77.00	0.68	$x_2 : y_0$	7.76
	P-P$_3^2$	125.25	1.72	$x_5 : y_2$	11.70		P-P$_3^2$	77.75	0.66	$x_1 : y_1$	4.70
	SN-N$_3^2$	74.50	1.16	$x_1 : y_1$	5.90		SN-N$_3^2$	74.50	1.16	$x_1 : y_5$	5.90
	SN-P$_3^2$	76.50	1.23	$x_4 : y_4$	6.56		SN-P$_3^2$	75.25	1.24	$x_5 : y_1$	6.52
SMS17	N-N$_2^3$	78.50	1.16	$x_1 : y_2$	6.48	SMS40	N-N$_2^3$	79.50	1.16	$x_1 : y_2$	6.58
	N-P$_2^3$	74.25	0.96	$x_4 : y_2$	5.82		N-P$_2^3$	74.75	1.17	$x_5 : y_3$	6.23
	P-N$_2^3$	80.75	1.04	$x_0 : y_4$	6.06		P-N$_2^3$	78.00	1.04	$x_0 : y_4$	5.90
	P-P$_2^3$	78.25	1.29	$x_3 : y_0$	6.16		P-P$_2^3$	77.75	1.20	$x_3 : y_0$	6.32
	SN-N$_2^3$	75.25	1.06	$x_4 : y_2$	5.83		SN-N$_2^3$	75.25	1.06	$x_4 : y_2$	5.83
	SN-P$_2^3$	77.00	1.21	$x_1 : y_2$	6.68		SN-P$_2^3$	77.00	1.21	$x_1 : y_2$	6.68
	N-N$_3^2$	94.50	1.16	$x_2 : y_4$	6.48		N-N$_3^2$	78.00	0.78	$x_2 : y_2$	4.68
	N-P$_3^2$	125.50	1.44	$x_0 : y_5$	10.78		N-P$_3^2$	79.25	0.74	$x_2 : y_2$	4.67
	P-N$_3^2$	87.00	1.35	$x_0 : y_5$	8.08		P-N$_3^2$	83.50	1.28	$x_1 : y_5$	6.77
	P-P$_3^2$	125.50	1.56	$x_5 : y_4$	11.79		P-P$_3^2$	118.50	1.72	$x_5 : y_1$	12.03
	SN-N$_3^2$	74.75	1.16	$x_1 : y_3$	5.93		SN-N$_3^2$	74.75	1.16	$x_1 : y_3$	5.93
	SN-P$_3^2$	76.50	1.25	$x_4 : y_5$	6.48		SN-P$_3^2$	75.50	1.33	$x_4 : y_5$	6.57

Table 15: Implementation details of SMS13, SMS19, SMS26, SMS38, SMS41, SMS52 with respect to different bases and field decompositons.

S-box	Basis	Composite Field				S-box	Basis	Composite Field			
		Area (GE)	Latency (ns)	S:E	Power(μW)			Area (GE)	Latency (ns)	S:E	Power(μW)
SMS13	N-N$_2^3$	137.25	0.80	$x_3 : y_3$	7.52	SMS38	N-N$_2^3$	137.50	0.92	$x_5 : y_1$	7.52
	N-P$_2^3$	137.25	0.80	$x_3 : y_3$	7.52		N-P$_2^3$	140.25	0.86	$x_2 : y_4$	7.67
	P-N$_2^3$	136.50	0.78	$x_1 : y_2$	7.66		P-N$_2^3$	137.00	0.83	$x_2 : y_0$	7.84
	P-P$_2^3$	136.00	0.78	$x_3 : y_1$	7.58		P-P$_2^3$	139.75	0.87	$x_5 : y_1$	8.15
	SN-N$_2^3$	153.25	2.16	$x_5 : y_3$	17.60		SN-N$_2^3$	152.25	2.07	$x_5 : y_0$	16.32
	SN-P$_2^3$	182.50	1.82	$x_0 : y_3$	18.68		SN-P$_2^3$	145.25	0.87	$x_1 : y_5$	7.64
	N-N$_3^2$	136.25	0.97	$x_3 : y_4$	7.55		N-N$_3^2$	137.00	0.88	$x_5 : y_4$	7.58
	N-P$_3^2$	137.00	0.74	$x_3 : y_4$	7.32		N-P$_3^2$	137.25	0.85	$x_3 : y_2$	7.52
	P-N$_3^2$	136.50	0.80	$x_1 : y_5$	7.56		P-N$_3^2$	138.25	0.84	$x_3 : y_0$	7.58
	P-P$_3^2$	135.25	1.72	$x_5 : y_3$	13.75		P-P$_3^2$	137.00	0.95	$x_0 : y_0$	7.72
	SN-N$_3^2$	132.25	2.13	$x_2 : y_3$	16.75		SN-N$_3^2$	133.50	2.36	$x_2 : y_0$	17.02
	SN-P$_3^2$	128.00	1.98	$x_4 : y_4$	13.76		SN-P$_3^2$	133.75	1.98	$x_5 : y_5$	12.66
SMS19	N-N$_3^3$	137.75	0.84	$x_3 : y_1$	7.42	SMS41	N-N$_3^3$	135.75	0.81	$x_3 : y_0$	7.29
	N-P$_2^3$	140.25	0.94	$x_4 : y_2$	7.83		N-P$_2^3$	137.75	0.91	$x_4 : y_4$	7.46
	P-N$_3^3$	136.50	0.85	$x_3 : y_1$	7.82		P-N$_2^3$	138.00	0.96	$x_2 : y_0$	7.56
	P-P$_2^3$	136.50	0.88	$x_1 : y_0$	7.53		P-P$_2^3$	136.50	0.85	$x_3 : y_0$	7.82
	SN-N$_2^3$	152.75	2.23	$x_5 : y_1$	17.11		SN-N$_2^3$	151.50	2.19	$x_5 : y_0$	17.20
	SN-P$_2^3$	181.00	1.88	$x_4 : y_1$	18.39		SN-P$_2^3$	185.50	1.78	$x_2 : y_0$	18.21
	N-N$_3^2$	135.75	0.81	$x_3 : y_1$	7.29		N-N$_3^2$	138.25	0.90	$x_3 : y_1$	7.28
	N-P$_3^2$	137.00	0.72	$x_3 : y_2$	7.60		N-P$_3^2$	138.50	0.79	$x_5 : y_4$	7.62
	P-N$_3^2$	137.00	0.85	$x_0 : y_2$	7.44		P-N$_3^2$	138.50	0.79	$x_5 : y_4$	7.62
	P-P$_3^2$	137.50	0.73	$x_3 : y_0$	7.37		P-P$_3^2$	117.00	1.76	$x_1 : y_5$	11.43
	SN-N$_3^2$	132.75	2.13	$x_2 : y_5$	17.44		SN-N$_3^2$	132.00	2.34	$x_5 : y_1$	16.26
	SN-P$_3^2$	124.75	2.19	$x_1 : y_5$	14.00		SN-P$_3^2$	132.00	1.83	$x_2 : y_5$	11.96
SMS26	N-N$_3^3$	135.75	0.81	$x_3 : y_4$	7.19	SMS52	N-N$_2^3$	137.50	0.90	$x_3 : y_1$	7.62
	N-P$_2^3$	135.75	0.81	$x_3 : y_4$	7.19		N-P$_2^3$	137.50	0.90	$x_3 : y_1$	7.62
	P-N$_3^3$	136.75	0.76	$x_5 : y_5$	7.61		P-N$_2^3$	136.25	0.90	$x_2 : y_1$	7.76
	P-P$_2^3$	137.25	0.74	$x_4 : y_0$	7.56		P-P$_2^3$	137.50	0.81	$x_2 : y_5$	7.69
	SN-N$_2^3$	150.75	2.14	$x_5 : y_3$	16.70		SN-N$_2^3$	153.25	2.21	$x_5 : y_0$	17.09
	SN-P$_2^3$	185.75	1.88	$x_2 : y_3$	19.00		SN-P$_2^3$	182.50	1.72	$x_1 : y_0$	18.69
	N-N$_3^2$	135.00	0.95	$x_3 : y_3$	7.56		N-N$_3^2$	137.50	0.88	$x_3 : y_1$	7.29
	N-P$_3^2$	137.00	0.72	$x_3 : y_4$	7.60		N-P$_3^2$	137.75	0.78	$x_2 : y_4$	7.78
	P-N$_3^2$	138.00	0.76	$x_4 : y_3$	7.97		P-N$_3^2$	137.50	0.87	$x_3 : y_0$	7.48
	P-P$_3^2$	136.75	0.79	$x_0 : y_4$	7.72		P-P$_3^2$	139.00	0.85	$x_3 : y_0$	7.54
	SN-N$_3^2$	132.75	1.94	$x_5 : y_3$	14.90		SN-N$_3^2$	131.25	2.32	$x_5 : y_1$	16.05
	SN-P$_3^2$	124.75	2.19	$x_1 : y_5$	14.00		SN-P$_3^2$	133.75	2.03	$x_1 : y_4$	12.44

Table 16: Implementation details of SMS13, SMS19, SMS26, SMS38, SMS41, SMS52 and x^{23}, x^{62} with respect to different bases and field decompositons.

S-box	Basis	Composite Field				S-box	Basis	Composite Field			
		Area (GE)	Latency (ns)	S:E	Power(μW)			Area (GE)	Latency (ns)	S:E	Power(μW)
SMSL13	N-N$_2^3$	127.00	0.84	$x_4 : y_5$	7.11	SMSL38	N-N$_2^3$	127.75	0.74	$x_1 : y_5$	6.90
	N-P$_2^3$	127.25	0.70	$x_2 : y_5$	7.22		N-P$_2^3$	127.75	0.74	$x_1 : y_5$	6.90
	P-N$_2^3$	126.00	0.85	$x_1 : y_2$	7.44		P-N$_2^3$	126.75	0.89	$x_4 : y_1$	7.20
	P-P$_2^3$	125.50	0.80	$x_5 : y_3$	6.97		P-P$_2^3$	126.75	0.78	$x_5 : y_3$	7.09
	SN-N$_2^3$	133.00	2.10	$x_0 : y_3$	14.24		SN-N$_2^3$	136.25	2.03	$x_5 : y_5$	15.67
	SN-P$_2^3$	134.00	0.78	$x_4 : y_4$	7.23		SN-P$_2^3$	135.50	0.91	$x_1 : y_3$	7.82
	N-N$_3^2$	120.75	0.69	$x_4 : y_2$	6.82		N-N$_3^2$	125.00	0.82	$x_2 : y_3$	7.10
	N-P$_3^2$	126.75	0.89	$x_1 : y_1$	7.44		N-P$_3^2$	127.50	0.78	$x_4 : y_1$	7.06
	P-N$_3^2$	123.50	0.80	$x_2 : y_5$	6.98		P-N$_3^2$	125.25	0.79	$x_2 : y_3$	7.30
	P-P$_3^2$	122.25	0.74	$x_4 : y_1$	6.92		P-P$_3^2$	123.00	0.74	$x_2 : y_5$	6.90
	SN-N$_3^2$	120.75	2.25	$x_0 : y_5$	12.98		SN-N$_3^2$	116.50	2.24	$x_0 : y_5$	13.36
	SN-P$_3^2$	125.50	1.71	$x_4 : y_3$	10.83		SN-P$_3^2$	130.25	1.85	$x_4 : y_3$	10.72
SMSL19	N-N$_2^3$	125.25	0.77	$x_1 : y_1$	6.86	SMSL41	N-N$_2^3$	130.00	0.80	$x_4 : y_3$	7.52
	N-P$_2^3$	129.75	0.81	$x_3 : y_0$	7.55		N-P$_2^3$	130.25	0.85	$x_2 : y_2$	7.61
	P-N$_2^3$	127.25	0.85	$x_2 : y_3$	7.38		P-N$_2^3$	124.50	0.79	$x_4 : y_5$	7.00
	P-P$_2^3$	125.00	0.78	$x_2 : y_2$	7.11		P-P$_2^3$	126.25	0.77	$x_5 : y_1$	7.02
	SN-N$_2^3$	139.50	2.04	$x_0 : y_5$	16.85		SN-N$_2^3$	136.00	2.07	$x_0 : y_1$	14.03
	SN-P$_2^3$	134.50	0.92	$x_1 : y_3$	7.47		SN-P$_2^3$	132.75	0.89	$x_4 : y_1$	7.48
	N-N$_3^2$	128.00	0.68	$x_4 : y_2$	7.28		N-N$_3^2$	125.50	0.66	$x_2 : y_2$	6.78
	N-P$_3^2$	124.50	0.94	$x_4 : y_5$	7.22		N-P$_3^2$	126.00	0.64	$x_1 : y_5$	6.90
	P-N$_3^2$	128.00	0.82	$x_1 : y_1$	7.01		P-N$_3^2$	123.00	0.82	$x_2 : y_2$	6.99
	P-P$_3^2$	122.75	0.70	$x_4 : y_5$	6.70		P-P$_3^2$	119.75	1.71	$x_1 : y_1$	11.50
	SN-N$_3^2$	119.25	2.39	$x_0 : y_3$	13.72		SN-N$_3^2$	116.50	2.22	$x_0 : y_2$	13.44
	SN-P$_3^2$	118.75	2.02	$x_5 : y_2$	11.39		SN-P$_3^2$	126.75	1.76	$x_4 : y_3$	11.58
SMSL26	N-N$_2^3$	128.75	0.76	$x_2 : y_5$	6.93	SMSL52	N-N$_2^3$	130.75	0.83	$x_4 : y_4$	7.07
	N-P$_2^3$	128.75	0.76	$x_2 : y_5$	6.94		N-P$_2^3$	130.75	0.83	$x_4 : y_4$	7.07
	P-N$_2^3$	124.25	0.73	$x_1 : y_3$	7.06		P-N$_2^3$	122.75	0.81	$x_4 : y_1$	7.27
	P-P$_2^3$	124.25	0.73	$x_1 : y_3$	7.06		P-P$_2^3$	124.50	0.79	$x_4 : y_2$	7.00
	SN-N$_2^3$	138.75	2.17	$x_0 : y_5$	14.44		SN-N$_2^3$	133.00	2.10	$x_0 : y_4$	14.24
	SN-P$_2^3$	133.75	0.74	$x_1 : y_2$	7.36		SN-P$_2^3$	136.50	0.86	$x_0 : y_2$	7.68
	N-N$_3^2$	123.00	0.86	$x_4 : y_2$	6.93		N-N$_3^2$	124.00	0.89	$x_4 : y_3$	7.15
	N-P$_3^2$	121.50	1.60	$x_0 : y_5$	13.17		N-P$_3^2$	125.00	0.86	$x_5 : y_3$	6.98
	P-N$_3^2$	124.00	0.86	$x_2 : y_2$	7.06		P-N$_3^2$	123.00	0.86	$x_1 : y_0$	7.12
	P-P$_3^2$	123.75	0.82	$x_1 : y_2$	7.33		P-P$_3^2$	123.50	0.76	$x_0 : y_2$	7.05
	SN-N$_3^2$	120.75	2.30	$x_0 : y_2$	12.99		SN-N$_3^2$	117.75	2.28	$x_0 : y_0$	13.59
	SN-P$_3^2$	119.75	2.39	$x_4 : y_3$	13.46		SN-P$_3^2$	130.25	1.86	$x_4 : y_1$	10.87
x^{23}	SN-N$_3^2$	127.75	0.98	$x_2 : y_3$	7.14	x^{62}	SN-N$_3^2$	137.75	2.89	$x_0 : y_3$	22.92
	SN-P$_3^2$	130.75	0.97	$x_4 : y_3$	7.18		SN-P$_3^2$	153.75	3.06	$x_1 : y_3$	39.63

E Critical Paths of SMSL41, SMS26, SMS34, x^{23}, x^{62}

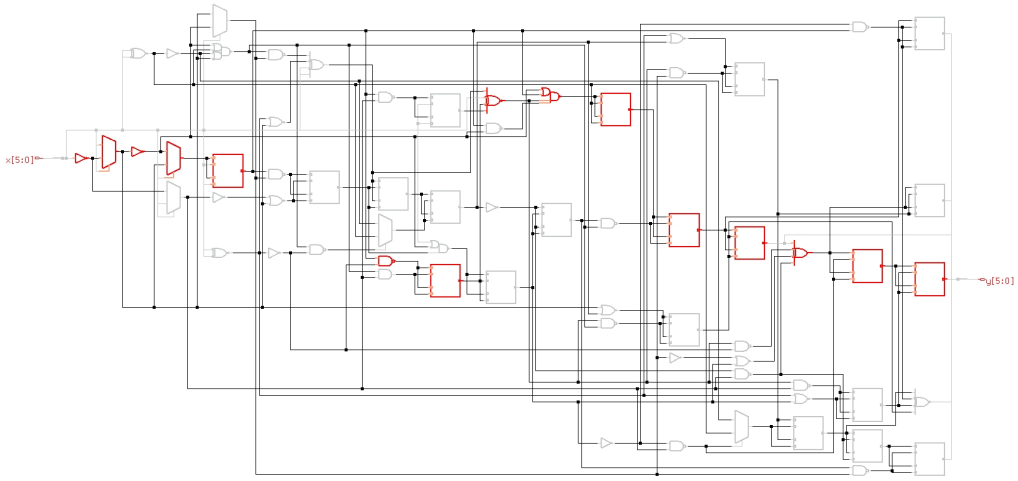

Figure 8: Schematic view of SMSL41 as per synthesized net-list using Cadence Genus highlighting the cell instances in the critical path.

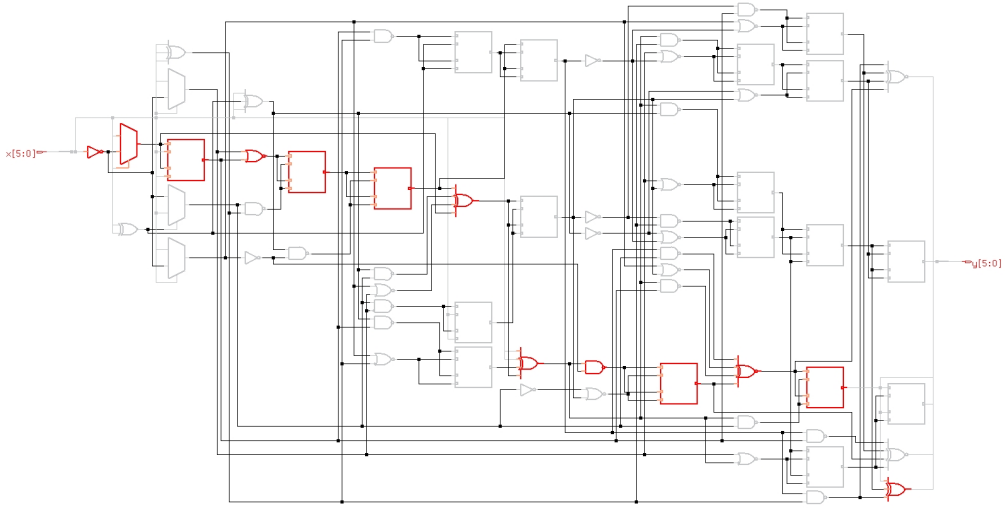

Figure 9: Schematic view of SMS26 as per synthesized net-list using Cadence Genus highlighting the cell instances in the critical path.

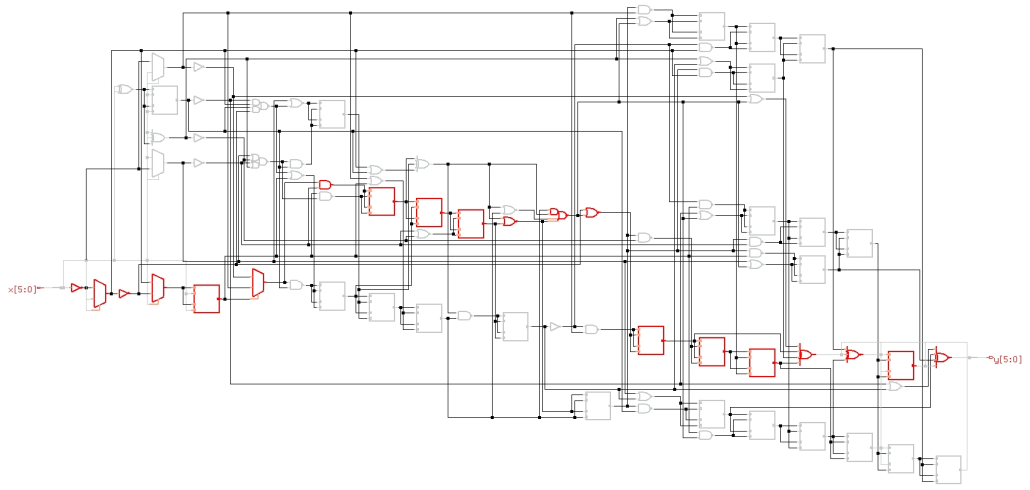

Figure 10: Schematic view of x^{62} as per synthesized net-list using Cadence Genus highlighting the cell instances in the critical path.

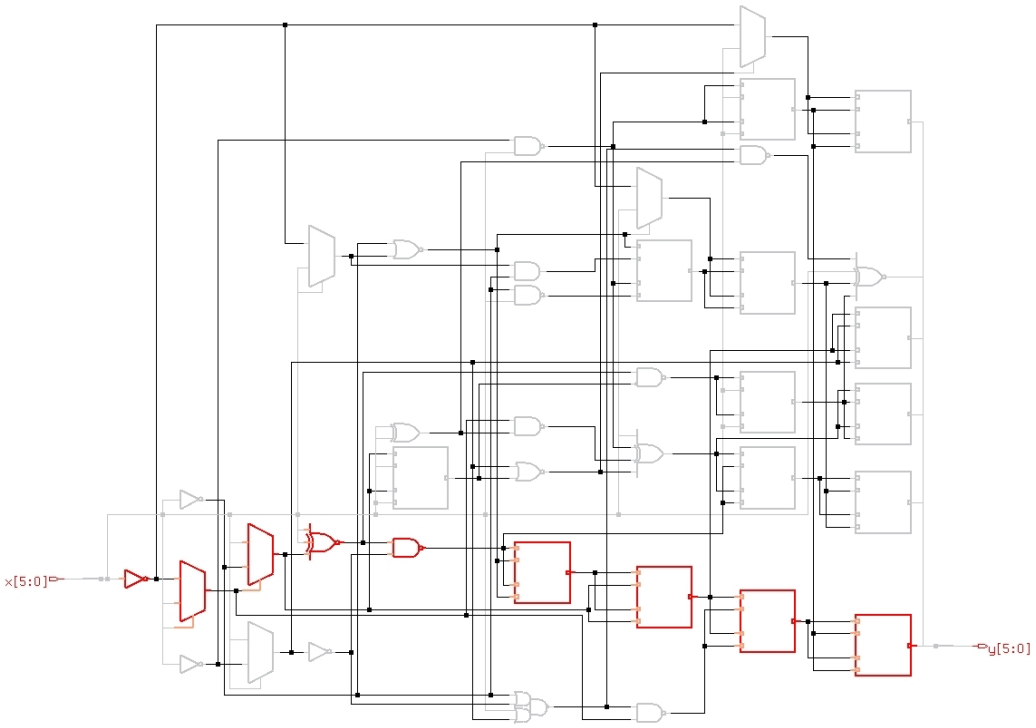

Figure 11: Schematic view of SMS34 as per synthesized net-list using Cadence Genus highlighting the cell instances in the critical path.

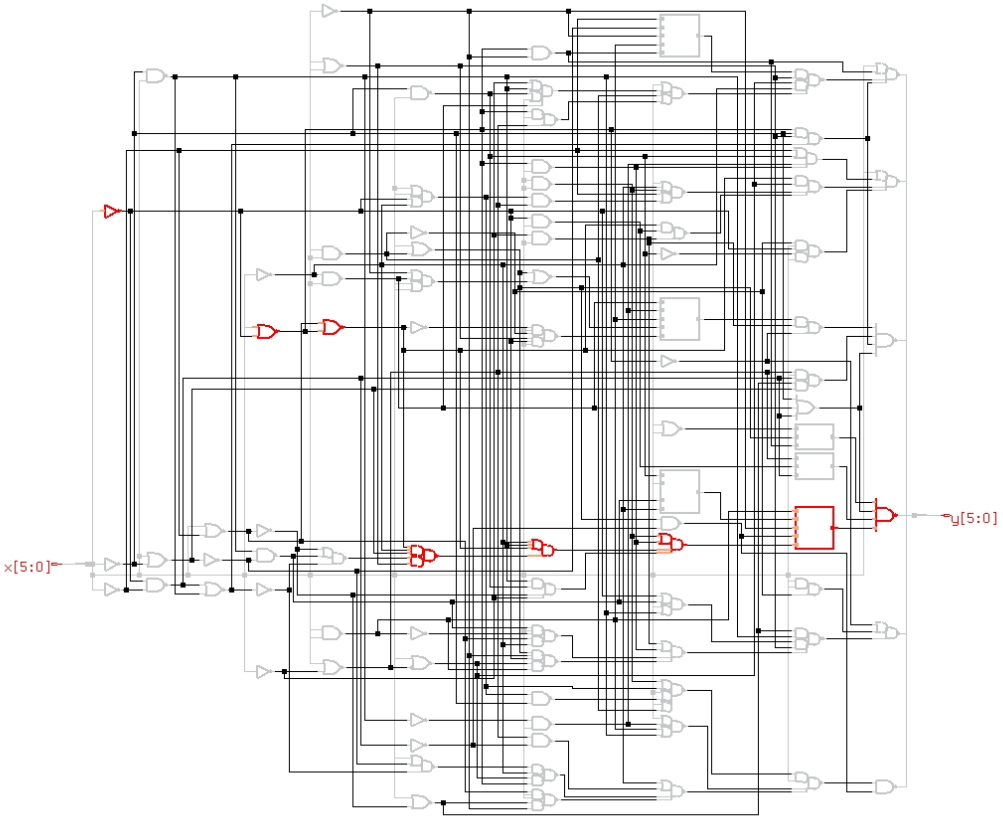

Figure 12: Schematic view of x^{23} as per synthesized net-list using Cadence Genus highlighting the cell instances in the critical path.