Constructions of a Family of Nonlinear Permutations of Any Possible Algebraic Degrees with the Optimal Threshold Implementations

Zhaolei Li[1] and Deng Tang[1*]

[1*]Shanghai Jiao Tong University, School of Electronic Information and Electrical Engineering, Dongchuan Road, Shanghai, 200240, China.

*Corresponding author(s). E-mail(s): dengtang@sjtu.edu.cn;
Authors: zhaoleli@sjtu.edu.cn;

Abstract

Side-channel attacks can uncover sensitive data by analyzing information leakages of cryptographic hardware devices caused by the power consumption, timing, electromagnetic, glitches, *etc.* An attack exploiting these leakages is the differential power analysis (DPA). Threshold Implementation (TI), introduced by Nikova et al. [JoC 24(2):292-321, 2011], was proposed to resist DPA on hardware implementations of block ciphers and eliminate information leakage due to glitches. TI is based on secret sharing and multi-party computation. Since the cost of implementing a TI is directly proportional to the number of shares, minimizing the number of shares is of importance. Note that Nikova et al. proved that, for a target function of algebraic degree $\boldsymbol{t \geq 2}$, the lower bound on the number of shares to implement a TI is $\boldsymbol{t+1}$. And we call a TI with $\boldsymbol{t+1}$ shares an optimal TI. However, achieving this bound is challenging. To date, the only universal construction for any bijective function of algebraic degree $\boldsymbol{t \geq 2}$ achieves a TI with $\boldsymbol{t+2}$ shares, which was proposed by Piccione et al. [IEEE TIT 69(10):6700-6710, 2023]. Only two studies managed to implement optimal TIs. They either concentrated on the Feistel structure or were based on Shannon's expansion. It should be noted that adding randomness can meet the $\boldsymbol{t+1}$ bound, but generating randomness is expensive in practice. Consequently, this paper endeavors to fill this gap by systematically investigating the substitution-boxes (S-boxes to be brief) that can achieve optimal TIs without additional randomness. In this paper, inspired by the Feistel structure in the design of S-boxes, we present two constructions of bijective S-boxes with optimal TIs. Of particular interest is the S-boxes constructed from two permutations exhibiting nonzero nonlinearity, making them potential candidates for S-boxes with desirable properties. For applications, our

constructions can interpret the existence of **3**-share or **4**-share TIs for certain functions in **3**, **4** and **5** variables, as previously reported by Bilgin et al. [CHES 7428:76-91, 2012] and Božilov et al. [ToSC 2017(1):398-404, 2017], including $\mathcal{Q}_5^{25}$, which cannot be interpreted by the previous works. We also give the bijective S-boxes, which are Examples 4 to 11, that possess the optimal TIs by our results.

Keywords: Vectorial Boolean Functions, S-box, DPA, Sharing, Threshold Implementations, Feistel Structure

1 Introduction

With the advancement of computers and network communication, the use of embedded devices is becoming more widespread. To ensure the security of data and related information within these devices, it is imperative to implement cryptographic algorithms on these unencrypted devices, thereby enhancing their resistance to cryptanalysis. However, despite being designed to withstand cryptanalytic attacks, cryptographic algorithms in hardware devices are still vulnerable to side-channel analysis (SCA). SCA are physical attacks which exploit information leakages from various physical effects, *e.g.,* timing, electromagnetic and power consumption [5–7]. In 1999, Kocher et al. [7] introduced the so-called differential power analysis (DPA), a method to extract cryptographic keys by analyzing the power consumption patterns of cryptographic hardware devices. They implemented DPA on DES and successfully retrieved the secret key. After that, developing countermeasures for cryptographic hardware devices against DPA has become an essential objective for cryptographers. One of the most prominent countermeasures against DPA is called sharing (also known as masking) [8], which has precise theoretical foundations. The idea of sharing is to divide the secret input into several shares, ensuring that each share is statistically independent of the original secret. This means that even if an adversary obtains all but one of the shares, he will not be able to recover the secret input. However, the presence of glitches is unavoidable in hardware devices, or alternatively, the glitch-free hardware comes at a high cost. When considering scenarios in which glitches occur within hardware devices, information leakage caused by glitches also occurs. And neglecting the impact of glitches can render a masked implementation vulnerable to attack [9]. The Threshold Implementation (TI), as introduced by Nikova et al. [10] in 2006, offers a solution by constructing a Boolean masking which takes into account the presence of glitches. Subsequently, recognizing the need for resisting higher-order DPA, TIs were extended to higher-order TI [11]. But later it was shown insecure against multivariate attacks [12] unless adding randomness as re-masking. Various papers then have proposed efficient ways to implement higher-order masking in hardware devices while maintaining resilience against glitches. Since then, the TI and its extensions have been intensively studied and applied to numerous symmetric cryptographic primitives, including the widely used cryptographic algorithms AES [13–18], Keccak [19–22], PRESENT [22–24], *etc.*

For a target function F (typically a bijective S-box), the dth-order TI of F is actually a vectorial Boolean function $\mathbf{F}$. The function $\mathbf{F}$ must have three properties

to ensure the security of the implementation: correctness, dth-order non-completeness and uniformity. The requirement for correctness is obvious, as it ensures every share of an input secret x is mapped by $\mathbf{F}$ to an output share of $F(x)$. The dth-order non-completeness states that any combination of up to d output shares of $\mathbf{F}$ is independent of at least one input share. And the uniformity implies that $\mathbf{F}$ yields a uniformly shared output if its input is uniformly shared. Given the aforementioned three properties, the function $\mathbf{F}$ ensures protection against dth-order DPA and maintains security in the presence of glitches. Furthermore, it has been demonstrated that for the target function of algebraic degree t, correctness and dth-order non-completeness of a dth-order TI require a minimum number of input shares, denoted as $s_{in} \geq dt + 1$, see [10, 11, 25]. The lower bound inherently suggests that the number of input shares and output shares increases together with the algebraic degree of the target function, for a given security order d. Notably, when $d = 1$, we have $s_{in} \geq t + 1$ and $s_{out} \geq t + 1$, which is simple to deal with. Hence, for the remainder of this paper, we focus on the specific scenario where the target function is a permutation and the number of input shares is equal to the number of output shares in TIs. Additionally, our discussion will be limited to the first-order TI, which we will refer to simply as TI for brevity. Moreover, if the number of shares of a TI for a permutation of algebraic degree t meets the lower bound $t + 1$, we say that the TI is optimal. There is a clear correlation between the cost of TIs and the number of shares as well as the amount of additional randomness. While adding randomness to restore uniformity of TIs can meet the $t + 1$ bound, the requirement of randomness can significantly inflate the cost of implementations in practice. Indeed, to be secure in the implementations of randomness generation, cryptographic standards demand high-quality for random number generators [26]. Hence, the implementations of TIs for permutations discussed in this paper are designed to avoid any additional randomness. Consequently, the cost of TIs solely relies on the number of shares, which, as it increases, can cause the cost of the implementations to rise. Therefore, minimizing the number of shares is a critical objective for the implementations of TIs. It should be noted that, any bijective function of algebraic degree $t \geq 2$ does have a $(t + 2)$-share TI [2] and the theoretical lower bound on the number of shares $t + 1$ is not possible for all bijective functions, with $t \geq 2$. For instance, the Gold function x^3 over $\mathbb{F}_{2^3}$ is a quadratic permutation, and it cannot be realized with a 3-share TI but necessitates a minimum of 4 shares for TIs [3].

1.1 The State of the Art

1.1.1 Four General Constructions of TIs

Constructing a TI with the minimum number of shares for any arbitrary function is a challenging task. Currently, there exist four methods as primary constructions of TIs with either $t + 1$ or $t + 2$ shares. The first method is using "direct sharing" alongside correction terms [3, 10], but this approach cannot guarantee success with $t + 1$ or $t + 2$ shares for any arbitrary bijective S-box. The second one involves using direct sharing and adding randomness in the re-masking step to preserve the uniformity to achieve an optimal TI. The third method, known as "the changing of the guards", was introduced by Daemen [20]. This method is a variation of the second method. It uses

the output shares of the ith S-box as the randomness for the $(i+1)$th S-box, so only the randomness is generated at the beginning and reused at each round. This reduces the randomness required but is limited to an S-box layer rather than an individual S-box. Recently, the work of Piccione et al. [2] represents a significant step in the implementations of TIs. They introduced a universal optimal construction for a TI of any bijective S-box with $t+2$ shares. This construction is optimal since some bijective functions of algebraic degree $t \geq 2$ do not admit an optimal TI. Later, Piccione further generalized the universal TI construction in [2] for two finite Abelian groups, which can be used to construct a TI with $s \geq t+2$ shares in input and $t+2$ shares in output [27]. Despite these advancements, a theoretical method for determining whether a function of algebraic degree t admits an optimal TI still remains undeveloped.

1.1.2 Optimal TIs of Certain S-boxes

Certain permutations with algebraic degree $t \geq 2$ are known to admit optimal TIs, as referenced in [3, 4, 28, 29]. Functions in [3, 4] are characterized by bad nonlinear and differential property. For instance, most of them typically exhibit 0 nonlinearity and have differential uniformity greater or equal to 2^{n-1}. Specifically, Bilgin et al. [3] derived TIs for the classification of the affine equivalent classes for 3-bit and 4-bit permutations, while Božilov et al. [4] presented TIs with 3 shares for certain 5-bit quadratic permutations. Additionally, an optimal TI designed for the Feistel structure was introduced in [28]. This construction can be seen as a primary construction of TIs, only for the Feistel structure S-boxes. Moreover, there is a secondary construction about TIs in [29]. Specifically, if an n-bit bijective S-box already has a TI, then the newly constructed $(n+1)$-bit and $(n+2)$-bit bijective S-boxes derived from it also admit TIs. Notably, these extended S-boxes require the same number of shares as the original n-bit S-box. Consequently, the existence of an n-bit bijective S-box with an optimal TI implies the existence of the $(n+1)$-bit and $(n+2)$-bit bijective S-boxes with optimal TIs constructed through this method.

1.1.3 TIs of Small S-boxes

Except for the general methods for constructing a TI of a bijective S-box, the TIs of small S-boxes have been studied in [3, 4, 30, 31]. Actually, Bilgin et al. [3] derived TIs of all 3-bit and 4-bit bijective S-boxes, as well as the DES S-box. In [30], the authors provided an efficient algorithm to find TIs for all 3-bit and 4-bit bijective S-boxes (permutations). Furthermore, they extended their investigation to include TIs of four 5-bit almost bent permutations and the only known 6-bit Almost Perfect Nonlinear (APN) permutations. Additionally, they also explored the method of decomposing S-boxes into small S-boxes of lower degrees. Meanwhile, the authors of [31] introduced two methodologies to efficiently implement certain 4-bit S-boxes with good cryptographic properties in 3-share TIs. Božilov et al. [4] explored all 75 affine equivalence classes of 5-bit quadratic permutations and provided the existence of TIs with 3 shares for certain classes.

1.1.4 TIs of Functions with High Algebraic Degrees

To reduce the significant cost of a TI of the function with high algebraic degree, it is an alternative to decompose the target function by means of functions with low algebraic degrees, and design TIs for those new functions, respectively. For example, [24] decomposed PRESENT S-box into two distinct quadratic S-boxes, while [31] proposed a decomposition utilizing two same quadratic functions with certain linear functions. Caforio et al. [32] decomposed the SKINNY 8-bit S-box (algebraic degree is 6) into three quadratic functions or two cubic functions. Meanwhile, Jati et al. [33] implemented three kinds of TIs of the GIFT S-box, that is, a composition of two quadratic permutations, a composition of two same quadratic functions, and the S-box without decomposition. For the AES S-box (an 8-bit S-box of algebraic degree 7), [2, 16, 18] decomposed it into two cubic permutations, while [13–15, 34–36] applied TIs to the Canright's tower field decomposition [37]. Since low-degree functions serve as building blocks in the TIs for decompositions of S-boxes with high algebraic degrees, the implementations of TIs for functions with low algebraic degrees, *e.g.,* quadratic and cubic, still attract particular attention.

1.2 Our Contribution

To date, the only universal construction achieves a TI with $t+2$ shares for any bijective function of algebraic degree $t \geq 2$, which is not optimal for certain S-boxes, see [3, 4, 28]. Therefore, discussing the S-boxes with optimal TIs can fill the gap in the previous construction and lead to a reduction in the implementation cost of TIs for such S-boxes. In this paper, inspired by the TIs of the Feistel structure, our contribution lies in providing constructions of permutations of algebraic degree t, whose number of shares for TIs is $t+1$. Specifically, we present two theorems to construct permutations with optimal TIs. Of particular interest is that the functions constructed by Theorem 1 have no linear component functions, *i.e.,* have nonzero nonlinearity, making them potential candidates for S-boxes with desirable properties. Indeed, Theorem 1, which is a generalization of Theorem 2, can obtain a permutation of algebraic degree t over $\mathbb{F}_2^{n+m}$ with an optimal TI using two permutations of algebraic degree at most $t-1$ over $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$, respectively. It should be noted that Theorems 1 and 2 achieve TIs by the construction in [2] and the fact that a balanced Boolean function can be constructed by the direct sum of a balanced Boolean function and an arbitrary Boolean function. Functions in both theorems can be seen as in the design of a general the Feistel structure S-boxes [38] with inputs and outputs passing through certain bijective S-boxes. For applications, we can interpret the existence of 3-share or 4-share TIs for certain quadratic functions in 4 and 5 variables in [3, 4] by our constructions. What's more, we can provide n-bit S-boxes with optimal TIs and nonzero nonlinearity for $n \geq 4$. All examples which can be interpreted by our results are $\mathcal{Q}_5^{25}$ and Examples 4 to 11.

1.3 Organization

The remainder of this paper is organized as follows. In Section 2, we present an introduction to Boolean functions and offer basic concepts about threshold implementations.

We then provide analysis of the known optimal TIs in Section 3. After introducing certain lemmas about the TIs of Boolean functions constructed by direct sum in Section 4, two constructions are then presented in Section 5, in which we show that the existence of functions of nonzero nonlinearity with optimal TIs and quadratic functions with 3-share TIs. The applications of our constructions are discussed in Section 6. We conclude with Section 7. Finally, the examples which have optimal TIs in this paper can be found in Appendix.

2 Preliminaries

In this section, we aim to provide an overview of the fundamental concepts related to Boolean functions and threshold implementations.

2.1 Boolean Functions

Let $\mathbb{F}_2$ be the field with two elements $\{0,1\}$ and $\mathbb{F}_2^n$ be the vector space of n-tuples over $\mathbb{F}_2$. We refer to a finite field F with 2^n elements as $\mathbb{F}_{2^n}$. For any set S, the cardinality of the set is $|S|$. We denote by $F[x]$ the set of all (univariate) polynomials with coefficients in F and by $F[x_1, x_2, \ldots, x_k]$ the set of all multivariate polynomials with coefficients in F with k variables. Given two vectors $a = (a_1, a_2, \ldots, a_n)$ and $b = (b_1, b_2, \ldots, b_n)$ in $\mathbb{F}_2^n$, $a \cdot b = a_1b_1 + a_2b_2 + \cdots + a_nb_n$ is the usual inner product.

A Boolean function in n variables is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. The set of all n-variable Boolean functions is denoted by $\mathcal{B}_n$. It is well-known that any Boolean function f in $\mathbb{F}_2[x_1, x_2, \ldots, x_n]/(x_1^2 + x_1, x_2^2 + x_2, \ldots, x_n^2 + x_n)$ can be expressed through its algebraic normal form (in brief, ANF)

$$f(x_1, x_2, \ldots, x_n) = \sum_{u \in \mathbb{F}_2^n} a_u x^u,$$

where $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$, $u = (u_1, u_2, \ldots, u_n) \in \mathbb{F}_2^n$, $a_u \in \mathbb{F}_2$ and the term $x^u = \prod_{i=1}^n x_i^{u_i}$ is called a monomial. The algebraic degree of f is then denoted by $\deg(f) = \max\{\mathrm{wt}(u) : u \in \mathbb{F}_2^n, a_u \neq 0\}$, where $\mathrm{wt}(u)$ denotes the Hamming weight of u and is defined as the number of nonzero tuples in the vector u. The Hamming weight of a Boolean function f is defined as $\mathrm{wt}(f) = |\{x \in \mathbb{F}_2^n : f(x) = 1\}|$. If a Boolean function has algebraic degree at most 1, we say that it is affine. And we shall call quadratic functions (resp. cubic functions) the Boolean functions of algebraic degree at most 2 (resp. 3).

The direct sum of two Boolean functions is a simple method to construct new Boolean functions. The following lemma, which constructs balanced Boolean functions by the direct sum, plays a crucial role in proving our main theorems.

Lemma 1 ([39]). *Let f be a balanced Boolean function in n variables and g be an m-variable Boolean function, then the $(n+m)$-variable Boolean function h defined by $h(x, y) = f(x) + g(y)$ is balanced.*

Any function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ can be considered as a vectorial Boolean function in n variables. That is, F can be presented in the form

$$F(x_1, x_2, \ldots, x_n) = (f_1(x_1, x_2, \ldots, x_n), f_2(x_1, x_2, \ldots, x_n), \ldots, f_m(x_1, x_2, \ldots, x_n)),$$

where the n-variable Boolean functions $f_1, f_2, \ldots, f_m$ are called coordinate functions of F. And a component function of F is a nonzero linear combination of coordinate functions, which is $v \cdot F = \sum_{i=1}^{n} v_i f_i$ for $v = (v_1, v_2, \ldots, v_n) \in \mathbb{F}_2^{n*}$. The algebraic degree of F is by definition the maximal algebraic degree of the component functions of F. A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is balanced if $n \geq m$ and F takes every value of $\mathbb{F}_2^m$ the same number 2^{n-m} of times. Specifically, if $n = m$, a balanced function is a permutation. Additionally, a balanced function can be characterized by the balancedness of its all component functions.

Lemma 2 ([39] Proposition 35)**.** *An (n, m)-function F is balanced if and only if its all component functions $v \cdot F$, $v \in \mathbb{F}_2^{m*}$, are balanced.*

Equivalence relations serve as a fundamental instrument in the study of Boolean functions. One particularly important concept is affine equivalence. Two functions f and g are affine equivalent if there exist two affine permutations A_1 and A_2 such that $f = A_1 \circ g \circ A_2$. Affine equivalence has significant applications, for instance, it is well-known that any n variable quadratic Boolean function is affinely equivalent to the Dickson form, as stated in the following lemma.

Lemma 3 ([39] Theorem 10)**.** *Every quadratic nonaffine Boolean function in n variables is affinely equivalent to one of three forms:*

(1) For balanced functions: $x_1x_2 + x_3x_4 + \cdots + x_{2r-1}x_{2r} + x_{2r+1}$, where $r \leq \frac{n-1}{2}$;
(2) For functions with Hamming weight smaller than 2^{n-1}: $x_1x_2 + x_3x_4 + \cdots + x_{2r-1}x_{2r}$, where $r \leq \frac{n}{2}$;
(3) For functions with Hamming weight greater than 2^{n-1}: $x_1x_2 + x_3x_4 + \cdots + x_{2r-1}x_{2r} + 1$, where $r \leq \frac{n}{2}$.

Consequently, by Lemma 3, any n-variable quadratic balanced Boolean function can be expressed in the form $x_1x_2 + x_3x_4 + \cdots + x_{2r-1}x_{2r} + x_{2r+1}$ after certain affine transformations. Since these transformations are affine, the variable x_{2r+1} is actually a sum of certain variables in the original function. Thus, we can say that the quadratic balanced Boolean function f is linear about the sum of certain x_i iff f is affine equivalent to the aforementioned form in the rest of our manuscript.

2.2 Nonlinearity of S-boxes

In the realm of symmetric-key cryptography, Boolean functions employed should exhibit high nonlinearity to provide confusion.

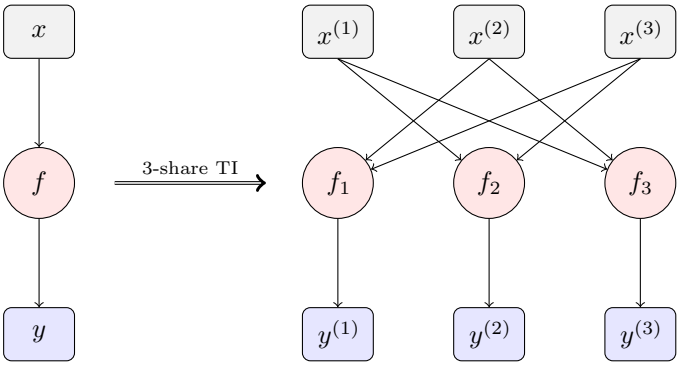

Fig. 1: A 3-share TI for the quadratic function $y = f(x)$

Definition 1 ([39]). *The nonlinearity of a Boolean function $f \in \mathcal{B}_n$ is defined as its minimum Hamming distance from f to all affine functions in n variables,*

$$nl(f) = \min_{g \in \mathcal{B}_n, \deg(g) \leq 1} d_H(f, g),$$

where $d_H(f, g)$ denotes the Hamming distance between f and g, i.e., $d_H(f, g) = \#\{x \in \mathbb{F}_2^n : f(x) \neq g(x)\}$.

For the S-boxes in symmetric-key cryptography, the nonlinearity is defined as the minimum of the nonlinearities of all component functions of S-boxes.

Definition 2 ([39]). *The nonlinearity of an S-box $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is defined as the minimum of the nonlinearities of all component functions of F,*

$$nl(F) = \min_{v \in \mathbb{F}_2^{m*}} nl(v \cdot F).$$

For symmetric-key encryption, the higher the nonlinearity of the employed S-boxes, the better resistance against fast correlation attacks [40] and best affine approximation attacks [41]. Thus, S-boxes utilized in symmetric-key encryption should have nonlinearity as high as possible.

2.3 Threshold Implementations

Given a variable $x \in \mathbb{F}_2^n$ and a positive integer s, we say that the variable x is split into a Boolean s-share as

$$\sum_{i=1}^{s} x^{(i)} = x,$$

where $x^{(i)} \in \mathbb{F}_2^n$ for $i = 1, 2, \ldots, s$. Denote $\mathbf{x} = (x^{(1)}, x^{(2)}, \ldots, x^{(s)}) \in (\mathbb{F}_2^n)^s$ by a Boolean s-share for the variable $x \in \mathbb{F}_2^n$. And the set of all Boolean s-shares for $x \in \mathbb{F}_2^n$

is denoted as

$$\mathrm{Sh}_s(x) := \left\{ \mathbf{x} = \left(x^{(1)}, x^{(2)}, \ldots, x^{(s)}\right) \in (\mathbb{F}_2^n)^s : \sum_{i=1}^{s} x^{(i)} = x \right\},$$

with $|\mathrm{Sh}_s(x)| = 2^{n(s-1)}$. Let s and s' be two positive integers, and both $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and $\mathbf{F} : (\mathbb{F}_2^n)^s \to (\mathbb{F}_2^m)^{s'}$ are two vectorial Boolean functions. Clearly $\mathbf{F} : (\mathbb{F}_2^n)^s \to (\mathbb{F}_2^m)^{s'}$ has the following form:

$$\mathbf{F} = (F^{(1)}, F^{(2)}, \ldots, F^{(s')}),$$

where the function $F^{(i)} : (\mathbb{F}_2^n)^s \to \mathbb{F}_2^m$ is the ith coordinate function of $\mathbf{F}$ for $i = 1, 2, \ldots, s'$. We say that the function $\mathbf{F} = (F^{(1)}, F^{(2)}, \ldots, F^{(s')})$ is a TI of F if $\mathbf{F}$ is correct, non-complete, and uniform with respect to F as defined below, respectively.

Correctness: We say that $\mathbf{F}$ is correct with respect to F, or $\mathbf{F}$ is correct, if for all $x \in \mathbb{F}_2^n$, we have $\sum_{i=1}^{s'} F^{(i)}(\mathbf{x}) = F(x)$, $\forall \mathbf{x} \in \mathrm{Sh}_s(x)$, where $F^{(i)}$ is the ith coordinate function of $\mathbf{F}$.

Non-completeness: For $i \in \{1, 2, \ldots, s\}$ and $j \in \{1, 2, \ldots, s'\}$, we say that the jth coordinate function $F^{(j)}$ is independent of its ith input Boolean-share $x^{(i)}$ if for all $(x^{(1)}, x^{(2)}, \ldots, x^{(s)}) \in (\mathbb{F}_2^n)^s$ and $a \in \mathbb{F}_2^n$, we have

$$F^{(j)}(x^{(1)}, x^{(2)}, \ldots, x^{(s)}) = F^{(j)}(x^{(1)}, x^{(2)}, \ldots, x^{(i-1)}, a, x^{(i+1)}, \ldots, x^{(s)}).$$

Thus, we say $\mathbf{F}$ is non-complete if for all $j \in \{1, 2, \ldots, s'\}$, there exists at least one $i \in \{1, 2, \ldots, s\}$ such that $F^{(j)}$ is independent of its ith input Boolean-share $x^{(i)}$.

Uniformity: Assume $\mathbf{F}$ is correct with respect to F. We say that $\mathbf{F}$ is uniform, if for all $x \in \mathbb{F}_2^n$ and $\mathbf{y} \in \mathrm{Sh}_{s'}(F(x))$, we have

$$|\{\mathbf{x} \in \mathrm{Sh}_s(x) \mid \mathbf{F}(\mathbf{x}) = \mathbf{y}\}| = \frac{2^{n(s-1)}}{2^{m(s'-1)}}.$$

It is worth mentioning that, achieving correctness and non-completeness is relatively straightforward by means of direct sharing, as demonstrated in [3].

The most difficult property to be satisfied when implementing TIs is the uniformity. To address this challenge, Piccione et al. [2] derived the following strong lemma regarding the bijective S-boxes.

Lemma 4 ([2]). *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Let s be a positive integer and $\mathbf{F} : (\mathbb{F}_2^n)^s \to (\mathbb{F}_2^n)^s$ be a function that is correct with respect to F. Then $\mathbf{F}$ is a permutation if and only if $\mathbf{F}$ is uniform and F is a permutation.*

In the rest of this manuscript, we focus on constructing (first-order) TIs for certain permutations in the case $s = s'$. We always use s shares instead of Boolean s-shares for brevity. We say that F admits a TI with s shares if there exists at least one TI of F with s shares. Moreover, the implementations of TIs avoid any additional randomness.

3 Analysis of the Known Optimal TIs of Permutations

The research on optimal TIs for permutations of algebraic degree t remains incomplete. There are two main known constructions, and actually they share the same idea: preserving uniformity of TIs by the direct sum.

3.1 TIs of the Feistel Structure S-boxes

Boss et al. [28] pointed out that TIs of the Feistel structure S-boxes are still Feistel structures. More precise, given $x, y \in \mathbb{F}_2^n$ and any (n, n)-function F with $\deg(F) = t$, the $(2n, 2n)$-Feistel structure (without swapping) S-box

$$R(x, y) = (x, F(x) + y)$$

has an optimal TI $\mathbf{R} = (R^{(1)}, R^{(2)}, \ldots, R^{(t+1)})$ and

$$\begin{cases} R^{(i)}(\mathbf{x}, \mathbf{y}) = (x^{(i+1)}, F^{(i)}(\mathbf{x}) + y^{(i+1)}), \text{ for } i = 1, 2, \ldots, t \\ R^{(t+1)}(\mathbf{x}, \mathbf{y}) = (x^{(1)}, F^{(t+1)}(\mathbf{x}) + y^{(1)}), \end{cases}$$

where $\mathbf{x} = (x^{(1)}, x^{(2)}, \ldots, x^{(t+1)})$ and $\mathbf{y} = (y^{(1)}, y^{(2)}, \ldots, y^{(t+1)})$ are $(t+1)$-shares of $x \in \mathbb{F}_2^n$ and $y \in \mathbb{F}_2^n$, respectively. And $(F^{(1)}, F^{(2)}, \ldots, F^{(t+1)})$ is a correct and non-complete $(t+1)$-share for F. It is easy to implement TIs of the Feistel structure S-boxes, since there is no requirement to preserve the uniformity of the $(t+1)$-share of F, which can be achieved by the direct sharing.

From the perspective of Boolean functions, the existence of optimal TIs of the Feistel structure S-boxes fundamentally relies on the idea of the direct sum. Specifically, the correctness and non-completeness of $\mathbf{R}$ are guaranteed by the correctness and non-completeness of $\mathbf{F}$. The uniformity of $\mathbf{R}$ is equivalent to the permutation of $\mathbf{R}$ by Lemma 4, which is equivalent to the balancedness of all component functions of $\mathbf{R}$. It can be seen that any component function of $\mathbf{R}$ is balanced due to the direct sum. That is, any nonzero linear combination of coordinate functions of $\mathbf{R}$ is balanced, as it is either $\sum_{j \in J} u_j \cdot x^{(j)}$ or the direct sum of a balanced Boolean function $\sum_{i \in I} v_i \cdot y^{(i)}$ and a Boolean function $\sum_{i \in I} v_i \cdot F^{(i)}(\mathbf{x}) + \sum_{j \in J} u_j \cdot x^j$, where $I, J \subseteq \{1, 2, \ldots, t+1\}$ and $v_i, u_j \in \mathbb{F}_2^{n*}$.

Remark 1. *The Feistel structure S-boxes $R(x, y) = (x, F(x) + y)$ are not suitable for cryptographic applications, since they always have linear coordinate functions, which means the S-boxes have* 0 *nonlinearity.*

3.2 TIs of Shannon's Expansion S-boxes

Varici et al. [29] presented the construction about $(n+1)$-bit S-boxes from n-bit S-boxes with known TIs by Shannon's expansion. The $(n+1)$-bit S-boxes also admit TIs, whose number of shares of TIs is the same as that of the original n-bit S-boxes. More precious, the constructions in [29] mainly concern about the s-share TIs of the

$(n+1)$-bit S-boxes in the form of

$$F(x,y)=\begin{cases}(S_1(x),g(x)), & \text{if } y=0,\\ (S_2(x),h(x)), & \text{if } y=1,\end{cases}$$

where $x\in\mathbb{F}_2^n$, $y\in\mathbb{F}_2$, both S_1,S_2 are n-bit S-boxes, both g,h are n-variable Boolean functions, S_2 is chosen in one of the $n+1$ forms: $S_1(x), S_1(x+1_i)$ for $i=1,2,\ldots,n$ and $g=h(S_2^{-1}(S_1(x)))+1$, where 1_i denotes the vector $(0,0,\ldots,1,\ldots,0)$ with 1 on the ith position.

Note that the TIs of constructed S-boxes in cases when $S_2(x)=S_1(x+1_i)$ can be derived from the TIs of the S-box where $S_1=S_2$ with the affine transformation. Thus, we only consider the case $S_1=S_2$ and in this case, we have

$$F(x,y)=(S_1(x),g(x)+y),$$

where both the n-bit bijective S-box $S_1(x)$ and the n-variable Boolean function $g(x)$ have known s-share TIs, see Theorem 2 in [29]. Therefore, it can be seen as the Feistel structure.

3.3 Discussions about Optimal TIs of Permutations

The difficulty of constructing TIs lies in the uniformity. Two constructions, presented in [28, 29], address the uniformity in the Feistel structure. In fact, these optimal TIs of the Feistel structure S-boxes achieve the uniformity through the direct sum. However, the Feistel structure always has linear part x, making it not suitable for cryptographic applications. Consequently, it becomes necessary to substitute this linear function x to a proper nonlinear function, which makes the new S-box nonzero nonlinearity while still admitting optimal TIs.

This idea is actually realized by [29] under the condition $S_1=S_2$, where the linear function x is replaced by $S_1(x)$. However, this approach introduces an additional challenge: ensuring the existence of TIs of the Boolean function $g(x)$ with desired number of shares. However, we cannot guarantee the existence of s-share TIs for $g(x)$, which significantly constrains the choice for $g(x)$. Therefore, the requirement for TIs of $g(x)$ is a major challenge in constructing TIs for the new S-boxes $F(x,y)=(S_1(x),g(x)+y)$. Actually, Theorem 2 in Section 5 offers a solution to this challenge, where the requirement for $g(x)$ is eliminated by employing the direct sum.

Additionally, the constructions in [29] are limited to increasing the S-box size by only one or two. A natural extension of this work would be to generalize the construction method to allow for increasing the S-box size by any possible number, while ensuring that the new S-boxes maintain TIs with the same number of shares as the original S-boxes. To achieve this, the right tuple of the Feistel structure should be a vectorial Boolean function $F(x)+H(y)$ instead of the Boolean function $g(x)+y$. This then yields a new S-box structure

$$R(x,y)=(G(x),F(x)+H(y)).$$

Here F, G and H must be carefully chosen to ensure that R is a permutation and admits desired TIs. In Theorem 1 of Section 5, we will detail the construction of TIs for these new S-boxes $R(x, y) = (G(x), F(x) + H(y))$ under the conditions described.

4 TIs of Boolean Functions Constructed by Direct Sum

We present two lemmas about the construction of TIs of some Boolean functions and of $(n+m, n)$-functions, both of them are constructed by the direct sum. These lemmas play a crucial role in proving our main theorems in the following section.

4.1 TIs of Some Boolean Functions Constructed by Direct Sum

TIs of certain Boolean functions can be easily constructed in theory. Consider the linear Boolean functions, given $a \in \mathbb{F}_2^{n*}$, the linear Boolean function $f(x) = a \cdot x$ over $\mathbb{F}_2^n$ has an s-share TI $\mathbf{f} = (f^{(1)}, f^{(2)}, \ldots, f^{(s)})$ such as

$$\begin{cases} f^{(i)} = a \cdot x^{(i+1)}, \text{ for } i = 1, 2, \ldots, s-1 \\ f^{(s)} = a \cdot x^{(1)}, \end{cases}$$

where $(x^{(1)}, x^{(2)}, \ldots, x^{(s)})$ is an s-share of x with $s \geq 3$.

For any Boolean function which is the direct sum of a Boolean function admitting s-share TIs and an arbitrary Boolean function, we have the following lemma.

Lemma 5. *Let g be an n-variable Boolean function of algebraic degree t which admits an s-share TI, h be an m-variable Boolean function with $\deg(h) \leq s-1$, then for the $(n+m)$-variable Boolean function defined by $f(x, y) = g(x) + h(y)$, there exists an s-share TI $\mathbf{f}$ for f.*

Proof Assume that $\mathbf{g}(\mathbf{x}) = (g^{(1)}, g^{(2)}, \ldots, g^{(s)})$ is an s-share TI for $g \in \mathcal{B}_n$, where $\mathbf{x} \in (\mathbb{F}_2^n)^s$ and $g^{(1)}, g^{(2)}, \ldots, g^{(s)}$ are functions from $(\mathbb{F}_2^n)^s$ to $\mathbb{F}_2$. Clearly we can construct a correct and non-complete s-share $\mathbf{h}(\mathbf{y}) = (h^{(1)}, h^{(2)}, \ldots, h^{(s)})$ with respect to $h \in \mathcal{B}_m$ by direct sharing, where $\mathbf{y} \in (\mathbb{F}_2^m)^s$ is an s-share of y and $h^{(1)}, h^{(2)}, \ldots, h^{(s)}$ are functions from $(\mathbb{F}_2^m)^s$ to $\mathbb{F}_2$. Thus, the function $\mathbf{f}(\mathbf{x}, \mathbf{y}) = (f^{(1)}, f^{(2)}, \ldots, f^{(s)})$, whose coordinate functions defined by $f^{(i)}(\mathbf{x}, \mathbf{y}) = g^{(i)}(\mathbf{x}) + h^{(i)}(\mathbf{y})$ for $i = 1, 2, \ldots, s$, is an s-share for f. In the following, we will prove the correctness, non-completeness and uniformity of $\mathbf{f}$.

Correctness: The correctness of $\mathbf{f}$ follows from the correctness of $\mathbf{g}$ and $\mathbf{h}$:

$$\begin{aligned} \sum_{i=1}^{t+1} f^{(i)}(\mathbf{x}, \mathbf{y}) &= \sum_{i=1}^{t+1} g^{(i)}(\mathbf{x}) + \sum_{i=1}^{t+1} h^{(i)}(\mathbf{y}) = g(x) + h(y) \\ &= f(x, y). \end{aligned}$$

Non-completeness: The non-completeness of $\mathbf{f}$ can be derived from the non-completeness of $\mathbf{g}$ and $\mathbf{h}$, that is, for any $i \in \{1, 2, \ldots, s\}$, $f^{(i)} = g^{(i)} + h^{(i)}$ is independent of $x^{(i)}$ as both $g^{(i)}$ and $h^{(i)}$ are independent of $x^{(i)}$. So does $y^{(i)}$, which means $f^{(i)}$ is independent of $(x^{(i)}, y^{(i)})$. Thus, we can say that $\mathbf{f}$ is non-complete.

Uniformity: All component functions of $\mathbf{g}$, *i.e.,* $\sum_{i\in I} g^{(i)}$ for certain nonempty sets $I \subseteq \{1,2,\ldots,t+1\}$, are balanced since $\mathbf{g}$ is an s-share TI for g. Thus, any component function of $\mathbf{f}$ is balanced, as it is a direct sum of a balanced Boolean function $\sum_{i\in I} g^{(i)}$ and a Boolean function $\sum_{i\in I} h^{(i)}(\mathbf{y})$, for any nonempty set $I \subseteq \{1,2,\ldots,t+1\}$. This means $\mathbf{f}$ is balanced and then $\mathbf{f}$ is uniform, as

$$|\{\mathbf{x} \in \mathrm{Sh}_s(x) \mid \mathbf{F}(\mathbf{x}) = \mathbf{y}\}| = \frac{2^{(n+m)(s-1)}}{2^{s'-1}}.$$

Thus, $\mathbf{f}$ is an s-share TI for f. □

Given $a \in \mathbb{F}_2^{n*}$, we known that the linear Boolean function $a \cdot x$ over $\mathbb{F}_2^n$ admits an s-share TI, where $s \geq 3$. Thus, we can obtain the following corollary of Lemma 5 when $g(x) = a \cdot x$.

Corollary 1. *For $a \in \mathbb{F}_2^{n*}$ and any Boolean function $h \in \mathcal{B}_m$, the $(n+m)$-variable Boolean function $f(x,y) = a \cdot x + h(y)$ admits an s-share TI, where $x \in \mathbb{F}_2^n$, $y \in \mathbb{F}_2^m$ and $s \geq \deg(h) + 1$.*

Additionally, consider the special case where the Boolean function is in the form of $f(x,y) = h(y)$. Treat it as $f(x,y) = 0 + h(y)$, and the function 0 has an s-share TI for any $s \geq 3$ as $(x^{(2)}, x^{(3)}, \ldots, x^{(s-1)}, x^{(2)} + x^{(3)} + \cdots + x^{(s-1)})$. Thus, we have the following corollary when $g(x)$ is vanished.

Corollary 2. *For any Boolean function $h \in \mathcal{B}_m$, the $(n+m)$-variable Boolean function $f(x,y) = h(y)$ admits an s-share TI, where $x \in \mathbb{F}_2^n$, $y \in \mathbb{F}_2^m$ and $s \geq \deg(h) + 1$.*

By Lemma 3, any n-variable balanced Boolean function is affinely equivalent to $x_1x_2 + x_3x_4 + \cdots + x_{2r-1}x_{2r} + x_{2r+1}$, where $r \leq \frac{n-1}{2}$, which is the direct sum of a balanced Boolean function x_{2r+1} and a Boolean function $x_1x_2 + x_3x_4 + \cdots + x_{2r-1}x_{2r}$. Thus, according to Corollaries 1 and 2, we have a simple but maybe impressive corollary about the TIs for balanced quadratic Boolean functions.

Corollary 3. *Any balanced quadratic Boolean function admits a 3-share TI.*

4.2 $(n+m, n)$-Functions Constructed by Direct Sum

Note that the direct sum of two Boolean functions is similar to the direct sum of two vectorial Boolean functions. More specifically, consider the (n, n')-function G and (m, m')-function H with $n' \geq m'$, by means of the direct sum, we have the $(n+m, n')$-function defined by $F(x,y) = G(x) + H(y)$ as

$$\begin{cases} F_i(x,y) = G_i(x) + H_i(y), \text{ for } i = 1,2,\ldots,m' \\ F_j(x,y) = G_j(x), \text{ for } j = m'+1, m'+2, \ldots, n'. \end{cases}$$

Then, we have the following lemma about the construction of TIs for $(n+m, n)$-functions, which can be seen as a generalization of Lemma 5.

Lemma 6. *Let G be a permutation of algebraic degree $t \geq 2$ over $\mathbb{F}_2^n$ and H be an (m, m')-function of algebraic degree d, where $m' \leq n$. Define the $(n+m, n)$-function by $F(x, y) = G(x) + H(y)$ for $(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$. Then any component function of F is balanced and F has a $\max\{t+2, d+1\}$-share TI $\mathbf{F}$ for F.*

Proof Assume that $G(x) = (G_1(x), G_2(x), \ldots, G_n(x))$ and $H(y) = (H_1(y), H_2(y), \ldots, H_{m'}(y))$. Thus, any component function of $F(x, y) = G(x) + H(y)$ is in the form

$$\sum_{i \in I}(G_i(x) + H_i(y)) + \sum_{j \in J} G_j(x) = \sum_{i \in I \cup J} G_i(x) + \sum_{i \in I} H_i(y),$$

with two sets $I \subseteq \{1, 2, \ldots, m'\}$ and $J \subseteq \{m'+1, m'+2, \ldots, n\}$, where $I \cup J$ is non-empty. Clearly any component function is the direct sum of a balanced Boolean function $\sum_{i \in I \cup J} G_i(x)$ and a Boolean function $\sum_{i \in I} H_i(y)$, so it is balanced.

Thus we only need to prove the existence of a $\max\{t+2, d+1\}$-share TI for F. First we consider the case $t + 2 > d + 1$. Note that we can always construct a $(t+2)$-share TI for G according to the universal TI construction for permutations [2], which we denote as $\mathbf{G} = (G^{(1)}, G^{(2)}, \ldots, G^{(t+2)})$. Clearly the uniformity of $\mathbf{G}$ is equivalent to the permutation of $\mathbf{G}$, that is, any component function of $\mathbf{G}$ is balanced. Additionally, a correct and non-complete $(t+2)$-share $\mathbf{H} = (H^{(1)}, H^{(2)}, \ldots, H^{(t+2)})$ with respect to H can be constructed by direct sharing. Thus, we have a $(t+2)$-share $\mathbf{F}$ as

$$\begin{aligned}\mathbf{F}(\mathbf{x}, \mathbf{y}) =& \mathbf{G}(\mathbf{x}) + \mathbf{H}(\mathbf{y}) \\ =& (G^{(1)} + H^{(1)}, G^{(2)} + H^{(2)}, \ldots, G^{(t+2)} + H^{(t+2)}).\end{aligned}$$

The correctness and non-completeness of $\mathbf{F}$ can be derived from the correctness and non-completeness of $\mathbf{G}$ and $\mathbf{H}$. It can be seen that any component function of $\mathbf{F}$ is balanced. This property is evident, as a component function of $\mathbf{F}$ is a direct sum of a component function of $\mathbf{G}(\mathbf{x})$ and a component function of $\mathbf{H}(\mathbf{y})$.

The rest of this proof addresses the case where $t + 2 \leq d + 1$. The proof is analogue to the case $t + 2 > d + 1$ with two distinctions: (1) we construct a $(d+1)$-share TI for G instead of a $(t+2)$-share TI by the generalization[1] of the universal TI construction in [2]. (2) we construct a correct and non-complete $(d+1)$-share with respect to H by direct sharing. □

5 Permutations with Optimal TIs

In this section, we present constructions of permutations of algebraic degree at most t, which admit optimal TIs, for $t \geq 2$. According to Lemma 6, we will obtain a theorem which can be seen as a primary construction of optimal TIs for the permutation of algebraic degree $t \geq 2$.

Theorem 1. *Let G be a permutation of algebraic degree $t_1 \geq 2$ over $\mathbb{F}_2^n$ and H be a permutation of algebraic degree $t_2 \geq 2$ over $\mathbb{F}_2^m$. Let F be an $(n+m, n+m)$-function in the form*

$$F(x, y) = (G(x) + H'(y), H(y)),$$

[1] This generalization can be realized by splitting x into $t + m$ shares instead of $t + 2$ shares, where $m \geq 2$. And the proofs of correctness, non-completeness and uniformity of the TI with $t + m$ shares are the same as those of the TI with $t + 2$ shares [2].

for $x \in \mathbb{F}_2^n$ and $y \in \mathbb{F}_2^m$, where H' is an (m, m')-function of algebraic degree $d \geq \max\{t_1 + 1, t_2 + 1\}$ with $m' \leq n$. Then, F is a permutation of algebraic degree d over $\mathbb{F}_2^{n+m}$ and F admits an optimal TI.

Proof To prove that F is a permutation over $\mathbb{F}_2^{n+m}$, it suffices to show that any component function of F is balanced. The component functions of F can be written as $u \cdot (G(x) + H'(y)) + v \cdot H(y)$, where $u \in \mathbb{F}_2^n$ and $v \in \mathbb{F}_2^m$ with u, v not simultaneously equal to zero. If $u \neq 0$ and $v = 0$, the component function is balanced since $G(x)$ is a permutation and $H'(y)$ is independent of $G(x)$. Similarly, if $u = 0$ and $u \neq 0$, the component function is also balanced as $H(y)$ is a permutation. Finally, if $uv \neq 0$, the component function takes the form $u \cdot G(x) + u \cdot H'(y) + v \cdot H(y)$. It is balanced since $G(x)$ is a permutation and $G(x)$ is independent of both $H'(y)$ and $H(y)$. Therefore, F is a permutation over $\mathbb{F}_2^{n+m}$.

Thus we only need to prove the existence of an optimal TI of F. Note that $\deg(F) = d$, thus, let $\mathbf{F} = (F^{(1)}, F^{(2)}, \ldots, F^{(d+1)})$ be a function from $(\mathbb{F}_2^{n+m})^{d+1}$ to itself in the form $\mathbf{F}(\mathbf{x}, \mathbf{y}) = (\mathbf{G}(\mathbf{x}) + \mathbf{H'}(\mathbf{y}), \mathbf{H}(\mathbf{y}))$ for $\mathbf{x} \in \mathbb{F}_2^{n(d+1)}$ and $\mathbf{y} \in \mathbb{F}_2^{m(d+1)}$, where $F^{(i)} = (G^{(i)} + H'^{(i)}, H^{(i)})$ for $1 \leq i \leq d$. In above form, $\mathbf{G}$ and $\mathbf{H}$ are $(d+1)$-share TIs achieved by the universal TI construction in [2]. $\mathbf{H'}$ is a correct and non-complete $(d+1)$-share achieved by direct sum.

Based on the previous discussion about $\mathbf{H}, \mathbf{H'}$ and $\mathbf{G}$, we can prove the correctness, non-completeness and uniformity of $\mathbf{F}$ with respect to F:

Correctness: We known that $\mathbf{G} = (G^{(1)}, G^{(2)}, \ldots, G^{(d+1)})$, $\mathbf{H} = (H^{(1)}, H^{(2)}, \ldots, H^{(d+1)})$ and $\mathbf{H'} = \left(H'^{(1)}, H'^{(2)}, \ldots, H'^{(d+1)}\right)$ are correct $(d+1)$-shares for G, H and H', respectively. Then for $\mathbf{F} = (F^{(1)}, F^{(2)}, \ldots, F^{(d+1)})$, we have

$$\begin{aligned}\sum_{i=1}^{d+1} F^{(i)} &= \sum_{i=1}^{d+1} \left(G^{(i)} + H'^{(i)}, H^{(i)}\right) \\ &= \left(\sum_{i=1}^{d+1} G^{(i)} + \sum_{i=1}^{d+1} H'^{(i)}, \sum_{i=1}^{d+1} H^{(i)}\right) = (G + H', H) = F.\end{aligned}$$

That is, $\mathbf{F}$ is correct with respect to F.

Non-completeness: We known that $\mathbf{G} = (G^{(1)}, G^{(2)}, \ldots, G^{(d+1)})$, $\mathbf{H} = (H^{(1)}, H^{(2)}, \ldots, H^{(d+1)})$ and $\mathbf{H'} = \left(H'^{(1)}, H'^{(2)}, \ldots, H'^{(d+1)}\right)$ are non-complete $(d+1)$-shares for G, H and H', respectively, Then, the coordinate function of $F^{(i)} = (G^{(i)} + H'^{(i)}, H^{(i)})$ is independent of $x^{(i)}$ and $y^{(i)}$ for $i = 1, 2, \ldots, d+1$, so is independent of $(x^{(i)}, y^{(i)})$ for $i = 1, 2, \ldots, d+1$. Thus, $\mathbf{F}$ is non-complete.

Uniformity: By Lemma 4, $\mathbf{F}$ is uniform with respect to F and F is a permutation over $\mathbb{F}_2^{n+m}$ iff $\mathbf{F}$ is a permutation over $\mathbb{F}_2^{(n+m)(d+1)}$. Consequently, it suffices to demonstrate that $\mathbf{F}$ is a permutation over $\mathbb{F}_2^{(n+m)(d+1)}$. To this end, we need only to prove that all component functions of $\mathbf{F}$ are balanced. Any component functions of $\mathbf{F}$ can be expressed in the form

$$v \cdot (\mathbf{G}(\mathbf{x}) + \mathbf{H'}(\mathbf{y})) + u \cdot \mathbf{H}(\mathbf{y}),$$

where $v \in \mathbb{F}_2^{n(d+1)}$ and $u \in \mathbb{F}_2^{m(d+1)}$ with v, u not simultaneously equal to zero. Then, according to the values of v and u, we can categorize the component functions of $\mathbf{F}$ into three cases:

(i) The case $v \neq 0$ and $u = 0$. It is equivalent to proving the balancedness of $\mathbf{G}(\mathbf{x}) + \mathbf{H'}(\mathbf{y})$, which can be done by Lemma 6.

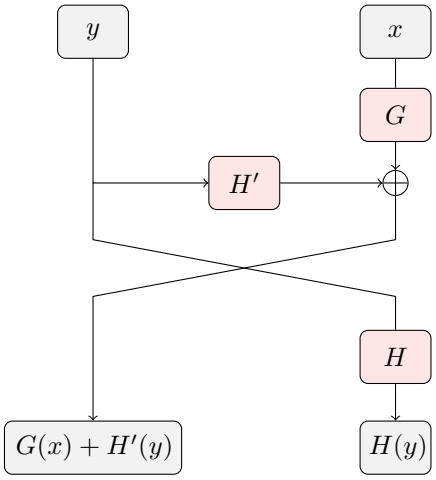

Fig. 2: The structure of F in Theorem 1, where both G and H are bijective

(ii) The case $v = 0$ and $u \neq 0$. It is equivalent to proving the balancedness of $\mathbf{H}(\mathbf{y})$, which can be promised by the universal TI construction in [2].

(iii) Otherwise, consider the case $uv \neq 0$. We can rewrite the component function as $v \cdot \mathbf{G}(\mathbf{x}) + (v \cdot \mathbf{H'}(\mathbf{y}) + u \cdot \mathbf{H}(\mathbf{y}))$. We can see that the component function is a direct sum of the balanced function $v \cdot \mathbf{G}(\mathbf{x})$ and the function $v \cdot \mathbf{H'}(\mathbf{y}) + u \cdot \mathbf{H}(\mathbf{y})$, and it is balanced.

Therefore, we have demonstrated that all component functions of $\mathbf{F}$ are balanced. Thus, $\mathbf{F}$ is a permutation, which implies that $\mathbf{F}$ is uniform with respect to F by Lemma 4.

Thus, $\mathbf{F}$ is an optimal TI of F. □

The structure of F in Theorem 1 is illustrated in Figure 2. It can been seen that this structure is similar to the Feistel structure. As a result, the TI of F can be constructed like the TI of the Feistel structure, see Figure 3.

Theorem 1 can be seen as a primary construction of optimal TIs. We can obtain a secondary construction of optimal TIs by adding or changing certain requirements on permutations G and H. That is, by replacing the conditions $\deg(G) = t_1, \deg(H) = t_2$ and $\deg(H') \geq \max\{t_1+1, t_2+1\}$ with $\deg(G) = \deg(H) = t \geq \deg(H')$, and assuming that both permutations G and H admit optimal TIs. Under these modified conditions, we can construct $(n+m)$-bit bijective S-boxes with optimal TIs from n-bit bijective S-boxes which admit optimal TIs.

Corollary 4. *Let G and H be permutations over $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$, respectively, where one of two permutations admits optimal TIs and has the larger algebraic degree $t \geq 2$. Define the $(n+m, n+m)$-function F as*

$$F(x, y) = (G(x) + H'(y), H(y)), \text{ for } x \in \mathbb{F}_2^n, y \in \mathbb{F}_2^m,$$

where H' is an (m, m')-function with $\deg(H') \leq t$. Then, F is a permutation of algebraic degree t over $\mathbb{F}_2^{n+m}$ and F admits an optimal TI.

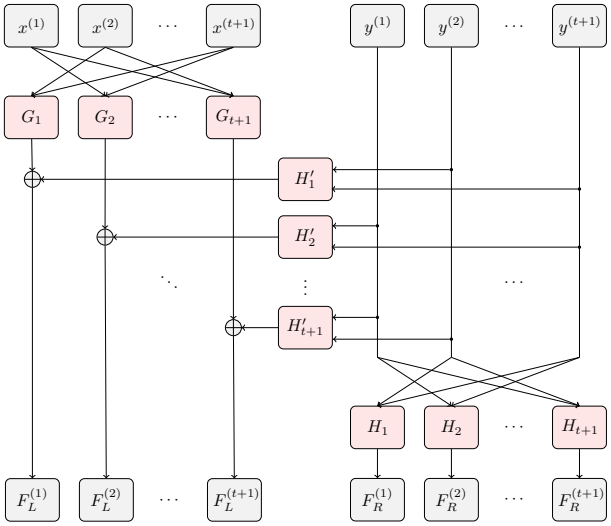

Fig. 3: The structure of the optimal TI $\boldsymbol{F} = (F^{(1)}, F^{(2)}, \ldots, F^{(t+1)})$ of F in Theorem 1 without swapping outputs with the output $F^{(i)} = (F_L^{(i)}, F_R^{(i)})$ for $i = 1, 2, \ldots, t+1$.

Remark 2. *Corollary 4 provides a secondary construction for n-bit permutations of algebraic degree t with optimal TIs, while Theorem 1 is a primary construction. This construction is based on the existence of m-bit and $(n-m)$-bit permutations of algebraic degree t with optimal TIs. In this secondary construction, the algebraic degree of the n-bit permutation constructed by Corollary 4 is equal to that of the original m-bit and $(n-m)$-bit permutations.*

If both G and H have nonzero nonlinearities, the constructed n-bit permutation via this method can have nonzero nonlinearity. Additionally, in the case where G has zero nonlinearity while H admits optimal TIs and nonzero nonlinearity, it is still possible to derive n-bit permutations with optimal TIs and nonzero nonlinearity, if H' is carefully chosen. Only the permutations with nonzero nonlinearity can be used to construct permutations with optimal TIs and nonzero nonlinearity. However, the choices about H' should be carefully considered to ensure the constructed permutations have nonzero nonlinearity.

Corollary 5. *In Theorem 1, if both the nonlinearities of G and H are nonzero, the nonlinearity of F is nonzero. Additionally, given that G is a permutation with zero nonlinearity, F has nonzero nonlinearity if the nonlinearity of (H', H) is nonzero.*

Proof For the first part, under the conditions of Theorem 1, we prove that the nonlinearity of component functions of F is nonzero. Assume that G and H have nonzero nonlinearities, we know that any component function of G or H has nonzero nonlinearity, which means that all component functions of G or H are nonlinear. Therefore, if the component function

of F consists of the coordinate functions of H, *i.e.,* the nonzero linear combination of the coordinate functions of H, then its nonlinearity is nonzero. Otherwise, the component function of F can be seen as the direct sum of the nonlinear component functions of G and arbitrary Boolean function, which also has nonzero nonlinearity. Thus, the nonlinearity of F is nonzero.

For the second part, we consider the worst case where G is a linear permutation. Assume that G is the identity mapping and H is a permutation with nonzero nonlinearity. Actually, any component function of F is the direct sum of the component function of $(H'(y), H(y))$ and the Boolean function $a \cdot x$ for $a \in \mathbb{F}_2^n$. Note that $a \cdot x$ does not influence whether or not the nonlinearity of F is zero. Thus, whether the nonlinearity of F is nonzero is determined by the nonlinearity of (H', H). □

Example 1. *There exists a* 5*-bit quadratic permutation* $\mathcal{Q}_{25}^5$ *[29]* $F(x_1, x_2, x_3, x_4, x_5) = (x_0x_4 + x_0 + x_1x_4 + x_2x_3, x_0x_4 + x_1, x_2, x_4, x_3)$ *admitting an optimal TI. Corollary 4 can be utilized to derive an optimal TI for this permutation, as* $G(x_0, x_1, x_4) = (x_0x_4 + x_0 + x_1x_4, x_0x_4 + x_1, x_4)$ *is a quadratic permutation* $\mathcal{Q}_2^3$*,* $H(x_2, x_3)$ *is the identity mapping* $\mathcal{A}_0^2$ *and* $H'(x_2, x_3) = (x_2x_3, 0, 0)$ *is a quadratic* $(2, 3)$*-function.*

Example 2. *There exists a* 6*-bit cubic permutation* $F = (x_1x_2+x_1+x_3+x_4x_5x_6, x_2x_3+x_1+x_2, x_1x_3+x_2+x_3, x_4x_5+x_4+x_6, x_5x_6+x_4+x_5, x_4x_6+x_5+x_6)$ *possessing a TI with* 4 *shares. Theorem 1 can be utilized to derive a* 4*-share TI for* F*, given* $n = m = 3$*,* $t_1 = t_2 = 2$ *and* $d = 3$*. Both* $G = (f_1, f_2, f_3)$ *and* $H = (f_4, f_5, f_6)$ *are Gold functions over* $\mathbb{F}_2^3$ *and we simply assume that* $H' = (h'_1, 0, 0) = (x_4x_5x_6, 0, 0)$ *is a cubic function. It can be verified that the nonlinearity of* F *is nonzero. A* 4*-share TI for* F *can be found in Appendix.*

Theorem 1 has a similar structure to the Feistel structure, it can degenerate to the Feistel structure with some constraints. This can be illustrated in the following theorem.

Theorem 2. *Let* F *be an* (n, n)*-function in the form*

$$F(x_1, x_2, \ldots, x_n) = (x_1 + g(x_2, \ldots, x_n), H(x_2, \ldots, x_n)),$$

where H *is a permutation of algebraic degree* $t - 1$ *over* $\mathbb{F}_2^{n-1}$ *and* g *is an* $(n-1)$*-variable Boolean function of algebraic degree* $t \geq 2$*. Then,* F *is a permutation of algebraic degree* t *over* $\mathbb{F}_2^n$ *and there is an optimal TI for* F*.*

Proof In Theorem 1, let $x = x_1$, $y = (x_2, x_3, \ldots, x_n)$, $G(x) = x_1$, $H'(y) = g(x_2, x_3, \ldots, x_n)$ and $H(y) = H(x_2, x_3, \ldots, x_n)$ be a permutation of algebraic degree $t \geq 2$. Then the rest of the proof has the same as the proof of Theorem 1. □

Remark 3. *According to the discussion in Subsection 3.3, the requirement for the existence of a desired TI of the Boolean function* g *is one of the difficulties of Theorem 2 in [29]. In contrast, our construction in Theorem 2 avoids this constraint, which represents a significant advantage. Specifically, our approach achieves uniformity of TIs through two key mechanisms:*

- *the direct sum of a balanced Boolean function and arbitrary Boolean functions,*
- *the universal TI construction for permutations [2].*

By means of the direct sum, our method eliminates the need of TIs for the Boolean function g. This distinguishes Theorem 2 in this manuscript from Theorem 2 in [29]. Consequently, Theorem 2 can be characterized as a primary construction of optimal TIs.

Remark 4. *There is a relaxation of the algebraic degree imposed on the permutation H in Theorem 2, where H still admits $(t+1)$-share TIs when $\deg(H) \leq t-1$. In fact, this condition can be satisfied by the generalization of the universal TI construction in [2]. Therefore, the condition that the permutation H of algebraic degree $t-1$ can be relaxed to the permutation of algebraic degree at most $t-1$.*

Theorem 2 can be seen as a primary construction of optimal TIs since it has no requirement for TIs of the Boolean function g and the permutation H. However, if adding certain constraints on the permutation G, we can obtain a secondary construction of optimal TIs. That is, by modifying the condition $\deg(g) = \deg(H) + 1$ to $\deg(g) \leq \deg(H)$, and assuming that the permutation H admits optimal TIs, we can derive a secondary construction of optimal TIs.

Corollary 6. *Let F be an (n,n)-function in the form*

$$F(x_1, x_2, \ldots, x_n) = (x_1 + g(x_2, \ldots, x_n), H(x_2, \ldots, x_n)),$$

where H is a permutation of algebraic degree $t \geq 2$ over $\mathbb{F}_2^{n-1}$ constructed by Theorem 2 and g is an $(n-1)$-variable Boolean function of algebraic degree at most t. Then, F is a permutation of algebraic degree t over $\mathbb{F}_2^n$ and there is an optimal TI for F.

Proof The proof of this corollary is analogue to that of Theorem 2 and we omit it here. □

Corollary 7. *There always exists a permutation of algebraic degree $2 \leq t \leq n-1$ over $\mathbb{F}_2^n$, which admits optimal TIs. Furthermore, if $t \geq 3$ and $n \geq 4$, this permutation can have nonzero nonlinearity.*

Proof The existence of permutations with optimal TIs relies on the existence of a permutation of algebraic degree $t-1 \leq n-2$ over $\mathbb{F}_2^{n-1}$ and a Boolean function $f_1(x_1, x_2, \ldots, x_n) = x_1 + x_2 x_3 \cdots x_{t+1}$. Let $F = (f_1, f_2, \ldots, f_n)$ be a function over $\mathbb{F}_2^n$, where $G = (f_2, f_3, \ldots, f_n)$ is a permutation of algebraic degree not greater than $t-1$ over $\mathbb{F}_2^{n-1}$ which is independent with x_1. It is obvious that any component function of F, *i.e.,* $\sum_{i=1}^{n} c_i f_i$ where $(c_1, c_2, \ldots, c_n) \in \mathbb{F}_2^n$, is not an affine function when $c_1 \neq 0$. Consequently, whether the nonlinearity of F is nonzero is determined by the nonlinearity of G. Note that there are always m-bit permutations with nonzero nonlinearities for $m \geq 3$. For example, the Gold function when m is odd and the multiplicative inverse function when m is even. Thus, the existence of n-bit permutation with optimal TIs and nonzero nonlinearity is always guaranteed, for $n \geq 4$. □

Example 3. *There exists a* 4*-bit cubic permutation* $\mathcal{C}^4_{301}$ *(notation in [3])* $F(x_1, x_2, x_3, x_4) = (x_1+x_2x_3x_4, x_2x_3+x_2+x_4, x_3x_4+x_2+x_3, x_2x_4+x_3+x_4)$ *admitting an optimal TI. Theorem 2 can be utilized to derive the optimal TI for* F*, given* $n = 4$*,* $g(x_2, x_3, x_4) = x_2x_3x_4$ *and the fact that the quadratic permutation* $H = (f_2, f_3, f_4)$*, which is the Gold function over* $\mathbb{F}_2^3$*, has a TI with* 4 *shares. The nonlinearity of* $\mathcal{C}^4_{301}$ *is* 2*.*

Example 4. *There exists a* 5*-bit cubic permutation* $F(x_1, x_2, x_3, x_4, x_5) = (x_1 + x_2x_3, x_2+x_3x_4x_5, x_3x_4+x_3+x_5, x_4x_5+x_3+x_4, x_3x_5+x_4+x_5)$ *admitting an optimal TI. This permutation admits an optimal TI by Corollary 6, since* $H = (f_2, f_3, f_4, f_5)$ *is a cubic permutation* $\mathcal{C}^4_{301}$ *with an optimal TI and* $\deg(g) = \deg(H)$ *with* $g(x_2, x_3, x_4, x_5) = x_2x_3$*. It has nonlinearity* 4 *and its algebraic degree is* 3*.*

Example 5. *There exists a* 5*-bit quartic permutation* $F(x_1, x_2, x_3, x_4, x_5) = (x_1 + x_2x_3x_4x_5, x_2+x_3x_4x_5, x_3x_4+x_3+x_5, x_4x_5+x_3+x_4, x_3x_5+x_4+x_5)$*. This permutation admits an optimal TI by Theorem 2, since* $H = (f_2, f_3, f_4, f_5)$ *is a cubic permutation* $\mathcal{C}^4_{301}$ *with an optimal TI and* $\deg(g) = \deg(H) + 1$ *with* $g(x_2, x_3, x_4, x_5) = x_2x_3x_4x_5$*. It has nonlinearity* 2 *and its algebraic degree is* 4*.*

6 Applications

In this section, we utilize the theoretical results established in Section 5 to construct bijective S-boxes with optimal TIs.

6.1 Analysis of Bijective S-boxes with Optimal TIs

Our analysis first focuses on the known bijective S-boxes with optimal TIs in four categories: 3-bit S-boxes, 4-bit S-boxes, certain 5-bit quadratic S-boxes, and the new constructed n-bit S-boxes for $n \geq 5$.

The Known 3-bit Bijective S-boxes There are only 4 classes of 3-bit bijective S-boxes with TIs, which are denoted as $\mathcal{A}^3_0$, $\mathcal{Q}^3_1$, $\mathcal{Q}^3_2$, and $\mathcal{Q}^3_3$, see [3]. Only $\mathcal{Q}^3_3$ (the Gold function over $\mathbb{F}_2^3$) has no optimal TIs and nonzero nonlinearity. And the left 3 classes have optimal TIs but have 0 nonlinearity. $\mathcal{A}^3_0$ and $\mathcal{Q}^3_1$ can be constructed from $\mathcal{A}^2_0$ by the constructions in [3].

The Known 4-bit Bijective S-boxes In [3], for all 302 classes of 4-bit bijective S-boxes, there are 10 classes of bijective S-boxes with optimal TIs, which are denoted as $\mathcal{A}^4_0, \mathcal{Q}^4_4, \mathcal{Q}^4_{12}, \mathcal{Q}^4_{293}, \mathcal{Q}^4_{294}, \mathcal{Q}^4_{299}, \mathcal{C}^4_1, \mathcal{C}^4_3, \mathcal{C}^4_{13}$, and $\mathcal{C}^4_{301}$. Our methods can interpret the existence of optimal TIs for those 10 classes of bijective S-boxes, but it is already proved in Table 2 of [29], so we omit it.

The Known 5-bit Quadratic Bijective S-boxes In [4], for the case of 5-bit quadratic bijective S-boxes, there are 30 known classes admitting optimal TIs. We can interpret the existence of optimal TIs for 21 out of 30 classes of quadratic permutations. These are $\mathcal{Q}^5_i$ with $i \in \{1, 2, \ldots, 7\} \cup \{12, 13, \ldots, 25\}$ and $\mathcal{Q}^5_{31}$ by Theorems 1 and 2 and Corollaries 4 and 6. Notably, our approach extends the existing literature by explaining the optimal TI of $\mathcal{Q}^5_{25}$, which is not characterized in [29].

Table 1: Extention of small bits S-boxes to large bits S-boxes

Small-bit S-box	Derived Large-bit S-box	Reference
$\mathcal{A}_0^2$	$\mathcal{A}_0^3, \mathcal{Q}_1^3$	[29]
$\mathcal{A}_0^3$	$\mathcal{A}_0^4, \mathcal{C}_1^4, \mathcal{Q}_4^4$	[29]
$\mathcal{Q}_1^3$	$\mathcal{C}_3^4, \mathcal{Q}_4^4, \mathcal{Q}_{294}^4$	[29]
$\mathcal{A}_0^2$	$\mathcal{Q}_{25}^5$	This paper
$\mathcal{A}_0^4$	$\mathcal{Q}_0^5, \mathcal{Q}_1^5, \mathcal{Q}_{14}^5$	[29]
$\mathcal{Q}_4^4$	$\mathcal{Q}_2^5, \mathcal{Q}_3^5, \mathcal{Q}_{15}^5, \mathcal{Q}_{18}^5$	[29]
$\mathcal{Q}_{12}^4$	$\mathcal{Q}_4^5, \mathcal{Q}_6^5, \mathcal{Q}_{13}^5, \mathcal{Q}_{17}^5, \mathcal{Q}_{20}^5, \mathcal{Q}_{21}^5$	[29]
$\mathcal{Q}_{293}^4$	$\mathcal{Q}_{24}^5, \mathcal{Q}_{31}^5$	[29]
$\mathcal{Q}_{294}^4$	$\mathcal{Q}_5^5, \mathcal{Q}_{12}^5, \mathcal{Q}_{16}^5, \mathcal{Q}_{19}^5, \mathcal{Q}_{23}^5$	[29]
$\mathcal{Q}_{299}^4$	$\mathcal{Q}_7^5, \mathcal{Q}_{22}^5$	[29]
$\mathcal{C}_1^4$	Examples 6 and 7	This paper
$\mathcal{C}_3^4$	Examples 8 and 9	This paper
$\mathcal{C}_{13}^4$	Examples 10 and 11	This paper
$\mathcal{C}_{301}^4$	Examples 4 and 5	This paper

The New Constructed n-bit Bijective S-boxes for $n \geq 5$ The n-bit bijective S-boxes with optimal TIs and nonzero nonlinearity can be easily constructed by Theorems 1 and 2 and Corollaries 4 and 6. For example, Examples 4 to 11 are all 5-bit bijective S-boxes with optimal TIs, while both Examples 4 and 5 have nonzero nonlinearity. The 6-bit bijective S-box with optimal TIs and nonzero nonlinearity is presented in Example 2 and its optimal TI can be found in Section 7.

In Table 1, we present n-bit bijective S-boxes with optimal TIs for $2 \leq n \leq 5$ interpreted by our methods. The new results in this table are marked with "This paper", which means that we can interpret the existence of optimal TIs by our results and cannot be interpreted by previously works.

6.2 Feistel-like Structure S-boxes with Optimal TIs

As we have discussed in Section 3.3, it is feasible to derive optimal TIs for the Feistel structure S-boxes. The ideas of generalizations of Feistel structure S-boxes with optimal TIs in Section 3.3 are realized by Theorems 1 and 2. It can be seen that the constructed permutations in Theorems 1 and 2 can be seen as the Feistel structure S-boxes with inputs and outputs passing through certain bijective S-boxes. As Theorem 1 is a generalization of Theorem 2, we only consider the structure of F in Theorem 1. In Theorem 1, permutation F over $\mathbb{F}_2^{n+m}$ is in the form

$$F(x, y) = (G(x) + H'(y), H(y)), \text{ for } x \in \mathbb{F}_2^n, y \in \mathbb{F}_2^m,$$

where $G(x)$ and $H(y)$ are permutations over $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$, respectively. Furthermore, H' is an (m, m')-function. We can see that F is a the Feistel-like structure, since one part of input can be seen as $G(x)$ instead of $x \in \mathbb{F}_2^n$, and one part of output can be seen as $H(y)$ instead of $y \in \mathbb{F}_2^m$.

7 Conclusion

In this paper, we focused on the constructions of permutations of algebraic degree t, which permit the first-order optimal TIs without the need for any randomness. By proving the existence of optimal TIs for some Boolean functions, we can introduce two new constructions of permutations that achieve optimal TIs. Given two permutations of algebraic degree at most $t-1$ over $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$, respectively, our first approach constructed permutations of algebraic degree t over $\mathbb{F}_2^{n+m}$ with nonzero nonlinearity, which admit optimal TIs. This approach leverages the universal optimal construction for TI established in [2] combined with the property of the direct sum. The second construction represents a specialized case of the first approach. Specifically, it constructed permutations of algebraic degree t over $\mathbb{F}_2^{n+1}$ with optimal TIs, given a permutation of algebraic degree at most $t-1$ over $\mathbb{F}_2^n$. At last, our constructions can interpret the existence of 3-share TIs for certain functions in 3, 4 and 5 variables, as previously illustrated in [3, 4]. This work enhanced the understanding the properties of permutations which admit optimal TIs.

Appendix

The following examples are the bijective S-boxes which admits optimal TIs that can be interpreted by our results.

Example 6. *There exists a 5-bit cubic permutation* $F(x_1,x_2,x_3,x_4,x_5) = (x_1 + x_3x_4x_5, x_2, x_3, x_4, x_5)$ *admitting an optimal TI. The permutation* F *can be constructed from* $\mathcal{A}_0^3$ *and* $\mathcal{A}_0^2$ *with* $(x_3x_4x_5, 0)$ *by Theorem 1. The optimal TI can be found in Appendix.*

Example 7. *There exists a 5-bit quartic permutation* $F(x_1,x_2,x_3,x_4,x_5) = (x_1 + x_2x_3x_4x_5, x_2 + x_3x_4x_5, x_3, x_4, x_5)$ *admitting an optimal TI. This permutation can be constructed from* $\mathcal{C}_1^4 = (f_2, f_3, f_4, f_5)$ *and* $f_1 = x_1 + x_2x_3x_4x_5$ *by Theorem 2. And the optimal TI can be constructed by direct sharing.*

Example 8. *There exists a 5-bit cubic permutation* $F(x_1,x_2,x_3,x_4,x_5) = (x_1 + x_2x_3x_4, x_2 + x_3x_4, x_3, x_4, x_5 + x_1x_2)$ *admitting an optimal TI. The permutation can be derived from* $\mathcal{C}_3^4 = (f_1, f_2, f_3, f_4)$ *and* $f_5 = x_5 + x_1x_2$ *by Corollary 6.*

Example 9. *There exists a 5-bit quartic permutation* $F(x_1,x_2,x_3,x_4,x_5) = (x_1 + x_2x_3x_4, x_2 + x_3x_4, x_3, x_4, x_5 + x_1x_2x_3x_4)$ *admitting an optimal TI. The permutation can be derived from* $\mathcal{C}_3^4 = (f_1, f_2, f_3, f_4)$ *and* $f_5 = x_5 + x_1x_2x_3x_4$ *by Theorem 2.*

Example 10. *There exists a 5-bit cubic permutation* $F(x_1,x_2,x_3,x_4,x_5) = (x_1 + x_3, x_2 + x_3x_4x_5, x_3x_5 + x_4, x_4x_5 + x_3 + x_4, x_5)$ *admitting an optimal TI. The permutation can be derived from* $\mathcal{C}_{13}^4 = (f_2, f_3, f_4, f_5)$ *and* $f_1 = x_1 + x_3$ *by Corollary 6. It can be also constructed from* $\mathcal{Q}_2^3 = (f_3, f_4, f_5)$ *and* $\mathcal{A}_0^2 = (x_1, x_2)$ *with* $H' = (x_3, x_3x_4x_5)$ *by Theorem 1.*

Example 11. *There exists a* 5*-bit quartic permutation* $F(x_1,x_2,x_3,x_4,x_5)=(x_1+x_2x_3x_4x_5, x_2+x_3x_4x_5, x_3x_5+x_4, x_4x_5+x_3+x_4, x_5)$ *admitting an optimal TI. The permutation can be derived from* $\mathcal{C}_{13}^4=(f_2,f_3,f_4,f_5)$ *and* $f_1=x_1+x_2x_3x_4x_5$ *by Theorem 2.*

Example 12. *In this example, to avoid the complexity form such as* $(x^{(i)})^2$*, we use the subscript to denote the shares of input variables,* i.e., $(x_1,x_2,\ldots,x_s)$ *is an* s*-share of* x*, and* x_i *represents the* i*th share of* x*. But the output share of a function* F *is still denoted by* $F^{(i)}$*. We give a* 4*-share TI for* F *over the finite field* $\mathbb{F}_{2^3}\times\mathbb{F}_{2^3}$*. That is,* $F(x,y)=(g(x)+(y+\alpha^5)^7+1, g(y))$*, where* $x,y\in\mathbb{F}_{2^3}$*,* g *is the Gold function over* $\mathbb{F}_{2^3}$ *and* α *is a primitive element of* $\mathbb{F}_{2^3}$ *satisfying* $\alpha^3+\alpha+1=0$*. First, the shares of* $(x,y)\in\mathbb{F}_{2^3}\times\mathbb{F}_{2^3}$ *are* $((x_1,y_1),(x_2,y_2),(x_3,y_3),(x_4,y_4))$*, where* (x_1,x_2,x_3,x_4) *are the* 4*-share of* $x\in\mathbb{F}_{2^3}$ *and* (y_1,y_2,y_3,y_4) *are the* 4*-share of* $y\in\mathbb{F}_{2^3}$*. Then, it can be verified that one* 4*-share TI* $(g^{(1)},g^{(2)},g^{(3)},g^{(4)})$ *for the Gold function* $g(x)$ *over* $\mathbb{F}_{2^3}$ *is*

$$\begin{cases} g^{(1)} = x_2 \\ g^{(2)} = x_4+x_1+(x_3+x_4+x_1)^3 \\ g^{(3)} = x_4+(x_2+x_4+x_1)^3+(x_4+x_1)^3 \\ g^{(4)} = x_1+x_2+x_2^3+x_3^3+(x_2+x_3)^3, \end{cases}$$

Meanwhile, one correct and non-complete 4*-share* $(h^{(1)},h^{(2)},h^{(3)},h^{(4)})$ *for* $h(y)=(y+\alpha^5)^7+1$ *over* $\mathbb{F}_{2^3}$ *is*

$$\begin{aligned}
h^{(1)} &= y_2^7+y_2^6(y_3+y_4)\\
&\quad +y_4^6y_3+y_2^5(y_3+y_4)^2+y_4^5y_3^2+y_2^3(y_3+y_4)^4+y_4^3y_3^4\\
&\quad +y_2^4y_3^2y_4+y_2^4y_4^2y_3+y_3^4y_2^2y_4+y_3^4y_4^2y_2+y_4^4y_2^2y_3+y_4^4y_3^2y_2\\
&\quad +\alpha^2y_2^4+\alpha y_2^2+\alpha^4y_2+\alpha^6(y_2+y_2^2)+\alpha^3(y_2+y_2^4)+\alpha^5(y_2^2+y_2^4)\\
h^{(2)} &= y_3^7+y_3^6(y_1+y_4)\\
&\quad +y_1^6y_4+y_3^5(y_1+y_4)^2+y_1^5y_4^2+y_3^3(y_1+y_4)^4+y_1^3y_4^4\\
&\quad +y_1^4y_3^2y_4+y_1^4y_4^2y_3+y_3^4y_1^2y_4+y_3^4y_4^2y_1+y_4^4y_1^2y_3+y_4^4y_3^2y_1\\
&\quad +\alpha^2y_3^4+\alpha y_3^2+\alpha^4y_3+\alpha^6(y_3+y_3^2)+\alpha^3(y_3+y_3^4)+\alpha^5(y_3^2+y_3^4)\\
h^{(3)} &= y_4^7+y_4^6(y_1+y_2)\\
&\quad +y_2^6y_1+y_4^5(y_1+y_2)^2+y_2^5y_1^2+y_4^3(y_1+y_2)^4+y_2^3y_1^4\\
&\quad +y_1^4y_2^2y_4+y_1^4y_4^2y_2+y_2^4y_1^2y_4+y_2^4y_4^2y_1+y_4^4y_1^2y_2+y_4^4y_2^2y_1\\
&\quad +\alpha^2y_4^4+\alpha y_4^2+\alpha^4y_4+\alpha^6(y_4+y_4^2)+\alpha^3(y_4+y_4^4)+\alpha^5(y_4^2+y_4^4)\\
h^{(4)} &= y_1^7+y_1^6(y_2+y_3)\\
&\quad +y_3^6y_2+y_1^5(y_2+y_3)^2+y_3^5y_2^2+y_1^3(y_2+y_3)^4+y_3^3y_2^4\\
&\quad +y_1^4y_2^2y_3+y_1^4y_3^2y_2+y_2^4y_1^2y_3+y_2^4y_3^2y_1+y_3^4y_1^2y_2+y_3^4y_2^2y_1\\
&\quad +\alpha^2y_1^4+\alpha y_1^2+\alpha^4y_1+\alpha^6(y_1+y_1^2)+\alpha^3(y_1+y_1^4)+\alpha^5(y_1^2+y_1^4),
\end{aligned}$$

with (y_1,y_2,y_3,y_4) *is the input shares of the* 4*-share correct and non-completeness TI for* h*. Therefore, we have a* 4*-share TI for* $F(x,y)=(x^3+(y+\alpha^5)^7+1, y^3)$ *over* $\mathbb{F}_{2^3}\times\mathbb{F}_{2^3}$ *as* $\mathbf{F}=((x_2+h^{(1)},y_2),(x_4+x_1+(x_3+x_4+x_1)^3+h^{(2)},y_4+y_1+(y_3+y_4+y_1)^3),(x_4+(x_2+x_4+x_1)^3+(x_4+x_1)^3+h^{(3)},y_4+(y_2+y_4+y_1)^3+(y_4+y_1)^3),(x_1+x_2+x_2^3+x_3^3+(x_2+$

$x_3)^3 + h^{(4)}, y_1 + y_2 + y_2^3 + y_3^3 + (y_2 + y_3)^3))$, *where* $(x_1, y_1), (x_2, y_2), (x_3, y_3), (x_4, y_4)$ *are the* 4*-share of the input* (x, y) *and* $(F^{(1)}, F^{(2)}, F^{(3)}, F^{(4)})$ *is a* 4*-share TI for* $F(x, y)$.

References

[1] Nikova, S., Rijmen, V., Schläffer, M.: Secure Hardware Implementation of Nonlinear Functions in the Presence of Glitches. J. Cryptol. **24**(2), 292–321 (2011) https://doi.org/10.1007/S00145-010-9085-7

[2] Piccione, E., Andreoli, S., Budaghyan, L., Carlet, C., Dhooghe, S., Nikova, S., Petrides, G., Rijmen, V.: An Optimal Universal Construction for the Threshold Implementation of Bijective S-Boxes. IEEE Trans. Inf. Theory **69**(10), 6700–6710 (2023) https://doi.org/10.1109/TIT.2023.3287534

[3] Bilgin, B., Nikova, S., Nikov, V., Rijmen, V., Stütz, G.: Threshold Implementations of All 3×3 and 4×4 S-Boxes. In: CHES 2012 vol. 7428, pp. 76–91. Springer, Berlin, Heidelberg (2012). https://doi.org/10.1007/978-3-642-33027-8_5

[4] Božilov, D., Bilgin, B., Sahin, H.A.: A Note on 5-bit Quadratic Permutations' Classification. IACR Trans. Symmetric Cryptol. **2017**(1), 398–404 (2017) https://doi.org/10.13154/TOSC.V2017.I1.398-404

[5] Dhem, J.-F., Koeune, F., Leroux, P.-A., Mestré, P., Quisquater, J.-J., Willems, J.-L.: A practical implementation of the timing attack. In: CARDIS'98, Louvain-la-Neuve, Belgium., pp. 167–182 (2000). Springer

[6] Carlet, C., Chérisey, E., Guilley, S., Kavut, S., Tang, D.: Intrinsic resiliency of S-boxes against side-channel attacks–best and worst scenarios. IEEE Transactions on Information Forensics and Security **16**, 203–218 (2020)

[7] Kocher, P.C., Jaffe, J., Jun, B.: Differential Power Analysis. In: Advances in Cryptology - CRYPTO'99, Santa Barbara, California, vol. 1666, pp. 388–397. Springer, Berlin, Heidelberg (1999). https://doi.org/10.1007/3-540-48405-1_25

[8] Chari, S., Jutla, C.S., Rao, J.R., Rohatgi, P.: Towards Sound Approaches to Counteract Power-Analysis Attacks. In: Advances in Cryptology - CRYPTO'99, Santa Barbara, California, vol. 1666, pp. 398–412. Springer, Berlin, Heidelberg (1999). https://doi.org/10.1007/3-540-48405-1_26

[9] Mangard, S., Pramstaller, N., Oswald, E.: Successfully Attacking Masked AES Hardware Implementations. In: International Workshop on CHES, pp. 157–171 (2005). Springer

[10] Nikova, S., Rechberger, C., Rijmen, V.: Threshold Implementations Against Side-Channel Attacks and Glitches. In: ICS vol. 4307, pp. 529–545. Springer, Berlin, Heidelberg (2006). https://doi.org/10.1007/11935308_38

[11] Bilgin, B., Gierlichs, B., Nikova, S., Nikov, V., Rijmen, V.: Higher-Order Threshold Implementations. In: Advances in Cryptology – ASIACRYPT 2014, pp. 326–343. Springer, Berlin, Heidelberg (2014). https://doi.org/10.1007/978-3-662-45608-8_18

[12] Reparaz, O.: A Note on the Security of Higher-Order Threshold Implementations. Cryptology ePrint Archive, Paper 2015/001 (2015)

[13] De Cnudde, T., Reparaz, O., Bilgin, B., Nikova, S., Nikov, V., Rijmen, V.: Masking AES with d+1 Shares in Hardware. In: International Conference on CHES, pp. 194–212 (2016). Springer

[14] Dhooghe, S., Shahmirzadi, A.R., Moradi, A.: Second-Order Low-Randomness d + 1 Hardware Sharing of the AES. In: Proceedings of the ACM CCS '22, pp. 815–828. Association for Computing Machinery, New York, NY, USA (2022). https://doi.org/10.1145/3548606.3560634

[15] Moradi, A., Poschmann, A., Ling, S., Paar, C., Wang, H.: Pushing the Limits: A Very Compact and a Threshold Implementation of AES. In: Advances in Cryptology - EUROCRYPT 2011, vol. 6632, pp. 69–88. Springer

[16] Shahmirzadi, A.R., Božilov, D., Moradi, A.: New First-Order Secure AES Performance Records. IACR Transactions on CHES, 304–327 (2021) https://doi.org/10.46586/tches.v2021.i2.304-327

[17] Sugawara, T.: 3-Share Threshold Implementation of AES S-box without Fresh Randomness. IACR Transactions on CHES, 123–145 (2018) https://doi.org/10.46586/tches.v2019.i1.123-145

[18] Wegener, F., Moradi, A.: A First-Order SCA Resistant AES Without Fresh Randomness. In: COSADE vol. 10815. Cham, pp. 245–262 (2018). https://doi.org/10.1007/978-3-319-89641-0_14

[19] Bilgin, B., Daemen, J., Nikov, V., Nikova, S., Rijmen, V., Van Assche, G.: Efficient and First-Order DPA Resistant Implementations of KECCAK. In: CARDIS 2014, Cham, pp. 187–199 (2014)

[20] Daemen, J.: Changing of the Guards: A Simple and Efficient Method for Achieving Uniformity in Threshold Sharing. In: CHES 2017 vol. 10529. Cham, pp. 137–153 (2017). https://doi.org/10.1007/978-3-319-66787-4_7

[21] Groß, H., Schaffenrath, D., Mangard, S.: Higher-Order Side-Channel Protected Implementations of KECCAK. In: DSD 2017, Vienna, 2017, pp. 205–212. IEEE Computer Society, ??? (2017). https://doi.org/10.1109/DSD.2017.21

[22] Shahmirzadi, A.R., Moradi, A.: Second-Order SCA Security with almost no Fresh Randomness. IACR Transactions on CHES (3), 708–755 (2021) https:

//doi.org/10.46586/tches.v2021.i3.708-755

[23] Baksi, A., Guilley, S., Shrivastwa, R.-R., Takarabt, S.: From Substitution Box to Threshold. In: Progress in Cryptology – INDOCRYPT 2023, pp. 48–67. Springer, Cham (2024)

[24] Poschmann, A., Moradi, A., Khoo, K., Lim, C., Wang, H., Ling, S.: Side-Channel Resistant Crypto for Less than 2, 300 GE. J. Cryptol. **24**(2), 322–345 (2011) https://doi.org/10.1007/S00145-010-9086-6

[25] Petrides, G.: On Non-Completeness in Threshold Implementations. In: Proceedings of ACM Workshop on Theory of Implementation Security Workshop, pp. 24–28. ACM, London United Kingdom (2019). https://doi.org/10.1145/3338467.3358951

[26] Tsukahara, M., Hirata, H., Yang, M., Miyahara, D., Li, Y., Hara-Azumi, Y., Sakiyama, K.: On the Practical Dependency of Fresh Randomness in AES S-box with Second-Order TI. In: 2023 CANDARW, pp. 286–291 (2023). https://doi.org/10.1109/CANDARW60564.2023.00054

[27] Piccione, E.: Threshold Implementations of Cryptographic Functions between Finite Abelian Groups. Cryptology ePrint Archive, Paper 2024/439 (2024)

[28] Boss, E., Grosso, V., Güneysu, T., Leander, G., Moradi, A., Schneider, T.: Strong 8-bit Sboxes with Efficient Masking in Hardware Extended Version. J Cryptogr Eng **7**(2), 149–165 (2017) https://doi.org/10.1007/s13389-017-0156-7

[29] Varici, K., Nikova, S., Nikov, V., Rijmen, V.: Constructions of S-Boxes with Uniform Sharing. Cryptogr. Commun. **11**(3), 385–398 (2019) https://doi.org/10.1007/s12095-018-0345-y

[30] Bilgin, B., Nikova, S., Nikov, V., Rijmen, V., Tokareva, N., Vitkup, V.: Threshold Implementations of Small S-boxes. Cryptogr. Commun. **7**(1), 3–33 (2015) https://doi.org/10.1007/s12095-014-0104-7

[31] Kutzner, S., Nguyen, P.H., Poschmann, A., Wang, H.: On 3-Share Threshold Implementations for 4-Bit S-boxes. In: COSADE. Lecture Notes in Computer Science, pp. 99–113. Springer, Berlin, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40026-1_7

[32] Caforio, A., Collins, D., Glamočanin, O., Banik, S.: Improving First-Order Threshold Implementations of SKINNY. In: Progress in Cryptology - INDOCRYPT 2021 vol. 13143. Cham, pp. 246–267 (2021). https://doi.org/10.1007/978-3-030-92518-5_12

[33] Jati, A., Gupta, N., Chattopadhyay, A., Sanadhya, S.K., Chang, D.: Threshold Implementations of GIFT: A Trade-Off Analysis. IEEE TIFS **15**, 2110–2120 (2019)

[34] Bilgin, B., Gierlichs, B., Nikova, S., Nikov, V., Rijmen, V.: A More Efficient AES Threshold Implementation. In: Progress in Cryptology – AFRICACRYPT 2014 vol. 8469, pp. 267–284. Springer, Cham (2014)

[35] Bilgin, B., Gierlichs, B., Nikova, S., Nikov, V., Rijmen, V.: Trade-Offs for Threshold Implementations Illustrated on AES. IEEE Trans. Com. Aid. Des. **34**(7), 1188–1200 (2015) https://doi.org/10.1109/TCAD.2015.2419623

[36] Ueno, R., Homma, N., Aoki, T.: Toward More Efficient DPA-Resistant AES Hardware Architecture Based on Threshold Implementation. In: COSADE vol. 10348. Cham, pp. 50–64 (2017). https://doi.org/10.1007/978-3-319-64647-3_4

[37] Canright, D.: A Very Compact S-box for AES. In: CHES 2005, pp. 441–455 (2005). Springer

[38] Liu, J., Sun, B., Liu, G., Dong, X., Liu, L., Zhang, H., Li, C.: New Wine Old Bottles: Feistel Structure Revised. IEEE Transactions on Information Theory **69**(3), 2000–2008 (2022)

[39] Carlet, C.: Boolean Functions for Cryptography and Coding Theory. Cambridge University Press, Cambridge (2020). https://doi.org/10.1017/9781108606806

[40] Meier, W., Staffelbach, O.: Fast correlation attacks on stream ciphers. In: Advances in Cryptology–EUROCRYPT 1988, pp. 301–314 (1988). Springer

[41] Ding, C., Xiao, G., Shan, W.: The Stability Theory of Stream Ciphers. Lecture Notes in Computer Science, vol. 561. Springer, ??? (1991). https://doi.org/10.1007/3-540-54973-0