New Constructions of Quadratic and Cubic Permutations Admitting Optimal Threshold Implementations

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

[1]Shanghai Jiao Tong University, School of Computer Science, Dongchuan Road, Shanghai, 200240, China.

*Corresponding author(s). E-mail(s): dengtang@sjtu.edu.cn;
Authors: z.l.li@foxmail.com;

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.* Threshold implementation (TI), introduced by Nikova et al., was proposed to resist differential power analysis side-channel attack on hardware implementations of block ciphers and eliminate information leakage due to glitches. For a function of algebraic degree $\boldsymbol{t \geq 2}$, a TI requires at least $\boldsymbol{t+1}$ shares. However, achieving this bound without fresh randomness is challenging, and we refer to such TIs as optimal. While a universal construction using $\boldsymbol{t+2}$ shares is available, attaining the $\boldsymbol{t+1}$ lower bound depends on the target permutation.

In this paper, we present four constructions for optimal TIs of bijective S-boxes. We first demonstrate how adjoining identity coordinate functions enables optimal TIs, and then prove that $\boldsymbol{\mathcal{Q}_{30}^{5}}$ admits optimal TIs. Second, we derive a matrix criterion for a class of quadratic permutations with optimal TIs, which covers all known examples, and can yield new **6**-bit quadratic classes with optimal TIs. Third, we introduce a weighted interpolation construction, which yields an infinite family of power permutations admitting optimal TIs. Notably, this family includes Bracken-Leander functions. To the best of our knowledge, this represents the first time optimal TIs have been constructed for permutations achieving differentially **4**-uniform. Furthermore, it provides counterexamples to the conjecture in Piccione et al. that nonlinear power permutations cannot meet the $\boldsymbol{t+1}$ lower bound. Finally, we present a derivative-uniform framework. Although this construction is not algebraic-degree-preserving for TIs and comes at a high cost of implementation,

it is of significant theoretical interest and enables us to prove that every **4**-bit cubic permutation admits optimal TIs.

Keywords: Vectorial Boolean functions, S-box, DPA, Sharing, Glitch, Threshold Implementations

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, the physical implementations 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 [3–5]. In 1999, Kocher et al. [5] introduced differential power analysis (DPA) and demonstrated secret-key recovery from a DES implementation. This establishes the need for developing countermeasures for cryptographic hardware devices against DPA.

Sharing, also known as masking [6], is one of the most prominent countermeasures against DPA, which has precise theoretical foundations. It splits the secret input into several shares by adding random values, 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. In hardware devices, however, glitches also lead to a side-channel leakage of sharing, and neglecting their impact can render a masked implementation vulnerable to attack [7–9]. Glitches is unavoidable, or alternatively, the glitch-free hardware comes at a high implementation cost.

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. A TI achieves this goal through three fundamental properties: correctness, non-completeness, and uniformity. Since its introduction, TI and related higher-order masking schemes have been extensively studied as a practical framework for protecting cryptographic algorithms against side-channel attacks, including the widely used algorithms AES [11–15], Keccak [16–18], Present [19, 20], *etc.*

For a target function F (typically a bijective S-box), its TI is actually a vectorial Boolean function $\boldsymbol{F}$. The function $\boldsymbol{F}$ must have three properties to ensure the security of the implementation: correctness, non-completeness and uniformity. The requirement for correctness is obvious, as the sum of the output shares must equal F evaluated at the sum of the input shares. Non-completeness requires each output shares of $\boldsymbol{F}$ to be independent of at least one input share, whereas uniformity implies that a uniformly distributed sharing of x to be mapped to a uniformly distributed sharing of $F(x)$. Given the aforementioned three properties, the function $\boldsymbol{F}$ ensures protection against 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 non-completeness of a TI require a minimum number of input and output shares, denoted as $s_{in} \geq t+1$ and $s_{out} \geq \binom{s_{in}}{t}$, see [10, 21, 22]. The lower bounds inherently suggest that the number of input shares and output shares increases together with the algebraic degree of the target function. Notably, 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. We further restrict our study to TIs of individual S-boxes that require no fresh randomness beyond the randomness used to form the input sharing. The number of shares and the consumption of fresh randomness are two major costs in masked hardware implementations. While adding fresh 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. Hence, the implementations of TIs for permutations discussed in this paper are designed to avoid any fresh randomness. Therefore, minimizing the number of shares is a critical objective for the implementations of TIs. Hence, if a permutation of algebraic degree t admits such a TI with $t+1$ shares, we call it an *optimal TI*, where optimality refers to the number of shares. Determining whether the lower bound $t+1$ can be achieved for some permutations is therefore a central problem.

1.1 The state of the art

1.1.1 General apporaches to construct TIs

At the construction of TIs, a correct and non-complete sharing is straightforward, the main difficulty is satisfying uniformity. Several approaches have been proposed to address this problem. The most significant step is that any bijective function of algebraic degree $t \geq 2$ does have a $(t+2)$-share TI, proposed by Piccione et al. [2]. It solves the universal existence problem with $t+2$ shares, but does not determine which permutations meet the $t+1$ lower bound. Other approaches involve *direct sharing* alongside *correction terms* [10, 23] and *fresh randomness*. The *direct sharing* distributes the monomials of the target function among the output functions to hold correctness and non-completeness, while *correction terms* whose sum is zero may then be added to try to make the shared map uniform. This approach does not provide guarantee of optimal TIs for any arbitrary permutations. Adding *fresh randomness* to re-mask can restore uniformity but introduces additional implementation costs and it is not considered in this paper. Another approach is the *changing of the guards*, introduced by Daemen [17]. This technique constructs a $(t+1)$-share TI of an S-box layer composed of bijective S-boxes of algebraic degree t. Its key idea is that uniformity is achieved through randomness in a layer, that is, the randomness for the $(i+1)$th S-box is the output shares of the ith S-box. Consequently, changing of the guards addresses a different implementation setting from the individual S-box problem studied here.

1.1.2 Known optimal TIs and structural constructions

The existence of optimal TIs has been investigated extensively for small S-boxes [23–26]. Bilgin et al. [23] derived TIs for all bijective 3×3 and 4×4 S-boxes, as well as for the

6×4 DES S-boxes. Subsequently, [27] introduced a more efficient method for finding TIs of all 3-bit and 4-bit permutations and investigated selected 5-bit almost-bent and 6-bit APN permutations. Božilov et al. [24] classified the 75 affine equivalence classes of 5-bit quadratic permutations and examined the existence of optimal TIs. Above classifications identify many instances admitting optimal TIs, but they do not provide an explanation of why optimal TIs are achieved until a construction for TIs [26] was proposed. Indeed, Varici et al. [26] present a secondary construction approach based on Shannon expansion: starting from an n-bit S-box with a known TI, they constructed larger S-boxes, including $(n+2)$-bit and $(n+1)$-bit S-boxes, which hold the number of shares. Such constructions demonstrate how the existence of a TI can be inherited by a larger S-box in a way, and they interpreted the existence of optimal TIs for some quadratic permutations. Additionally, Feistel structure provides a straightforward construction of TIs, and Boss et al. [25] investigated 8-bit S-boxes constructed from smaller Feistel, SPN, and MISTY networks.

1.1.3 Functions of high algebraic degrees

For a high algebraic degree S-box, an alternative strategy is to decompose the target into a composition of lower-degree functions and implement each functions separately. Registers must be inserted between components to prevent glitches from propagating, and therefore lead to a trade-off between a lower per-stage share count for additional register cost, latency, and implementation complexity. In particular, a decomposed implementation does not imply that the original S-box admits a optimal TI in one stage.

For example, Poschmann et al. [20] decomposed Present S-box into two distinct quadratic S-boxes, while Kutzner et al. [28] proposed a decomposition utilizing two same quadratic functions with certain linear functions. Caforio et al. [29] decomposed the SKINNY 8-bit S-box (algebraic degree is 6) into three quadratic functions or two cubic functions. Meanwhile, Jati et al. [30] 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, 13, 15] decomposed it into two cubic permutations, while [11, 12, 31–34] applied TIs to the Canright's tower field decomposition [35]. 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.

These results explain the continuing interest in TIs of low-degree functions, particularly quadratic and cubic permutations, because such functions serve as fundamental building blocks for protected implementations of larger S-boxes. Nevertheless, decomposition-based methods do not resolve the optimal TI problem considered in this paper. To the best of our knowledge, no general necessary and sufficient structural criterion is currently known for determining whether a permutation admits optimal TIs.

1.2 Our contribution

We develop four related approaches to construct permutations with optimal TIs. We first show that adjoining n identity coordinate functions can make the $t+1$ lower

bound attainable, even the original n-bit permutation admits no optimal TIs. We then investigate how the number of additional identity coordinates can be reduced by conditional uniformity, and prove $\mathcal{Q}_{30}^5$ has optimal TIs. Second, we apply the conditional-uniformity framework to quadratic permutations, which covers the constructions in [26]. This approach provides a matrix criterion of the correction terms used in the shared implementation, and gives concrete 5-bit and 6-bit quadratic permutations with optimal TIs. Next, we introduce an interpolation construction based in the order, first correctness and uniformity, then non-completeness. In particular, it provides an infinite family of power permutations admitting optimal TIs, including Bracken-Leander functions [36, 37], which disproves Conjecture 1 of Piccione et al. [2]. Moreover, to the best of our knowledge, it is the first time optimal TIs can be constructed for permutations with 4-differential uniformity. At last, we develop a construction of TIs based on the derivatives. The underlying idea is to use one input share as the derivative direction and combine suitable sharings of the derivatives. In particular, we establish that every 4-bit cubic permutation admits optimal TIs.

Conjecture 1 ([2]). *No power permutation of algebraic degree $t \geq 2$ admits optimal TIs.*

Table 1: The smallest number of shares for known TIs of bijective S-boxes of 3 and 4 bits and bijective quadratic S-boxes of 5 and 6 bits without fresh randomness

Size	Algebraic degree	3-share	4-share	5-share
3	2	2	1	
4	2	5	1	
	3	–	295	0
5	2	42	33	
6	2	476	1787	

1.3 Organization

The remainder of this paper is organized as follows. Section 2 introduces the notation, the relevant properties of Boolean and vectorial Boolean functions, and the Threshold Implementations. Section 3.1 develops identity extensions and conditional uniformity; Section 3.2 studies quadratic permutations with parameter-dependent affine blocks; Section 3.3 introduces weighted interpolation and its applications to power permutations; and Section 3.4 develops the derivative-based constructions, including the result on 4-bit cubic permutations; Section 3.5 compares our construction of optimal TIs and the known $(t+2)$-share TI construction. Section 4 concludes the paper. The appendices provide explicit 3-share TIs of $\mathcal{Q}_{30}^5$ and supplementary proofs.

2 Preliminaries

In this section, we provide an overview of the fundamental concepts related to Boolean functions and Threshold Implementations.

2.1 Boolean functions

Let $\mathbb{F}_2 = \{0, 1\}$ denote the field with two elements and $\mathbb{F}_2^n$ be the vector space of n-tuples over $\mathbb{F}_2$. We refer to a finite field $\mathbb{F}$ with 2^n elements as $\mathbb{F}_{2^n}$. We use $|S|$ to denote the cardinality of a finite set S. The set of $n \times n$ matrices over $\mathbb{F}_2$ and its group of invertible elements are denoted by $\mathrm{Mat}_n(\mathbb{F}_2)$ and $\mathrm{GL}(n, 2)$, respectively. Moreover, we write I for the identity matrix of the appropriate size, and id_V for the identity map on a vector space V. 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 $\mathbb{F}_2$. It is well-known [38] 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 call quadratic functions (resp. cubic functions) the Boolean functions of algebraic degree 2 (resp. 3).

A vectorial Boolean function, or an (n, m)-function, is a map $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$. Writing

$$F = (f_1, f_2, \ldots, f_m),$$

the n-variable Boolean functions $f_1, f_2, \ldots, f_m$ are its coordinate functions. For each nonzero vector $v \in \mathbb{F}_2^m$, the Boolean function

$$v \cdot F = \sum_{i=1}^{n} v_i f_i,$$

is called a component function of F. The algebraic degree of F is by definition the maximal algebraic degree of the component functions of F,

$$\deg(F) = \max_{1 \leq i \leq m} \deg(f_i) = \max_{v \in \mathbb{F}_2^m \setminus \{0\}} \deg(v \cdot F).$$

A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is balanced with $n \geq m$, if $|F^{-1}(y)| = 2^{n-m}$ for every $y \in \mathbb{F}_2^m$. In particular, an (n, m)-function is balanced if and only if it is a permutation. The following provides useful criteria for establishing balancedness.

Lemma 1 ([38]). *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 $F, G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ are affine equivalent if $F = A_1 \circ G \circ A_2$, where A_1 and A_2 are affine permutations of $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$, respectively. Affine equivalence preserves algebraic degree, balancedness, and the existence of Threshold Implementations. It therefore allows these properties to be studied using convenient representatives of affine-equivalence classes.

2.2 Boolean sharings and Threshold Implementations

We work with Threshold Implementations, for brevity TIs, based on Boolean sharing. The relevant algebraic requirements are correctness, non-completeness, and uniformity.

Let $x \in \mathbb{F}_2^n$, and let s be a positive integer, a Boolean s-sharing of x is a tuple

$$\boldsymbol{x} = (x^{(1)}, x^{(2)}, \ldots, x^{(s)}) \in (\mathbb{F}_2^n)^s,$$

such that

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

And the set of all Boolean s-sharings of $x \in \mathbb{F}_2^n$ is

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

with $|\mathrm{Sh}_s(x)| = 2^{n(s-1)}$. Throughout this paper, no fresh randomness means that the shared computation introduces no randomness beyond that used to generate the input sharing. Let s and s' be two positive integers, and let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a target function, consider a shared map

$$\boldsymbol{F} : (\mathbb{F}_2^n)^s \to (\mathbb{F}_2^m)^{s'}, \quad \boldsymbol{F} = (F^{(1)}, F^{(2)}, \ldots, F^{(s')}).$$

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

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

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

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

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

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

A shared map satisfying these three properties is called a TI of F, when $s = s'$, we call it an s-share TI.

The general definition of uniform should be maintained, because some auxiliary functions have different input and output dimensions or are not permutations. It is worth mentioning that, achieving correctness and non-completeness is relatively straightforward by means of direct sharing, as demonstrated in [23]. 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 2 ([2]). *let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$. let s be a positive integer and $\boldsymbol{F} : (\mathbb{F}_2^n)^s \to (\mathbb{F}_2^n)^s$ be a function that is correct with respect to F. then $\boldsymbol{F}$ is a permutation if and only if $\boldsymbol{F}$ is uniform and F is a permutation.*

Then, the proof of uniformity for TIs is based on a triangular inversion form in [2],

$$\begin{cases} y_1 = f_1(x_1), \\ y_j = f_j(x_j) + h_j(x_1, x_2, \ldots, x_{j-1}), \quad 2 \le j \le n, \end{cases}$$

where all f_i is invertible. Its inverse can be obtained successively,

$$x_1 \leftarrow y_1,\ x_2 \leftarrow y_2 + h_2(x_1),\ x_3 \leftarrow y_3 + h_3(x_1, x_2), \ldots, x_n \leftarrow y_n + h_n(x_1, x_2, \ldots, x_{n-1}),$$

hence is uniform. Therefore, Piccione et al. [2] introduce a universal $(t+2)$-share TI construction of any arbitrary bijective S-boxes of algebraic degree at most t. And later, Piccione extends it to functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, see [39, Theorem 1].

Theorem 1 ([39]). *Any function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ with $n \ge m$ of algebraic degree $t \ge 1$ has $(t+2)$-share TIs.*

3 Main result

This section develops four approaches to constructing optimal TIs. In Section 3.1, we first investigate identity extensions of the $\mathrm{id}_n \times F$, focusing on n for the extended permutation admitting optimal TIs. As an application, we prove $\mathcal{Q}_{30}^5$ has optimal TIs. We next present a general construction that covers the Shannon-expansion constructions [26] as special cases, in Section 3.2. This construction provides a common explanation for the existence of optimal TIs for the 30 five-bit quadratic classes previously reported and additionally yields an optimal TI for $\mathcal{Q}_{45}^5$. We also identify 475 six-bit quadratic permutations admitting optimal TIs. In Section 3.3, we introduce a weighted interpolation construction and apply it to obtain power permutations with optimal TIs, thereby providing counterexamples to Conjecture 1 in [2]. In Section 3.4, we develop a derivative-uniform framework for constructing optimal TIs of permutations, and use it to prove that every 4-bit cubic permutation admits optimal TIs. Finally, we compare the cost of implementations of TIs for certain quadratic and cubic permutations, including the PRESENT S-box and inversion in $\mathbb{F}_{2^4}$, in $(t+2)$-share TIs and optimal TIs.

3.1 Identity extensions and U-uniform

Varici et al. [26] construct optimal TIs of larger quadratic S-boxes based on the existence of optimal TIs for quadratic S-boxes. However, those S-boxes admitting no optimal TIs can also be used to construct new S-boxes with optimal TIs. For example, $\mathcal{Q}_{30}^5$, which is affine equivalent to $\mathrm{id}_2 \times \mathcal{Q}_3^3$, has an optimal TI, see Section A, but the Gold function $\mathcal{Q}_3^3$ has no optimal TIs by exhausted search [23]. That is,

$$\mathcal{Q}_3^3 \to \mathcal{Q}_{300}^4 \to \mathcal{Q}_{30}^5 \not\to \mathcal{Q}_3^3 \to \mathcal{Q}_{30}^5.$$

We first show that adjoining n identity coordinates is sufficient for any permutation of $\mathbb{F}_2^n$. We then introduce U-uniformity, which requires uniformity after fixing the sharing of a parameter block, and use this property to obtain more refined bounds on the number of additional coordinates. Finally, we derive the optimal TIs for $\mathcal{Q}_{30}^5$.

Before proving the optimal TIs for such $2n$-variable permutations, we first introduce a construction about the correct and non-complete sharing of any permutation G, and uniformity is not required at this construction.

Construction 1. *Let $t \geq 2$, and let $G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a function of algebraic degree at most t. Define*

$$\begin{cases} G^{(1)}(\boldsymbol{y}) = G\left(\sum_{j=2}^{s} y^{(j)}\right) + G\left(\sum_{j=3}^{s} y^{(j)}\right), \\ G^{(2)}(\boldsymbol{y}) = G\left(y^{(1)} + \sum_{j=3}^{s} y^{(j)}\right), \\ G^{(i)}(\boldsymbol{y}) = \sum_{I \subseteq \{1,\ldots,i-1\}} G\left(\sum_{j=i+1}^{s} y^{(j)} + \sum_{j \in I} y^{(j)}\right), \quad 3 \leq i \leq s, \end{cases}$$

where $\boldsymbol{y} = (y^{(1)}, y^{(2)}, \ldots, y^{(s)})$ and $s = t + 1$, then $\boldsymbol{G} = (G^{(1)}, G^{(2)}, \ldots, G^{(s)})$ is a correct and non-complete s-sharing of G.

Proof The non-completeness of Construction 1 is clear. And its correctness follows from

$$G\left(\sum_{i=1}^{s} y^{(i)}\right) + \sum_{i=1}^{s} G^{(i)}(\boldsymbol{y}) = \Delta_{y^{(1)}, y^{(2)}, \ldots, y^{(s)}} G(0) = 0,$$

as s-th order derivatives of G always vanishes, or see [2, Lemma 3]. □

The first output sharing has a useful property: once $\sum_{j=3}^{s} y^{(j)}$ is known, it determines $y^{(2)}$ whenever G is a permutation. The following construction uses this sharing and identity coordinates to recover the remaining shares.

Theorem 2. *Let $G : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a permutation of algebraic degree $t \geq 2$ with $n \geq 3$. Then $F(x, y) = (x, G(y))$ has optimal TIs, where $x, y \in \mathbb{F}_2^n$.*

Proof The permutation of F is clear, so we only prove it has optimal ITs, i.e., $(t+1)$-share TIs with $t = \deg(G)$. Let input shares be $\left(x^{(i)}, y^{(i)}\right) \in \mathbb{F}_2^{2n}$ with $i = 1, 2, \ldots, s$ and $s = t + 1$ with $\boldsymbol{x} = (x^{(1)}, \ldots, x^{(s)})$ and $\boldsymbol{y} = (y^{(1)}, \ldots, y^{(s)})$.

Then define the output share $\boldsymbol{F}(\boldsymbol{x},\boldsymbol{y}) = (\boldsymbol{X},\boldsymbol{Y})$ as follows,

$$\begin{cases} X^{(1)} = x^{(s)} + \sum_{j=3}^{s} y^{(j)}, \\ X^{(i)} = y^{(i+1)}, \quad 2 \le i \le s-1, \\ X^{(s)} = \sum_{j=1}^{s-1} x^{(j)}, \\ Y^{(1)} = G^{(1)}(\boldsymbol{y}), \\ Y^{(i)} = G^{(i)}(\boldsymbol{y}) + x^{(i-1)}, \quad 2 \le i \le s-1, \\ Y^{(s)} = G^{(s)}(\boldsymbol{y}) + \sum_{j=1}^{s-2} x^{(j)}, \end{cases} \tag{1}$$

where $\boldsymbol{G} = (G^{(1)}, G^{(2)}, \ldots, G^{(s)})$ is a sharing from Construction 1. Then, the correctness and non-completeness of $\boldsymbol{F}$ can be easily verified. To prove uniform, by Lemma 2, we need to prove that the output sharing is bijective. Given the output shares, the unshared input (x, y) can be determined by the correctness,

$$\begin{cases} x = \sum_{i=1}^{s} X^{(i)}, \\ y = G^{-1}\left(\sum_{i=1}^{s} Y^{(i)}\right), \\ y^{(i)} = X^{(i-1)}, \quad 3 \le i \le s, \end{cases}$$

and we also get

$$\sum_{j=3}^{s} y^{(j)} = \sum_{i=2}^{s-1} X^{(i)}.$$

Denote $r = \sum_{j=3}^{s} y^{(j)}$, by Construction 1,

$$Y^{(1)} = G\left(y^{(2)} + r\right) + G(r),$$

$y^{(2)}$ can be determined as follows due to the permutation of G,

$$y^{(2)} = r + G^{-1}\left(Y^{(1)} + G(r)\right).$$

We then have

$$y^{(1)} = y + y^{(2)} + r,$$

which means that $\boldsymbol{y}$ is fully determined. Once we get $\boldsymbol{y}$, since $Y^{(i)} = G^{(i)}(\boldsymbol{y}) + x^{(i-1)}$, we obtain

$$x^{(i)} = Y^{(i+1)} + G^{(i+1)}(\boldsymbol{y}), \quad 1 \le i \le s-2.$$

Finally, we can recover $x^{(s)}$ by

$$x^{(s)} = X^{(1)} + \sum_{i=2}^{s-1} X^{(i)},$$

and then $x^{(s-1)} = x + x^{(s)} + \sum_{i=1}^{s-2} x^{(i)}$. Consequently, every input share is uniquely determined by the output shares. Therefore $\boldsymbol{F}$ is bijective and hence is uniform. □

It can be seen that Equation (1) is a triangular inversion form, after certain linear transformations, as G is a permutation,

$$\begin{cases} X^{(i)} = y^{(i+1)}, \quad 2 \le i \le s-1, \\ Y^{(1)} = G^{(1)}(\boldsymbol{y}) = G\left(y^{(2)} + r\right) + G(r), \quad \text{with } r = \sum_{i=2}^{s-1} y^{(i+1)}, \\ \sum_{i=1}^{s} Y^{(i)} = G\left(y^{(1)} + y^{(2)} + r\right), \\ Y^{(i)} = x^{(i-1)} + G^{(i)}(\boldsymbol{y}), \quad 2 \le i \le s-1, \\ X^{(1)} = x^{(s)} + \sum_{j=3}^{s} y^{(j)}, \\ \sum_{i=1}^{s} X^{(i)} = x^{(s-1)} + \sum_{j=1}^{s-2} x^{(j)} + x^{(s)}. \end{cases}$$

Clearly, the first n identity coordinates in $2n$-variable permutations $\mathrm{id}_n \times F$ contribute additional freedom to achieve uniform. It costs half of variables, and this naturally raises the question whether the identity variables for some special permutations can be reduced. To measure the number of additional identity coordinates required, define

$$r_s(F) = \min\left\{m \ge 0 : \mathrm{id}_{\mathbb{F}_2^m} \times F \text{ has } s\text{-share TIs}\right\},$$

and we only consider the case of $s = \deg(F) + 1$, as $s \ge \deg(F) + 2$ always leads to $r_s(F) = 0$ by the universal optimal TI construction [2]. To reduce the number of identities, we next consider situations, where part of a sharing can be recovered independently of the remaining input blocks.

Definition 1. *Let $G : U \times \mathbb{F}_2^n \to \mathbb{F}_2^m$ with $n \ge m$, and let $\boldsymbol{G}$ be a correct s-sharing of G. We call $\boldsymbol{G}$ is U-uniform if, for every $\boldsymbol{u} \in U^s$, every $x \in \mathbb{F}_2^n$ and every $\boldsymbol{y} \in \mathrm{Sh}_s(G(u, x))$, one has*

$$|\{\boldsymbol{x} \in \mathrm{Sh}_s(x) : \boldsymbol{G}(\boldsymbol{u}, \boldsymbol{x}) = \boldsymbol{y}\}| = 2^{(n-m)(s-1)}.$$

Thus U-uniformity fixes the sharing $\boldsymbol{u}$, rather than only the unshared u. It is stronger than uniform, as it implies uniformity by summing the above equality over $\boldsymbol{u} \in \mathrm{Sh}_s(u)$ gives the required preimage count for a uniform sharing of G.

Consider the case $G : U \oplus W \to W$. The U-uniformity means that for every fixed $\boldsymbol{u}$ and w, the restriction

$$\mathrm{Sh}_s(w) \to \mathrm{Sh}_s(G(u, w))$$

is bijective. If $G_u : w \mapsto G(u, w)$ is a permutation for every u, then

$$\boldsymbol{w} \mapsto \boldsymbol{G}(\boldsymbol{u}, \boldsymbol{w})$$

is a permutation of W^s for every fixed $\boldsymbol{u}$. Therefore, we have a simple example by direct sum.

Example 1. *Let $G : W \to W$ be a permutation admitting s-share TIs, and let $H : U \to W$ be a function of algebraic degree at most $s-1$. Choose a correct and non-complete s-sharing $\boldsymbol{H}$, and define*

$$F^{(i)}(\boldsymbol{u}, \boldsymbol{w}) = G^{(i)}(\boldsymbol{w}) + H^{(i)}(\boldsymbol{u}),$$

and the map $\boldsymbol{G}$ is U-uniform.

Theorem 3. *Let $t \geq 2$ and $s = t+1$, and let $W = W_1 \oplus W_2 \oplus \cdots \oplus W_r$. Let $G_j : U \oplus W_j \to W_j$ be a function of $\deg(G_j) \leq t$ with $w_j \mapsto G_j(u, w_j)$ being a permutation for every fixed $u \in U$. Suppose that each G_j has a correct, non-complete and U-uniform s-sharing. For $1 \leq j \leq r$, let $H_j : U \oplus W_1 \oplus W_2 \cdots \oplus W_{j-1} \to W_j$ have algebraic degree at most t, and $H_1 : U \to W_1$. If $G : U \to U$ of $\deg(G) \leq t$ is a permutation admitting s-share TIs, then*

$$\begin{aligned}(u, w_1, w_2, \ldots, w_r) \mapsto (&G(u),\\ &G_1(u, w_1) + H_1(u),\\ &G_2(u, w_2) + H_2(u, w_1),\\ &G_3(u, w_3) + H_3(u, w_1, w_2),\\ &\cdots\\ &G_r(u, w_r) + H_r(u, w_1, w_2, \ldots, w_{r-1})),\end{aligned}$$

has optimal TIs.

Proof We give a proof for $F(u, w) = (G(u), G_1(u, w) + H_1(u))$ and the generalized case can be proved analogue. Its i-th output sharings can be written as follows,

$$F^{(i)} = \left(G^{(i)}(\boldsymbol{u}), G_1^{(i)}(\boldsymbol{u}, \boldsymbol{w}) + H_1^{(i)}(\boldsymbol{u})\right), \quad 1 \leq i \leq s,$$

it is a triangle inverse form. Thus, its uniform can be proved by successively solving equations

$$\boldsymbol{u} \leftarrow \boldsymbol{G}(\boldsymbol{u}), \quad \boldsymbol{w} \leftarrow \boldsymbol{G}_1(\boldsymbol{u}, \boldsymbol{w}) + \boldsymbol{H}_1(\boldsymbol{u}),$$

since $\boldsymbol{G}_1$ is a U-uniform sharing, i.e., $\boldsymbol{G}_1$ is a permutation of W^s for every fixed $\boldsymbol{u} \in U^s$. □

The following example provides a useful U-uniform sharing for quadratic maps.

Example 2. *For the $(n+1, n)$-function $G(x, y) = L_x y$ of $\deg(G) = 2$, where $x \in \mathbb{F}_2$, $y \in \mathbb{F}_2^n$ and $L_0, L_1 \in \mathrm{GL}(n, 2)$. For a three-sharing $\boldsymbol{x} = (x^{(1)}, x^{(2)}, x^{(3)})$, define $\boldsymbol{G}$ as follows,*

$$\boldsymbol{G} = \begin{pmatrix} 0 & L_{x^{(3)}} & L_{x^{(2)}} + L_{x^{(3)}} \\ L_{x^{(1)}} + L_{x^{(3)}} & 0 & L_{x^{(1)}} \\ L_{x^{(2)}} & L_{x^{(1)}} + L_{x^{(2)}} & 0 \end{pmatrix} \boldsymbol{y},$$

it is then invertible for any fixed $\boldsymbol{x} \in \mathbb{F}_2^3$*, as the determinant of the matrix is* $\det(L_{x^{(1)}} L_{x^{(2)}} L_{x^{(3)}}) = 1$*. Thus,* $\boldsymbol{G}$ *is a correct, non-complete and* $\mathbb{F}_2$*-uniform 3-sharing of* G*. In particular, assigning* $L_0 = I$ *and* $L_1 = I + L$ *gives a 3-sharing of* $G(x, y) = (I + xL)y$*, whenever* $I + L$ *is invertible.*

We now apply U-uniformity to identity extensions. Define $r_s(K \mid U)$ for the function $K : U \oplus W \to W$ in below,

$$r_s(K \mid U) = \min\{l \geq 0 : \mathrm{id}_{\mathbb{F}_2^l} \times K \text{ has correct, non-complete and } U\text{-uniform } s\text{-sharings}\}.$$

If $\deg(K) \leq s$ and $s \geq 3$, then $r_s(K \mid U) \leq \dim W$. To get this, we can apply Theorem 2 to K with the fixed u.

Theorem 4. *Let* $F(u, w) = (G(u), K(u, w))$ *be a permutation of* $U \oplus W$ *satisfying* $\deg(F) < s$ *with* $s \geq 3$*. If the sharings from* $r_s(G)$ *and* $r_s(K \mid U)$ *can be chosen with compatible omitted-share indices. Then,* $r_s(F) \leq r_s(G) + r_s(K \mid U)$*.*

Proof Choose A, B to be vector spaces of dimensions $\dim A = r_s(G)$ and $\dim B = r_s(K \mid U)$. We can construct an s-share TI $\boldsymbol{T_G}$ on $(A \oplus U)^s$ of the permutation $(a, u) \mapsto (a, G(u))$, and a correct, non-complete and U-uniform s-sharing $\boldsymbol{S_K}$ from $(B \oplus U \oplus W)^s$ to $(B \oplus W)^s$ of the function $(b, u, w) \mapsto (b, K(u, w))$. Therefore, define $F' = (a, b, F(x)) = (a, b, F(u, w))$, and define its output share by above two sharings,

$$\boldsymbol{F'}(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{u}, \boldsymbol{w}) = (\boldsymbol{T_G}(\boldsymbol{a}, \boldsymbol{u}), \boldsymbol{S_K}(\boldsymbol{b}, \boldsymbol{u}, \boldsymbol{w}))\,.$$

The correctness and non-completeness follow immediate. It remains to prove uniformity, i.e., the bijectivity. From the first output block, invert $\boldsymbol{T_G}$ and recover $\boldsymbol{a}$ and $\boldsymbol{u}$. Now $\boldsymbol{u}$ is fixed, we can recover $\boldsymbol{b}$ and $\boldsymbol{w}$ from the second output block. Thus all input shares are recovered uniquely, hence $\boldsymbol{F'}$ is uniform. This implies that $(a, b, F(x))$ has optimal TIs, i.e., $r_s(F) \leq \dim A + \dim B = r_s(G) + r_s(K \mid U)$. □

In particular, the first block $r_s(G)$ will be zero, when $\deg(G) \leq t - 1$, by the universal optimal TI constructions, or when $\deg(G) = t$ and an optimal TI is available. Thus, the number of additional identities is determined by the W-part instead of F.

Corollary 1. *Let* F *be a permutation of* $\mathbb{F}_2^n$ *with* $t = \deg(F) \geq 2$*. If* F *is affine equivalent to* $F(u, w) = (G(u), K(u, w))$ *with* $\dim U = r$ *and* G *admitting* $(t+1)$*-share TIs, then* $r_s(F) \leq n - r$*.*

Proof Consider the permutation $F(u, w) = (G(u), K(u, w))$ on $U \oplus W$, we have $r_s(G) = 0$ if and only if G already has s-share TIs, with $s \geq t + 1$. Thus, we get $r_s(F) \leq r_s(K \mid U) \leq n - r$. □

Theorem 4 requires the first output block to depend only on u. We next remove this constraint. That is, for the permutation $G = (G_U, G_W) : U \oplus W \to U \oplus W$ of $\deg(G) = t$, if $G_W : U \oplus W \to W$ has correct, non-complete and U-uniform $(t + 1)$-sharings, the permutation $\mathrm{id}_{U^2} \times G$ admitting optimal TIs.

Theorem 5. *Let $\mathbb{F}_2^n = U \oplus W$, and let $G = (G_U, G_W) : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a permutation of $t \geq 2$. Assume that $G_W : \mathbb{F}_2^n \to W$ admits a correct, non-complete and U-uniform $(t+1)$-sharing. Then*

$$F(x, y, u, w) = (x, y, G(u, w)), \quad x, y, u \in U,\ w \in W,$$

has optimal TIs, or equivalently,

$$r_s(G) \leq 2 \dim U.$$

Proof Let the input sharings be $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{u}, \boldsymbol{w})$. Then define the i-th output share $\left(X^{(i)}, Y^{(i)}, Z_U^{(i)}, Z_W^{(i)}\right)$ by

$$\begin{cases} \boldsymbol{X} = \Pi(\boldsymbol{x}) + P(\boldsymbol{y}) + P(\boldsymbol{u}), \\ \boldsymbol{Y} = P(\boldsymbol{x}) + \Pi(\boldsymbol{y}), \\ \boldsymbol{Z}_U = \boldsymbol{G}_U(\boldsymbol{u}, \boldsymbol{w}) + P(\boldsymbol{y}), \\ \boldsymbol{Z}_W = \boldsymbol{G}_W(\boldsymbol{u}, \boldsymbol{w}), \end{cases}$$

where $\Sigma_V : V^s \to V$ by $\Sigma_V(\boldsymbol{v}) = \sum_i v^{(i)}$, and

(1) $\Pi = (1\ 2\ \cdots\ s)$ for the standard basis $\{e_1, e_2, \ldots, e_s\}$ of $\mathbb{F}_2^s$,

(2) $P = \mu + e_1 \Sigma_U$, where $\mu = (2\ 3\ \cdots\ s)$ and $e_1 v = (v, 0, 0, \ldots, 0)$.

The correctness can be derived from $\Sigma_U \Pi = \Sigma_U$ and $\Sigma_U P = 0$, while the non-completeness follows from $\mathrm{diag}(\Pi) = \mathrm{diag}(P) = 0$ for all $1 \leq i \leq s$ due to $s \geq 3$.

Before proving the uniformity, we deduce the involution of $T = \Pi^{-1} P$ on $\mathrm{Sh}_s(0)$. That is, $e_1 + e_j$, for $2 \leq j \leq s$, are a basis of $\mathrm{Sh}_s(0)$, and we have

$$T(e_1 + e_j) = \Pi^{-1} P(e_1 + e_j) = \Pi^{-1}(e_1 + e_{\mu(j)}) = e_s + e_j, \quad 2 \leq j \leq s-1,$$

is an involution of $\mathrm{Sh}_s(0)$, which means $T^2 = I$ on $\mathrm{Sh}_s(0)$.

It remains to prove the uniformity, which is equivalent to the injective as the input and output have the same cardinality. Consider the input sharing of (x, y, u, w), and suppose that two input sharings give the same output sharing. Assume the difference of two input sharings be $(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma}, \boldsymbol{\omega})$, this implies $\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma}, \boldsymbol{\omega} \in \mathrm{Sh}_s(0)$, and we then have

$$\begin{cases} \Pi\boldsymbol{\alpha} + P\boldsymbol{\beta} + P\boldsymbol{\gamma} = 0, \\ P\boldsymbol{\alpha} + \Pi\boldsymbol{\beta} = 0, \end{cases} \Rightarrow \begin{cases} \boldsymbol{\alpha} + T\boldsymbol{\beta} + T\boldsymbol{\gamma} = 0, \\ T\boldsymbol{\alpha} + \boldsymbol{\beta} = 0, \end{cases} \Rightarrow \begin{cases} T\boldsymbol{\alpha} + T^2\boldsymbol{\beta} + T^2\boldsymbol{\gamma} = 0, \\ T\boldsymbol{\alpha} = \boldsymbol{\beta}, \end{cases} \Rightarrow \boldsymbol{\gamma} = 0.$$

Therefore, the two input sharings for u are identical. According to the U-uniformity of $\boldsymbol{G}_W$ of Definition 1, we then have $\boldsymbol{\omega} = 0$, thus, the two input sharings for w is identical. Consequently, $\boldsymbol{G}_U(\boldsymbol{u}, \boldsymbol{w})$ are identical for two input sharings, so $P\beta = 0$. Since P is invertible on $\mathrm{Sh}_s(0)$, we have $\boldsymbol{\beta} = 0$, and then $\boldsymbol{\alpha} = 0$. Therefore the shared map is injective, so it is bijective, and then it is uniform. □

Corollary 2. *$\mathcal{Q}_{30}^5$ has optimal TIs.*

Proof Let $\mathbb{F}_{2^3} = \mathbb{F}_2(\alpha)$ with $\alpha^3 + \alpha + 1 = 0$, and let $\omega \in \mathbb{F}_4$ satisfy $\omega^2 + \omega + 1 = 0$. Define the linear isomorphism

$$\phi : \mathbb{F}_8 \to \mathbb{F}_2 \oplus \mathbb{F}_4, \quad \phi(a + b\alpha + c\alpha^2) = (a, b + c\omega).$$

Writing $z = b + c\omega$, we have $z^3 = b + c + bc$ and $\omega^a z = (b + ab + ac) + (c + ab)\omega$. Consequently, $\phi\left((a + b\alpha + c\alpha^2)^3\right) = (a + b + c + bc, (b + ab + ac) + (c + ab)\omega) = (a + z^3, \omega^a z)$. Thus, x^3 is linearly equivalent to $G(a, z) = (a + z^3, \omega^a z)$. By Example 2, $\omega^a z$ admits correct, non-complete and U-uniform 3-sharings, so we have

$$(x, y, a, z) \mapsto (x, y, a + z^3, \omega^a z), \quad x, y, a \in \mathbb{F}_2,$$

has optimal TIs, that is, $\mathrm{id}_2 \times \mathcal{Q}_3^3 \cong \mathcal{Q}_{30}^5$ has optimal TIs. □

3.2 Quadratic permutations with optimal Threshold Implementations

We now apply U-uniform to construct quadratic permutations with optimal TIs. The constructions considered in this section have the form $F(x, y) = ((I + A(y))x + H(y), G(y))$, where $x \in \mathbb{F}_2^n$, $y \in \mathbb{F}_2^m$, and $A(y)$ is a linear operator on $\mathbb{F}_2^n$, where the form is motivated by Example 2. We first establish a matrix criterion for this conditional invertibility and then give two explicit families satisfying it. Finally, we describe affine reductions that simplify the classification of the resulting permutations.

Let $G : \mathbb{F}_2^m \to \mathbb{F}_2^m$ be a permutation admitting 3-share TIs. For a fixed sharing of y, the construction of optimal TIs for

$$F(x, y) = ((I + A(y))x + H(y), G(y)),$$

reduces to constructing a conditionally uniform sharing of the first component. The following proposition expresses this requirement as the determination of a $2n \times 2n$ block matrix.

Proposition 6. *Let n, m be two positive integers. Let $F(x, y) = ((A(y) + I)x + H(y), G(y))$ on $\mathbb{F}_2^n \times \mathbb{F}_2^m$ be a quadratic function with $x \in \mathbb{F}_2^n$ and $y \in \mathbb{F}_2^m$. If*

(1) $A : \mathbb{F}_2^m \to \mathrm{Mat}_n(\mathbb{F}_2)$ is affine, and $A(y) + I \in \mathrm{GL}(n, 2)$ for every $y \in \mathbb{F}_2^m$,
(2) $H : \mathbb{F}_2^m \to \mathbb{F}_2^n$ be a function of $\deg(H) \leq 2$,
(3) G be a permutation of $\mathbb{F}_2^m$ with $\deg(G) \leq 2$ admitting 3-share TIs,
(4) and there exist affine maps $R, P, Q : \mathbb{F}_2^m \to \mathrm{Mat}_n(\mathbb{F}_2)$ such that, for every $(y^{(1)}, y^{(2)}, y^{(3)}) \in \mathbb{F}_2^{3m}$, the matrix

$$\begin{pmatrix} I + A_2 + A_3 + P_2 & A_2 + Q_3 \\ A_3 + R_1 & I + A_1 + R_1 + Q_3 \end{pmatrix},$$

is invertible, where $A_i = A(y^{(i)}), R_1 = R(y^{(1)}), P_2 = P(y^{(2)})$ and $Q_3 = Q(y^{(3)})$.

then F has optimal TIs.

Proof The permutation of F is easy to derive. Given $f(x, y) = (u, v)$, we can recover $y = G^{-1}(v)$ and then $x = (A(y) + I)^{-1}(u + H(y))$ is uniquely determined as $A(y) + I \in \mathrm{GL}(n, 2)$.

Assume that 3-share sharing of x is $\boldsymbol{x} = (x^{(1)}, x^{(2)}, x^{(3)})$, and 3-share sharing of y is $\boldsymbol{y} = (y^{(1)}, y^{(2)}, y^{(3)})$. Let $\boldsymbol{F} = \left(F^{(1)}, F^{(2)}, F^{(3)}\right)$ be a 3-share of F with $F^{(i)} = (Z^{(i)}, G^{(i)})$, where $(G^{(1)}, G^{(2)}, G^{(3)})$ is a 3-share TI of G, and

$$\begin{cases} Z^{(1)} = (I + A_2 + A_3 + P_2)x^{(2)} + (A_2 + Q_3)x^{(3)} + H^{(1)}(\boldsymbol{y}), \\ Z^{(2)} = (A_3 + R_1)x^{(1)} + (I + A_1 + A_3 + Q_3)x^{(3)} + H^{(2)}(\boldsymbol{y}), \\ Z^{(3)} = (I + A_1 + A_2 + R_1)x^{(1)} + (A_1 + P_2)x^{(2)} + H^{(3)}(\boldsymbol{y}), \end{cases} \tag{2}$$

where $(H^{(1)}, H^{(2)}, H^{(3)})$ is a correct and non-complete 3-sharing, R_1, P_2, Q_3 are correction terms. The correctness and non-completeness of $\boldsymbol{F}$ can be easily checked, we only verify its uniformity. Since G is a permutation and $\boldsymbol{G}$ is uniform, $\boldsymbol{G}$ is bijective and then $\boldsymbol{y}$ can be uniquely determined. Therefore, all the operators, and all $H^{(i)}(\boldsymbol{y})$ are known. It remains to prove the coefficient matrix in the below form is invertible,

$$\begin{pmatrix} Z^{(1)} \\ Z^{(2)} \\ Z^{(3)} \end{pmatrix} = \begin{pmatrix} 0 & I + A_2 + A_3 + P_2 & A_2 + Q_3 \\ A_3 + R_1 & 0 & I + A_1 + A_3 + Q_3 \\ I + A_1 + A_2 + R_1 & A_1 + P_2 & 0 \end{pmatrix} \begin{pmatrix} x^{(1)} \\ x^{(2)} \\ x^{(3)} \end{pmatrix} + c,$$

i.e.,

$$\det(I + A_1 + A_2 + A_3) \det \begin{pmatrix} I + A_2 + A_3 + P_2 & A_2 + Q_3 \\ A_3 + R_1 & I + A_1 + R_1 + Q_3 \end{pmatrix} \neq 0.$$

Thus, M uniquely determines $\boldsymbol{x}$, and therefore every input share is uniquely determined by the output shares. The shared map is bijective and hence uniform. □

Remark 1. *The trivial case $A = 0$ corresponds to $F(x, y) = (x + H(y), G(y))$, and it has been proved by Varici et al. [26], see Table 2.*

The matrix criterion has a simple solution when the dependence of $A(y)$ on y is through a linear Boolean function. In this case, the correction terms P, Q, R can be chosen all equal to A.

Theorem 7. *Let n, m be two positive integers. Let $F(x, y) = ((\lambda(y)L + I)x + H(y), G(y))$ on $\mathbb{F}_2^n \times \mathbb{F}_2^m$ be a quadratic function with $x \in \mathbb{F}_2^n$, $y \in \mathbb{F}_2^m$. If*

(1) $L : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is linear and $L + I$ is invertible,
(2) $\lambda : \mathbb{F}_2^m \to \mathbb{F}_2$ is linear,
(3) $H : \mathbb{F}_2^m \to \mathbb{F}_2^n$ is a function of $\deg(H) \leq 2$,
(4) and G is a permutation of $\mathbb{F}_2^m$ with $\deg(G) \leq 2$ admitting 3-share TIs,

then F has optimal TIs.

Proof Let $A(y) = \lambda(y)L$, where $L + I$ is invertible, then $I + A(y)$ is either I or $L + I$, and is invertible. We can choose $P = Q = R = A = \lambda(y)L$, Condition (4) of Proposition 6 then becomes

$$\det \begin{pmatrix} I + A_3 & A_2 + A_3 \\ A_1 + A_3 & I + A_3 \end{pmatrix} = \det(I + (a_1a_2 + a_1a_3 + a_2a_3)L^2) = 1,$$

where $a_i = \lambda(y^{(i)}) \in \mathbb{F}_2$, which means that Condition (4) always holds true. Therefore, the case $A = \lambda(y)L$ with $L + I$ invertible corresponds to quadratic permutations with optimal TIs. □

Table 2: Quadratic bijective S-boxes with optimal TIs in [26]

S-box	(n,m)	H	G	S-box	(n,m)	H	G
$\mathcal{Q}_1^3$	$(1,2)$	y_1y_2	I_2	$\mathcal{Q}_{13}^5$	$(1,4)$	y_2y_3	$\mathcal{Q}_{293}^4$
$\mathcal{Q}_4^4$	$(1,3)$	y_2y_3	I_3	$\mathcal{Q}_{14}^5$	$(1,4)$	$y_1y_4+y_2y_3$	I_4
$\mathcal{Q}_{12}^4$	$(1,3)$	0	$\mathcal{Q}_2^3$	$\mathcal{Q}_{15}^5$	$(1,4)$	$y_1y_4+y_2y_3$	$\mathcal{Q}_4^4$
$\mathcal{Q}_{293}^4$	$(1,3)$	y_1y_2	$\mathcal{Q}_2^3$	$\mathcal{Q}_{16}^5$	$(1,4)$	$y_1y_4+y_2y_3$	$\mathcal{Q}_{294}^4$
$\mathcal{Q}_{294}^4$	$(1,3)$	y_1y_3	$\mathcal{Q}_1^3$	$\mathcal{Q}_{17}^5$	$(1,4)$	$y_1y_4+y_2y_3$	$\mathcal{Q}_{12}^4$
$\mathcal{Q}_1^5$	$(1,4)$	y_3y_4	I_4	$\mathcal{Q}_{18}^5$	$(1,4)$	y_1y_2	$\mathcal{Q}_4^4$
$\mathcal{Q}_2^5$	$(1,4)$	y_2y_4	$\mathcal{Q}_4^4$	$\mathcal{Q}_{19}^5$	$(1,4)$	$y_1y_3+y_2y_3$	$\mathcal{Q}_{294}^4$
$\mathcal{Q}_3^5$	$(1,4)$	y_1y_4	$\mathcal{Q}_4^4$	$\mathcal{Q}_{20}^5$	$(1,4)$	y_1y_3	$\mathcal{Q}_{12}^4$
$\mathcal{Q}_4^5$	$(1,4)$	0	$\mathcal{Q}_{12}^4$	$\mathcal{Q}_{21}^5$	$(1,4)$	$y_1y_2+y_2y_3+y_2y_4$	$\mathcal{Q}_{12}^4$
$\mathcal{Q}_5^5$	$(1,4)$	y_1y_4	$\mathcal{Q}_{294}^4$	$\mathcal{Q}_{22}^5$	$(1,4)$	y_2y_3	$\mathcal{Q}_{299}^4$
$\mathcal{Q}_6^5$	$(1,4)$	y_1y_4	$\mathcal{Q}_{12}^4$	$\mathcal{Q}_{23}^5$	$(1,4)$	y_1y_2	$\mathcal{Q}_{294}^4$
$\mathcal{Q}_7^5$	$(1,4)$	0	$\mathcal{Q}_{299}^4$	$\mathcal{Q}_{24}^5$	$(1,4)$	$y_1y_4+y_2y_3$	$\mathcal{Q}_{293}^4$
$\mathcal{Q}_{12}^5$	$(1,4)$	y_2y_3	$\mathcal{Q}_{294}^4$	$\mathcal{Q}_{31}^5$	$(1,4)$	y_1y_2	$\mathcal{Q}_{293}^4$

The preceding construction allows an arbitrary L satisfying an invertible condition, but it uses only one Boolean function as coefficient. We next allow several coefficients by requiring the relevant operators to belong to the field generated by a single irreducible operator. This field structure makes it possible to cancel the mixed terms in the determinant and choose its remaining affine part to avoid zero.

Consider a simple situation in Condition (1) of Proposition 6, where $A(y) = \sum_{i=1}^{d} \lambda_i(y)L^i$ with L satisfying an irreducible polynomial of degree $d+1$ in $\mathbb{F}_2[x]$. Then $I + A(y)$ is an element of $\mathbb{F}_2[L] \setminus \{0\} \cong \mathbb{F}_{2^{d+1}}^*$, and of course invertible. This makes Condition (1) true. We furthermore assume P, Q, R being affine functions on A, which indicates commutative of the multiplication between blocks. Then

$$\begin{aligned}\det \begin{pmatrix} I + A_2 + A_3 + P_2 & A_2 + Q_3 \\ A_3 + R_1 & I + A_1 + R_1 + Q_3 \end{pmatrix} = 1 &+ A_1 + A_2 + A_3 \\ &+ C_1 + C_2 + C_3 \\ &+ A_1A_2 + A_2A_3 + A_3A_1 \\ &+ C_1C_2 + C_2C_3 + C_3C_1 \\ &+ A_1C_2 + A_2C_3 + A_3C_1\end{aligned}$$

is very structured, and we conclude it as Theorem 8.

Theorem 8. *Let $d \geq 2$ be a positive integer. Assume that L is a linear map whose minimal polynomial $p(x) \in \mathbb{F}_2[x]$ of degree $d+1$ is irreducible. Let $F(x,y) = ((I + A(y))x + H(y), G(y))$ be a quadratic function with $x \in \mathbb{F}_2^n$ and $y \in \mathbb{F}_2^m$. If*

(1) $A(y) = \sum_{j=1}^{d} \lambda_j(y) L^j$ *with* $\lambda_j : \mathbb{F}_2^m \to \mathbb{F}_2$ *linear,*
(2) $H : \mathbb{F}_2^m \to \mathbb{F}_2^n$ *is a function of* $\deg(H) \leq 2$*,*
(3) G *is a permutation admitting 3-share TIs,*

then F *has optimal TIs.*

Proof Since the minimal polynomial of L is irreducible of degree $d+1$, $E = \mathbb{F}_2[L] \cong \mathbb{F}_{2^{d+1}}$. The elements $I, L, L^2, \ldots, L^d$ are linearly independent over $\mathbb{F}_2$. Define $U = \mathrm{Span}_{\mathbb{F}_2}\left\{L, L^2, \ldots, L^d\right\}$, then $A(y) \in U$ and $I \notin U$. In particular, $I + A(y)$ is a nonzero element of the field E, and hence an invertible operator on $\mathbb{F}_2^n$.

It remains to construct correction terms P, Q, R satisfying Condition (4). We seek correction maps depending only on $A(y)$ in the form,

$$P, Q, R : U \to \mathbb{F}_{2^{d+1}}, \quad P(u) = p_0 + p(u), Q(u) = q_0 + q(u), R(u) = r_0 + r(u),$$

where $p, q, r, p_0, q_0, r_0 \in E$. Denote $u_i = A(y^{(i)}), P_i = P(u_i), Q_i = Q(u_i), R_i = R(u_i)$, and then

$$M = \begin{pmatrix} 1 + u_2 + u_3 + P_2 & u_2 + Q_3 \\ u_3 + R_1 & 1 + u_1 + R_1 + Q_3 \end{pmatrix},$$

and the quadratic terms in $\det(M)$ over E is

$$(p(r+1)+1)u_1u_2 + (r(q+1)+1)u_1u_3 + (q(p+1)+1)u_2u_3.$$

If $p(r+1) = r(q+1) = q(p+1) = 1$, all quadratic coefficients vanish. Therefore, we define

$$\tau(x) = \frac{1}{x+1},$$

and then

$$p \xrightarrow{\tau} q = \frac{1}{p+1} \xrightarrow{\tau} r = \frac{p+1}{p} \xrightarrow{\tau} p,$$

which implies the quadratic terms vanish when $(p, q, r) = \left(p, \frac{1}{p+1}, \frac{p+1}{p}\right)$.

After choosing (p, q, r), the determinant has no quadratic terms, i.e.,

$$\det(M) = c_0 + c_1u_1 + c_2u_2 + c_3u_3,$$

where

$$\begin{cases} c_0 = 1 + p_0 + q_0 + r_0 + p_0q_0 + q_0r_0 + p_0r_0, \\ c_1 = 1 + p_0 + r(p_0 + q_0 + 1), \\ c_2 = 1 + q_0 + p(q_0 + r_0 + 1), \\ c_3 = 1 + r_0 + q(r_0 + p_0 + 1), \end{cases}$$

and we hope to find (p_0, q_0, r_0) such that $\det(M) = c_0 + c(u_1 + u_2 + u_3) = c_0 + cA(y) \neq 0$ for all y. Assume that $R(0) = 0$, we have $r_0 = 0$, and the condition $(p, q, r) = \left(p, \frac{1}{p+1}, \frac{p+1}{p}\right)$ then gives

$$\begin{cases} c_1 = 1 + p_0 + \dfrac{p+1}{p}(p_0 + q_0 + 1), \\ c_2 = (p+1)(q_0+1), \\ c_3 = 1 + \dfrac{p_0+1}{p+1}. \end{cases}$$

It remains to prove there exists (p_0, q_0, r_0) satisfying above equations with $c_1 = c_2 = c_3$. The condition $c_2 = c_3$ gives $(p^2+1)(q_0+1) = p + p_0$, so assume $q_0 = q = \frac{1}{p+1}$, then $p_0 = p^2$. Then it can be verified $c_1 = c_2 = c_3 = p$ and $c_0 = p^2 + p$, therefore,

$$\det(M) = p^2 + p + pA(y) = p(p + 1 + A(y)),$$

for all $y^{(i)}$. We can simply choose $p = L$, then $p + 1 + A(y) \neq 0 \Rightarrow \det(M) \neq 0$. This means Condition (4) holds, so F has optimal TIs, with the correct terms

$$\begin{cases} P(u) = L^2 + Lu, \\ Q(u) = (L+I)^{-1} + (L+I)^{-1}u, \\ R(u) = \dfrac{L+I}{L}u. \end{cases}$$

□

Corollary 3. *$\mathcal{Q}_{45}^5$ has optimal TIs.*

Proof Let $x = (x_1, x_2, x_3)^{\mathrm{T}}$, then $\mathcal{Q}_{45}^5$ can be rewritten as $((I + y_1L_1 + y_2L_2)x, y_1, y_2)$, where $L_1^3 + L_1^2 + I = 0$ and

$$L_1 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad L_2 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = L_1^2.$$

The rest follows from that the polynomial $p(x) = x^3 + x^2 + 1$ is irreducible over $\mathbb{F}_2$, $G = \mathrm{id}_2$ and $H = 0$. □

We now return to the permutation

$$F(x, y) = \big((I + \lambda(y)L)x + H(y),\, G(y)\big)$$

of Theorem 7. The existence of a 3-share TI is already established. Therefore, Table 3 contains all $3, 4, 5$-bit quadratic permutations marked admitting optimal TIs in [24], without being proved in any previous works.

Note that all L in Table 3 are invertible. It seems that invertible L is redundant, since Condition (1) of Theorem 7 only needs $L + I$ invertible. However, it can be proved that any linear map $L : \mathbb{F}_2^n \to \mathbb{F}_2^n$ with $\ker(L) \neq 0$ corresponds to the case $(1, n + m - 1)$, and the latter can be handled by $(x + H(y), G(y))$ with $x \in \mathbb{F}_2$ and $y \in \mathbb{F}_2^{n-1+m}$, see [26].

Corollary 4. *If $F(x, y) = \big((I + \lambda(y)L)x + H(y), G(y)\big)$ and $\ker(L) \neq 0$, then F is affine equivalent to $\Big(u + \widetilde{H}(z), \widetilde{G}(z)\Big)$ with $(u, z) \in \mathbb{F}_2 \times \mathbb{F}_2^{n-1+m}$.*

Proof See Section B.1. □

That is why Table 3 contains only L with $\mathrm{rank}(L) = n \geq 2$, although Theorem 7 does not force it. Additionally, the $(n, 1)$ case can be exactly solved by conjugacy/inversion of $L + I$.

Table 3: Quadratic bijective S-boxes with optimal TIs by Theorem 7

S-box	(n,m)	L	λ	H	G
$\mathcal{Q}_2^3$	$(2,1)$	(x_1+x_2, x_1)	y_1	0	I_1
$\mathcal{Q}_{299}^4$	$(3,1)$	$(x_1+x_3, x_1+x_2+x_3, x_2+x_3)$	y_1	0	I_1
$\mathcal{Q}_8^5$	$(4,1)$	$(x_1+x_2, x_1, x_3+x_4, x_3)$	y_1	0	I_1
$\mathcal{Q}_9^5$	$(4,1)$	$(x_1+x_2+x_4, x_1, x_3+x_4, x_3)$	y_1	0	I_1
$\mathcal{Q}_{10}^5$	$(4,1)$	$(x_1+x_4, x_1+x_2+x_4, x_2+x_3, x_3+x_4)$	y_1	0	I_1
$\mathcal{Q}_{11}^5$	$(4,1)$	$(x_1+x_4, x_1+x_2+x_4, x_2+x_3+x_4, x_3)$	y_1	0	I_1
$\mathcal{Q}_{25}^5$	$(2,3)$	(x_1+x_2, x_1)	y_3	$(y_1y_2, 0)$	I_3
$\mathcal{Q}_{26}^5$	$(2,3)$	(x_1+x_2, x_1)	y_3	$(y_1y_2, 0)$	$\mathcal{Q}_1^3$
$\mathcal{Q}_{27}^5$	$(2,3)$	(x_1+x_2, x_1)	y_3	$(y_1y_2, 0)$	$\mathcal{Q}_2^3$
$\mathcal{Q}_{33}^5$	$(2,3)$	(x_1+x_2, x_1)	y_1+y_3	0	$\mathcal{Q}_1^3$
$\mathcal{Q}_{34}^5$	$(2,3)$	(x_1+x_2, x_1)	y_2+y_3	0	$\mathcal{Q}_2^3$

Corollary 5. *Let $n \geq 2$, $m = 1$, and $L, L' \in \mathrm{GL}(n,2)$ such that both $L+I_n$ and $L'+I_n$ are invertible. Then $F_L(x,y) = (x+yL(x), y)$ is affine equivalent to $F_{L'} = (x+yL'(x), y)$ if and only if*

$$L' + I_n = P^{-1}(L + I_n)P$$

or

$$L' + I_n = P^{-1}(L + I_n)^{-1}P,$$

for some $P \in \mathrm{GL}(n,2)$.

Proof See Section B.2. □

Table 4: The number of conjugacy/inversion classes of $L+I_n$

n	2	3	4	5	6	7
conjugacy/inversion classes of $L+I_n$	1	1	4	4	13	17

The $(n,2)$ case does not appear in Table 3, as those functions are always affine equivalent to the functions in $(1, n+1)$ case.

Corollary 6. *Let $n \geq 1$ and $m = 2$. Then $F_L(x,y) = (x + \lambda(y)L(x) + H(y), G(y))$ is affine equivalent to a function $\left(u + \widetilde{H}(z), \widetilde{G}(z)\right)$ with $u \in \mathbb{F}_2$ and $z \in \mathbb{F}_2^{n+1}$.*

Proof See Section B.3. □

With these reductions as the structural framework, we conducted a computational search for 6-bit quadratic permutations covered by the construction. The resulting counts are summarized in Table 5.

Table 5: 6-bit quadratic permutation classes obtained from Theorem 7

Parameter (n, m)	Conditions	Number of classes
$(1, 5)$	$\deg(G) = 2$	372
$(1, 5)$	$\deg(G) = 1$	2
$(5, 1)$	Conjugacy/inversion classes of $L + I_5$	4
$2 \le n \le 4, m = 6 - n$	$\mathrm{rank}(L) = n$	97

Table 6: The known 5-bit quadratic permutations admitting optimal TIs

Class $\mathcal{Q}_i^5$	Theoretical explanation	TI construction
$1-7, 12-24, 31$	[26], Remark 1	[24]
$8-11, 25-27, 33, 34$	Theorem 7	[24]
30	Theorem 5 and Corollary 2	Section A
45	Theorem 8	This paper†
$28, 29, 32, 37-42, 44$	-	This paper†

†https://github.com/gggaaarrryyyabs/3-share-TIs-of-5-bit-quadratic-permuations

Table 6 summarizes the constructions of 3-share TIs for 42 affine-equivalence classes of five-bit quadratic permutations. For 32 classes, the existence of such implementations follows from the cited structural results, whereas implementations for the remaining 10 classes are obtained by computational search. Compared with the 30 classes reported by Božilov et al. [24], the table includes 12 additional classes, namely $\mathcal{Q}_{28}^5, \mathcal{Q}_{29}^5, \mathcal{Q}_{30}^5, \mathcal{Q}_{32}^5, \mathcal{Q}_{37}^5, \ldots, \mathcal{Q}_{42}^5, \mathcal{Q}_{44}^5$, and $\mathcal{Q}_{45}^5$. All implementations use the minimum number of shares and require no fresh randomness.

3.3 Weighted interpolation constructions

Given a permutation of algebraic degree t, correctness and non-completeness can be achieved with $t + 1$ shares, but uniformity is not automatic with unknown reason. The difficulty is therefore to construct a sharing that also preserves the uniform distribution

on each sharing space. The construction below addresses this difficulty through an inversion order. It begins with a weighted interpolation identity satisfying correctness, and preserving uniformity by a triangular inversion form. Non-completeness is obtained by a common mask that cancels the i-th input share from the i-th evaluation.

Theorem 9. *Let $s \geq 3$, $m \mid n$, and let F be a permutation of $\mathbb{F}_{2^n}$. If there are s distinct nonzero elements $\lambda_1, \lambda_2, \ldots, \lambda_s \in \mathbb{F}_{2^m}$ and nonzero elements $\omega_1, \omega_2, \ldots, \omega_s \in \mathbb{F}_{2^m}$, such that for all $x, y \in \mathbb{F}_{2^n}$,*

$$\sum_{i=1}^{s} \omega_i F(x + \lambda_i y) = F(x),$$

then F has s-share TIs.

Proof Let the input share of x be

$$\boldsymbol{x} = (x^{(1)}, x^{(2)}, \ldots, x^{(s)}),$$

then $x = \sum_{j=1}^{s} x^{(j)}$. And define the output share by

$$\begin{cases} F^{(1)} = \omega_1 F(x + \lambda_1 y), \\ F^{(i)} = \omega_i F(x + \lambda_i y) + x^{(i-1)}, \quad 2 \leq i \leq s-1, \\ F^{(s)} = \omega_s F(x + \lambda_s y) + \sum_{j=1}^{s-2} x^{(j)}, \end{cases}$$

where the common mask is

$$y = \lambda_1^{-1} x^{(1)} + \lambda_2^{-1} x^{(2)} + \cdots + \lambda_s^{-1} x^{(s)}.$$

The correctness is clear and the non-completeness follows from the fact that $x + \lambda_i y = \sum_{j \neq i} \left(1 + \lambda_i \lambda_j^{-1}\right) x^{(j)}$ is independent of $x^{(i)}$, as $1 + \lambda_i \lambda_i^{-1} = 0$. To prove uniformity, we show that the input shares can be uniquely recovered from the output shares. That is, we first recover the unshared input,

$$x = F^{-1}\left(\sum_{i=1}^{s} F^{(i)}\right).$$

And then y can be determined,

$$y = \lambda_1^{-1}\left(F^{-1}\left(\omega_1^{-1} F^{(1)}\right) + x\right),$$

which means that we can successively recover $x^{(i-1)}$ by $F^{(i)}$ with $x, y, \omega_i, \lambda_i$, for $2 \leq i \leq s-1$. Finally, $x^{(s-1)}$ and $x^{(s)}$ can be recover in the following,

$$\begin{cases} x^{(s-1)} + x^{(s)} = x + \sum_{i=1}^{s-2} x^{(i)}, \\ \lambda_{s-1}^{-1} x^{(s-1)} + \lambda_s^{-1} x^{(s)} = y + \sum_{i=1}^{s-2} \lambda_i^{-1} x^{(i)}, \end{cases}$$

as the matrix $\begin{pmatrix} 1 & 1 \\ \lambda_{s-1}^{-1} & \lambda_s^{-1} \end{pmatrix}$ is invertible due to nonzero $\lambda_{s-1} \neq \lambda_s$. Thus, the output shared map is a permutation of $\mathbb{F}_{2^n}^s$, this proves uniformity. □

The weighted interpolation identity admits an equivalent description in terms of the polynomial representation. Let $F(x) = \sum_{d=0}^{2^n-1} c_d x^d$ be the polynomial representation of F. Therefore,

$$\begin{aligned}\sum_{i=1}^{s} \omega_i F(x+\lambda_i y) &= \sum_{i=1}^{s} \omega_i \sum_{d=0}^{2^n-1} c_d \sum_{k \preceq d} \lambda_i^k x^{d-k} y^k, \\ &= \sum_{d=0}^{2^n-1} c_d \sum_{k \preceq d} \left(\sum_{i=1}^{s} \omega_i \lambda_i^k \right) x^{d-k} y^k, \\ &= F(x),\end{aligned}$$

where $k \preceq d$ means that k is covered by d. The term $k = 0$ will recover $F(x)$, and each term $1 \leq k \preceq d$ must vanish.

Theorem 10. *Let $s \geq 3$, $m \mid n$, and let $F(x) = \sum_{d=0}^{2^n-1} c_d x^d$ be a permutation of $\mathbb{F}_{2^n}$. If there are s distinct nonzero elements $\lambda_1, \lambda_2, \ldots, \lambda_s \in \mathbb{F}_{2^m}$ and nonzero elements $\omega_1, \omega_2, \ldots, \omega_s \in \mathbb{F}_{2^m}$, such that*

$$\sum_{i=1}^{s} \omega_i = 1, \quad \sum_{i=1}^{s} \omega_i \lambda_i^k = 0, \quad 1 \leq k \preceq d \text{ for all } c_d \neq 0,$$

then F has s-share TIs.

Furthermore, in the optimal case, once all λ_i are fixed, all weights ω_i are then uniquely determined, according to Theorem 10.

Corollary 7. *For any arbitrary permutation F with optimal TIs and $s = \deg(F) + 1$, every fixed s distinct nonzero $\lambda_1, \lambda_2, \ldots, \lambda_s$ admits at most one weight vector up to the ordering.*

Proof Consider the case $s = \deg(F) + 1$, then the corresponding exponent $d = \sum_{i=1}^{s-1} 2^{d_i}$ with $d_1 < d_2 < \cdots < d_{s-1}$. Define any d-degree polynomial $P(X) = \prod_{i=1}^{s-1} (X + \lambda_i)^{2^{d_i}} = \sum_{k \preceq d} a_k X^k$, we then have $P(\lambda_i) = 0$ for all $1 \leq i \leq s-1$ and $P(\lambda_s), P(0) \neq 0$. Then weighted sum is,

$$\sum_{i=1}^{s} \omega_i P(\lambda_i) = \omega_s P(\lambda_s),$$

and by Theorem 10 with $2^{d_i} \preceq d$, expanding $P(\lambda_i)$ also gives

$$\sum_{i=1}^{s} \omega_i P(\lambda_i) = a_0 \sum_{i=1}^{s} \omega_i + \sum_{j=1}^{s-1} a_j \sum_{i=1}^{s} \omega_i \lambda_i^{2^{d_j}} = a_0 = P(0).$$

Therefore, $\omega_s = \frac{P(0)}{P(\lambda_s)}$, and other weights can be solved similarly as follows,

$$\omega_j = \prod_{i=1,\ i\neq j}^{s} \left(\frac{\lambda_i}{\lambda_j + \lambda_i}\right)^{2^{d_i}}, \quad 1 \leq j \leq s. \qquad \square$$

Suppose that for every $x, y \in \mathbb{F}_{2^n}$, the map $\lambda \mapsto F(x + \lambda y)$ is represented by a $\mathbb{F}_{2^n}$-valued polynomial over $\mathbb{F}_{2^m}$ of degree at most t. Given any $s = t + 1$ distinct nonzero elements $\lambda_1, \lambda_2, \ldots, \lambda_s \in \mathbb{F}_{2^m}$, the Lagrange interpolation evaluated at 0 provides unique nonzero weights $\omega_i \in \mathbb{F}_{2^m}$, such that every polynomial h of degree at most t satisfies $h(0) = \sum_{i=1}^{s} \omega_i h(\lambda_i)$. Apply this to $h(\lambda) = F(x + \lambda y)$, then

$$F(x) = \sum_{i=1}^{s} \omega_i F(x + \lambda_i y),$$

always holds true. Therefore, we call this construction a weighted interpolation method based on a triangular inversion form. And we therefore have a sufficient condition for existence of optimal TIs by the degree of F over $\mathbb{F}_{2^m}$.

Corollary 8. *Let $s \geq 3$, $m \mid n$, and let F be a permutation of $\mathbb{F}_{2^n}$ with algebraic degree $t \geq 2$. Suppose $2^m \geq t + 2$, if for every $x, y \in \mathbb{F}_{2^n}$, the function $\lambda \mapsto F(x + \lambda y)$ has degree at most t, then F has optimal TIs.*

The preceding corollary transforms the construction of optimal TIs to finding permutations whose restrictions to affine $\mathbb{F}_{2^m}$-lines have degree at most their algebraic degree. A natural choice is given by products of $\mathbb{F}_{2^m}$-linear maps, that is, the product of the Frobenius maps.

Theorem 11. *Let $F(x) = x^d$ be a permutation of $\mathbb{F}_{2^n}$, where $d = 2^{k_1} + 2^{k_2} + \cdots + 2^{k_t}$ with $0 \leq k_1 < k_2 < \cdots < k_t < n$ and $t \geq 2$. Define $h = \gcd(n, k_2 - k_1, k_3 - k_1, \ldots, k_t - k_1)$, if $2^h \geq t + 2$, then F has optimal TIs.*

Proof We only consider the permutation $G(x) = x^{d_0}$ with $d_0 = \sum_{i=1}^{t} 2^{k_i - k_1}$, as $G(x)$ is affine equivalent to $F(x)$. Let $q = 2^h$, then $\mathbb{F}_q \subseteq \mathbb{F}_{2^n}$. Define a Frobenius map $\sigma = 2^{k_1}$, so for every $\lambda \in \mathbb{F}_q^*$, we have $\lambda^{2^{k_i}} = \lambda^{\sigma}$. Therefore,

$$(x + \lambda y)^{d_0} = \prod_{j=1}^{t} \left(x^{2^{k_j - k_1}} + \lambda^{2^{k_j - k_1}} y^{2^{k_j - k_1}}\right) = \prod_{j=1}^{t} \left(x^{2^{k_j - k_1}} + \lambda y^{2^{k_j - k_1}}\right),$$

which means that $\lambda \mapsto (x + \lambda y)^{d_0}$ has degree at most t. The rest follows from Corollary 8. $\square$

Corollary 9. *Let $k \geq 3$ be odd and $q = 2^k$. Then the Bracken-Leander permutation $F(x) = x^{q^2+q+1}$ of $\mathbb{F}_{q^4}$ has optimal TIs.*

Consequently, nonlinear power permutations can meet the lower bound of $t+1$ shares. This disproves Conjecture 1 in [2]. A smaller counterexample, x^5 on $\mathbb{F}_{2^6}$ admitting optimal TIs with $d = 5$ and $n = 6$, is given in the following.

Example 3. *Consider the quadratic permutation $F(x) = x^5$ on $\mathbb{F}_{2^6}$. For simplicity we use $(x_1, x_2, x_3) \in \mathbb{F}_{2^6}^3$ to be a 3-sharing of input $x \in \mathbb{F}_{2^6}$. Then its optimal TI $\boldsymbol{F} = (F^{(1)}, F^{(2)}, F^{(3)})$ can be constructed as follows,*

$$\begin{cases} F^{(1)} = \omega^2(\omega x_2 + x_3)^5 \\ F^{(2)} = \omega^2(\omega x_3 + x_1)^5 + x_1 \\ F^{(3)} = \omega^2(\omega x_1 + x_2)^5 + x_1, \end{cases}$$

where $\omega^2 + \omega + 1 = 0$ for $\omega \in \mathbb{F}_4$.

3.4 Derivative-uniform constructions

Let F be a permutation of $\mathbb{F}_{2^n}$, and let $\boldsymbol{x} = (x^{(1)}, x^{(2)}, \ldots, x^{(s)})$ be an s-sharing of x. It holds

$$D_{x^{(s)}}F\left(\sum_{i=1}^{s-1} x^{(i)}\right) = F\left(\sum_{i=1}^{s-1} x^{(i)}\right) + F\left(\sum_{i=1}^{s-1} x^{(i)} + x^{(s)}\right) = F(x + x^{(s)}) + F(x),$$

which implies

$$F(x) = F(x + a) + D_a F(u),$$

where $u = \sum_{i=1}^{s-1} x^{(i)}$ and $a = x^{(s)}$. In above derivative, $F(x + a)$ is independent of $x^{(s)}$ and can serve as s-th output share. Although F is a permutation, its derivatives need not be permutations. Therefore, uniformity of $D_a F$ must be understood fiberwise, that is, the bijectivity of $\mathrm{Sh}_{s-1}(x) \mapsto \mathrm{Sh}_{s-1}(D_a F(x))$ for every x. Note that we do not need to consider $a = 0$, since the sharing of $D_0 F = 0$ is trivial.

Theorem 12. *Let F be a permutation of $\mathbb{F}_{2^n}$ of algebraic degree $t \geq 3$. If $D_a F$ admits t-share TIs for every $a \in \mathbb{F}_{2^n}^*$, then F has optimal TIs.*

Proof Let $\boldsymbol{x} = (x^{(1)}, x^{(2)}, \ldots, x^{(s)})$ be s-share input sharing with $s = t + 1$. Denote

$$u = \sum_{i=1}^{s-1} x^{(i)}, \quad a = x^{(s)},$$

and for simplicity, we use $H(a; x) = D_a F(x)$. Define the s-share output sharing of F as follows,

$$\begin{cases} F^{(i)} = H^{(i)}(x^{(s)}; x^{(1)}, x^{(2)}, \ldots, x^{(s-1)}), \quad 1 \leq i \leq s-1, \\ F^{(s)} = F(u), \end{cases}$$

with $\boldsymbol{H}(a; \cdot) = \left(H^{(1)}(a; \cdot), H^{(2)}(a; \cdot), \ldots, H^{(s-1)}(a; \cdot)\right)$ is a t-share TI for every fixed $a \in \mathbb{F}_{2^n}^*$.

The correctness and non-completeness are easy to check, and its uniformity can be proved in the following. Given the output shares, we first recover

$$u = F^{-1}\left(F^{(s)}\right),$$

and then by correctness, we obtain

$$x^{(s)} = a = u + F^{-1}\left(\sum_{i=1}^{s} F^{(i)}\right).$$

Once u and a are known, the first $s-1$ output shares recover

$$x^{(1)}, x^{(2)}, \ldots, x^{(s-1)},$$

as $\boldsymbol{H}$ is bijective on $\mathrm{Sh}_{s-1}(u)$ for every a. Thus, the shared map is a permutation and is uniform. □

Remark 2. *The derivative-uniform is not necessarily degree-preserve construction, that is,* $\deg(\boldsymbol{F}) \geq \deg(F)$. *Although each derivative has algebraic degree at most* $t-1$ *for a fixed direction* a*, the corresponding shared may depend nonlinearly on* a*. Since* $a = x^{(s)}$ *is an input share in the TI of* F*, this dependence can increase the algebraic degree of the TI.*

Remark 3. *The restriction* $t \geq 3$ *cannot be reduced to* $t \geq 2$*. Every nonconstant derivative of a quadratic function is an affine map, whereas a nonconstant affine map from* $\mathbb{F}_2^n$ *to itself admits 2-share TIs only when it is bijective. But, every quadratic function has a nonconstant derivative which is not bijective, as* $D_aF(x) = D_aF(x+a)$ *with a nonzero direction* a*.*

Theorem 12 reduces the construction of optimal TIs for an algebraic degree-t permutation to the construction of t-share TIs for its derivatives. Since $\deg(D_aF) \leq t-1$ for every nonzero a, the only difficulty lies in derivatives whose algebraic degree is exactly $t-1$. The case for $\deg(D_aF) \leq t-2$ is already addressed by Theorem 1, see [39]. We therefore consider an extreme case, where derivatives for which all but one output coordinate have degree at most $t-2$. The following theorem gives a sufficient condition on such permutations.

Theorem 13. *Let* F *be a permutation of* $\mathbb{F}_{2^n}$ *of algebraic degree* $t \geq 3$*. If there exists* $v \in \mathbb{F}_{2^n}^*$ *such that*

$$\deg(\pi_v \circ F) \leq t-1,$$

where $\pi_v : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}/\langle v \rangle$*, then* F *has optimal TIs.*

Proof Consider D_aF for fixed $a \in \mathbb{F}_{2^n}^*$, let $\mathbb{F}_{2^n} = U_{in} \oplus \langle a \rangle$ and $\mathbb{F}_{2^n} = U_{out} \oplus \langle v \rangle$. Write an input as $x = z + a\alpha$ with $z \in U_{in}$ and $\alpha \in \mathbb{F}_2$. Since $D_aF(x+a) = D_aF(x)$, D_aF does not depend on α, and we can express D_aF by (z, α),

$$D_aF(z, \alpha) = (G(z), H(z)),$$

where $G : U_{in} \to U_{out}$ and $H : U_{in} \to \mathbb{F}_2$ with

$$\deg(G) \leq t-2, \quad \deg(H) \leq t-1.$$

The function G with $\deg(G) \leq t-2$ has a t-share TI $\boldsymbol{G}$, according to Theorem 1, so it remains to lift $\boldsymbol{G}$ to a t-share TIs for D_aF. Denote the shared output $H^{(i)}$ constructed by direct sharing, then

$$(D_aF)^{(i)}(\boldsymbol{z}, \boldsymbol{\alpha}) = \left(G^{(i)}(\boldsymbol{z}), H^{(i)}(\boldsymbol{z}) + 0^{(i)}(\boldsymbol{\alpha})\right), \quad 1 \leq i \leq t,$$

where $\mathbf{0}(\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(t)}) = \left(\alpha^{(2)}, \ldots, \alpha^{t-1}, \alpha^{(1)}, \sum_{j=1}^{t-1} \alpha^{(j)}\right)$. Therefore, $D_a F$ must have t-share TIs for every $a \in \mathbb{F}_{2^n}^*$. The rest follows from Theorem 12. □

Remark 4. *The hypothesis of Theorem 13 is equivalent to the existence of a decomposition* $F(x) = G(x) + vf(x)$*, where* $\deg(G) \leq t-1, v \neq 0$*, and* $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$.

Theorem 13 gives a common explanation of four 4×4 cubic S-boxes in [23], $\mathcal{C}_1^4, \mathcal{C}_3^4, \mathcal{C}_{13}^4$ and $\mathcal{C}_{301}^4$. Furthermore, it also yields 14 additional 4×4 cubic S-boxes with optimal TIs, that is, $\mathcal{C}_i^4$ with

$$i \in \{5, 11, 17, 214, 215, 216, 243, 244, 246, 258, 259, 260, 292, 298\}.$$

Indeed, we can prove that every cubic permutation of $\mathbb{F}_{2^4}$ has optimal TIs, by reducing to construct 3-share TIs of its derivatives. By the same idea of Theorem 13, each derivative has the form, after suitable linear transformations,

$$D_a F(u, t) = (G(u), h(u)),$$

where $G(u) = L(u) + f(u)u$ admits 3-share TIs and $\deg(h) \leq 2$ for $h : \mathbb{F}_2^3 \to \mathbb{F}_2$. The only challenge lies on the G, where the following lemma proves such G admitting 3-share TIs. The proof is analogue to those of Proposition 6.

Lemma 3. *Let* $L : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *and* $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ *be affine with* $n \geq 3$*. Then* $F(x) = L(x) + f(x)x$ *has 3-share TIs.*

Proof Write $f(x) = \ell(x) + \epsilon$ with ℓ linear and $\epsilon \in \mathbb{F}_2$, then assign ϵx into $L(x)$, therefore assume $F(x) = L(x) + \ell(x)x$ with L, ℓ linear and $F(0) = 0$. If $\ell(x) \equiv 0$, then $F(x)$ is linear and has 3-share TIs. So assume that $\ell \neq 0$, and denote $Z = \ker(\ell)$, then

$$\mathbb{F}_{2^n} = Z \oplus E,$$

where $E = \langle e \rangle$ and $\ell(e) = 1$ for some $e \in \mathbb{F}_{2^n}$. Thus, $x \in \mathbb{F}_{2^n}$ can be uniquely expressed as

$$x = z + ce, \quad c \in \mathbb{F}_2, \quad z \in Z,$$

so, assume that

$$L(x) = L(z + ce) = Az + cb + (\lambda(z) + \alpha c)e,$$

where both $A : Z \to Z, \lambda : Z \to \mathbb{F}_2$ are linear and $b \in Z, \alpha \in \mathbb{F}_2$. We obtain

$$F(z, c) = ((A + cI)z + cb, \lambda(z) + \beta c),$$

with $\beta = \alpha + 1$, and it suffices to prove that F has 3-share TIs, without any restriction on A, b, λ, β.

Assume that 3-share sharings to be $(z^{(i)}, c^{(i)})$, with $z = z^{(1)} + z^{(2)} + z^{(3)}$ and $c = c^{(1)} + c^{(2)} + c^{(3)}$. Let $\boldsymbol{F} = \left(F^{(1)}, F^{(2)}, F^{(3)}\right)$ be a 3-share of F with $F^{(i)} = (G^{(i)}, H^{(i)})$, where $(G^{(1)}, G^{(2)}, G^{(3)})$ is a 3-share TI of $(A + cI)z + cb$, and $(H^{(1)}, H^{(2)}, H^{(3)})$ is a 3-share TI of

$\lambda(z)+\beta c$,

$$\begin{cases} G^{(1)} = (A+(c^{(2)}+c^{(3)})I+P_2)z^{(2)} + (c^{(2)}I+Q_3)z^{(3)} + bc^{(2)}, \\ G^{(2)} = (c^{(3)}I+R_1)z^{(1)} + (A+(c^{(1)}+c^{(3)})I+Q_3)z^{(3)} + bc^{(3)}, \\ G^{(3)} = (A+(c^{(1)}+c^{(2)})I+R_1)z^{(1)} + (c^{(1)}I+P_2)z^{(2)} + bc^{(1)}, \\ H^{(1)} = c^{(2)}, \\ H^{(2)} = \lambda(z^{(1)}+z^{(3)}) + \beta(c^{(1)}+c^{(3)}) + c^{(1)}, \\ H^{(3)} = \lambda(z^{(2)}) + (\beta+1)c^{(2)} + c^{(1)}, \end{cases} \tag{3}$$

with $R_1 = R(c^{(1)}), P_2 = P(c^{(2)})$ and $Q_3 = Q(c^{(3)})$. The correctness and non-completeness are easy to follow, we only prove its uniformity.

Fixing the unshared values z and c, we show that we can uniquely determine the input sharing. We first obtain $c^{(2)}$ from $H^{(1)}$, then $c^{(1)}+c^{(3)} = c+c^{(2)}$ is known. Thus, the sharing $H^{(3)}$ gives

$$\begin{cases} c^{(1)} = \lambda(z^{(2)}) + (\beta+1)c^{(2)} + H^{(3)}, \\ c^{(3)} = c + c^{(1)} + c^{(2)} = c + \lambda(z^{(2)}) + \beta c^{(2)} + H^{(3)}, \\ c^{(2)} = H^{(1)}. \end{cases}$$

Substituting $z^{(1)} = z+z^{(2)}+z^{(3)}$ and $c^{(1)}, c^{(2)}, c^{(3)}$ into Equation (3), the map $(z^{(2)}, z^{(3)}) \mapsto (G^{(2)}, G^{(3)})$ is

$$\begin{pmatrix} G^{(2)} \\ G^{(3)} \end{pmatrix} = M(z^{(2)}) \begin{pmatrix} z^{(2)} \\ z^{(3)} \end{pmatrix} + T(z^{(2)}),$$

where

$$M(z^{(2)}) = \begin{pmatrix} c^{(3)}I+R_1+B & A+c^{(1)}I+R_1+Q_3 \\ A+c^{(2)}I+R_1+P_2+B & A+(c^{(1)}+c^{(2)})I+R_1 \end{pmatrix},$$

with $B: Z \to Z$ defined by $Bz = b\lambda(z)$, and

$$T(z^{(2)}) = \begin{pmatrix} (c^{(3)}I+R_1)z + b(c+\beta c^{(2)}+H^{(3)}) \\ (A+(c^{(1)}+c^{(2)})I+R_1)z + b((\beta+1)c^{(2)}+H^{(3)}) \end{pmatrix}.$$

We now prove that there exist P, R, Q such that resulting map is affine and invertible for every $c^{(1)}, c^{(2)}$ and $c^{(3)}$.

The second column of M are

$$\begin{cases} M_{12} = A + c^{(1)}I + R_1 + Q_3, \\ M_{22} = A + (c^{(1)}+c^{(2)})I + R_1, \end{cases}$$

both entries share $A + c^{(1)}I + R_1$. We therefore choose $R_1 = A + c^{(1)}I$, which reduces $\begin{pmatrix} M_{12} \\ M_{22} \end{pmatrix} = \begin{pmatrix} Q_3 \\ c^{(2)}I \end{pmatrix}$, and we therefore take $Q_3 = I$. Note that $R_1 = A + c^{(1)}I$ and $Q_3 = I$ also reduce $T(z^{(2)})$ to be independent of $z^{(2)}$,

$$T(z^{(2)}) = \begin{pmatrix} C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} (A+(c+c^{(2)})I)z + b(c+\beta c^{(2)}+H^{(3)}) \\ c^{(2)}z + b((\beta+1)c^{(2)}+H^{(3)}) \end{pmatrix}.$$

Furthermore,

$$M(z^{(2)}) = \begin{pmatrix} A+(c+c^{(2)})I+B & I \\ (c^{(1)}+c^{(2)})I+P_2+B & c^{(2)}I \end{pmatrix},$$

and $c^{(1)}$ is dependent of $z^{(2)}$. So, the map $(z^{(2)}, z^{(3)}) \mapsto (G^{(2)}, G^{(3)})$ is

$$\begin{pmatrix} G^{(2)} \\ G^{(3)} \end{pmatrix} = M(z^{(2)}) \begin{pmatrix} z^{(2)} \\ z^{(3)} \end{pmatrix} + T,$$

where T is independent of $z^{(2)}$. and

$$M(z^{(2)}) = \begin{pmatrix} A + (c + c^{(2)})I + B & I \\ (\lambda(z^{(2)}) + \beta c^{(2)} + H^{(3)})I + P_2 + B & c^{(2)} I \end{pmatrix} \sim \begin{pmatrix} A + (c + c^{(2)})I + B & I \\ c^{(2)} A + \lambda(z^{(2)})I + \delta I + P_2 + (c^{(2)} + 1)B & 0 \end{pmatrix},$$

where $\delta = H^{(3)} + (c + \beta + 1)c^{(2)}$. We need to find P_2 to make

$$c^{(2)} A + \lambda(z^{(2)})I + \delta I + P_2 + (c^{(2)} + 1)B$$

invertible and independent of $z^{(2)}$, which makes the map $(z^{(2)}, z^{(3)}) \mapsto (G^{(2)}, G^{(3)})$ affine and invertible. This can be done by assigning $P_2 = c^{(2)} A + (c^{(2)} + 1)B + D + \lambda(z^{(2)})I$ with both D and $D + I$ invertible. Such D always exists since its size is $n - 1 \geq 2$. Therefore, we have obtained 3-share TIs of $F(z, c) = ((A + cI)z + bc, \lambda(z) + \beta c)$ as Equation (3) with correction terms

$$\begin{cases} R(c) = A + cI, \\ P(c, z) = cA + D + (c + 1)B + \lambda(z)I, \\ Q(c) = I, \end{cases}$$

where both $D, D + I$ are invertible and $Bz = b\lambda(z)$. Therefore, we have uniquely determined $z^{(1)}, z^{(2)}$ and $z^{(3)}$, so we can determine $c^{(1)}$ and $c^{(3)}$. This implies Equation (3) is uniform. □

Based on the following observation, we can express the derivative of any arbitrary cubic permutation of $\mathbb{F}_2^4$ in the form $D_a F(u, t) = (L(u) + f(u)u, h(u))$ with $L : \mathbb{F}_2^3 \to \mathbb{F}_2^3$ affine, $f : \mathbb{F}_2^3 \to \mathbb{F}_2$ linear and $h : \mathbb{F}_2^3 \to \mathbb{F}_2$ quadratic or affine.

Observation 1. *Any two quadratic Boolean functions $f, g : \mathbb{F}_2^3 \to \mathbb{F}_2$ with $\deg(f+g) = 2$ must have the form, after certain linear transformations,*

$$\begin{cases} f(\alpha, \beta, \gamma) = \alpha\gamma + A_1(\alpha, \beta, \gamma), \\ g(\alpha, \beta, \gamma) = \beta\gamma + A_2(\alpha, \beta, \gamma), \end{cases}$$

where A_1, A_2 affine.

Proof By Dickson's form, every quadratic Boolean function over $\mathbb{F}_2^3$ is affinely equivalent to $x_1x_2 + x_3$ or x_1x_2, so it must have a linear structure. Consider two functions f and g, if they have the same linear structure, $f + g$ is affine, contradiction. If they have distinct linear structure, for example a and b, respectively, choose $e \notin \langle a, b \rangle$ and then we can express $x = b\alpha + a\beta + e\gamma$. Since $D_a f$ is constant, its quadratic part contains no β, and so it is $\alpha\gamma$, we can obtain the similar for $D_b g$. Thus, we have $f = \alpha\gamma + A_1(\alpha, \beta, \gamma)$ and $g = \beta\gamma + A_2(\alpha, \beta, \gamma)$. □

Theorem 14. *Every 4-bit cubic permutation has optimal TIs.*

Proof Let $F : \mathbb{F}_2^4 \to \mathbb{F}_2^4$ be any arbitrary cubic permutation. Consider its derivative $H = D_a F : \mathbb{F}_2^4 \to \mathbb{F}_2^4$, let $\mathbb{F}_2^4 = U \oplus \langle a \rangle$, we obtain $x = u + ta \in \mathbb{F}_2^4$ with $u \in U$ and $t \in \mathbb{F}_2$. Therefore,

$$H(u, t) = H(u, 0),$$

as $H(x + a) = H(x)$. Set $u = (\alpha, \beta, \gamma) \in \mathbb{F}_2^3$, by Observation 1, H is affine equivalent to $\widetilde{H}$, where $\widetilde{H}$ has three possible forms,

(1) $\big(\alpha\gamma + A_1, \beta\gamma + A_2, \alpha\beta + A_3, A_4\big) \Leftrightarrow (L(u) + f(u)u, h(u))$, where $h(u) = \alpha\beta + A_3$, $f(u) = \gamma$ and $L(u) = (A_1, A_2, A_4 + \gamma)$,

(2) $\big(\alpha\gamma + A_1, \beta\gamma + A_2, A_3, A_4\big) \Leftrightarrow (L(u) + f(u)u, h(u))$, where $h(u) = A_3$, $f(u) = \gamma$ and $L(u) = (A_1, A_2, A_4 + \gamma)$

(3) $\big(\alpha\gamma + A_1, A_2, A_3, A_4\big) \Leftrightarrow (h(u), L(u))$, where $h(u) = \alpha\gamma + A_1$ and $L(u) = (A_2, A_3, A_4)$,

where $\deg(A_i) \leq 1$. Thus, we have

$$\widetilde{H}(u, t) = (L(u) + f(u)u, h(u)).$$

By Lemma 3, $L(u) + f(u)u$ has 3-share TIs, and the left is analogue to the proof of Theorem 13. □

3.5 Comparison of hardware implementation costs

We evaluate the hardware costs of explicit optimal TIs obtained from Section 3. The selected permutations are $\mathcal{Q}_{30}^5$, $\mathcal{Q}_{45}^5$, x^5 over $\mathbb{F}_{2^6}$, the Bracken-Leander permutation x^{73} over $\mathbb{F}_{2^{12}}$, the PRESENT S-box $\mathcal{C}_{266}^4$, and inversion over $\mathbb{F}_{2^4}$, corresponding to $\mathcal{C}_{282}^4$. For a target permutation of algebraic degree t, the proposed constructions provide $(t+1)$-share TIs without fresh randomness. We compare them with the universal $(t+2)$-share TI construction of Piccione et al. [2]. For PRESENT, we additionally include implementations of the 3-share of two quadratic S-boxes decompositions of Poschmann et al. [20] and Kutzner et al. [28]. The area is measured in gate equivalences (GE), i.e., the S-box area normalised to the area of a 2-input NAND gate in a given standard cell library. In this work, we use the `NANGATE` 45nm Open Cell Library where the synthesis results are obtained with the Yosys `0.69+150`. We note that by using the correction terms, one could get improved area costs. However, we did not pursue this direction and leave this possible optimization for future investigation.

All implementations in Table 7 require zero fresh randomness, this property is therefore ignored rather than reported in a separate column. Compared with the universal $(t + 2)$-share construction, the proposed $(t + 1)$-share implementations reduce share by 1, and this leads to the reduction in generating the initial input sharing.

For the first four target permutations, the proposed implementations reduce both the share count and the area, relative to the universal construction. The area reductions for $\mathcal{Q}_{30}^5$, $\mathcal{Q}_{45}^5$, and x^5 over $\mathbb{F}_{2^6}$ are approximately 4.87%, 15.03%, and 32.74%, respectively. The largest relative reduction is obtained for the Bracken-Leander permutation, a reduction of approximately 53.32%. All four proposed shared maps preserve the algebraic degree of their respective target permutations.

For the two power permutations, these favorable results are consistent with the compact structure of the weighted-interpolation construction. The optimal TIs contains $t + 1$ unshared target functions. In contrast, the formula of the universal construction of Piccione et al. [2] contains $2^{t+1} - 2$ nonconstant target functions, excluding the fixed value $F(0)$.

Table 7: Hardware cost of the masked S-boxes in the `NANGATE` 45nm library

Permutation	TI Construction	Shares	Area[GE]	deg($\boldsymbol{F}$)
$\mathcal{Q}_{30}^5$	Piccione et al. [2]	4	102.67	2
	Theorem 5	3	97.67	2
$\mathcal{Q}_{45}^5$	Piccione et al. [2]	4	179.67	2
	Theorem 8	3	152.67	2
x^5 over $\mathbb{F}_{2^6}$	Piccione et al. [2]	4	565.00	2
	Theorem 11	3	380.00	2
Bracken-Leander function x^{73} over $\mathbb{F}_{2^{12}}$	Piccione et al. [2]	5	7559.33	3
	Theorem 11	4	3529.00	3
PRESENT S-box, $\mathcal{C}_{266}^4$	Poschmann et al. [20]	3; 3	228.67	2
	Kutzner et al. [28]	3; 3	190.00	2
	Piccione et al. [2]	5	335.33	3
	Theorem 14	4	998.67	5
Inversion in $\mathbb{F}_{2^4}$, $\mathcal{C}_{282}^4$	Piccione et al. [2]	5	376.67	3
	Theorem 14	4	1321.00	6

The derivative-uniform implementations of PRESENT and inversion exhibit a different trade-off. Their share counts decrease, but their areas increase by approximately 197.82% and 250.70%, respectively, compared with the universal $(t+2)$-share TI construction. Their shared-map algebraic degrees also increase. A potential source of the large area is the direction-dependent transformations from TIs of derivatives to optimal TIs and corrections. This dependence can introduce additional nonlinear terms, and cause higher hardware area. Although those higher algebraic degree terms do not contribute to the correctness of original target function, they may be important for the uniformity of TIs.

The additional PRESENT baselines illustrate the role of decomposition. The implementations based on Poschmann et al. [20] and Kutzner et al. [28] use 3 shares at each of two quadratic S-boxes and require 228.67 and 190.00 GE, respectively. Both are smaller than the direct implementations considered here. This does not contradict the 4-share optimality of our direct PRESENT TI: the 3-share implementations rely on intermediate registers, whereas our construction shares the undecomposed cubic permutation without such registers.

4 Conclusion

In this paper, we investigated the construction of optimal Threshold Implementations for bijective S-boxes. Our objective is to meet the $t+1$ lower bound on the number of shares, while satisfying correctness, non-completeness, and uniformity, without fresh randomness. To this end, we developed four constructions based on identity extensions,

a generalization of existing uniform-sharing constructions, weighted interpolation, and a derivative-uniform framework.

First, we demonstrated how adjoining identity coordinates enables the existence of optimal TIs, and apply this approach to $\mathcal{Q}_{30}^5$. We then provided a common explanation for the 30 five-bit quadratic classes previously reported [24] to admit optimal TIs, and we established optimal TIs for $\mathcal{Q}_{45}^5$. Our investigation further identified 475 six-bit quadratic permutations with optimal TIs. Furthermore, using weighted interpolation, we constructed an infinite family of power permutations admitting optimal TIs, such as differentially 4-uniform Bracken-Leander functions, thereby disproving Conjecture 1. Notably, it is the first time to construct optimal TIs for differentially 4-uniform permutations. The derivative-uniform framework is of interest and exhibits somewhat paradoxical properties. It gives the existence of optimal TIs for certain permutations, however, it does not preserve the algebraic degree, and the direction-dependent TI incurs a high implementation cost. Nevertheless, using this framework, we successfully proved that every 4-bit cubic permutation admits optimal TIs. Together, our result expand the known classes of quadratic and cubic permutations with optimal TIs, see Table 1.

While differentially 4-uniform permutations are now known to admit optimal TIs, it remains an open question whether APN permutations and APN functions also admit them. To date, the only known APN permutation whose optimal TI status is fully determined is x^3 over $\mathbb{F}_2^3$, and we even do not know any APN functions with optimal TIs in $\mathbb{F}_2^4$. Based on existing literature [23, 24, 27] and our result, we believe that high algebraic degree, e.g., cubic, and a large number of variables make the optimal TIs for APN permutations or APN functions possible.

Declaration of Generative AI Usage.

During the preparation of this manuscript, the authors used ChatGPT (OpenAI) and Gemini (Google) to conduct computational experiments, to derive explicit optimal TI expressions from completed theoretical proofs, and to polish the English language and readability. The authors reviewed and verified all content and take full responsibility for the content and results of this work.

Note on Concurrent and Independent Work

Concurrently with and independently of this work, Piccione et al. [40] studied closely related questions regarding optimal TIs. While both papers establish the existence of optimal TIs for 4-bit cubic and 5-bit quadratic permutations, and triangular/conditional-uniform construction, investigate matrix-based, (projective) interpolation-based, and derivative-based constructions, the two works offer complementary perspectives and distinct contributions. Their work develops degree-controlled optimal TI algorithmic constructions, formulates a commutative algebra matrix criterion, an interpolation condition for $q \geq t+1$. Their work covers a broader 5-bit quadratic classes alongside $\mathcal{Q}_{300}^4$ and 45 five-bit cubic classes, and provides full-cipher hardware implementations. Conversely, our work focuses on analytical existence proofs of 4-bit cubic permutations,

structural constructions (such as for Q_{30}^5, Q_{45}^5, $G(x)+vf(x)$ and $L(x)+f(x)x$), general bounds on additional identity coordinates, and 6-bit quadratic classifications.

Appendix A An optimal TI of $\mathcal{Q}_{30}^5$

Assume $\mathcal{Q}_{30}^5(x) = (F_1, \ldots, F_5)$ with $x = (x_1, x_2, \ldots, x_5) \in \mathbb{F}_2^5$ and

$$\begin{cases} F_1(x) = x_1 \\ F_2(x) = x_2 \\ F_3(x) = x_3 \oplus x_5 \oplus x_3x_4 \\ F_4(x) = x_4 \oplus x_5 \oplus x_3x_4 \oplus x_4x_5 \\ F_5(x) = x_3x_4 \oplus x_3x_5 \oplus x_4x_5, \end{cases}$$

then one of optimal TIs $\boldsymbol{F} = (F^{(1)}, F^{(2)}, F^{(3)})$ is

$$\begin{cases} F_1^{(1)} = x_1^{(2)} \oplus x_5^{(2)} \oplus x_2^{(3)}x_5^{(3)}, \\ F_2^{(1)} = x_2^{(2)} \oplus x_2^{(3)}, \\ F_3^{(1)} = x_3^{(2)} \oplus x_5^{(2)} \oplus x_2^{(3)} \oplus x_3^{(2)}x_4^{(2)} \oplus x_3^{(2)}x_4^{(3)} \oplus x_4^{(2)}x_3^{(3)} \oplus x_1^{(3)}x_5^{(3)} \oplus x_2^{(3)}x_5^{(3)} \oplus x_4^{(3)}x_5^{(3)}, \\ F_4^{(1)} = x_5^{(2)} \oplus x_2^{(3)} \oplus x_3^{(2)}x_4^{(2)} \oplus x_3^{(2)}x_4^{(3)} \oplus x_4^{(2)}x_3^{(3)} \oplus x_4^{(2)}x_5^{(3)} \oplus x_5^{(2)}x_4^{(3)} \oplus x_1^{(3)}x_5^{(3)} \oplus x_2^{(3)}x_5^{(3)}, \\ F_5^{(1)} = x_2^{(3)} \oplus x_4^{(3)} \oplus x_3^{(2)}x_4^{(2)} \oplus x_3^{(2)}x_4^{(3)} \oplus x_3^{(2)}x_5^{(3)} \oplus x_4^{(2)}x_5^{(2)} \oplus x_4^{(2)}x_3^{(3)} \oplus x_4^{(2)}x_5^{(3)} \oplus x_5^{(2)}x_3^{(3)} \\ \qquad\qquad \oplus x_5^{(2)}x_4^{(3)} \oplus x_1^{(3)}x_5^{(3)} \oplus x_2^{(3)}x_5^{(3)}, \end{cases}$$

$$\begin{cases} F_1^{(2)} = x_1^{(1)} \oplus x_1^{(3)} \oplus x_2^{(3)}x_5^{(3)}, \\ F_2^{(2)} = x_5^{(1)}, \\ F_3^{(2)} = x_1^{(1)} \oplus x_2^{(3)} \oplus x_3^{(3)} \oplus x_5^{(3)} \oplus x_3^{(1)}x_4^{(3)} \oplus x_4^{(1)}x_3^{(3)} \oplus x_1^{(3)}x_5^{(3)} \oplus x_2^{(3)}x_5^{(3)} \oplus x_3^{(3)}x_4^{(3)} \oplus x_4^{(3)}x_5^{(3)}, \\ F_4^{(2)} = x_1^{(1)} \oplus x_2^{(3)} \oplus x_4^{(3)} \oplus x_5^{(3)} \oplus x_3^{(1)}x_4^{(3)} \oplus x_4^{(1)}x_3^{(3)} \oplus x_4^{(1)}x_5^{(3)} \oplus x_5^{(1)}x_4^{(3)} \oplus x_1^{(3)}x_5^{(3)} \oplus x_2^{(3)}x_5^{(3)} \\ \qquad\qquad \oplus x_3^{(3)}x_4^{(3)} \oplus x_4^{(3)}x_5^{(3)}, \\ F_5^{(2)} = x_1^{(1)} \oplus x_3^{(1)} \oplus x_4^{(1)} \oplus x_2^{(3)} \oplus x_4^{(3)} \oplus x_3^{(1)}x_4^{(3)} \oplus x_3^{(1)}x_5^{(3)} \oplus x_4^{(1)}x_3^{(3)} \oplus x_4^{(1)}x_5^{(3)} \oplus x_5^{(1)}x_3^{(3)} \\ \qquad\qquad \oplus x_5^{(1)}x_4^{(3)} \oplus x_1^{(3)}x_5^{(3)} \oplus x_2^{(3)}x_5^{(3)} \oplus x_3^{(3)}x_4^{(3)} \oplus x_3^{(3)}x_5^{(3)} \oplus x_4^{(3)}x_5^{(3)}, \end{cases}$$

$$
\begin{cases}
F_1^{(3)} = x_5^{(2)}, \\
F_2^{(3)} = x_2^{(1)} \oplus x_5^{(1)}, \\
F_3^{(3)} = x_1^{(1)} \oplus x_3^{(1)} \oplus x_5^{(1)} \oplus x_3^{(1)}x_4^{(1)} \oplus x_3^{(1)}x_4^{(2)} \oplus x_4^{(1)}x_3^{(2)}, \\
F_4^{(3)} = x_1^{(1)} \oplus x_4^{(1)} \oplus x_5^{(1)} \oplus x_4^{(2)} \oplus x_3^{(1)}x_4^{(1)} \oplus x_3^{(1)}x_4^{(2)} \oplus x_4^{(1)}x_5^{(1)} \oplus x_4^{(1)}x_3^{(2)} \oplus x_4^{(1)}x_5^{(2)} \\
\qquad\qquad \oplus x_5^{(1)}x_4^{(2)} \oplus x_4^{(2)}x_5^{(2)}, \\
F_5^{(3)} = x_1^{(1)} \oplus x_3^{(1)} \oplus x_4^{(1)} \oplus x_3^{(1)}x_4^{(1)} \oplus x_3^{(1)}x_5^{(1)} \oplus x_3^{(1)}x_4^{(2)} \oplus x_3^{(1)}x_5^{(2)} \oplus x_4^{(1)}x_5^{(1)} \oplus x_4^{(1)}x_3^{(2)} \\
\qquad\qquad \oplus x_4^{(1)}x_5^{(2)} \oplus x_5^{(1)}x_3^{(2)} \oplus x_5^{(1)}x_4^{(2)} \oplus x_3^{(2)}x_5^{(2)},
\end{cases}
$$

where $(x_1^{(i)}, x_2^{(i)}, \ldots, x_5^{(i)})$ is i-th sharing of x.

Appendix B Supplementary proofs

B.1 Proof of Corollary 4

Proof Choose $0 \neq e \in \ker(L)$, let $P \in \mathrm{GL}(n,2)$ be the corresponding change-of-basis matrix, so that the first basis vector is e. Consider the linearly equivalent function $F' = (P^{-1} \times I_m) \circ F \circ (P \times I_m)$. Writing $x = P(u,w)$ with $(u,w) \in \mathbb{F}_2 \times \mathbb{F}_2^{n-1}$, we then have

$$F'(u,w,y) = \left((u,w) + \lambda(y)L'(u,w) + H'(y), G(y)\right),$$

where $L' = P^{-1}LP$ and $H' = P^{-1}H$. Since $L(x)$ depends only on w, i.e., $L(x) = L(u,w) = (L_1(w), L_2(w)) \in \mathbb{F}_2 \times \mathbb{F}_2^{n-1}$, and we can also write $H(y) = (H_1(y), H_2(y))$. Thus,

$$F'(u,w,y) = (u + \lambda(y)L_1(w) + H_1(y), w + \lambda(y)L_2(w) + H_2(y), G(y)).$$

Set $z = (w,y) \in \mathbb{F}_2^{n-1+m}$, and define

$$\widetilde{H}(z) = \widetilde{H}(w,y) = \lambda(y)L_1(w) + H_1(y),$$
$$\widetilde{G}(z) = \widetilde{G}(w,y) = \left(w + \lambda(y)L_2(w) + H_2(y), G(y)\right),$$

then

$$F'(u,z) = \left(u + \widetilde{H}(z), \widetilde{G}(z)\right).$$

Since F' is linearly equivalent to F, the claim follows. □

B.2 Proof of Corollary 5

Proof We have $F_L(x,y) = \begin{cases} (x,0), & y = 0, \\ ((L+I)x, 1), & y = 1, \end{cases}$ and similarly for $F_{L'}$.

Suppose first that $L' + I = P^{-1}(L+I)P$. The affine permutations $S(x,y) = (Px, y)$ and $T(u,v) = (P^{-1}u, v)$ satisfying $F_{L'} = T \circ F \circ S$. Then, suppose that $L' + I = P^{-1}(L+I)^{-1}P$. Define $S(x,y) = (Px, y+1)$ and $T(u,v) = (P^{-1}(L+I)^{-1}u, v+1)$, thus, $F_{L'} = T \circ F_L \circ S$ also in this case.

On the contrary, suppose that F_L is affine on another affine hyperplane $U = w + W$. Define $H_i = \{(x,i) : x \in \mathbb{F}_2^n\}$ with $i = 0, 1$. Since $U \notin \{H_0, H_1\}$, we have $W \neq H_0$. Therefore, the projection of W onto the last coordinate is surjective, and $\dim(W \cap H_0) = n - 1 \geq 1$. Thus, there exist $(a,0) \in W \cap H_0$, for some $a \neq 0$, and $(b,1) \in W$. Consider the bilinear form of F_L, we have

$$\beta_{F_L}((a,\alpha),(b,\gamma)) = (\alpha Lb + \gamma La, 0),$$

and then

$$\beta_{F_L}((a,0),(b,1)) = (La,0) \neq 0.$$

Since F_L is quadratic, for every $u, v \in W$,

$$\beta_{F_L}(u,v) = F_L(w+u+v) + F_L(w+u) + F_L(w+v) + F_L(w) = 0,$$

a contradiction. This proves that H_0 and H_1 are the only affine hyperplanes on which F_L is affine. Now assume that $F_{L'} = T \circ F_L \circ S$ for affine permutations S, T. Since $F_{L'}$ is affine on H_0 and H_1, the function F_L must be affine on each of the affine hyperplanes $S(H_0)$ and $S(H_1)$. Then,

$$S(\{H_0, H_1\}) = \{H_0, H_1\},$$

thus, we have $S(H_i) = H_{i+c}$ for some $c \in \mathbb{F}_2$. Furthermore, F_L and $F_{L'}$ each map H_i bijectively onto itself. Hence $T(H_{i+c}) = T(F_L(S(H_i))) = F_{L'}(H_i) = H_i$, which means T preserves the two hyperplanes when $c = 0$ and interchanges them otherwise. Therefore S and T must have the form

$$S(x,y) = (Px + yp + a, y + c),$$
$$T(u,v) = (Qu + vq + b, v + c),$$

where $P, Q \in \mathrm{GL}(n,2), p, q, a, b \in \mathbb{F}_2^n$ and $c \in \mathbb{F}_2$. There are two cases.

(1) $c = 0$, then $T \circ F_L \circ S(x,0) = (QPx + Qa + b, 0)$ and $F_{L'}(x,0) = (x,0)$ force $QP = I_n$. With the same method for $(x,1)$, we get $T((L+I)(Px+p+a)) = ((L'+I)x, 1)$, which gives $Q(L+I)P = L' + I$.

(2) We can obtain $L' + I = P^{-1}(L+I)^{-1}P$ for the case of $c = 1$ with the same reason.

□

B.3 Proof of Corollary 6

Proof Since every 2-bit permutation is affine, we can assume $G(y_1, y_2) = (y_1, y_2)$ and $\lambda(y) = y_2$. Then the affine terms of $H(y_1, y_2) = h_0 + y_1h_1 + y_2h_2 + y_1y_2h_{12}$ can be removed by an affine transform of the output. Thus, every functions in $(n,2)$ decomposition can be affine equivalent to $F(x, y_1, y_2) = (x + y_2L(x) + y_1y_2h_{12}, y_1, y_2)$. By grouping $x = (x, y_1)$, this becomes $F(x, y_2) = \left(x + y_2\widetilde{L}(x), y_2\right)$ with $\widetilde{L}(x) = \widetilde{L}(x, y_1) = (L(x) + y_1h_{12}, 0)$. Hence $\mathrm{rank}(\widetilde{L}) \leq n < n+1$, and therefore, such functions can be reduced to the form $\left(u + \widetilde{H}(v), \widetilde{G}(v)\right)$ by Corollary 4, as $\ker(\widetilde{L}) \neq 0$. □

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] 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

[4] 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)

[5] 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

[6] 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

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

[8] Mangard, S., Popp, T., Gammel, B.M.: Side-channel leakage of masked cmos gates. In: Cryptographers' Track at the RSA Conference, pp. 351–365 (2005). Springer

[9] Suzuki, D., Saeki, M., Ichikawa, T.: Random switching logic: A countermeasure against dpa based on transition probability. Cryptology ePrint Archive (2004)

[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] 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

[12] 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

[13] 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

[14] 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

[15] 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

[16] 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)

[17] 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

[18] 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

[19] 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)

[20] 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

[21] Bilgin, B.: Threshold implementations: as countermeasure against higher-order differential power analysis. Phd thesis - research ut, graduation ut, University of Twente, Netherlands (May 2015). https://doi.org/10.3990/1.9789036538916 . Cum laude

[22] 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

[23] 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

[24] 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

[25] 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

[26] 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

[27] 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

[28] 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

[29] 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

[30] 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)

[31] 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)

[32] 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

[33] 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

[34] 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

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

[36] Dobbertin, H.: One-to-one highly nonlinear power functions on gf (2n). Applicable Algebra in Engineering, Communication and Computing **9**(2), 139–152 (1998)

[37] Bracken, C., Leander, G.: A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree. Finite Fields and Their Applications **16**(4), 231–242 (2010)

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

[39] Piccione, E.: Threshold Implementations of Cryptographic Functions Between Finite Abelian Groups. https://eprint.iacr.org/2024/439 Accessed 2024-05-27

[40] Piccione, E., Perehuda, Y., Leander, G., Felke, P.: Optimal Threshold Implementations of all bijective 4-bit S-boxes and new Infinite Families. Cryptology ePrint Archive, Paper 2026/2449 (2026). https://eprint.iacr.org/2026/2449