Modifications of Bijective S-Boxes with Linear Structures

Kaisa Nyberg

Department of Computer Science
Aalto University School of Science, Finland
kaisa.nyberg@aalto.fi

Abstract. Various systematic modifications of vectorial Boolean functions have been used for finding new previously unknown classes of S-boxes with good or even optimal differential uniformity and nonlinearity. In this paper, a new general modification method is given that preserves the bijectivity property of the function in case the inverse of the function admits a linear structure. A previously known construction of such a modification based on bijective Gold functions in odd dimension is a special case of the new method.

1 Introduction

Differential uniformity is one of the most extensively studied cryptographic property of vectorial Boolean functions. By definition, an APN function is differentially δ-uniform with $\delta = 2$, which is the lowest attainable value of δ. Differential uniformity is motivated by differential cryptanalysis: the lower differential uniformity, the smaller probabilities of differentials. Another property of Boolean functions of cryptanalytic interest is nonlinearity, that is, distance from the set of affine functions. An APN function cannot have linear components, but already a 4-uniform vectorial Boolean function can have components with null nonlinearity. An early example of such a phenomenon was achieved by replacing one component of an APN function by all-zero Boolean function [Nyb94].

APN permutations are known to exist in all odd dimensions. Their existence in even dimension is unknown with the exception of dimensions 2 and 4, where no APN permutations exist, and dimension 6, where only one APN permutation has been found so far. In the hunt of new examples, researchers are using various smart heuristics. For example, one can start from a known highly nonlinear permutation and search over its modifications.

Beierle and Leander suggested that a differentially 4-uniform permutation with a linear component could be a good starting point when constructing a 4-uniform 2-1 function, which in turn could be extended to a 4-uniform, or possibly even to an APN permutation [BL20]. Further, they give a construction of a differentially 4-uniform permutation with null linearity. In odd dimension, their construction is based on Gold functions, while in even dimension the starting point is the finite field inversion function.

In this paper, we give a new general construction using which a component of a permutation can be replaced by a linear function while preserving the bijectivity property. The only assumption needed in this construction is that the inverse of the permutation has a component that admits a linear structure. It is well known that the components of Gold functions have linear structures. Interestingly, when applied to the inverse of a Gold function, our construction is identical to the one given by [BL20].

More accurately speaking, our construction for replacing a component by a linear function requires the linear structure to be of type 1. When added to the input, a linear structure of type 1 flips the value of the function. Another type of linear structures are those of type 0, which have no effect to the value of the function when added to the input.
We show that also linear structures of type 0 of the components of the inverse of a permutation can be exploited in constructions of bijective modifications of the permutation. In that case, the modification is done by adding a linear function to a component of the permutation in which case the nonlinearity remains unchanged.
These constructions are based on the known properties of the support of the Walsh transform of a Boolean function with a linear structure.

Outline. We start by introducing the necessary notation and definitions in Section 2. In Section 3 we recall the properties of the Walsh transform of a Boolean function admitting a linear structure. A linear structure gives rise to a specific involution as will be shown in Section 4. Our general construction of the bijective modifications of S-Boxes is given in Section 5 followed by an application to Gold functions in Section 6 and conclusions in Section 7.

2 Linear Structures

We consider the vector space $\mathbb{F}_2^n$ of dimension n over $\mathbb{F}_2$ where n is a positive intger. A vector $x \in \mathbb{F}_2^n$ can be represented as an n-tuple $x = (x_1, \dots, x_n)$ of coordinates $x_i \in \mathbb{F}_2$, $i = 1, \dots, n$. For two vectors $x = (x_1, \dots, x_n) \in \mathbb{F}_2^n$ and $y = (y_1, \dots, y_n) \in \mathbb{F}_2^n$ we define an inner product denoted as $x \cdot y$ by setting

$$x \cdot y = x_1 y_1 \oplus \cdots \oplus x_n y_n.$$

We denote by '$\oplus$' the addition in $\mathbb{F}_2^n$, while we omit a product sign when denoting multiplication by an element in $\mathbb{F}_2$. The zero element in $\mathbb{F}_2^n$ is denoted by 0_n, where the subscript is omitted if $n = 1$.
Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. Then f is said to have a linear structure if there is a vector $w \in \mathbb{F}_2^n$, $w \neq 0_n$, such that

$$f(x \oplus w) \oplus f(x) = \delta, \text{ for all } x \in \mathbb{F}_2^n,$$

where $\delta \in \mathbb{F}_2$ is a constant [MS89]. Then we say that w is a linear structure of type δ of f. Let us denote by W a complemented subspace of $\{0, w\}$. Then $\mathbb{F}_2^n = \{0, w\} \oplus W$ and any $x \in \mathbb{F}_2^n$ has a unique expression of the form $x = u \oplus v$, where $u \in \{0, w\}$ and $v \in W$. Then the function f can be written as

$$f(x) = f(u \oplus v) = \lambda \cdot u \oplus g(v), \tag{1}$$

for a suitable $\lambda \in \mathbb{F}_2^n$ and a Boolean function $g : \mathbb{F}_2^n \to \mathbb{F}_2$, which is independent of the part $u \in \{0, w\}$ of the input $x \in \mathbb{F}_2^n$, see e.g. [Car21]. On the other hand, a Boolean function of the form (1) has a linear structure w, and moreover, $f(x) \oplus f(x \oplus w) = \lambda \cdot w$, for all $x \in \mathbb{F}_2^n$ meaning that the type of the linear structure is determined by $\lambda \cdot w$. The vector λ in the representation is not unique as any λ satisfying $\lambda \cdot w = \delta$ can be used there. In particular, we can choose $\lambda = 0$ for type 0 linear structure. The function g is not unique either and depends on the choice of the complemented subspace W of $\{0, w\}$.

3 Balancedness and Linear Structures

A Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is said to be balanced if the size of its support is equal to 2^{n-1}. This is equivalent to saying that the Walsh transform of f at 0_n is equal to 0. All non-constant linear functions are balanced, and therefore, any function f of the form (1) is balanced if $\lambda \cdot w = 1$. The following result is a straightforward consequence of this property.

Proposition 1. *Suppose that a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ has a linear structure w. Let $\gamma \in \mathbb{F}_2^n$ and assume that one of the following two conditions holds:*

1. *w is of type 0 and $\gamma \cdot w = 1$, or*
2. *w is of type 1 and $\gamma \cdot w = 0$.*

Then the function $x \mapsto f(x) \oplus \gamma \cdot x$ is balanced.

Proof. Let us express the function f in the form (1). Then

$$f(x) \oplus \gamma \cdot x = (\lambda \oplus \gamma) \cdot u \oplus (g(v) \oplus \gamma \cdot v),$$

from where we see that $x \mapsto f(x) \oplus \gamma \cdot x$ is balanced if $(\lambda \oplus \gamma) \cdot w = 1$. Both conditions 1 or 2 make this happen. □

Recalling that the value of the Walsh transform of $x \mapsto f(x) \oplus \gamma \cdot x$ at 0_n is equal to the value of the Walsh transform of f at γ we see that the following result can also be derived from Proposition 29 of [Car21].

Corollary 1. *Suppose that a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ has a linear structure w. Then the following statements hold:*

1. *w is of type 0 if and only if the function $x \mapsto f(x) \oplus \gamma \cdot x$ is balanced for all γ such that $\gamma \cdot w = 1$.*
2. *w is of type 1 if and only if the function $x \mapsto f(x) \oplus \gamma \cdot x$ is balanced for all γ such that $\gamma \cdot w = 0$.*

Proof. The "only if" parts of the statements are given by Proposition 1. Let us assume now that the function $x \mapsto f(x) \oplus \gamma \cdot x$ is balanced for all γ such that $\gamma \cdot w = 1$. If then w is of type 1, it follows by Proposition 1 that this function is balanced also for all γ such that $\gamma \cdot w = 1$, that is, for all $\gamma \in \mathbb{F}_2^n$, which is impossible by Parseval's theorem. It follows that w is of type 0 as claimed. The proof of the "if" part of the second statement is analogical. □

4 Permutations Related To Linear Structures

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a vectorial Boolean function. Given a vector $\beta \in \mathbb{F}_2^m$, $\beta \neq 0$, we define a component of F as the Boolean function

$$x \mapsto \beta \cdot F(x), \; x \in \mathbb{F}_2^n,$$

and denote this function by $\beta \cdot F$.

A vectorial Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ is a permutation (bijection) if and only if all its components are balanced. For a proof of this known fact, see e.g. [Nyb94], Appendix.

Given a non-zero vector $w \in \mathbb{F}_2^n$, the orthogonal complement of $\{0, w\}$, denoted as $w^\perp$, is a vector subspace of $\mathbb{F}_2^n$ of dimension $n - 1$ consisting of all $x \in \mathbb{F}_2^n$ such that $w \cdot x = 0$. Assume that we have a function $\pi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ such that all its components $\gamma \cdot \pi$ are given, where $\gamma \in w^\perp$. Then it suffices to give one component of π, say $\alpha \cdot \pi$, where $\alpha \cdot w = 1$ to determine the entire function $\pi : \mathbb{F}_2^n \to \mathbb{F}_2^n$. We use this approach for two alternative constructions of a permutation related to a linear structure of a Boolean function.

Theorem 1. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function with a linear structure w. We define a function $\pi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ by setting*

$$(\gamma \cdot \pi)(x) = \gamma \cdot x, \; x \in \mathbb{F}_2^n,$$

for all $\gamma \in w^\perp$. The remaining components are defined by first fixing an $\alpha \notin w^\perp$, that is, $\alpha \cdot w = 1$.

1. *If w is of type 0, we set*

$$\alpha \cdot \pi(x) = f(x) \oplus \alpha \cdot x,\ x \in \mathbb{F}_2^n.$$

2. *If w is of type 1, we set*

$$\alpha \cdot \pi(x) = f(x),\ x \in \mathbb{F}_2^n.$$

Then π is a permutation.

Proof. In the second case, as follows from Proposition 1, the Boolean function $x \mapsto f(x) \oplus \gamma \cdot x$ is balanced for all $\gamma \in w^\perp$. Then all components of π are balanced, and hence, π is a bijection.
In the first case, we observe that w is a linear structure of type 1 of the function $x \mapsto f(x) \oplus \alpha \cdot x$, and then apply the result of the second case to this function. □

Corollary 2. *In the context of Theorem 1, the permutation π has the following representations:*

1. $\pi(x) = x \oplus f(x)w$, *if w is of type 0, or*
2. $\pi(x) = x \oplus (\alpha \cdot x \oplus f(x))\, w$, *if w is of type 1.*

The permutation π is not only a permutation but an involution. To see this, let us first prove the following property.

Lemma 1. *Let w be a linear structure of type δ of a Boolean function f, $\alpha \in \mathbb{F}_2^n$ satisfying $\alpha \cdot w = 1$, and π the permutation constructed as in Theorem 1. Then*

$$f(\pi(x)) = \begin{cases} f(x), & \text{if } \delta = 0, \\ \alpha \cdot x, & \text{if } \delta = 1. \end{cases}$$

Proof. If $\delta = 0$, then

$$f(\pi(x)) = f(x \oplus f(x)w) = \begin{cases} f(x), & \text{if } f(x) = 0, \\ f(x \oplus w) = f(x), & \text{if } f(x) = 1. \end{cases}$$

If $\delta = 1$, then

$$f(\pi(x)) = f\left(x \oplus (\alpha \cdot x \oplus f(x))w\right) \begin{cases} f(x), & \text{if } \alpha \cdot x \oplus f(x) = 0, \\ f(x \oplus w) = f(x) \oplus 1, & \text{if } \alpha \cdot x \oplus f(x) = 1, \end{cases}$$

from where we see that the equality $f(\pi(x)) = \alpha \cdot x$ holds for all x. □

Corollary 3. *In the context of Theorem 1, the permutation π is an involution.*

Proof. If the linear structure is of type 0, then by Lemma 1 and Corollary 2 we get

$$\pi\left(\pi(x)\right) = \pi(x) \oplus f(\pi(x))w = x \oplus f(x)w \oplus f(x)w = x.$$

If the linear structure is of type 1, we get similarly as above and recalling $\alpha \cdot \pi = f$ that

$$\begin{aligned} \pi\left(\pi(x)\right) &= \pi(x) \oplus \left(\alpha \cdot \pi(x) \oplus f\left(\pi(x)\right)\right) \\ &= x \oplus \left(\alpha \cdot x \oplus f(x)\right) w \oplus \left(\alpha \cdot \pi(x) \oplus \alpha \cdot x\right) w = x. \end{aligned}$$

□

5 Modification of S-Boxes

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a bijective S-box. Let us assume that one of its components, say $\beta \cdot F$, has a linear structure of type 1 and let us construct the permutation π for this Boolean function. Then one component of π equals $\beta \cdot F$ meaning that one component of $\pi \circ F^{-1}$ is linear. By the construction of π we also see that 2^{n-1} other components of $\pi \circ F^{-1}$ are just components of F^{-1}. In this way, we obtain a bijective modification of F^{-1} where one component has been replaced by a linear function. For a linear structure of type 0 the corresponding replacement does not give a linear function. We state the result as the following theorem.

Theorem 2. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a bijective vectorial Boolean function and assume that one of its components, say $\beta \cdot F$ has a linear structure w. Let $\alpha \in \mathbb{F}_2^n$ be such that $\alpha \cdot w = 1$. Then F^{-1} can be modified in such a way that the changed function is a bijection by replacing the component $\alpha \cdot F^{-1}$*

1. *by the function $x \mapsto \alpha \cdot F^{-1}(x) \oplus \beta \cdot x$, if the linear structure w is of type 0, or*
2. *by the linear function $x \mapsto \beta \cdot x$, if the linear structure w is of type 1.*

Proof. Let us recall the constructions of a bijective function π given in Theorem 1 and apply them to the Boolean function $f = \beta \cdot F$ and the given α. Since in both cases π is bijective, also $\pi \circ F^{-1}$ is bijective. We also observe that $\gamma \cdot \left(\pi \circ F^{-1}\right) = \gamma \cdot F^{-1}$ for all $\gamma \in w^{\perp}$. So those components of F^{-1} remain unchanged. Let us now consider the component $\alpha \cdot F^{-1}$.

1. If the linear structure w of $\beta \cdot F$ is of type 0, then

$$\begin{aligned}\alpha \cdot \left(\pi \circ F^{-1}\right)(x) &= \beta \cdot F\left(F^{-1}(x)\right) \oplus \alpha \cdot F^{-1}(x) \\ &= \beta \cdot x \oplus \alpha \cdot F^{-1}(x),\end{aligned}$$

   for all $x \in \mathbb{F}_2^n$.

2. If the linear structure w of $\beta \cdot F$ is of type 1, then

$$\alpha \cdot \left(\pi \circ F^{-1}\right)(x) = \beta \cdot F\left(F^{-1}(x)\right) = \beta \cdot x,$$

   for all $x \in \mathbb{F}_2^n$.

Hence in both cases, the composition $\pi \circ F^{-1}$ gives the claimed bijective modification of F^{-1}. □

Recalling that π is an involution we get the following corollary.

Corollary 4. *In the context of Theorem 2 we have*

$$\left(\pi \circ F^{-1}\right)^{-1} = F \circ \pi.$$

This gives a modification of the original permutation F. By Lemma 1, the component $\beta \cdot (F \circ \pi)$ of this modification is equal to $\beta \cdot F$ if the linear structure is of type 0, that is, this component remains unchanged, while in the case of type 1 we have

$$\beta \cdot (F \circ \pi)(x) = \alpha \cdot x,$$

for all $x \in \mathbb{F}_2^n$, that is, this component of F is changed to a linear function.

6 Application to APN Gold Functions

Let $\mathbb{F}_{2^n}$ be an extension field of $\mathbb{F}_2$ of dimension n. The absolute trace function $\mathrm{Tr} : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is then defined as

$$\mathrm{Tr}(x) = x + x^2 + x^{2^2} + \cdots + x^{2^{n-1}},\ x \in \mathbb{F}_{2^n}.$$

The trace function is a linear function, and any linear function $L : \mathbb{F}_{2^n} \to \mathbb{F}_2$ can be given in a form

$$L(x) = \mathrm{Tr}(\omega x), \text{ where } \omega \in \mathbb{F}_{2^n}.$$

The identification $(\mathbb{F}_2^n, \oplus) = (\mathbb{F}_{2^n}, +)$ induces a linear space structure to $\mathbb{F}_{2^n}$. Using a suitable linear isomorphism the identification of vectors in $\mathbb{F}_2^n$ and field elements in $\mathbb{F}_{2^n}$ can be done in such a way that

$$x \cdot y = \mathrm{Tr}(xy),\ \ x, y \in \mathbb{F}_{2^n} = \mathbb{F}_2^n,$$

where we omit a product sign for field multiplication.
The power monomials $x \mapsto x^{2^i+1}$, $x \in \mathbb{F}_{2^n}$, where i is a positive integer, are known as Gold functions. Gold functions are differentially 2^s-uniform, where $s = \gcd(i, n)$, and permutations if and only if n/s is odd [Gol68, Nyb93]. The nonlinearity of a Gold function is equal to

$$2^{n-1} - 2^{\frac{n+s}{2}-1},$$

and its algebraic degree is equal to 2.
Let us denote by F the Gold function $x \mapsto x^{2^i+1}$ with n/s odd. Then the inverse F^{-1} is also a power permutation with the exponent $d = (2^i + 1)^{-1}$. The inverse F^{-1} has the same differential uniformity and nonlinearity as F. Its algebraic degree is equal to the Hamming weight of the binary representation of d which in general is higher than 2.
Beierle and Leander studied Gold functions with $s = 1$ and n odd. They showed that the inverse of such a Gold function, which is APN and has high nonlinearity, can be modified by replacing one component by a linear function in such a way that the resulting modification is also a permutation [BL20]. In such a modification, in general, the differential unifomity is at most doubled, see e.g. [Nyb94], and in the APN case, strictly doubled to become 4. Since the algebraic degree of all components is the same, lowering the degree of one component does not change the algebraic degree. As a result, they obtained an example of a permutation with differential uniformity 4, high algebraic degree, and null nonlinearity.
Using the notation of [BL20] this construction is given as

$$G_{\alpha,d} : x \mapsto x^d + \mathrm{Tr}\left(\alpha x^d + x\right),$$

where $\alpha \in \mathbb{F}_{2^n}$ is any element with $\mathrm{Tr}(\alpha) = 1$. To prove that $G_{\alpha,d}$ is a bijection, they express $G_{\alpha,d}(x)$ as $G'_{\alpha,d}(x^d)$ where

$$G'_{\alpha,d}(x) = x + \mathrm{Tr}\left(\alpha x + x^{2^i+1}\right),$$

and show that $G'_{\alpha,d}$ is an involution and hence a permutation.
Next we show that this result, with an identical construction of the modification, can be obtained by application of Theorem 2.
It is easy to see that the component $x \mapsto \mathrm{Tr}(F(x))$ has a linear structure $w = 1$ of type 1. Indeed,

$$(x+1)^{2^i+1} + x^{2^i+1} = x^{2^i} + x + 1,$$

which has the absolute trace $\mathrm{Tr}(1) = 1$ for all $x \in \mathbb{F}_{2^n}$ and odd n. We fix an $\alpha \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}(\alpha) = 1$. It follows that $\mathrm{Tr}(\alpha w) = \mathrm{Tr}(\alpha) = 1$. Then the permutation π given in Theorem 1 for $f(x) = \mathrm{Tr}(F(x))$ can be expressed as follows

$$\pi(x) = x \oplus (\alpha \cdot x \oplus f(x))\, w = x + (\mathrm{Tr}(\alpha x) + \mathrm{Tr}(F(x)) = x + \mathrm{Tr}\left(\alpha x + F(x)\right)$$

using the representation of π given in Corollary 2. We observe that $\pi = G'_{\alpha,d}$ and conclude that $G_{\alpha,d} = \pi \circ F^{-1}$. Let us also note that the inverse of $G_{\alpha,d}$ gives another example of a differentially 4-uniform permutation with a linear component.

The proof of the bijectivity of the function $G'_{\alpha,d}$ by [BL20] depends heavily on the form of the Gold function and many arithmetical properties of the field $\mathbb{F}_2^n$. Our approach to this modification is more general and works for any permutation from the linear space $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ that has a component with a linear structure. The modification $F \circ \pi$, which can be applied even if F is not a permutation, remains to be studied.

7 Conclusions

In this paper, we presented a new general method of how to modify a component of a permutation from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ using a linear function while preserving bijectivity. This method allows to replace the component by a linear function or to add a linear function to the component depending on the type of the linear structure. Only a linear structure of type 1 allows a modification that changes the nonlinearity of the permutation.

We also showed that the bijective transform, using which the modification of the permutation is done, has appeared already in [BL20] in the context of APN Gold functions in odd dimension. Against this background our main contribution is the discovery of the connection between the existence of linear structures of type 1 and this modification method. This connection also allowed us to generalise the method and extend its applicability beyond bijective APN Gold functions in odd dimension. Note that the modification is independent of the APN property, and when applying it, the differential uniformity is at most doubled. For APN functions, it is strictly doubled, but in general it may remain less. Potential applications to be studied are bijective Gold functions in even dimension, which in the best case are differentially 4-uniform, and more generally, permutations with partially bent components.

Acknowledgements

The author thanks the anonymous reviewers for a number comments that helped to improve the presentation of this work. The author also thanks the members of the Inria team in Paris for discussions, and Léo Perrin, in particular, for observing that π is an involution more generally than only in the case of Gold functions.

References

[BL20] Christof Beierle and Gregor Leander. 4-uniform permutations with null nonlinearity. *Cryptogr. Commun.*, 12(6):1133–1141, 2020.

[Car21] Claude Carlet. *Boolean Functions for Cryptography and Coding Theory.* Cambridge University Press, 2021.

[Gol68] Robert Gold. Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp.). *IEEE Transactions on Information Theory*, 14(1):154–156, 1968.

[MS89] Willi Meier and Othmar Staffelbach. Nonlinearity criteria for cryptographic functions. In Jean-Jacques Quisquater and Joos Vandewalle, editors, *Advances in Cryptology - EUROCRYPT '89, Workshop on the Theory and Application of of Cryptographic Techniques, Houthalen, Belgium, April 10-13, 1989, Proceedings*, volume 434 of *Lecture Notes in Computer Science*, pages 549–562. Springer, 1989.

[Nyb93] Kaisa Nyberg. Differentially uniform mappings for cryptography. In Tor Helleseth, editor, *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, volume 765 of *Lecture Notes in Computer Science*, pages 55–64. Springer, 1993.

[Nyb94] Kaisa Nyberg. S-boxes and round functions with controllable linearity and differential uniformity. In Bart Preneel, editor, *Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings*, volume 1008 of *Lecture Notes in Computer Science*, pages 111–130. Springer, 1994.