Some Examples of New Nonlinearity Preserving Bijective Mappings

İ. Sertkaya, A. Doğanaksoy

***Abstract*—It is well known that the affine equivalency mappings preserve nonlinearity. Aside from the affine equivalency mappings, it is proved that there exist non-affine bijective mappings that act Boolean functions and keep nonlinearity invariant for all Boolean functions. For a fixed Boolean function, the explicitly constructed nonlinearity preserving bijective mappings create the same orbit structure with the affine equivalency mappings. On the other hand, the authors proved the existence of new nonlinearity preserving mappings that do not coincide with affine equivalency mappings based on the nonlinearity distributions. In the pursue of the explicit construction of this new nonlinearity preserving bijective mappings, here we give some examples for 3, 4 and 6 variable Boolean functions. We believe that if a generic construction method will be derived, these mappings would be used as a practical tool for constructing new Boolean function families.**

***Index Terms*—Boolean functions, affine equivalency mappings, nonlinearity preserving mappings.**

I. Introduction

MEIER and Staffelbach proved that nonlinearity is invariant under the action of general affine group AGL_n of degree n over $\mathbb{F}_2$ [1]. Later, by extending the result of [2, p. 417], Preneel proved that affine equivalency mappings $\mathsf{AGL}_n \ltimes \mathscr{A}_n$ also preserve nonlinearity [3].

Searching Boolean functions that possess high cryptographic design criteria values is an ongoing research subject [4], [5]. The aim is to find new families of Boolean functions not equivalent to the existing ones which would lead to obtain better primitives for cryptographic design.

The orbits of the action of $\mathsf{AGL}_n \ltimes \mathscr{A}_n$ on the set of n variable Boolean functions $\mathscr{F}_n$ partitions the set into equivalence classes. These classes are comprised of the functions having the same degree, nonlinearity and frequency distribution of absolute Walsh spectrum values, see [1], [3], for the other properties that also preserved please refer to [6, Section 5.1, p. 81]. Therefore they constitute a practical tool for classifying the Boolean functions into families. When a Boolean function having highly desirable design properties is achieved with either heuristic search or direct construction methods, affine equivalency mappings are used to verify that these new functions does not belong to an existing family.

Since the cardinality of $\mathscr{F}_n$ is 2^{2^n}, the maximal group of bijective mappings that can act on $\mathscr{F}_n$ is the symmetric group $\mathsf{Sym}(\mathscr{F}_n)$ and isomorphically $\mathcal{S}_{2^{2^n}}$. $\mathsf{AGL}_n \ltimes \mathscr{A}_n$ is a proper subgroup of AGL_{2^n} which also a proper subgroup of $\mathcal{S}_{2^{2^n}}$. Commonly, $\mathsf{AGL}_n \ltimes \mathscr{A}_n$ are considered as the only mappings that keep nonlinearity invariant for all Boolean functions. However, the authors explicitly constructed nonlinearity preserving bijective mappings in $\mathsf{AGL}_{2^n} - (\mathsf{AGL}_n \ltimes \mathscr{A}_n)$ and furthermore in $\mathcal{S}_{2^{2^n}} - \mathsf{AGL}_{2^n}$, see [7] and [8]. However given a Boolean function, the orbits of these mappings coincides with $\mathsf{AGL}_n \ltimes \mathscr{A}_n$ [9]. On the other hand, in the same study the authors give the exact number of nonlinearity preserving bijective mappings for $n \leq 6$ and moreover without constructing explicitly, they proved that the existence of new bijective mappings that do not coincide with $\mathsf{AGL}_n \ltimes \mathscr{A}_n$.

Exact classification or enumeration of nonlinearity preserving mappings is still an open problem. The current state of the classification of nonlinearity preserving bijective mappings is illustrated in Figure 1 and for values $n \leq 6$, where nonlinearity distributions is computable, the enumeration of nonlinearity preserving bijective mappings is given in [9].

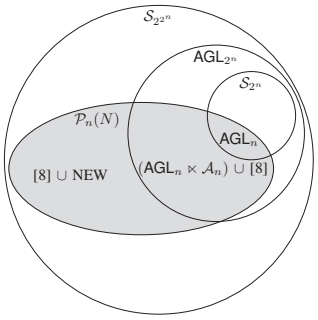

Fig. 1. Current state of nonlinearity preserving bijective transformations. (Here, NEW represents new maps for which the examples given in this work.)

Classification and enumeration of nonlinearity preserving mappings, has both theoretical and practical influences in cryptographic research. Indeed without loosing the satisfied security margins, choosing efficiently implementable Boolean function or if possible maximizing other security margins by using these mappings is a research goal. In this study, in order the clarify these concepts we are constructing some examples for 3, 4 and 6 variable Boolean functions. These examples may not be generic but they emphasize the notions given above. The paper is organized as follows: in Section II we give notations and definitions and in Section III we recall necessary propositions, next we give the examples of new nonlinearity preserving bijective mappings in Section IV and finally Section V concludes the study.

İ. Sertkaya is with the Institute of Applied Mathematics, METU, Ankara, and the Mathematical and Computational Sciences Labs, TÜBİTAK BİLGEM UEKAE, Gebze, Kocaeli, TURKEY e-mail: isa.sertkaya@tubitak.gov.tr

A. Doğanaksoy is with the Institute of Applied Mathematics and the Department of Mathematics, METU, Ankara, TURKEY email: aldoks@metu.edu.tr

Manuscript received July 30; revised September 1, 2014.

II. Preliminaries

Unless otherwise stated explicitly, the following definitions and notions are given regarding [10], [11].

Let $\mathbb{F}_2^n$ be the n-dimensional $\mathbb{F}_2-$ vector space admitting the usual *lexicographical* ordering as follows: for any $\alpha, \beta \in \mathbb{F}_2^n$, $\alpha < \beta$ if and only if there exists $i \in \{1, 2, \ldots, n\}$, such that $a_1 = b_1, \ldots, a_{i-1} = b_{i-1}$ and $a_i < b_i$. According to this ordering we label each element of $\mathbb{F}_2^n$ as

$$\alpha_0 = (0, 0, \ldots, 0) < \alpha_1 < \alpha_2 < \ldots < \alpha_{2^n-1} = (1, 1, \ldots, 1),$$

and we denote $n \times 1$ vectors by $[\alpha] = (a_1, a_2, \ldots, a_n)^t$.

Any function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is called a *Boolean function* and can be represented uniquely by

- the corresponding *truth table* given by

$$T_f = (f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{2^n-1})),$$

  where T_f is lexicographically ordered, or equivalently,
- the corresponding *algebraic normal form* that is the multivariate polynomial over $\mathbb{F}_2$ given by

$$\begin{aligned} f(x_n, x_{n-1}, \ldots, x_1) = c_0 &\oplus c_1 x_1 \oplus \cdots \oplus c_n x_n \\ &\oplus c_{12} x_1 x_2 \oplus \cdots \\ &\oplus c_{123} x_1 x_2 x_3 \oplus \cdots \\ &\vdots \\ &\oplus c_{12\ldots n} x_1 x_2 \cdots x_n. \end{aligned} \tag{1}$$

The set of all Boolean functions defined on $\mathbb{F}_2^n$ is denoted by $\mathscr{F}_n$. The *degree* $deg(f)$ of f is the degree of its algebraic normal form, i.e. the number of variables in the highest order term with nonzero coefficient. If $deg(f) \leq 1$ then f is called *affine*, i.e., it is of the form $f(x_n, x_{n-1}, \ldots, x_1) = \langle c, x \rangle \oplus c_0$, where $c_0 \in \mathbb{F}_2$ and $\langle c, x \rangle = c_1 x_1 \oplus \cdots \oplus c_n x_n$ is the *standard inner product* with $x, c \in \mathbb{F}_2^n$. The set of all affine Boolean functions on $\mathbb{F}_2^n$ is denoted by $\mathscr{A}_n$, where each function in $\mathscr{A}_n$ will be given by

$$\ell_{(\alpha_i, a)} : x \mapsto \langle x, \alpha_i \rangle \oplus a.$$

For a given function f, the *Hamming weight* $w(f)$ is given as usual as the number of ones in T_f. The set $Sup(f) := \{\alpha \in \mathbb{F}_2^n \mid f(\alpha) = 1\}$ is called the *support* of the function f. For given functions f and g, the *Hamming distance* $d(f, g)$ is the Hamming weight of $f \oplus g$.

The matrices defined over $\mathbb{R}$ and constructed iteratively with the Kronecker product $\otimes$ satisfying

$$H_n = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes H_{n-1} = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix}.$$

are called *Sylvester Hadamard matrices* [12], [13].

The *Walsh transform* $W_f : \mathbb{F}_2^n \to \mathbb{R}$ of a function f is given by

$$W_f(\omega) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \langle x, \omega \rangle}, \text{ for all } \omega \in \mathbb{F}_2^n.$$

The truth table of the Walsh transform

$$W_f := (W_f(\alpha_0), W_f(\alpha_1) \ldots, W_f(\alpha_{2^n-1}))$$

is called the *Walsh Spectrum* of f, and it can be expressed as $W_f = \zeta_f H_n$ (see [14]) where

$$\zeta_f = ((-1)^{f(\alpha_0)}, (-1)^{f(\alpha_1)}, \ldots, (-1)^{f(\alpha_{2^n-1})})$$

is the truth table of the *signed function* $(-1)^{f(x)}$ of f.

Definition 1: [15], [1] The *nonlinearity* N_f of a function f is its distance to the nearest affine function. N_f can be expressed with the Walsh transform of f as follows:

$$N_f = \min_{\ell_{(\beta,a)} \in \mathcal{A}_n} d(f, \ell_{(\beta,a)}) = 2^{n-1} - \frac{1}{2} \max_{\omega \in \mathbb{F}_2^n} |W_f(\omega)| \quad .$$

A function f is called a *bent function* if $W_f(w) = \pm 2^{n/2}$ for any $w \in \mathbb{F}_2^n$. Bent functions only exist if n is even [16], [17], and form a special set $\mathscr{B}_n$ of Boolean functions attaining maximal nonlinearity for a fixed positive even integer n [1].

III. Nonlinearity Preserving Bijective Mappings

A. Affine equivalency

We start with constructing the group which comprised of affine equivalency mappings.

Definition 2: [18] Let GL_n be the group of all nonsingular matrices of order n over $\mathbb{F}_2$. Let further AGL_n be the group

$$\mathsf{GL}_n \ltimes \mathbb{F}_2^n := \{(A, \alpha) |\ A \in \mathsf{GL}_n,\ \alpha \in \mathbb{F}_2^n\},$$

with respect to the operation $\bullet$. The group law and its inverse are given by

$$\begin{aligned} (A, \alpha) \bullet (A', \alpha') &:= (A'A, \alpha' A + \alpha), \\ (A, \alpha)^{-1} &:= (A^{-1}, \alpha A^{-1}) \end{aligned}$$

for all $(A, \alpha), (A', \alpha') \in \mathsf{AGL}_n$.

Similarly, we define the group

$$\mathsf{AGL}_n \ltimes \mathscr{A}_n := \{(\tau, \ell_{(\beta,a)}) |\ \tau \in \mathsf{AGL}_n,\ \ell_{(\beta,a)} \in \mathscr{A}_n\},$$

which can be given more explicitly as follows:

$$\mathsf{AGL}_n \ltimes \mathscr{A}_n := \{(A, \alpha, \beta, a) \mid A \in \mathsf{GL}_n,\ \alpha, \beta \in \mathbb{F}_2^n,\ a \in \mathbb{F}_2\},$$

where τ and $\ell_{(\beta,a)}$ are given by the mappings $\tau : x \mapsto xA \oplus \alpha$ and $\ell_{(\beta,a)} : x \mapsto \langle x, \beta \rangle \oplus a$.

We have an immediate action of the group $\mathsf{AGL}_n \ltimes \mathscr{A}_n$ on $\mathcal{F}_n$ as follows

$$(A, \alpha, \beta, a) f := f(xA \oplus \alpha) \oplus \langle x, \beta \rangle \oplus a.$$

Two Boolean functions f and g are said to be affine equivalent if and only if for $(A, \alpha, \beta, a) \in \mathsf{AGL}_n \ltimes \mathscr{A}_n$ the following holds

$$f(x) = (A, \alpha, \beta, a) g = g(xA \oplus \alpha) \oplus \langle x, \beta \rangle \oplus a.$$

B. Non-affine Nonlinearity Bijective Preserving Mappings

The truth table of an n-variable Boolean function is an ordered 2^n tuple over $\mathbb{F}_2$. Hence, any bijective mapping acting on such functions can be regarded as a permutation of 2^{2^n} elements. In particular, we can view every bijective mapping as an element of $\mathcal{S}_{2^{2^n}}$.

Let $\psi \in \mathcal{S}_{2^{2^n}}$. We say that ψ preserves nonlinearity if $N_f = N_{\psi f}$ for all $f \in \mathcal{F}_n$. Hence, it follows that ψ preserves nonlinearity if and only if the absolute maximum of the Walsh spectra of f remains invariant, that is

$$\max_{\omega \in \mathbb{F}_2^n} |W_f(\omega)| = \max_{\omega \in \mathbb{F}_2^n} |W_{\psi f}(\omega)| \text{ for all } f \in \mathcal{F}_n.$$

We denote the set of all nonlinearity preserving bijective maps acting on the n-variables Boolean functions by

$$\mathcal{P}_n(N) = \{\psi \in \mathcal{S}_{2^{2^n}} \mid N_f = N_{\psi f} \text{ for all } f \in \mathcal{F}_n\} .$$

In general any mapping $\psi : \mathbb{F}_2^{2^n} \to \mathbb{F}_2^{2^n}$ can be written as

$$\begin{aligned}\psi : (x_1, x_2, x_3, \ldots, x_{2^n}) \mapsto & (\psi_1(x_1, x_2, \ldots, x_{2^n}),\\ & (\psi_2(x_1, x_2, \ldots, x_{2^n}),\\ & \vdots\\ & \psi_{2^n}(x_1, x_2, \ldots, x_{2^n})),\end{aligned}$$

or,

$$\psi : [x] \mapsto \begin{bmatrix} \psi_1(x_1, x_2, \ldots, x_{2^n}) \\ \psi_2(x_1, x_2, \ldots, x_{2^n}) \\ \vdots \\ \psi_{2^n}(x_1, x_2, \ldots, x_{2^n}) \end{bmatrix} , \tag{2}$$

where each $\psi_i : \mathbb{F}_2^{2^n} \to \mathbb{F}_2$ is a 2^n variable Boolean function called *coordinate function* of ψ. Each ψ_i's can be represented by their algebraic normal form uniquely;

$$\begin{aligned}\psi_i(x_1, x_2, \cdots, x_{2^n}) = & c_0^{(i)} \oplus c_1^{(i)} x_1 \oplus \ldots\\ & \oplus c_{12\cdots 2^n}^{(i)} x_1 x_2 \cdots x_{2^n} .\end{aligned} \tag{3}$$

Then, by porting (3) into (2) and re-labeling, we get

$$\begin{aligned}\psi : [x] \mapsto & \underbrace{\begin{bmatrix} c_0^{(1)} \\ c_0^{(2)} \\ \vdots \\ c_0^{(2^n)} \end{bmatrix}}_{[\lambda_0]} \oplus \underbrace{\begin{bmatrix} c_1^{(1)} \\ c_1^{(2)} \\ \vdots \\ c_1^{(2^n)} \end{bmatrix}}_{[\lambda_1]} x_1 \oplus \cdots \oplus\\ & \underbrace{\begin{bmatrix} c_{12}^{(1)} \\ c_{12}^{(2)} \\ \vdots \\ c_{12}^{(2^n)} \end{bmatrix}}_{[\lambda_{12}]} x_1 x_2 \oplus \cdots \oplus \underbrace{\begin{bmatrix} c_{12\cdots 2^n}^{(1)} \\ c_{12\cdots 2^n}^{(2)} \\ \vdots \\ c_{12\cdots 2^n}^{(2^n)} \end{bmatrix}}_{[\lambda_{12\cdots 2^n}]} x_1 x_2 \cdots x_{2^n} ,\end{aligned}$$

and now equivalently we have

$$\begin{aligned}\psi : [x] \mapsto & [\lambda_0] \oplus M[x] \oplus [\lambda_{12}] x_1 x_2 \oplus \cdots\\ & \oplus [\lambda_{123}] x_1 x_2 x_3 \oplus \cdots\\ & \vdots\\ & \oplus [\lambda_{12\cdots 2^n}] x_1 x_2 \cdots x_{2^n}\end{aligned} \tag{4}$$

where

- $x = (x_1, x_2, \ldots, x_{2^n}) \in \mathbb{F}_2^{2^n}$ hence each $x_i \in \mathbb{F}_2$,
- $\lambda_j \in \mathbb{F}_2^{2^n}$ with each $c_j^i \in \mathbb{F}_2$,
- M is the $2^n \times 2^n$ matrix whose column form is $M = [[\lambda_1]\ [\lambda_2]\ \ldots\ [\lambda_{2^n}]]$.

The above representation gives the following classifications.

- $\psi \in \mathsf{AGL}_n \ltimes \mathscr{A}_n$ if
  - $\lambda_0 \in \mathscr{A}_n$ and $M \in \mathcal{S}_{2^n}$ correspond to the permutation matrix representation of an element in AGL_n and
  - $\lambda_j = (0\ 0\ \ldots\ 0)$ for all $j \neq 0, 1, 2, 3, 4, \ldots, 2^n$.
- $\psi \in \mathsf{AGL}_{2^n}$ if
  - $\lambda_0 \in \mathbb{F}_2^{2^n}$ and $M \in \mathsf{GL}_{2^n}$ and
  - $\lambda_j = (0\ 0\ \ldots\ 0)$ for all $j \neq 0, 1, 2, 3, 4, \ldots, 2^n$.
- $\psi \in \mathcal{S}_{2^{2^n}}$ is called *non-affine* if it has at least one non-zero λ_j, for $j \in \{12, 13, \ldots, 12\cdots 2^n\}$.

In truth more detailed but not complete lattice of subgroups of $\mathcal{S}_{2^{2^n}}$ is shown in Fig. 2.

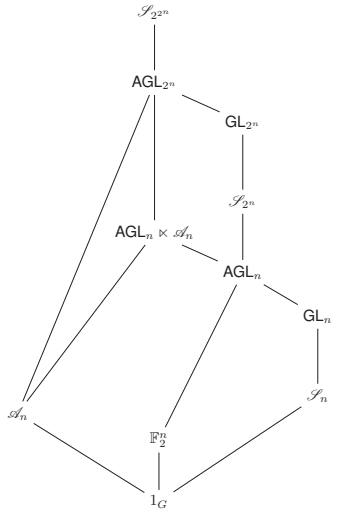

Fig. 2. Lattice of subgroups of $\mathscr{S}_{2^{2^n}}$ (not a complete list)

It is not difficult to see that $\mathsf{AGL}_n \ltimes \mathscr{A}_n \subseteq \mathsf{AGL}_{2^n}$. Furthermore, AGL_{2^n} is as a proper subgroup of $\mathcal{S}_{2^{2^n}}$.

These observations led not only to generalize the action under the larger group AGL_{2^n} (instead of considering the equivalency under $\mathsf{AGL}_n \ltimes \mathscr{A}_n$), but also to prove the existence of new classes of nonlinearity preserving mappings lying in $\mathsf{AGL}_{2^n} \setminus \mathsf{AGL}_n \ltimes \mathscr{A}_n$ [7].

In [8, Proposition 3.8], the existence of nonlinearity preserving non-affine bijective mappings is proved by explicit construction and in [9] it is further proved that even if they are non-affine mappings these mappings actually produce the

same orbit structure as $\mathsf{AGL}_n \ltimes \mathscr{A}_n$ for any fixed function, that is;

Proposition 3: [9] Let the notations be as above. Let further $\psi \in \mathcal{S}_{2^{2^n}}$ be a non-affine mapping satisfying

1) $\lambda_0 \in \mathscr{A}_n$,
2) The matrix $M = (P' \oplus B)$ with $P' \in \mathcal{S}_{2^n}$ corresponds to a matrix representation of an element in AGL_n and $B = [\varepsilon_1\ \varepsilon_2\ \ldots\ \varepsilon_{2^n}]$ with $\varepsilon_i \in \mathscr{A}_n$, $1 \leq i \leq 2^n$,
3) $\lambda_j \in \mathscr{A}_n$ for all $j \in \{12, 13, \ldots, 12\cdots 2^n\}$ where at least one of $\lambda_j \neq (0\ldots 0)$.

Then ψ is an element of $\mathsf{AGL}_n \ltimes \mathscr{A}_n$ for a fixed function $f \in \mathcal{F}_n$.

Furthermore it is proved that

Theorem 4: [9] For $n \geq 3$ there exist nonlinearity preserving non-affine mappings not lying in the class of Proposition 3.

IV. Examples of New Mappings

The proof of Theorem 4 rely on the cardinalities gathered from nonlinearity distributions and beside the existence, it does not state any families. Here we will give some examples to illustrate these mappings. The examples may seem to be basic and in a way they are. However, we believe examining such example would give clues about structure of these new nonlinearity preserving mappings.

Due to the space constraints the algebraic normal form of the nonlinearity preserving transformations are not given explicitly for $n \geq 4$. However, since any transformation is an element of $\mathcal{S}_{2^{2^n}}$, it is possible to represent the permutations as a product of disjoint cycles. Within these cycles, the functions will be given by their truth table in hexadecimal value without the "0x" prefix.

Example 5: Let $\psi \in S_{2^{2^3}}$ be the mapping, whose explicit permutation representation is given in Appendix, satisfying,

$$\begin{aligned}[T_f] \mapsto &[\lambda_0] \oplus M[T_f] \oplus \\ &[\lambda_{123458}] f(\alpha_0)f(\alpha_1)f(\alpha_2)f(\alpha_3)f(\alpha_4)f(\alpha_7) \oplus \\ &[\lambda_{123457}] f(\alpha_0)f(\alpha_1)f(\alpha_2)f(\alpha_3)f(\alpha_4)f(\alpha_6) \oplus \\ &[\lambda_{1234568}] f(\alpha_0)f(\alpha_1)f(\alpha_2)f(\alpha_3)f(\alpha_4)f(\alpha_5)f(\alpha_7) \oplus \\ &[\lambda_{1234567}] f(\alpha_0)f(\alpha_1)f(\alpha_2)f(\alpha_3)f(\alpha_4)f(\alpha_5)f(\alpha_6)\end{aligned}$$

where $\lambda_0 = (0,0,0,0,1,1,1,1)$, $\lambda_{123458} = \lambda_{123457} = \lambda_{1234568} = \lambda_{1234567} = (0,0,0,0,0,1,0,1)$ and M is the matrix;

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Trivially, ψ is not an affine mapping, indeed it does not satisfies the conditions given in Proposition 3, since $(0,0,0,0,0,1,0,1)$ is not truth table of an affine function. Moreover, it can be easily checked that this map is invertible and preserves nonlinearity for all functions.

Example 6: Assume $\psi \in \mathcal{S}_{2^{2^4}}$ be a permutation of $\mathbb{F}_2^{2^4}$ with cycle representation,

$$\begin{aligned}\pi_\psi = &(0002, 3ec3, fffe, 33ce, 7fff, 2ff0)(001b, 33aa, e48d, f681, \\ &6a77, 97f7, 050a, 027c, 665a, 1370, fff0)(059c, a63f, \\ &e1ee, 36af, 72be, fca9)\end{aligned}$$

It can be easily verified that ψ keeps nonlinearity values invariant for all $f \in \mathcal{F}_n$, that is $\psi \in \mathcal{P}_4(N)$. When the algebraic normal form of ψ is written explicitly, it will be seen that some non-affine terms are not the truth table of an affine function. Thus ψ is not of the form given in Proposition 3.

Example 7: Let $\psi \in \mathcal{S}_{2^{2^6}}$ be the permutation such that its disjoint cycle representation is

$$\pi_\psi = (9556566a3ffcfcc0, 0ddfcbb3a4456dd9)$$

Trivially, ψ maps all functions to itself except the ones in the disjoint cycles, i.e. it keeps nonlinearity invariant for those functions. The cycle has bent functions whose nonlinearity values are 28. Thus, $\psi \in \mathcal{P}_6(N)$. However, the bent function 9556566a3ffcfcc0 has algebraic degree 2 while its image under ψ, 0ddfcbb3a4456dd9, has algebraic degree 3. ψ can not be of the form as given in Proposition 3 since in that case it should have also kept the algebraic degree invariant.

Indeed, in a generic way, one can easily construct new nonlinearity preserving mappings in the following way. Consider two different affine equivalency classes of the same nonlinearity values, for instance regard the classes given in [19], [18], [20], [6]. Taking into account of the bijectivity property of the transformation, map the one of affine equivalency class members to the other class. Basically, while mapping the rest to themselves, select at least two functions belonging to the different affine equivalency classes and then map each to the other to produce a bijective nonlinearity preserving mapping. By Proposition 3, it is certain that the transformations created as above won't belong to the explicitly known non-affine bijective nonlinearity preserving mapping. Moreover these transformations will not produce the same orbit structure as affine equivalency mappings.

When an expressive construction or classification given for these explicitly unknown mappings, such mappings may probably be used as a practical tool especially to construct new functions that are not belonging to the same equivalency classes may be performed.

V. Conclusion

Studying the elements $\mathcal{S}_{2^{2^n}}$ and classifying them with respect to nonlinearity preserving property is still an open problem. Due to the huge cardinality of the mappings, pursuing this research may seem to be highly involved. Despite this fact, it may lead to a deeper insight to the nonlinear functions or nonlinearity classes and additionally it may become a practical tool for constructions of new Boolean functions. In this work, some examples of new transformations keeping nonlinearity invariant are given. For future studies, it would be interesting to further investigate nonlinearity preserving mappings in order to construct these mappings with explicit

methods. Such constructions may be used as a practical tool for finding new Boolean function families.

APPENDIX
EXPLICIT PERMUTATION REPRESENTATION OF EXAMPLE 5

The bijective mapping presented in Example 5, is given below regarding the disjoint cycle representation.

$$\begin{aligned}\pi_\psi =&(00,0f,55,3c,5a,66,33)(01,0e,54,3d,5b,67,32)(02,\\ &0b,45,3e,5e,76,31,04,1f,57,38,4a,64,37,10,0d,51,\\ &2c,58,62,23)(03,0a,44,3f,5f,77,30,05,1e,56,39,4b,\\ &65,36,11,0c,50,2d,59,63,22)(06,1b,47,3a,4e,74,\\ &35,14,1d,53,28,48,60,27,12,09,41,2e,5c,72,21)\\ &(07,1a,46,3b,4f,75,34,15,1c,52,29,49,61,26,13,\\ &08,40,2f,5d,73,20)(16,19,43,2a,4c,70,25)(17,18,\\ &42,2b,4d,71,24)(6a,6c,78)(6b,6d,79)(6e,7c,7a)\\ &(6f,7d,7b)(82,84,90)(83,85,91)(86,94,92)(87,95,\\ &93)(88,cf,fa,e4,b8,c5,b1,8b,ca,eb,e2,ac,d7,b7,9f,\\ &d8,ed,f6,be,d1,a3,8d,de,f9,e1,a9,c6,b4,9a,c9,ee,\\ &f3,af,d2,a6,9c,dd,fc,f5,bb,c0,a0)(89,ce,fb,e0,a8,\\ &c7,b5,9b,c8,ef,f2,ae,d3,a7,9d,dc,fd,f4,ba,c1,a1)\\ &(8a,cb,ea,e3,ad,d6,b6,9e,d9,ec,f7,bf,d0,a2,8c,\\ &df,f8,e5,b9,c4,b0)(8e,db,e8,e7,bd,d4,b2)(8f,da,\\ &e9,e6,bc,d5,b3)(98,cd,fe,f1,ab,c2,a4)(99,cc,ff,\\ &f0,aa,c3,a5)\end{aligned}$$

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable comments on the preliminary version of this work.

REFERENCES

[1] W. Meier and O. Staffelbach, "Nonlinearity Criteria for Cryptographic Functions," in *Advances in Cryptology — EUROCRYPT '89*, ser. Lecture Notes in Computer Science, J. Quisquater and J. Vandewalle, Eds. Springer Berlin Heidelberg, 1990, vol. 434, pp. 549–562.
[2] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, 2nd ed. Amsterdam: North-holland Publishing Company, 1978.
[3] B. Preneel, "Analysis and Design of Cryptographic Hash Functions," Ph.D. dissertation, Katholieke Universiteit Leuven, Leuven, Belgium, Jan. 1993.
[4] S. Kavut and M. D. Yücel, "9-variable Boolean functions with nonlinearity 242 in the generalized rotation symmetric class," *Information and Computation*, vol. 208, no. 4, pp. 341 – 350, 2010.
[5] S. Maitra, "Boolean functions on odd number of variables having nonlinearity greater than the bent concatenation bound," in *NATO Advanced Study Institute on Boolean Functions in Cryptology and Information Security (NATO ASI Zvenigorod, 2007)*, ser. NATO Science for Peace and Security Series, B. Preneel and O. A. Logachev, Eds. IOS Press books, 2008, pp. 173–182.
[6] A. Braeken, "Cryptographic Properties of Boolean Functions and S-Boxes," Ph.D. dissertation, Katholieke Universiteit Leuven, Leuven, Belgium, 2006.
[7] İ. Sertkaya and A. Doğanaksoy, "On Nonlinearity Preserving Bijective Transformations," in *Proceedings of the National Cryptology Symposium II*, Ankara, Turkey, 2006, pp. 27–36.
[8] ——, "Some Results on Nonlinearity Preserving Bijective Transformations," in *Proceedings of BFCA'07 Conference*, Paris, France, 2007, pp. 27–42.
[9] İ. Sertkaya, A. Doğanaksoy, O. Uzunkol, and M. S. Kiraz, "Affine Equivalency and Nonlinearity Preserving Bijective Mappings over $\mathbb{F}_2$," submitted to the International Workshop on the Arithmetic of Finite Fields (WAIFI 2014).
[10] C. Carlet, *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, 1st ed. New York, NY, USA: Cambridge University Press, 2010, ch. Boolean Functions for Cryptography and Error Correcting Codes, pp. 257–397.
[11] İ. Sertkaya, "Nonlinearity Preserving Post-Transformations," Master's thesis, Middle East Technical University, Ankara, Turkey, June 2004.
[12] J. J. Sylvester, "Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tessellated pavements in two or more colors, with applications to Newton's rule, ornamental tile-work, and the theory of numbers," *Philosophical Magazine*, vol. 34, pp. 461–475, 1867.
[13] J. Hadamard, "Résolution d'une question relative aux déterminants," *Bull. Sciences Math.*, vol. 2, no. 17, pp. 240–246, 1893.
[14] J. Seberry and X.-M. Zhang, "Highly nonlinear 0–1 balanced Boolean functions satisfying strict avalanche criterion (extended abstract)," in *Advances in Cryptology — AUSCRYPT '92*, ser. Lecture Notes in Computer Science, J. Seberry and Y. Zheng, Eds. Springer Berlin Heidelberg, 1993, vol. 718, pp. 143–155.
[15] J. Pieprzyk and G. Finkelstein, "Towards effective nonlinear cryptosystem design," *Computers and Digital Techniques, IEE Proceedings E*, vol. 135, no. 6, pp. 325–335, 1988.
[16] O. S. Rothaus, "On "bent" functions," *Journal of Combinatorial Theory, Series A*, vol. 20, no. 3, pp. 300 – 305, 1976.
[17] J. F. Dillon, "A Survey of Bent Functions," *The NSA Technical Journal*, vol. Spacial Issue, pp. 191–215, 1972.
[18] J. A. Maiorana, "A Classification of the Cosets of the Reed-Muller Code $R(1,6)$," *Mathematics of Computation*, vol. 57, no. 195, pp. 403–414, 1991.
[19] E. Berlekamp and L. Welch, "Weight Distributions of the Cosets of the $(32,6)$ Reed-Muller Code," *Information Theory, IEEE Transactions on*, vol. 18, no. 1, pp. 203–207, Jan 1972.
[20] J. E. Fuller, "Analysis of affine equivalent Boolean functions for cryptography," Ph.D. dissertation, Queensland University of Technology, Queensland, Australia, 2003.

İsa Sertkaya received M.Sc. and Ph.D. Degrees in cryptography from the Middle East Technical University, Ankara, in 2004 and 2014 respectively. His area of research interest includes Boolean functions.

Ali Doğanaksoy received M.Sc. and Ph.D. Degrees in mathematics from the Middle East Technical University, Ankara, in 1983 and 1987 respectively. After a period of research in differential geometry, he directed to cryptography. His area of interest includes Boolean functions, randmoness tests.