1-2008

G-Perfect Nonlinear Functions

James A. Davis
University of Richmond, jdavis@richmond.edu

Laurent Poinsot

G-PERFECT NONLINEAR FUNCTIONS

JAMES A. DAVIS, LAURENT POINSOT

Abstract. Perfect nonlinear functions are used to construct DES-like cryptosystems that are resistant to differential attacks. We present generalized DES-like cryptosystems where the XOR operation is replaced by a general group action. The new cryptosystems, when combined with G-perfect nonlinear functions (similar to classical perfect nonlinear functions with one XOR replaced by a general group action), allow us to construct systems resistant to modified differential attacks. The more general setting enables robust cryptosystems with parameters that would not be possible in the classical setting. We construct several examples of G-perfect nonlinear functions, both $\mathbb{Z}_2$-valued and $\mathbb{Z}_2^a$-valued. Our final constructions demonstrate G-perfect nonlinear planar permutations (from $\mathbb{Z}_2^a$ to itself), thus providing an alternative implementation to current uses of almost perfect nonlinear functions.

1. Background on cryptosystems and group action modifications

In an r-round iterative block cipher such as the Data Encryption Standard (DES) [17] or the Advanced Encryption Standard (AES) [9, 18] the ciphertext x_r is obtained from a plaintext x_0 by r iterations of the round function f

$$x_i = f(x_{i-1}, k_i)\ 1 \leq i \leq r$$

where k_i is the ith round key. The function f usually contains some particular components called *S-boxes*. These (vectorial) Boolean functions B map m-bit vectors to n-bit vectors and are often used just after an XOR (*i.e.* a component-wise modulo-two sum) combination of the block x_{i-1} and the key k_i *i.e.*

$$y = B(k_i + x_{i-1})\ .$$

The S-boxes are designed to be resistant against last-round attacks that intend to recover the last-round key. In particular the XOR differences of the output values for input values with a fixed XOR difference must be close to the uniform distribution; otherwise a statistical bias could be exploited by the differential attack of Biham and Shamir [4]. Nyberg [25] introduced *perfect nonlinear S-boxes* for this purpose.

The differential cryptanalysis takes advantage of the XOR combinations with the round keys. Nevertheless there are many ways to operate on bit-strings other than XOR: for instance Lai and Massey's IDEA [22] uses the classical XOR but also the addition in a cyclic group and the multiplication in the group of units of a finite field. Additionally, the Russian analogue of DES has S-boxes that use addition in a cyclic group [34]. Pott [32] says the following: "... It seems that in most applications (in particular in cryptography) people use nonlinear functions on finite fields. However, there is no technical reason why you should restrict yourselves to this case." This

Key words and phrases. G-perfect nonlinear functions, difference sets.

paper proposes constructing cryptosystems with operations other than XOR. The new cryptosystems will be r-round iterative block ciphers as in the classical case, and our task will be to provide S-boxes that are robust against a modified differential attack.

Suppose that the round keys are chosen in a finite group G that acts on a nonempty finite set X via a group homomorphism ϕ from G to the symmetric group $S(X)$ and let H be a finite group. Then in this case the S-boxes are used as follows

$$y = B(\phi(k_i)(x_{i-1})) \tag{1.1}$$

where $x_{i-1} \in X$, $y \in H$, $k_i \in G$ and $\phi(k_i)(x_{i-1})$ denotes the action of the ith round key k_i on the message x_{i-1}. Note that in many cryptosystems the output of one S-box is used as input for another S-box and so we may require $y \in X$ rather than $y \in H$. But an operation of output difference is necessary to lead to differential cryptanalysis, so we need to consider an algebraic structure that provides such an operation and then the output values must belong to a group. An alternative way, not followed in this contribution, would be to consider that X is equipped with a group structure and G acts on its carrier set. We do not choose this possibility because it is an important constraint and we want to present a more general theory. The differential attack can be adapted to this context: let f be a round function (then for each round key k, $f_k : x \mapsto f(x, k)$ is a permutation) that makes use of S-boxes exactly as in equation (1.1). Then the algorithm of a group action version of the differential attack can be easily derived from the classical one.

(1) Find a pair $(g, \beta) \in G \times H$ so that the probability
$$\mathsf{Pr}(R(\phi(g)(x)) - R(x) = \beta)$$
is far from the uniform distribution, where R is the *reduced cipher* defined as $R = f_{k_{r-1}} \circ \ldots \circ f_{k_1}$;
(2) Choose at random a plaintext x_0 and encrypt both x_0 and $\phi(g)(x_0)$. Two pairs of plaintexts/ciphertexts are obtained: (x_0, x_r) and $(\phi(g)(x_0), x'_r)$;
(3) Find all the rth round keys $\hat{k}_r$ such that
$$f^{-1}_{\hat{k}_r}(x_r) - f^{-1}_{\hat{k}_r}(x'_r) = \beta \ .$$
(4) Iterate steps (2) and (3) until a value $\hat{k}_r$ occurs more than the others. It will be considered as a candidate for the last round key.

The purpose of this paper is the construction of S-boxes that ensure the best resistance of the generalized DES-like cryptosystem to this G-differential cryptanalysis. We observe that some of the new systems presented in this paper will have robust S-boxes in cases where the traditional theory of Boolean perfect nonlinear functions concludes that these classical objects can not exist.

2. Perfect nonlinear functions: the classical approach

In this paper, the groups we consider are always finite. Note that if a group G is written additively (resp. multiplicatively) then 0 (resp. 1) denotes its identity element and G^* stands for the set of nonidentity elements of G.

Definition 2.1. *Let G and H be (abelian or nonabelian) groups (written additively), and let $f : G \to H$ be a function from G to H. Then f is called* **perfect nonlinear** *if for every $(g, h) \in G^* \times H, |\{x \in G | f(g + x) - f(x) = h\}| = \frac{|G|}{|H|}$.*

Let X and Y be two finite nonempty sets. A function $g : X \to Y$ is called **balanced** if for each $y \in Y$, $|\{x \in X | g(x) = y\}| = \frac{|X|}{|Y|}$ therefore $f : G \to H$ is perfect nonlinear if and only if for each $g \in G^*$ the map, usually called **derivative**, $x \mapsto f(g + x) - f(x)$ is balanced. Perfect nonlinear functions only exist if $|H|$ divides $|G|$. In particular, if $H = \mathbb{Z}_2$, then we need $|G|$ to be an even number. Perfect nonlinear functions from $\mathbb{Z}_2^a$ to $\mathbb{Z}_2^b$ are equivalent to bent functions [24, 25]. We will not define bent functions in this paper (see [33]), but we have the following important result [25] coming from bent functions that restricts the possibilities for perfect nonlinear functions.

Theorem 2.2. *If $f : \mathbb{Z}_2^a \to \mathbb{Z}_2^b$ is perfect nonlinear, then a is even and $a \geq 2b$.*

Note also that such (Boolean) bent functions can not be balanced (Proposition 14 of [7]). We will see in section 4 that we can construct a function f from $\mathbb{Z}_2^a$ to $\mathbb{Z}_2$ so that f is both balanced and a modified version of perfect nonlinear (known as "G-perfect nonlinear"; see next section).

Bent functions (and hence perfect nonlinear functions) are equivalent to a special type of difference set, so another approach to understanding perfect nonlinear functions is to use the known results from difference sets. We include the definitions of difference sets and relative difference sets below.

Definition 2.3.

1. *A subset D of cardinality k of a group G (in a multiplicative representation) of order v is a (v, k, λ)* **difference set** *if for every $g \in G^*$ there are exactly λ elements $(x, y) \in D^2$ satisfying $y = gx$.*
2. *A subset R of cardinality k of a group G (in a multiplicative representation) of order mn is an (m, n, k, λ)* **relative difference set of G relative to a normal subgroup H of order** *n if there are exactly λ elements (x, y) of R^2 satisfying $y = gx$ for every $g \in G \backslash H$ and there are no elements $(x, y) \in R^2$ satisfying $y = gx$ for every $g \in H^*$.*

The most important family of difference sets for this paper, called *Hadamard difference sets*, have parameters $(4N^2, 2N^2 - N, N^2 - N)$ or its complement $(4N^2, 2N^2 + N, N^2 + N)$, where N is an integer. The following theorem describes all known abelian groups containing a Hadamard difference set (see [3] for details).

Theorem 2.4. *Let $G = H \times K \times (\prod_{i=1}^{r} (\mathbb{Z}_{p_i})^4)$ be an abelian group so that:*

i: $|H| = 2^{2a+2}, expH \leq 2^{a+2}$;

ii: $K = \prod_{j=1}^{s} (\mathbb{Z}_{3^{b_j}})^2$;

iii: p_i *prime;*

then G contains a $(4N^2, 2N^2 \pm N, N^2 \pm N)$ difference set where $N = 2^a 3^{\Sigma b_j} \prod_{j=1}^{r} (p_j)^2$.

Define the **indicator function** i_D of a subset $D \subset G$ to satisfy $i_D(g) = 1$ if $g \in D$ and $i_D(g) = 0$ otherwise. The following theorem due to Dillon [11] demonstrates the connection between Hadamard difference sets and perfect nonlinear functions.

Theorem 2.5. *The subset D of the finite group G is a $(4N^2, 2N^2 \pm N, N^2 \pm N)$ Hadamard difference set if and only if i_D is a perfect nonlinear function from G to $\mathbb{Z}_2$.*

A similar connection can be made between relative difference sets and general perfect nonlinear functions. A relative difference set is called *semiregular* if $k = m$. Pott [32] showed the following result which is a minor variation of theorem 14 of Arasu et al [1].

Theorem 2.6. *Let G and H be arbitrary finite groups and $f : G \to H$. The set $R_f := \{(g, f(g))|g \in G\} \subset G \times H$ is a semiregular $(|G|, |H|, |G|, |G|/|H|)$ relative difference set in $G \times H$ relative to $\{1_G\} \times H$ if and only if f is perfect nonlinear.*

We comment that there are other applications of perfect nonlinear functions in difference sets not studied in this paper; indeed Ding and Yuan [12] recently presented a family of new perfect nonlinear functions and constructed a family of skew Hadamard difference sets using these functions which are shown to be inequivalent to the so-called Paley-Hadamard difference sets [28], refuting a longstanding conjecture on the subject.

We will generalize some connections between difference sets and perfect nonlinear functions in the following sections.

3. Group action approach

A group G is said to act on a nonempty set X if there is a group homomorphism $\phi : G \to S(X)$, where $S(X)$ is the set of permutations of X. Let $p \in X$. The *orbit* of p under the action of G on X is the set $\mathcal{O}_p = \{x \in X|x = \phi(g)(p) \text{ for } g \in G\}$. The action is called *faithful* if the homomorphism is one-to-one; the action is called *transitive* if there is only one orbit; and the action is called *regular* if for each $x \in X$ the function that maps $g \in G$ to $\phi(g)(x) \in X$ is bijective. Such a regular action is faithful and transitive (the reciprocal assertion is also true when G is abelian).

One example of an action, the so-called *left regular action* of G on itself, is defined by the homomorphism $\phi(g)(x) = gx, g, x \in G$. This action is also called *left translation*, and it is the action that is used in the classical definition of the DES cryptosystem in the form of the XOR operation. As indicated in section 1, we will consider a different group action on the bits than XOR. The generalized differential attack motivates our need to balance the outputs based on the group action, leading to the following definition ([29, 30, 31]).

Definition 3.1. *Let G and H be groups, let X be a finite nonempty set with G acting faithfully on X via the homomorphism ϕ, and let $f : X \to H$ be a function from X to H. Then f is called G-***perfect nonlinear** *if for every $(g, h) \in G^* \times H, |\{x \in X|f(\phi(g)(x)) - f(x) = h\}| = \frac{|X|}{|H|}$.*

We need the action to be faithful in order to avoid the existence of $g \in G^*$ such that $\phi(g)(x) = x$ for all $x \in X$. If such a g exists, then $|\{x \in X|f(\phi(g)(x)) - f(x) =$

$h\}| = \begin{cases} 0 & \text{if } h \neq 0, \\ |X| & \text{if } h = 0 \end{cases}$. The existence of G-perfect nonlinear functions is then impossible. We implicitly assume that all group actions are faithful for the remainder of the paper. Moreover, note that $|H|$ must divide $|X|$ in order to have a G-perfect nonlinear function.

We now consider the connection between G-perfect nonlinear functions and difference sets. The key part of the definition of a difference set is the statement that for every nonidentity $g \in G$ there are exactly λ solutions $(x, y) \in D^2$ satisfying $y = gx$ (similar for relative difference set). We are implicitly using the left regular action of G on itself, so once again we generalize this by allowing other group actions. This amounts to finding exactly λ solutions $(x, y) \in D^2 \subset X^2$ satisfying $y = \phi(g)(x)$. We extend the (faithful) group action ϕ of G on X to an (faithful) action Φ of $G \times H$ on $X \times H$ defined by $\Phi(g, h)(x, h') = (\phi(g)(x), hh')$. We call it the **extension of** ϕ. The following definitions generalize difference sets and relative difference sets.

Definition 3.2. *Let $\phi : G \to S(X)$ define a group action of the group G on the nonempty set X of cardinality v, and let Φ be the extension of ϕ for the group H of cardinality n described above.*

1. *A subset D of cardinality k of X is a $G-(v, k, \lambda)$* **difference set** *of X if for every $g \in G^*$ there are exactly λ elements (x, y) of D^2 satisfying $y = \phi(g)(x)$.*
2. *A subset R of cardinality k of $X \times H$ is a $G \times H - (v, n, k, \lambda)$-***relative difference set** *of $X \times H$ relative to $\{1_G\} \times H$ if (i) for every $(g, h) \neq (1_G, h) \in G \times H$ there are exactly λ elements $((x_1, h_1), (x_2, h_2)) \in R^2$ so that $\Phi((g, h))((x_1, h_1)) = (x_2, h_2)$ and (ii) if $(x, h), (x, h') \in R$, then $h = h'$.*
   Such a $G \times H - (v, n, k, \lambda)$-relative difference set is called **semiregular** *if $v = k$.*

We remark that each $G \times H$-semiregular relative difference set R gives rise to a function $f : X \to H$ such that $R = \{(x, f(x))|x \in X\}$.

Although the definition of G-(relative) difference sets and its traditional counterpart are quite similar, we note that group actions can be much more general than action via translation. This suggests that we can expect results which are impossible in the classical framework; for example, the construction of a function that is simultaneously G-perfect nonlinear and balanced (see theorem 4.4).

We also note the similarity between G-difference sets and (v, K, λ)-*difference families* in G as defined in Beth, Jungnickel, and Lenz [3]. A (v, K, λ) difference family is a collection of s sets $B_i \subset G, 1 \leq i \leq s, |G| = v, \Sigma|B_i| = K$ so that every nonidentity element of the group G can be represented exactly λ times as differences $b - b'$ where $b, b' \in B_i$ for some i. If our action is regular on all of its orbits (not a requirement), then the G-difference set counts the number of solutions $\phi(g) \circ \phi(g_1)(p) = \phi(g_2)(p)$, which implies that $g = g_2 g_1^{-1}$. Our new context, where the group is acting on a set X, is motivated by the connection to G-perfect nonlinear functions and their application to DES-like cryptosystems.

In this paper, we will be exclusively interested in $G-(v,k,\lambda)$-difference sets with $k-\lambda=\frac{v}{4}$. In that case, we get the following theorem linking G-difference sets and $\mathbb{Z}_2$-valued G-perfect nonlinear functions.

Theorem 3.3. *Let $\phi : G \to S(X)$ define a group action of the group G on a nonempty set X of cardinality v, and let $D \subset X$. The function i_D is G-perfect nonlinear if and only if D is a $G-(v,k,\lambda)$-difference set of X so that $k-\lambda=\frac{v}{4}$.*

Proof: Suppose that D is a $G-(v,k,\lambda)$-difference set of X so that $k-\lambda=\frac{v}{4}$. By the definition of G-difference sets, we see that $\lambda=|\phi(g)(D)\cap D|$ for all $g\in G^*$. A counting argument demonstrates that $|\{x\in X|i_D(\phi(g)(x))+i_D(x)=1\}|=2(|D|-|\phi(g)(D)\cap D|)$ (where "+" is the modulo-two sum) since $i_D(\phi(g)(x))+i_D(x)=1$ if exactly one of $\phi(g)(x)$ and x is in D. This implies that $i_D(\phi(g)(x))+i_D(x)$ takes the value 1 exactly $2(k-\lambda)=\frac{v}{2}$ times, implying that $i_D(\phi(g)(x))+i_D(x)$ takes the value 0 exactly $\frac{v}{2}$ times as well. This implies that i_D is G-perfect nonlinear.

Conversely, suppose that i_D is G-perfect nonlinear. By applying the same counting argument as before, we see that $2(|D|-|\phi(g)(D)\cap D|)=\frac{v}{2}$ for all $g\in G^*$. Solving this, we get $|\phi(g)(D)\cap D|=k-\frac{v}{4}$, which implies that $\lambda=|\phi(g)(D)\cap D|$ is the same for all nonidentity g. Thus, D is a $G-(v,k,\lambda)$-difference set as claimed. □

Extending Theorem 2.6 to the group action setting, it is also possible to characterize G-perfect nonlinear functions by $G\times H$-relative difference sets.

Theorem 3.4. *Let $\phi : G \to S(X)$ define a group action of the group G on the finite nonempty set X, H be a group written additively, and $\Phi : G\times H \to S(X\times H)$ be the extension of ϕ. If $f : X \to H$, then f is G-perfect nonlinear if and only if the set $R_f=\{(x,f(x))\in X\times H|x\in X\}$ is a $G\times H-(|X|,|H|,|X|,\frac{|X|}{|H|})$-semiregular relative difference set of $X\times H$ relative to $\{1_G\}\times H$.*

Proof: Since f is a mapping, $|R_f|=|G|$ and therefore we need to prove that f is G-perfect nonlinear if and only if R_f satisfies axiom (ii) of $G\times H$-relative difference sets with $\lambda=\frac{|X|}{|H|}$. This last assertion is equivalent to the following ones for each $(g,h)\in G^*\times H$.

$$\begin{aligned}
& |\{((x_1,h_1),(x_2,h_2))\in R_f^2|\Phi((g,h))((x_1,h_1))=(x_2,h_2)\}| &=& \tfrac{|X|}{|H|}\\
\Leftrightarrow\ & |\{((x_1,h_1),(x_2,h_2))\in R_f^2|(\phi(g)(x_1),h+f(x_1))=(x_2,f(x_2))\}| &=& \tfrac{|X|}{|H|}\\
& \text{(by the definition of the action } \Phi \text{ and the definition of } R_f.)\\
\Leftrightarrow\ & |\{x\in X|f(\phi(g)(x))-f(x)=h\}| &=& \tfrac{|X|}{|H|}\\
\Leftrightarrow\ & f \text{ is } G\text{-perfect nonlinear .}
\end{aligned}$$

□

In this paper many of our results concern $\mathbb{Z}_2$-valued functions rather than the S-boxes themselves. This is a good place to start our understanding of G-perfect nonlinear functions due to the following relationship between nonbinary perfect nonlinear functions and their binary components.

Theorem 3.5. *Let V_n be a n-dimensional Hilbert space over the finite field with two elements $\mathbb{Z}_2$ and let $\langle .,. \rangle_n$ be its dot-product. Suppose that the group G acts faithfully on a finite nonempty set X (via ϕ). A function $f : X \to V_n$ is G-perfect nonlinear if and only if for each $\beta \in V_n^*$, $\langle \beta, f \rangle_n : X \to \mathbb{Z}_2$ is G-perfect nonlinear.*

Proof. We can show that $g : X \to V_n$ being balanced is equivalent to

$$\forall \beta \in V_n^*, \ \sum_{x \in X} (-1)^{\langle \beta, g(x) \rangle_n} = 0 \ . \tag{3.1}$$

(This is a simple adaptation of proposition 14 of [7].) Moreover it is obvious to see that f is G-perfect nonlinear if and only if for each $g \in G^*$, the map

$$\begin{array}{rccc} d_g f : & X & \to & V_n \\ & x & \mapsto & f(\phi(g)(x)) + f(x) \end{array}$$

is balanced. Using equation (3.1), this is equivalent to the fact that for each $g \in G^*$ and for each $\beta \in V_n^*$, $\sum_{x \in X} (-1)^{\langle \beta, d_g f(x) \rangle_n} = 0$. By bilinearity, f is G-perfect nonlinear if and only if for each $g \in G^*$ and for each $\beta \in V_n^*$, $\sum_{x \in X} (-1)^{d_g(l_\beta \circ f)(x)} = 0$ where $l_\beta : y \mapsto \langle \beta, y \rangle_n$. By applying equation (3.1) with $n = 1$, the last fact is equivalent to the balancedness of $d_g(l_\beta \circ f)$ for every $g \in G^*$ and therefore $l_\beta \circ f$ is also G-perfect nonlinear.

□

Our approach in the next section is to construct G-difference sets with $|X| = 4(k - \lambda)$, which by Theorem 3.3 will provide relevant cryptographic examples of G-perfect nonlinear $\mathbb{Z}_2$-valued functions.

4. G-Difference Set Constructions

We begin this section with a general theorem that will allow us to build G-difference sets from smaller G-difference sets.

Theorem 4.1. *Let $\phi : G \to S(X)$ define a group action of the group G on the nonempty set X of cardinality v, and suppose D_i is a $G - (v, k_i, \lambda_i)$-difference set of X for $1 \leq i \leq t$. Suppose $Y = \{y_1, y_2, \ldots, y_t\}$ is a set of cardinality t, and define the group action Φ of G on $X \times Y$ by $\Phi(g)((x, y)) = (\phi(g)(x), y)$ for $(x, y) \in X \times Y$. Then $D = \bigcup_{i=1}^{t} (D_i \times \{y_i\})$ is a $G - (vt, \sum_{i=1}^{t} k_i, \sum_{i=1}^{t} \lambda_i)$-difference set of $X \times Y$.*

Proof: Suppose that all of the D_i are $G - (v, k_i, \lambda_i)$-difference sets of X, and form $D \subset X \times Y$ as described. For every $g \in G^*$, the number of solutions of $\Phi(g)((x, y)) = (x', y')$, where $(x, y), (x', y') \in D$, must satisfy $(\phi(g)(x), y) = (x', y')$. Thus, $y = y'$, and we are simply counting the number of solutions to $\phi(g)(x) = x'$ in each D_i. This yields a total number of solutions of $\sum_{i=1}^{t} \lambda_i$ as claimed. The other parameters are obvious. □

We note that if all of the D_i in Theorem 4.1 satisfy $v = 4(k_i - \lambda_i)$, then $vt = 4(\sum_{i=1}^{t} k_i - \sum_{i=1}^{t} \lambda_i)$. The combined G-difference set D can be used to construct G-perfect nonlinear functions as described in Theorem 3.3.

As one application of this direct product construction, we combine Theorem 2.4 with Theorem 4.1 to yield the following G-difference sets all of which satisfy $v = 4(k - \lambda)$.

Corollary 4.2. *Let $G = H \times K \times (\prod_{i=1}^{r} (\mathbb{Z}_{p_i})^4)$ be an abelian group so that:*

i: $|H| = 2^{2a+2}, expH \leq 2^{a+2}$;

ii: $K = \prod_{j=1}^{s} (\mathbb{Z}_{3^{b_j}})^2$;

iii: p_i *prime.*

Let $\phi : G \to S(G)$ be the left regular action on G, and let Φ be the action on $G \times Y$ defined by $\Phi(g)((g', y)) = (gg', y)$ for Y a set of cardinality t. Then there is a $G - (4N^2t, j(2N^2 - N) + (t - j)(2N^2 + N), j(N^2 - N) + (t - j)(N^2 + N))$-difference set in $G \times Y$ for all $0 \leq j \leq t$ where $N = 2^a 3^{\sum b_j} \prod_{i=1}^{r} (p_i)^2$.

Proof: Theorem 2.4 provides $G - (4N^2, 2N^2 \pm N, N^2 \pm N)$-difference sets based on the left regular action of G on itself, and Theorem 4.1 allows us to combine them into a G-difference set on $G \times Y$. The different j values come from how many of the D_i used in the construction have the parameters $(4N^2, 2N^2 - N, N^2 - N)$. □

As an example of the power of this corollary, we can construct G-difference sets with parameters $(512, 192, 64), (512, 196, 68), (512, 200, 72), \ldots, (512, 320, 192)$ by using 32 copies of the $(16, 6, 2)$ difference set or its complement in the group G, where G is a group of order 16 that acts regularly on the 32 orbits of a set X of order 512. Since 512 is an odd power of 2, Theorem 2.2 implies that there are no perfect nonlinear functions with these parameters. Thus, this theorem provides great flexibility in producing G-perfect nonlinear functions for parameters that are impossible for traditional perfect nonlinear functions.

We remark here that there are G-difference sets with the same parameters as the previous corollary that are not necessarily on a set that is a direct product of G and Y. If we have a group action of G on a set X with the property that the action is faithful and regular on each of its orbits (sometimes called a *free* action), then we can use a Hadamard difference set in each orbit $\mathcal{O}_i$ to choose the elements of X from that orbit. We do this by identifying a point $p_i \in \mathcal{O}_i$, write all other points $q \in \mathcal{O}_i$ as $q = \phi(g)(p_i)$ for some $g \in G$, and let $\mathcal{D}_i = \{x \in \mathcal{O}_i | x = \phi(d)(p_i) \text{ for some } d \in D_i\}$. The union of the $\mathcal{D}_i$ is the G-difference set. These may or may not be equivalent to the G-difference sets listed in the corollary, and this brings up the question of equivalent G-difference sets. For a related discussion of equivalent difference sets, see Kantor [21]. We leave this question open for now.

The second general theorem below provides a way to modify existing G-difference sets to get new ones. The technique in the theorem is based on the trivial result in difference sets that the complement of a (v, k, λ) difference set is a $(v, v-k, v-2k+\lambda)$ difference set.

Theorem 4.3. *Let G be a group that acts on a nonempty set X, and suppose D is a $G-(v, k, \lambda)$-difference set of X. If $\mathcal{O}_p$ is the orbit containing $p \in X$ and $C_p = D \cap \mathcal{O}_p$, then $D' = (D \backslash C_p) \cup (\mathcal{O}_p \backslash C_p)$ is a $G-(v, k+|\mathcal{O}_p|-2|C_p|, \lambda+|\mathcal{O}_p|-2|C_p|)$-difference set of X.*

Proof: Suppose D meets the conditions of the statement of the theorem. For a given $g \in G^*$, there are ℓ solutions to the equation $y = \phi(g)(x)$, where $(x, y) \in C_p$. By a counting argument, there are $2(|C_p| - \ell)$ pairs (x, y) with exactly one of the components in C_p. This implies that there are $|\mathcal{O}_p|-(2(|C_p|-\ell))-\ell = |\mathcal{O}_p|-2|C_p|+\ell$ elements $x \in (\mathcal{O}_p \backslash C_p)$ for which $y = \phi(g)(x) \in (\mathcal{O}_p \backslash C_p)$. Thus, the number of solutions to $y = \phi(g)(x)$ is changed by $|\mathcal{O}_p|-2|C_p|$, independent of the group element g. Similarly, the size of the G-difference set is changed by adding $|\mathcal{O}_p| - |C_p|$ and subtracting $|C_p|$, yielding the result. □

Any G-difference set constructed by the method suggested in Theorem 4.3 will preserve the equation $k - \lambda = \frac{v}{4}$. Thus, once we get a G-difference set with the appropriate property, we can construct a whole family with differing parameters that still satisfy the conditions needed to build G-perfect nonlinear functions.

A permutation π of a set X (that contains at least two distinct elements) is a **fixed-point free involution** if

i: $\pi \circ \pi$ is the identity map of X (or equivalently $\pi = \pi^{-1}$);
ii: $\forall x \in X$, $\pi(x) \neq x$.

Theorem 4.4. *Let m be a nonzero positive integer. Let X and Y be two sets of same cardinality $2m$ and such that $X \cap Y = \emptyset$. Let $\pi \in S(X \cup Y)$ such that $\pi(x) = x$ for all $x \in X$, $\pi(y) \neq y$, $\pi(\pi(y)) = y$ and $\pi(y) \in Y$ for all $y \in Y$ (i.e. the permutation π is the identity on X and a fixed-point free involution on Y). There is a function $f : X \cup Y \to \mathbb{Z}_2$ such that f is $\langle \pi \rangle$-perfect nonlinear and balanced. Moreover the $\langle \pi \rangle$-difference set of $X \cup Y$ corresponding to f has parameters $(4m, 2m, m)$.*

Proof: Let $\{X_1, X_2\}$ be a partition of X such that $|X_i| = m$ for $i = 1, 2$. Since π is a fixed-point free involution on Y we can choose Y_1 as a subset of Y of cardinality m such that for each $y \in Y_1$, $\pi(y) \in Y_2 := Y \backslash Y_1$. Then $\{Y_1, Y_2\}$ is a partition of Y such that $|Y_i| = m$ for $i = 1, 2$. Let define $f : X \cup Y \to \mathbb{Z}_2$ as follows

$$f(x) = \begin{cases} 1 & x \in X_1 \cup Y_1 \ , \\ 0 & x \in X_2 \cup Y_2 \ . \end{cases}$$

Thus f is obviously balanced. Moreover if $x \in X$ then $\pi(x) = x$ and therefore $f(\pi(x)) + f(x) = 0$ and if $y \in Y_1$ (resp. $y \in Y_2$) then $\pi(y) \in Y_2$ (resp. $\pi(y) \in Y_1$), so $f(\pi(y)) + f(y) = 1$. We conclude that f is $\langle \pi \rangle$-perfect nonlinear since $|X| = |Y| = 2m$ and $\frac{|X \cup Y|}{2} = 2m$. Since f is the indicator function of $D := \{x \in X \cup Y | f(x) = 1\} = X_1 \cup Y_1$, by Theorem 3.3, D is a $\langle \pi \rangle - (4m, 2m, \lambda)$ difference set of $X \cup Y$ such that $2m - \lambda = m$. Hence $\lambda = m$. □

If we choose in the previous theorem $\{X, Y\}$ as a partition of $\mathbb{Z}_2^{k+2}$ (with $k \geq 0$) such that both X and Y have the same cardinality 2^{k+1} (here $m = 2^k$) and we define π as the identity on X and a fixed-point free involution on Y then we can construct a balanced $\langle\pi\rangle$-perfect nonlinear Boolean function $f : \mathbb{Z}_2^{k+2} \to \mathbb{Z}_2$ which is impossible in the traditional setting. Finally if $m = 1$ then the *minimal* G-difference set corresponding to a G-perfect nonlinear function built as in the previous theorem has parameters $(4, 2, 1)$ which are different from the trivial classical difference sets $(4, 1, 0)$ or $(4, 3, 2)$.

A group G is called a **group of fixed-point free involutions** of a nonempty set X if the homomorphism for the group action maps each nonidentity element of G to a fixed-point free involution. Note that the action of such a group is always faithful. As an example, let a and b be two integers such that $a \geq b$. For each $x = (x_1, x_2, \ldots, x_b) \in \mathbb{Z}_2^b$ and each $y = (y_1, y_2, \ldots, y_a) \in \mathbb{Z}_2^a$, define $\phi(x)(y) = (x_1 + y_1, x_2 + y_2, \ldots, x_b + y_b, y_{b+1}, \ldots, y_a)$. The group $G = \mathbb{Z}_2^b$ and all its conjugate group are (isomorphic) groups of fixed-point free involutions of the set $X = \mathbb{Z}_2^a$. Such involutional groups are rather interesting in cryptography since their action on $\mathbb{Z}_2^a$ is similar to the classical XOR combination and therefore constitute a natural extension to the traditional addition of the round-key in block ciphers. The following theorem uses groups of fixed-point free involutions to demonstrate that not all G-difference sets with $k - \lambda = \frac{v}{4}$ will be constructed as in Corollary 4.2.

Theorem 4.5 (Hyperplane construction)**.** *Let G be a group of order 2^a of fixed-point free involutions acting on $\mathbb{Z}_2^{2a}$. There is a $G - (2^{2a}, (2^{a-1} - 1)(2^a - 1) + 1, (2^{a-1} - 1)(2^{a-1} - 2))$ difference set of $\mathbb{Z}_2^{2a}$.*

Proof:

Since all of the nonidentity elements of G have order 2, G must be isomorphic to $\mathbb{Z}_2^a$. There are $2^a - 1$ subgroups of G of order 2^{a-1}, denoted $H_i, 1 \leq i \leq 2^a - 1$. We observe that each G-orbit has 2^a elements since all of the involutions are fixed-point free, so there are 2^a distinct orbits. We identify a special element of each orbit, $p_i \in \mathcal{O}_i$. We associate the subgroup H_i to the i^{th} orbit $\mathcal{O}_i$, and we construct the set $D_i = \{\phi(h)(p_i) | h \in H_i, h \neq 1\} \subset \mathcal{O}_i$. We claim that $D = (\bigcup_{i=1}^{2^a-1} D_i) \cup \{p_{2^a}\}$ is a G-difference set with the parameters listed in the theorem. We can easily see that v and k have the correct sizes, so we are left with verifying that there are λ solutions $(x, y) \in D \times D$ to the equation $y = \phi(g)(x)$ for a given nonidentity $g \in G$. We need only consider ordered pairs (x, y) where x and y are in the same orbit (if not, then there won't be any solutions to our equation). Suppose $(x, y) \in (D_i)^2$ satisfies $y = \phi(g)(x)$ for $g \notin H_i$. Then $y = \phi(h)(p_i)$ and $x = \phi(h')(p_i)$ for some $h, h' \in H_i$ implies that $\phi(h)(p_i) = y = \phi(g)(x) = \phi(g)(\phi(h')(p_i)) = \phi(gh')(p_i)$. Since the group action on the orbit is regular, we get that $h = gh'$, or $g = h(h')^{-1} \in H_i$. This contradiction shows that there are no solutions $(x, y) \in (D_i)^2$ when $g \notin H_i$. A similar argument shows that we will have solutions when $(x, y) \in (D_i)^2$ and $g \in H_i$, and we will have a solution whenever $g = h(h')^{-1}$ for $h, h' \in H_i$. There are $2^{a-1} - 2$ solutions $h, h' \in H_i$ (there are $|H_i| = 2^{a-1}$ solutions in elements of H_i, but we lose

two of those solutions since we excluded the identity element in the construction of the D_i). Since g is contained in $2^{a-1}-1$ subgroups, we get $\lambda = (2^{a-1}-1)(2^{a-1}-2)$. □

We note that G-difference sets in Theorem 4.5 satisfy $k - \lambda = \frac{v}{4}$ and hence can be used to construct G-perfect nonlinear functions. We could construct G-difference sets in similar sets by using subspaces other than the hyperplanes, but those constructions fall outside the scope of this paper.

Using the hyperplane construction and Theorem 4.1 we can establish the following corollary that leads to relevant cryptographic examples.

Corollary 4.6. *Let ϕ be a homomorphism from $G = \mathbb{Z}_2^a$ to the symmetries of the set $X = \mathbb{Z}_2^{2a+b}$ defined by $\phi((g_1, g_2, \ldots, g_a)((x_1, x_2, \ldots, x_{2a+b})) = (g_1 + x_1, \ldots, g_a + x_a, x_{a+1}, \ldots, x_{2a+b})$. There is a $G - (2^{2a+b}, 2^b((2^{a-1}-1)(2^a-1)+1), 2^b(2^{a-1}-1)(2^{a-1}-2))$ difference set of $\mathbb{Z}_2^{2a+b}$.*

Proof: By Theorem 4.5, there exists a $G - (2^{2a}, (2^{a-1}-1)(2^a-1)+1, (2^{a-1}-1)(2^{a-1}-2))$ difference set D of $\mathbb{Z}_2^{2a}$. By Theorem 4.1, $\bigcup_{y \in \mathbb{Z}_2^b} (D \times \{y\})$ is a $G - (2^{2a+b}, 2^b((2^{a-1}-1)(2^a-1)+1), 2^b(2^{a-1}-1)(2^{a-1}-2))$ difference set of $\mathbb{Z}_2^{2a+b}$. □

If we choose a and b to be odd integers and G is $\mathbb{Z}_2^a$ so that there is no perfect nonlinear (or bent) functions $f : \mathbb{Z}_2^a \to \mathbb{Z}_2$ or $f : \mathbb{Z}_2^{2a+b} \to \mathbb{Z}_2$, then Corollary 4.6 demonstrates that we are able to construct Z_2^a-perfect nonlinear functions from $\mathbb{Z}_2^{2a+b}$ to $\mathbb{Z}_2$. The group action based approach for perfect nonlinearity (and difference set) ensures the existence of G-perfect nonlinear functions in cases impossible for the traditional theory.

Finally we can combine all of the constructions in this section by applying Theorems 4.1 and 4.3 to Corollary 4.2 and Theorem 4.5, yielding the following corollary.

Corollary 4.7. *Let G be a group of order 2^{2a} of fixed-point free involutions acting on a set X with $2^{4a}t$ elements. There is a $G - (2^{4a}t, (2^{2a-1}-1)(s(2^{2a}-1)-i) + (2^{2a-1}+1)i + (s-j) + (2^{2a}-1)j + (2^{2a-1}-2^a)(t-s-\ell) + (2^{2a-1}+2^a)\ell, (2^{2a-1}-1)(2^{2a-1}-2)s + (2^{2a-2}-2^a)(t-s) + 2i + (2^{2a}-2)j + 2^{a+1}\ell)$-difference set of X for $0 \le s \le t, 0 \le i \le (2^{2a}-1)s, 0 \le j \le s$, and $0 \le \ell \le t-s$.*

Proof: We will use Hadamard difference sets in $2^{2a}s$ of the orbits of this group action; we can choose to use the Hadamard difference set or its complement in these orbits. In the remaining $2^{2a}(t-s)$ orbits, we will have $(t-s)$ complete hyperplane constructions each of which uses 2^{2a} orbits. We can complement any of the orbits: the parameter i in the corollary refers to the orbits associated to the hyperplanes; the parameter j refers to the orbit with a single element in the hyperplane construction; the parameter ℓ refers to the orbits with Hadamard difference sets. Simple counting gives the result. □

The number of G-difference sets with different orbit-intersection sizes in Corollary 4.7 is $\sum_{s=0}^{t} [\{(t-s)2^{2a}+1\}(s+1)(s(2^{2a}-1)+1)]$. As an example, there are

12,790 different G-difference sets, where G is a group of order 16 acting on a set X with 1024 elements. Not all of these G-difference sets will have distinct values for $k = |D|$, but they will have distinct patterns of orbit-intersection sizes. Compare this with the classical difference set case, where all of the difference sets in a group of order 1024 have either 496 or 528 elements (only two choices). All of these G-difference sets coming from Corollary 4.7 satisfy $k - \lambda = \frac{v}{4}$ and hence can be used to construct G-perfect nonlinear functions.

5. G-Relative Difference Set Constructions and vector-valued G-perfect nonlinear functions

By Theorem 3.4, H-valued G-perfect nonlinear functions are equivalent to $G \times H$ semiregular relative difference sets (RDSs) in $X \times H$ relative to $\{1_G\} \times H$. This motivates our search for $G \times H$-RDSs with $H = \mathbb{Z}_2^a$ for $a > 1$: any constructions will yield G-perfect nonlinear functions whose range is larger than $\mathbb{Z}_2$ and hence can be used to construct generalized S-boxes. The next theorem involves $G \times H$-relative difference set constructions modelled on the G-difference set constructions presented in Theorem 4.1 (the proof is similar and is omitted).

Theorem 5.1. *Let $\phi : G \to S(X)$ define a group action of the group G on the nonempty set X of cardinality m, let H be a group of order n, and suppose D_i is a $G \times H - (m, n, k_i, \lambda_i)$-relative difference set of $X \times H$ for $1 \leq i \leq t$. Suppose $Y = \{y_1, y_2, \ldots, y_t\}$ is a set of cardinality t, and define the group action Φ of $G \times H$ on $X \times H \times Y$ by $\Phi((g,h))((x,h',y)) = (\phi(g)(x), hh', y)$ for $(x,h',y) \in X \times H \times Y$. Then $D = \bigcup_{i=1}^{t}(D_i \times \{y_i\})$ is a $G \times H - (mt, n, \sum_{i=1}^{t} k_i, \sum_{i=1}^{t} \lambda_i)$-difference set of $X \times H \times Y$.*

If G is any abelian group of order 2^{2a} with a subgroup isomorphic to $\mathbb{Z}_2^a$ and if $H = \mathbb{Z}_2^a$, then [10] demonstrates that there is a $(2^{2a}, 2^a, 2^{2a}, 2^a)$-relative difference set in $G \times H$ relative to $\{1_G\} \times H$. If we allow $X = G$ and $\phi(g)(x) = gx$ (left translation as the group action), then we get the following $G \times H$-RDSs.

Corollary 5.2. *Suppose G is a group of order 2^{2a} with a subgroup isomorphic to $\mathbb{Z}_2^a$, $H = \mathbb{Z}_2^a$, and Y is a set of cardinality t. If G acts on itself by left translation, then there is a $G \times H - (2^{2a+t}, 2^a, 2^{2a+t}, 2^{a+t})-$relative difference set in $G \times H \times Y$ relative to $\{1_G\} \times H$.*

As indicated in Theorem 3.4, this implies G-perfect nonlinear vector-valued functions from $X \times Y$ to H where G and H are as in the Corollary.

The following construction yields a very nice application indicating the potential applications of the generalized approach. In the classical case, many cryptographic applications, namely **substitution-permutation networks** [16] such as the AES, require functions $f : \mathbb{Z}_2^a \to \mathbb{Z}_2^a$. In this case, it is clearly impossible to have a perfect nonlinear function: if x is a solution of $f(\alpha + x) + f(x) = \beta$, then $\alpha + x$ is a distinct second solution of the derivative equation, and only one solution is allowed. The optimal resistance against the classical differential attack is represented by **Almost Perfect Nonlinear** (APN) functions that come as close to perfect nonlinear as possible. An APN function $f : \mathbb{Z}_2^a \to \mathbb{Z}_2^a$ requires that for each nonzero $\alpha \in \mathbb{Z}_2^a$ and

each $\beta \in \mathbb{Z}_2^a$, the equation $f(\alpha+x)+f(x) = \beta$ has either 0 or 2 solutions. Since their introduction by Nyberg [26] and their initial study by Chabaud and Vaudenay [8] a large literature has arisen around constructions of APN functions. The substitution-permutation networks use invertible S-boxes and therefore need APN permutations. Unfortunately it is conjectured that such permutations exist only when a is an odd integer [6, 20]; for instance the AES uses as a S-box the inverse involution in a finite field $GF(2^a)$ which is an APN permutation when a is odd and differentially 4-uniform when a is even [27]. However, the following theorem demonstrates that we can construct G-perfect nonlinear permutations $f : \mathbb{Z}_2^a \to \mathbb{Z}_2^a$ for a very large group G even if a is an even integer. An associative division ring (also called *skew field*) satisfies all the properties as a field except possibly commutativity of multiplication.

Theorem 5.3 (Planar construction)**.** *Let $\mathbb{K}$ be any associative division ring, let M be a left $\mathbb{K}$-module, and let f be any automorphism of the additive group of M. If $\mathbb{K}^*$ is the multiplicative group of $\mathbb{K}$ that acts on M by left multiplication (which is a faithful action), then f is a $\mathbb{K}^*$-perfect nonlinear function from M to itself.*

Proof: First note that the notion of G-perfect nonlinearity for functions from M to itself is here implicitly and rather naturally extended to an eventual infinite setting. We need to show that $f(\alpha x) - f(x) = \beta$ has a unique solution for $\alpha \in \mathbb{K}^*, \alpha \neq 1$ and $\beta \in M$. Since f is an additive automorphism, $f(\alpha x) - f(x) = f(\alpha x - x) = f((\alpha - 1)x)$. Now since f is a bijection, f^{-1} exists and $(\alpha - 1)x = f^{-1}(\beta)$. Finally, since $\alpha \neq 1$, $(\alpha - 1)$ is invertible in the division ring, and $x = (\alpha - 1)^{-1} f^{-1}(\beta)$ is the unique solution to the derivative equation as required. □

As indicated above, if we choose in the previous theorem the finite field with 2^a elements $GF(2^a)$ as $\mathbb{K}$ and M, we obtain $GF(2^a)^*$-perfect nonlinear permutations of $GF(2^a)$ whether a is an even or an odd integer.

We comment that this result works for all associative division rings, even infinite and/or nonabelian (for instance the quaternions). Thus, if there were ever an application for an infinite-dimensional (abelian or nonabelian) S-box, this construction could be adapted for that situation. The proof also works for any semifield $\mathbb{S}$ (a kind of nonassociative skew field; for instance the octonions) and module M over the semifield. Since the nonzero elements of a semifield $\mathbb{S}^*$ form a loop (a kind of nonassociative group), they do not operate as a permutation group on the module. Therefore in this case we do not formally obtain an $\mathbb{S}^*$-perfect nonlinear function $f : M \to M$. However for each $\alpha \in \mathbb{S}^*$, $x \mapsto \alpha x$ is a permutation of M and if $\alpha \neq 1$, then $\alpha x \neq x$ for every $x \neq 0_M$; so the left multiplication is close to a faithful group action and f seems like a $\mathbb{S}^*$-perfect nonlinear function.

Until recently [5, 15] the only known examples of APN functions were some power function $x \mapsto x^d$ in a (characteristic 2) finite field [2, 13, 14, 19, 27]. Our last construction gives similar result in the group action setting.

Theorem 5.4 (Monomial construction)**.** *Let p be a prime number, let $GF(p^a)^*$ act faithfully on $GF(p^a)$ by multiplication and let $d \in \mathbb{N}$ such that $1 \leq d \leq p^a - 1$ which is invertible modulo $p^a - 1$. Then the monomial mapping $f : x \mapsto x^d$ of $GF(p^a)$ is a $GF(p^a)^*$-perfect nonlinear permutation.*

Proof: Since d is invertible modulo $p^a - 1$, f is a permutation. To see that f is also $GF(p^a)^*$-perfect nonlinear, we need to compute the number of solutions to the equation

$$(\alpha x)^d - x^d = \beta \tag{5.1}$$

for each $(\alpha, \beta) \in (GF(p^a)^* \backslash \{1\}) \times GF(p^a)$. The above equation is equivalent to $x^d = \frac{\beta}{\alpha^d - 1}$ $(\alpha \neq 1)$. If we raise both sides to the power e corresponding to the inverse of d modulo $p^a - 1$ we get $x = (\frac{\beta}{\alpha^d - 1})^e$ as the unique solution to the equation (5.1). □

Obviously not all power permutations are additive automorphisms of a finite field (for instance the APN power permutations), therefore the monomial and planar constructions can lead to possibly different G-perfect nonlinear permutations.

References

[1] K. T. Arasu, C. Ding, T. Helleseth, P. V. Kumar and H. Martinsen, Almost difference sets and their sequences with optimal autocorrelations, IEEE Trans. Information Theory, Vol. 47, No. 7 (2001) pp. 2934-2943.

[2] T. Beth and C. Ding, On almost perfect nonlinear permutations, Advances in Cryptology - Eurocrypt '93, Lecture Notes in Computer Science, Springer, 765 (1994) pp. 65-76.

[3] T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, Second Edition, Cambridge University Press, Cambridge (1999).

[4] E. Biham and A. Shamir, Differential cryptanalysis of DES-like cryptosystems, Journal of Cryptology, Vol. 4, No. 1 (1991) pp. 3-72.

[5] L. Budaghyan, C. Carlet, P. Felke and G. Leander, An infinite class of quadratic APN functions which are not equivalent to power mappings, preprint, http://eprint.iacr.org/2005/359 (2005).

[6] C. Carlet, P. Charpin and V. Zinoviev, Codes, bent functions and permutations suitable for DES-like Cryptosystems, Designs, Codes and Cryptography, Vol. 15, No. 2 (1998) pp. 125-146.

[7] C. Carlet and C. Ding, Highly nonlinear mappings, Journal of Complexity, Vol. 20, No. 2 (2004) pp. 205-244.

[8] F. Chabaud and S. Vaudenay, Links between differential and linear cryptanalysis, Advances in Cryptology - Eurocrypt '94, Lecture Notes in Computer Science, Springer, 950 (1995) pp. 356-365.

[9] J. Daemen and V. Rijmen, The design of Rijndael: AES - The Advanced Encryption Standard, Springer-Verlag (2002).

[10] J. A. Davis, Construction of relative difference sets in p-groups, Discrete Math, Vol. 103 (1992) pp. 7-15.

[11] J.F. Dillon, Elementary Hadamard difference sets, PhD thesis, University of Maryland (1974).

[12] C. Ding and J. Yuan, A family of skew Hadamard difference sets, Journal of Combinatorial Theory A, Vol. 113, No. 7 (2006) pp. 1526-1535.

[13] H. Dobbertin, Almost perfect nonlinear power functions on $GF(2^n)$: The Niho case, Information and Comutation, Vol. 151 (1999) pp. 57-72.

[14] H. Dobbertin, Almost perfect nonlinear power functions on $GF(2^n)$: a new case for n divisible by 5, D. Jugnickel and H. Niederreiter (Eds.), Proceedings of Finite Fields and Applications Fq5, Springer (2000) pp. 113-121.

[15] Y. Edel, G. Kyureghyan and A. Pott, A new APN function which is not equivalent to a power mapping, preprint, http://arxiv.org/abs/math.CO/0506420 (2005).

[16] H. Feistel, Cryptography and computer privacy, Scientific american, Vol. 228, No. 5 (1973) pp. 15-23.

[17] FIPS 46-3, Data encryption standard, Federal Information Processing Standards Publication 46-3 (1999), U.S. Department of Commerce/N.I.S.T.

[18] FIPS 197, Advanced encryption standard, Federal Information Processing Standards Publication 197 (2001), U.S. Department of Commerce/N.I.S.T.
[19] R. Gold, Maximal recursive sequences with 3-valued recursive crosscorrelation functions, IEEE Trans. Inform. Theory, Vol. 14 (1968) pp. 154-156.
[20] X.-D. Hou, Affinity of permutations of $\mathbb{F}_2^n$, D. Augot, P. Charpin and G. Kabatiansky (Eds.), Workshop on Coding and Cryptography 2003 (2003) pp. 273-280.
[21] W. Kantor, Exponential numbers of two-weight codes, difference sets, and symmetric designs, Discrete Math, Vol. 46 (1983) pp. 95-98.
[22] X. Lai and J. L. Massey, A proposal for a new block encryption standard, Advances in Cryptology - Eurocrypt '90, Lecture Notes in Computer Science, Springer, 473 (1991) pp. 389-404.
[23] M. Matsui, Linear cryptanalysis method for DES cipher, Advances in cryptology - Eurocrypt '93, Lecture Notes in Computer Science, Springer, 765 (1994) pp. 386-397.
[24] W. Meier and O. Staffelbach, Nonlinearity criteria for cryptographic functions, Advances in Cryptology - Eurocrypt '89, Lecture Notes in Computer Science, Springer, 434 (1990) pp. 549-562.
[25] K. Nyberg, Perfect nonlinear S-boxes, Advances in Cryptology - Eurocrypt '91, Lecture Notes in Computer Science, Springer, 547 (1992) pp. 378-386.
[26] K. Nyberg, On the construction of highly nonlinear permutations, Advances in Cryptology - Eurocrypt '92, Lecture Notes in Computer Science, Springer, 658 (1993) pp. 92-98.
[27] K. Nyberg, Differentially uniform mappings for cryptography, Advances in Cryptology - Eurocrypt '93, Lecture Notes in Computer Science, Springer, 765 (1994) pp. 55-64.
[28] R. E. A. C. Paley, On orthogonal matrices, J. Math. Phys. MIT, Vol. 12 (1933) pp. 311-320.
[29] L. Poinsot, Non linéarité parfaite généralisée au sens des actions de groupes, contribution aux fondements de la solidité cryptographique (available at http://poinsot.univ-tln.fr/These.pdf), PhD thesis, University of South Toulon-Var, 2005.
[30] L. Poinsot and S. Harari, Generalized Boolean bent functions, Progress in Cryptology - Indocrypt 2004, Lecture Notes in Computer Science, Springer, 3348 (2004) pp. 107-119.
[31] L. Poinsot and S. Harari, Group actions based perfect nonlinearity, GESTS International Transaction on Computer Science and Engineering, Vol. 12, No. 1 (2005) pp. 1-14.
[32] A. Pott, Nonlinear functions in abelian groups and relative difference sets, Discrete Applied Mathematics, Vol. 138 (2004) pp. 177-193.
[33] O. S. Rothaus, On bent functions, J. Comb. Theory 20 A (1976), pp. 300-305.
[34] V. V. Shorin, V. V. Jelezniakov and E. M. Gabidulin, Linear and differential cryptanalysis of Russian GOST, D. Augot, C. Carlet (Eds.), Workshop on Coding and Cryptography 2001 (2001) pp. 467-476.

Department of Mathematics and Computer Science, University of Richmond, Richmond, VA 23173, USA, email: jdavis@richmond.edu

Institut des Sciences de l'Ingénieur de Toulon et du Var, Université du Sud Toulon-Var, Avenue Georges Pompidou, B.P. 56, 83 162 La Valette cédex, France, email: poinsot@univ-tln.fr