Boolean Bent Functions in Impossible Cases: Odd and Plane Dimensions

Laurent Poinsot†

†*Université du Sud Toulon-Var, Institut des Sciences de l'Ingénieur de Toulon et du Var, Avenue G. Pompidou, BP 56, 83 162 La Valette du Var cédex, France*

Summary
Bent or perfect nonlinear Boolean functions represent the best resistance against the so-called linear and differential cryptanalysis. But this kind of cryptographic relevant functions only exists when the number of input bits m is an even integer and is larger than the double of the number of output bits n. Unfortunately the non-existence cases, the *odd dimension* (m is an odd integer) or the *plane dimension* ($m = n$), are not illegitimate from a cryptographic point of view and even commonly considered. New notions of bentness and perfect nonlinearity are then needed in those impossible cases for the traditional theory. In this paper, by replacing the usual XOR by another kind of bit-strings combination, we explicitly construct new "bent" Boolean functions in traditionally impossible cases.

Key words: cryptography, bent functions, perfect nonlinearity, group actions, fixed-point free involutions

1. Introduction

When used as components of a secret-key cryptosystem, Boolean functions must be highly nonlinear in order to avoid vulnerabilities to a differential [1] or linear attack [6]. Informally speaking, linear cryptanalysis relies on the probability of success of a linear approximation of a function. Basically the differential cryptanalysis exploits the differences between plain and ciphered binary strings, *i.e.* the XOR combination of these bit-strings, which appear more often than at random. The objective of both attacks is to discover the secret key used in the ciphering process. Then Boolean functions must exhibit the optimal resistances against at least these two attacks.
Boolean bent functions [3, 12] are those Boolean functions whose Fourier spectrum contains only two values. In other words, their frequential representation has the simplest form. They ensure the best resistance against linear attacks. Perfect nonlinear Boolean functions [7] are those Boolean functions whose XORed outputs for XORed inputs are uniformly distributed over the set of all possible values. The best resistance against a differential attack is obtained by this kind of functions. These two notions are actually equivalent by duality using the Fourier transform. Nevertheless such functions only exist in very restrictive cases: the number of input bits m is an even integer and it is larger than two times the number n of output bits. Unfortunately the impossible cases *i.e.* when m is an odd integer (call it "*odd dimension*") or when m is equal to n (call it "*plane dimension*") occur in many cryptographic applications: for instance, a ciphering function generally maps plain bit-strings to ciphered bit-strings, both with the same length. As linear and differential attacks can obviously be applied in such cases, we need to define a new kind of resistances or in other terms, a new kind of bentness and perfect nonlinearity.
In recent contributions [9, 10], we introduce the concept of G-perfect nonlinearity, which is a natural extension of the traditional one, obtained by replacing the XOR operation by other kinds of binary strings combinations. This combinatorial property has an equivalent characterization by the Fourier transform called G-bentness as in the classical setting. In this paper by using this new approach for nonlinearity, we construct some Boolean G-bent functions in cases impossible for the traditional theory: in odd and plane dimensions. We also present the principle of a G-differential attack and we exhibit a possible weakness of the S-boxes of the famous DES against such new cryptanalysis.

2. Boolean bent functions: the classical approach

2.1 Boolean bent and perfect nonlinear functions

In this paper $GF(2)$ denotes the finite field of modulo-2 integers and, as usually, it is considered as the subset $\{0,1\}$ in the real field $\mathbb{R}$ and the modulo-2 sum (or XOR) is designed by the symbol "$\oplus$".
A m-dimensional vector space over $GF(2)$ is designed by V_m. It can be interpreted as the $GF(2)$-vector space of

Manuscript received July 25, 2006.
Manuscript revised August 25, 2006.

m-tuples $GF(2)^m$ or as the finite field (in characteristic 2) of 2^m elements $GF(2^m)$. These two structures can be equipped with a dot-product: for $(x, y) \in (GF(2)^m)^2$, we have

$$x.y = x_1y_1 \oplus x_2y_2 \oplus ... \oplus x_my_m$$

and for $(x, y) \in (GF(2^m))^2$, the dot-product becomes

$$x.y = tr(xy)$$

where "*tr*" is the absolute trace of $GF(2^m)$. As two $GF(2)$-Hilbert spaces of the same (finite) dimension are isomorphic, we use the same symbol "." which stands for a dot-product for V_m (which is the ideal m-dimensional $GF(2)$-Hilbert space) and can take one of the previous forms. We also use the symbol "$\oplus$" to denote at the same time the component-wise modulo 2 sum of $GF(2)^m$ and the addition law in $GF(2^m)$. Then this symbol is used for the addition in V_m.

The zero of V_m is denoted 0_m. For any group *G*, G^* is the set of all non-identity elements of *G*.

Using these notations, a *Boolean function* is simply a function $f : V_m \to V_n$ (some time called a (*m*,*n*)-Boolean function).

The notion of Boolean bent functions originally introduced by [3] and [12], is very relevant in cryptography since such functions exhibit the best resistance against the so-called linear cryptanalysis [6]. This notion is closely related to the Hadamard-Walsh transform which is a particular case of the (discrete) Fourier transform.

Definition 1.

Let $\varphi : V_m \to \mathbb{R}$ be a function, we denote by $\hat{\varphi} : V_m \to \mathbb{R}$ the Walsh-Hadamard transform of φ:

$$\forall \alpha \in V_m, \hat{\varphi}(\alpha) = \sum_{x \in V_m} \varphi(x)(-1)^{\alpha.x}.$$

In order to use this transform, we need to identify Boolean functions with real-valued ones. This is done using the notion of characters.

Definition 2.

Let $\alpha \in V_m$. The character of α is the map χ_m^α defined by

$$\chi_m^\alpha : V_m \to \{\pm 1\}$$
$$x \mapsto (-1)^{\alpha.x}.$$

Then a function $f : V_m \to V_n$ is transformed as a real-valued function defined on V_m by considering the maps $f_\beta := \chi_n^\beta \circ f : x \mapsto (-1)^{\beta.f(x)}$ for $\beta \in V_n$.

Definition 3.

A Boolean function $f : V_m \to V_n$ is bent if for all $\beta \in V_n^*$ and for all $\alpha \in V_m$, we have

$$\hat{f}_\beta(\alpha) = \pm 2^{\frac{m}{2}}.$$

Boolean bentness has also a combinatorics characterization called *perfect nonlinearity* [7].

Perfect nonlinear functions are those functions that exhibit the best resistance against the famous differential attack [1].

Definition 4.

A Boolean function $f : V_m \to V_n$ is called perfect nonlinear if for all $\alpha \in V_m^*$ and for all $\beta \in V_n$,

$$|\{x \in V_m \mid f(\alpha \oplus x) \oplus f(x) = \beta\}| = 2^{m-n}$$

where $|X|$ is the cardinality of a finite set X.

Theorem 1. *[7]*

A Boolean function $f : V_m \to V_n$ is bent if and only if it is perfect nonlinear.

Bent functions are difficult to exhibit but there exist some explicit constructions. For instance, the famous Maiorana-McFarland construction.

Proposition 1. *[3]*

Let m be an even integer. Let $g : V_{\frac{m}{2}} \to V_1 = GF(2)$ be any function and π a permutation over $V_{\frac{m}{2}}$. Then the function

$$f : V_m \to \mathrm{V}_1$$
$$(x, y) \mapsto x.\pi(y) \oplus g(y)$$

is bent (we have identified V_m with $V_{\frac{m}{2}} \times V_{\frac{m}{2}}$).

Bent functions do not exist for each choice of (m, n): there are some important constraints on these exponents.

Theorem 2. *[7]*

Bent functions exist only for $m \geq 2n$ and m is even.

In particular bent functions do not exist in *odd dimension* (m is an odd integer) nor in *plane dimension* ($m = n$). This is very restrictive since many cryptographic

applications used functions that maps bit-strings to bit-stings of the same length. Then we need other objects to define resistances against differential or linear cryptanalysis. In this paper, we present a group action approach to solve this problem; nevertheless some authors have already worked on the subject and used another method.

2.2 Almost bent and almost perfect nonlinear functions

If m is even or $m < 2n$, bent functions do not exist and we need other bounds to define differential and linear resistant functions. Some results have been found by Chabaud and Vaudenay [2].

Definition 5.
Let $f : V_m \to V_m$ be a Boolean function. f is almost perfect nonlinear if for all $\alpha \in V_m^*$ and $\beta \in V_m$,

$$|\{x \in V_m \mid f(\alpha \oplus x) \oplus f(x) = \beta\}| \in \{0,2\}.$$

As differential resistance is measured as the minimum over all maps $f : V_m \to V_m$ of the maximum over all $(\alpha, \beta) \in V_m^* \times V_m$ of

$$|\{x \in V_m \mid f(\alpha \oplus x) \oplus f(x) = \beta\}|$$

in the plane dimension case ($m = n$), the best possible value is 2. Then almost perfect nonlinear functions have the optimum resistance to differential cryptanalysis.

In a similar way, we can define the optimum resistance against linear cryptanalysis as follows.

Definition 6.
Let $f : V_m \to V_m$. The Boolean function f is called almost bent if for all $(\alpha, \beta) \in V_m \times V_m^*$,

$$\hat{f}_\beta(\alpha) = \{0, \pm 2^{\frac{m+1}{2}}\}.$$

Such functions only exist when m is an odd integer. Finally we have

Theorem 3. *[2]*
If the function $f : V_m \to V_m$ is almost bent then it is also almost perfect nonlinear.

The reciprocal assertion of the theorem above is false in general since the map $\sigma : GF(2^m) \to GF(2^m)$ defined by $\sigma(x) = x^{-1}$ if $x \in GF(2^m)^*$ and $\sigma(0_m) = 0_m$ is almost perfect nonlinear (when m is an odd integer [8]) but it is not almost bent (it a consequence of [5]).

In this paper we present another way to treat a similar problem using group actions.

3. Boolean bent functions: the group action approach

3.1 Basics on the theory of characters and group actions

In the remainder of this paper, the letter "G" stands for a finite abelian group in multiplicative representation. Our approach of nonlinearity and bentness is described using the Fourier transform and the notion of group actions. So in this subsection are recalled some basics on them.

3.1.1 Theory of characters

A *character* of a group G is a group homomorphism from G to the unit circle of the complex field $\mathbb{C}$. The set of all characters, denoted by $\hat{G}$, when equipped with the point-wise multiplication of functions, is a group isomorphic to G itself. We always suppose that an isomorphism from G to $\hat{G}$ is fixed and the image of $\alpha \in G$ by such isomorphism (called the *character of* α) is denoted by χ^α. For instance the character of $\alpha \in V_m$ is given by the function χ_m^α as already introduced. Using the theory of characters we can define the (discrete) Fourier transform on G.

Definition 7.
Let $\varphi : V_m \to \mathbb{C}$ be a function. The Fourier transform of φ is the map $\hat{\varphi}$ defined by

$$\hat{\varphi} : G \to \mathbb{C}$$
$$x \mapsto \sum_{\alpha \in G} \varphi(x) \chi^\alpha(x).$$

The Walsh-Hadamard transform is a particular instance of the discrete Fourier transform for elementary abelian 2-groups.

3.1.2 Group actions

A *group action* of a group G on a nonempty set X is a group homomorphism φ from G so $S(X)$ the symmetric group of X (the group of all permutations over X). For instance we can define the *regular action by translation* of a group G on itself as follows

$$\varphi : G \to \mathrm{S(G)}$$
$$\alpha \mapsto (\varphi(\alpha) : x \mapsto \alpha x).$$

Instead of writing "$\varphi(\alpha)(x)$" for $(\alpha, x) \in G \times X$, we use the convenient notation "$\alpha.x$" similar to the regular action by translation. The *orbital* of an element $x \in X$ under the action of G is

$$O_G(x) = \{\alpha.x \mid \alpha \in G\}.$$

The orbitals define a partition of the set X.

An action is called *faithful* if the corresponding homomorphism φ is injective or in other terms there is no $\alpha \in G^*$, such that $\alpha.x = x$ for all $x \in X$. An action is called *regular* if for all $(x, y) \in X^2$ there exists one and only one $\alpha \in G$ such that $\alpha.x = y$ (in particular a regular action is also faithful). For instance, the regular action by translation is regular.

There is a particular kind of group actions on Boolean vector spaces which will be useful in the sequel. A *fixed-point free involution* σ of V_m is an element of $S(V_m)$ such that

1. $\sigma^{-1} = \sigma$,
2. for all $x \in V_m$, $\sigma(x) \neq x$.

For instance the translations over V_m, $\sigma_\alpha : x \mapsto \alpha \oplus x$, are fixed-point free involutions. Let identify V_k as a subvector space of V_m of dimension k (with $1 \leq k \leq m$). A group action of V_k on V_m can be naturally defined as follows: for $(\alpha, x) \in V_k \times V_m$, we define $\alpha.x = \alpha \oplus x$. Moreover it is obvious that V_k acts faithfully (and even regularly if $k = m$) on V_m.

3.2 *G*-perfect nonlinearity and *G*-bentness

Embedded in the definition of perfect nonlinearity is the regular action by translation of V_m. So we can naturally extend this notion of nonlinearity by replacing translations by another kind of group actions. In [9, 10], we have introduced the concept of *G*-perfect nonlinearity that we briefly recall in the Boolean setting.

Definition 8.
Let G be a finite abelian group thats acts faithfully over V_m. A Boolean function $f : V_m \to V_n$ is called G-perfect nonlinear if for all $\alpha \in G^*$ and all $\beta \in V_n$, we have

$$|\{x \in V_m \mid f(\alpha.x) \oplus f(x) = \beta\}| = 2^{m-n}.$$

This notion is similar to the classical one except that we have replaced the translations by the action of G on V_m.

On an other hand, we can define a group action based notion of bentness.

Definition 9.
Let G be a finite abelian group thats acts faithfully over V_m. A Boolean function $f : V_m \to V_n$ is called G-bent if for all $\beta \in V_n^*$ and all $\alpha \in G$, we have

$$\frac{1}{2^m} \sum_{x \in V_m} |\hat{f}_{x_\beta}(\alpha)|^2 = |\mathrm{G}|$$

where for each $x \in X$, f_x is defined as

$$f_x : G \to \mathrm{V_n}$$
$$\alpha \mapsto f(\alpha.x)$$

and $|z|$ is the complex modulus of $z \in \mathbb{C}$.
These two concepts are actually identical as it is the case in the traditional setting.

Theorem 4. *[10]*
Let G be a finite abelian group thats acts faithfully over V_m. A Boolean function $f : V_m \to V_n$ is G-perfect nonlinear if and only if it is G-bent.
This definition of *G*-bentness permits us to explicitly construct (see Section 4) "bent" functions in cases otherwise impossible with the standard notion of bentness. These constructions rely on the characterization of *G*.

3.3 *G*-difference sets

In the paper [10] we gave a combinatorics characterization of *G*-bentness and *G*-perfect nonlinearity for V_1-valued functions in terms of some special objects called *G*-difference sets.

Definition 9.
Let G be a finite abelian group thats acts faithfully over V_m. *A subset D of* V_m *is called a G-*(K,λ)*-difference set of* V_m *if*
1. $K = |D|$,
2. *for each* $\alpha \in G^*$, *there exist exactly* λ *solutions* $(x,y) \in D^2$ *to the equation* $\alpha.x = y$.

In the case where $G = V_m$ and the action is the regular action by translation, this notion is equivalent to the traditional concept of difference sets in V_m.

The *indicator function* of a subset S of a set X is the map $i_S : X \to V_1 = \{0,1\}$ defined by $i_S(x) = 1$ if $x \in S$ and $i_S(x) = 0$ if $x \notin S$.

Theorem 5. *[10]*
Let G be a finite abelian group that acts faithfully over V_m. *Let* $D \subset V_m$. *Then D is a G-* (K,λ) *-difference set of* V_m *such that* $2^m = 4(K-\lambda)$ *if and only if* $i_D : V_m \to V_1 = \{0,1\}$ *is G-bent.*

In the following section, we use this particular characterization to construct a *G*-bent function in odd dimension.

4. Boolean bent functions in odd and plane dimensions

In this section we construct some *G*-bent Boolean functions $f : V_m \to V_n$ in some cases impossible for the traditional theory: *m* is an odd integer or *m=n*. As we want these constructions to be relevant for cryptographic applications we restrict our choices for *G*: either V_k or $GF(2^m)^*$. With these particular choices, we remain in the Boolean setting which is important for implementations of cryptosystems.

4.1 Boolean bent functions in odd dimension

In this subsection, we present two constructions of V_k-bent functions $f : V_m \to V_n$ where m is an odd parameter. Note that the action of V_k over V_m has been described at the end of paragraph 3.1.2.

Theorem 6.
Let $f : V_k \to V_n$ *be a (classical) bent function and* $g : V_l \to V_n$ *be any function. Let m=k+l and* V_m *is identified with* $V_k \times V_l$. *Then the map h defined by*

$$h : V_m \to V_n$$
$$(x,y) \mapsto f(x) \oplus g(y)$$

is a V_k *-bent Boolean function.*

Proof. Let $(x,y) \in V_m^2$ and $\beta \in V_n^*$. We must compute $\hat{h}_{(x,y)_\beta}(\alpha)$ *i.e.* the Fourier transform of $\chi_n^\beta \circ h_{(x,y)}$ in $\alpha \in V_k$.

$$\hat{h}_{(x,y)_\beta}(\alpha) = \sum_{x' \in V_k} (-1)^{\beta.h_{(x,y)}(x')} (-1)^{\alpha.x'}$$
$$= \sum_{x' \in V_k} (-1)^{\beta.h(x' \oplus x, y) \oplus \alpha.x'}$$
$$= \sum_{x' \in V_k} (-1)^{\beta.(f(x' \oplus x) \oplus g(y)) \oplus \alpha.x'}$$
$$= (-1)^{\beta.g(y)} \sum_{x' \in V_k} (-1)^{\beta.f(x' \oplus x) \oplus \alpha.x'}$$
$$= (-1)^{\beta.g(y)} \sum_{x'' \in V_k} (-1)^{\beta.f(x'') \oplus \alpha.(x \oplus x'')}$$
$$= (-1)^{\beta.g(y) \oplus \alpha.x} \hat{f}_\beta(\alpha).$$

Then we have for all $\alpha \in V_k$ and for all $\beta \in V_n^*$,

$$\frac{1}{2^k} \sum_{(x,y) \in V_m} |\hat{h}_{(x,y)_\beta}(\alpha)|^2 = \frac{1}{2^k} \sum_{(x,y) \in V_m} |\hat{f}_\beta(\alpha)|^2 = \frac{1}{2^k} \sum_{(x,y) \in V_m} 2^k$$

(because f is bent). Then the sum is equal to 2^m and therefore h is V_k-bent. ***QED***

In particular if l is chosen so that *m=k+l* is odd then we have constructed a "bent" function in the odd dimension. However this construction is not satisfactory since it is

based on a classical bent function. We now give another construction which is independent of the traditional notion of bentness.

Lemma 1.
Let m be a non-zero positive integer. Each $\alpha \in V_m^*$ *is contained in* $2^{m-1}-1$ *subvector spaces of* V_m *of dimension m-1 over* $GF(2)$.

Proof. We will build up a basis that contains α. We can not use 0_m or α for the second vector in the basis, so we have 2^m-2 choices for how to fill the second basis vector (call it v_2). Once we have chosen v_2, we can not take any linear combination of α and v_2, so we have 2^m-4 choices for the third vector (call it v_3). Continuing in this manner, we will have 2^m-2^{m-2} choices for v_{m-1} since we can not use any linear combination of the collection $\{\alpha, v_2, v_3, ..., v_{m-2}\}$. We have over-counted, so we need to divide by the number of basis for a given (m-1)-dimensional subspace (that contains α). We have $2^{m-1}-2$ choices for the second vector since we can take any element of this subspace other than 0_m or α; we have $2^{m-1}-4$ choices for the third basis vector; and we continue until we have $2^{m-1}-2^{m-2}$ choices for the final vector. Writing this as a fraction, we have

$$\frac{(2^m-2)(2^m-4)(2^m-8)...(2^m-2^{m-2})}{(2^{m-1}-2)(2^{m-1}-4)(2^{m-1}-8)...(2^{m-1}-2^{m-2})}$$

By pulling out all of the powers of 2 and then canceling all the terms, this reduces to $2^{m-1}-1$. ***QED***

Theorem 7.
Let k and l be *any positive integers,* $k \neq 0$ *and l can be equal to zero. There exists a*

$$V_k\text{-}(2^l((2^{k-1}-1)(2^k-1)+1), 2^l(2^{k-1}-1)(2^{k-1}-2))$$

-difference set of V_{2k+l}. *In particular its parameters satisfy the equation*

$$2^{2k+l} = 4(K-\lambda).$$

Proof. Since V_k is a k-dimensional vector space, it contains 2^k-1 subvector spaces of dimension k - 1 denoted W_i for $1 \le i \le 2^k-1$. We observe that each orbital of V_{2k+l} under the action of V_k has exactly 2^k elements since all nonzero element of V_k acts as a fixed-point free involutions on V_{2k+l}, thus there are exactly 2^{k+l} such orbitals in V_{2k+l}. We choose one and only one element of each orbital: for $(i, j) \in \{1,...,2^k\} \times \{0,...,2^l-1\}$ $x_{i,j}$ is the representative of the $i + j\,2^k$ -th orbital

$$O_{V_k}(x_{i,j}) = \{\alpha \oplus x_{i,j} \in V_{2k+l} \mid \alpha \in V_k\}.$$

In particular if $x_{i,j} \neq x_{i',j'}$ then

$$O_{V_k}(x_{i,j}) \cap O_{V_k}(x_{i',j'}) = \emptyset.$$

For each $j \in \{0,...,2^l-1\}$, we associate the subvector space W_i to the orbital $O_{V_k}(x_{i,j})$ (so for i from 1 to 2^k-1) and we build-up the set

$$D_{i,j} = \{\alpha \oplus x_{i,j} \in V_{2k+l} \mid \alpha \in W_i, \alpha \neq 0_{2k+l}\}$$

which is a subset of $O_{V_k}(x_{i,j})$. Finally we construct

$$D_j = \bigcup_{i=1}^{2^k-1}(D_{i,j}) \cup \{x_{2^k,j}\}.$$

By construction, with a fixed j, $D_{i,j} \cap D_{i',j} = \emptyset$ for all $i \neq i'$. In particular $|D_j| = 1 + \sum_{i=1}^{2^k-1} |D_{i,j}|$. But

$$|D_{i,j}| = |W_i| - 1 = 2^{k-1} - 1$$

and then

$$|D_j| = (2^k-1)(2^{k-1}-1) + 1.$$

Then we construct the following set:

$$D = \bigcup_{j=0}^{2^l-1} D_j.$$

We note easily that $D_j \cap D_{j'} = \emptyset$ for all $j \neq j'$ and then D is a disjoint union. Its cardinality is then equal to

$$\sum_{j=0}^{2^l-1} |D_j| = 2^l((2^k-1)(2^{k-1}-1)+1).$$

We have already proved that the parameter $K = |D|$ is equal to the value given in the statement of the theorem. It is now sufficient to prove that D is a V_k-(K, λ) -difference set of V_{2k+l} with

$$\lambda = 2^l(2^{k-1}-1)(2^{k-1}-2).$$

Now we show that for all nonzero $\alpha \in V_k$, they are exactly λ solutions in D^2 to the equation $x = \alpha \oplus y$. Note that if x and y are not in the same orbital, we have no solution.

So let $(i, j) \in \{1,...,2^k\} \times \{0,...,2^l - 1\}$. If $i = 2^k$ then there is no solution in D^2 for a nonzero $\alpha \in V_k$ (because D only contains $x_{2^k,j}$ and α acts as a fixed-point free involution). Let suppose that $i \in \{1,...,2^k - 1\}$.

If $(x, y) \in O_{V_k}(x_{i,j})^2$ is a solution in D^2 of the equation $x = \alpha \oplus y$ for $\alpha \in W_i$, then $x = \beta \oplus x_{i,j}$ and $y = \beta' \oplus x_{i,j}$ for $(\beta, \beta') \in W_i^2$ implies that $\beta \oplus x_{i,j} = x = \alpha \oplus y = (\alpha \oplus \beta').(x_{i,j})$. Since the action of V_k on each its orbital is regular, we have $\beta = \alpha \oplus \beta'$ and then $\alpha = \beta \oplus \beta' \in W_i$, which is a contradiction and there is no solution of this form.

A similar argument shows that for each fixed $(i, j) \in \{1,...,2^k - 1\} \times \{0,...,2^l - 1\}$, we have at least one solution when $(x, y) \in O_{V_k}(x_{i,j})^2$ and $\alpha \in W_i$ and this is true as soon as $\alpha = \beta \oplus \beta'$ for $(\beta, \beta') \in W_i^2$. There are $2^{k-1} - 2$ solutions $(\beta, \alpha \oplus \beta) \in W_i^2$ (we have $|W_i| = 2^{k-1}$ pairs $(\beta, \alpha \oplus \beta)$ for a fixed α but we exclude the solutions $(0_k, \alpha)$ and $(\alpha, 0_k)$ otherwise $x = x_{i,j}$ or $y = x_{i,j}$ which is impossible by construction of $D_{i,j}$).

Moreover note that if $(\beta.x_{i,j_0}, (\alpha \oplus \beta).x_{i,j_0})$ is a solution in D^2 to the equation $x = \alpha \oplus y$ ($\alpha \in W_i$) then for each $j \in \{0,...,2^l - 1\}$, $(\beta.x_{i,j}, (\alpha \oplus \beta).x_{i,j})$ is a different solution (if $j \neq j_0$). Then there are 2^l such solutions.

Finally each nonzero $\alpha \in V_k$ is contained in $2^{k-1} - 1$ subspaces W_i (according to lemma 1). Then we have $\lambda = 2^l(2^{k-1} - 1)(2^{k-1} - 2)$.

QED

Since the parameters of the G-difference set satisfy the assumption of theorem 5, the indicator function of this set is V_k-bent. Moreover this construction is much more relevant than the previous one. Indeed we can choose the parameters k and l that make impossible the existence of any traditional bent function in this setting. If k is an odd integer, then for each $x \in V_{2k+l}$, the function $f_x : V_k \to V_1$ can not be (classical) bent and if l is also an odd integer, there is no bent function from V_{2k+l} to V_1 but with this construction, we know that there exists a V_k-Boolean bent function from V_{2k+l} to V_1.

4.2 Boolean bent functions in plane dimension

In this subsection we present a construction of G-bent function from V_m to V_m which is traditionally impossible since there only exist almost bent functions in plane dimension. In order to build this construction, we use the faithful action of $GF(2^m)^*$ on $GF(2^m)$ by multiplication. Indeed for

$$(\alpha, x) \in GF(2^m)^* \times GF(2^m)$$

we define

$$\alpha.x = \alpha x .$$

Theorem 8.
Let $f : GF(2^m) \to GF(2^m)$ be an additive automorphism. Then f is $GF(2^m)^*$-Boolean bent.

Proof. Let $x \in GF(2^m)$, $\alpha \in GF(2^m)^*$ different of 1 (the neutral element for the multiplication) and $\beta \in GF(2^m)$. We have

$$f(\alpha.x) \oplus f(x) = \beta$$
$$\Leftrightarrow f(\alpha x \oplus x) = \beta$$
$$\Leftrightarrow (\alpha \oplus 1)x = f^{-1}(\beta)$$
$$\Leftrightarrow x = \frac{f^{-1}(\beta)}{(\alpha \oplus 1)}$$

because $\alpha \neq 1$. Then there exists one and only one solution to the equation $f(\alpha.x) \oplus f(x) = \beta$ and then for all $\alpha \in GF(2^m)^*$ different of 1 and for all $\beta \in GF(2^m)$,

$$|\{x \in GF(2^m) \mid f(\alpha x) \oplus f(x) = \beta\}| = \frac{|GF(2^m)|}{|GF(2^m)|}$$

=1.

Then f is $GF(2^m)^*$-perfect nonlinear and by equivalence it is also $GF(2^m)^*$-bent.

QED

The interest of such construction seems to be less clear than the previous one if we remain in the traditional setting with a DES-like cryptosystem equipped with XOR as internal operation since the automorphisms are in particular linear and do not offer great resistance against cryptanalysis. Nevertheless if we think about a DES-like system in which the key is combined with the message by a multiplication rather than an addition, this construction gives the best-resistant function against a differential attack where the difference is taken in the sense of multiplication whereas such functions in the traditional setting are impossible: the best ones are almost perfect nonlinear. Moreover it is widely conjectured that almost perfect nonlinear permutations on $GF(2^m)$ exist only if m is odd whereas with our construction we always have bijective functions no matter if m is an odd or even integer.

5. *G*-differential attack

5.1 G-differential attack algorithm

Bentness and perfect nonlinearity are closely related to differential and linear cryptanalysis. By analogy we can interpret *G*-bentness and *G*-perfect nonlinearity as resistances against *G*-linear and *G*-differential attacks. The group action based differential attack would be similar to the classical one except that we replace the XOR differences by their group actions based counterparts: the *G*-difference of $(x, y) \in V_m$, $\Delta x = \alpha \in G$ (if there exists) such that $x = \alpha.y$ (with G acting faithfully on V_m). The sketch of a *G*-differential attack, when applied on a cryptosystem with round function f that maps an encrypted message C_{i-1} (that consists in a m bit-string) of the (i-1)-th round on a encrypted message $C_i = f(C_{i-1}, K_i) = f_{K_i}(C_i)$ ($x \mapsto f_K(x)$ is a permutation on m-bit strings) where K_i is the i-th round key, could be represented by a four steps algorithm:

1. Find a *G*-difference $\alpha \in G^*$ and a classical XOR difference $\beta \in V_m$ at the round i-1 such that the probability

$$\Pr(\Delta C_{i-1} = \beta \mid \Delta M = \alpha)$$

is as far away as possible from the equidistribution, where M is the clear message to encrypt.

2. Choose at random a clear text M and submit M and $\alpha.M$ to ciphering. We obtain two pairs clear-encrypted (M, C_i) and $(M' = \alpha.M, C_i')$ at the round i.

3. Find all the possible values for K_i' such that

$$f_{K_i}^{-1}(M) \oplus f_{K_i'}^{-1}(M) = \beta .$$

4. Iterate steps 2. and 3. until one of the values K_i' occurs more than others. We will consider this value as the i-th round key.

5.2 A possible weakness in the S-boxes of the DES

In this last subsection, we present an amazing structure in the S-boxes of the famous DES, based on fixed-point free involutions, that could be used in a *G*-differential attack of this system. However this raises a question not answered in this paper: how to use this structure in a *G*-differential attack? But since the DES cryptosystem has been widely used since its introduction in the 1970s, any theoretical advances could lead to new generation of DES-like cryptosystem.

The DES has eight S-boxes S_i (i = 1,…,8) from V_6 to V_4 and its solidity is based on these particular nonlinear functions. Nevertheless it appears that each S-box has a remarkable structure that seems to be a weakness regarding to the *G*-differential attack.

Theorem 9.
For each $i \in \{1,...,8\}$ *and for each* $\beta \in V_4$, *there exists a fixed-point free involution* $\sigma : V_6 \mapsto V_6$ *such that for all* $x \in V_6$, *we have*

$$S_i(\sigma(x)) \oplus S_i(x) = \beta.$$

In other words, there exists a fixed-point free involution σ *such that the difference in output of* S_i *of all input x and x', that differ from the application of* σ, *is constant equals to* β.

Proof. In each S-box S_i, each output occurs exactly four times (because they are equidistributed). So if we arrange each input by its output value, we obtain 16 sets I_y with 4 elements

$$I_y = \{x \in V_6 \mid S_i(x) = y\}$$

for $y \in V_4$.

Since all output values in V_4 are possible, we can choose a particular $\beta \in V_4^*$ and build-up 8 sets O_β^j (for j = 1,…,8) with two elements y and y' in V_4 such that $y \oplus y' = \beta$.

In order to build-up a fixed-point free involution σ such that $S_i(\sigma(x)) \oplus S_i(x) = \beta$ for all $x \in V_6$, from each $O_\beta^j = \{y, y'\}$ we construct 4 sets of 2 elements: the first one is taken in I_y and the second one in $I_{y'}$ with the restriction that each value in I_y and $I_{y'}$ is used one and only one time.

Then we obtain a collection of 32 sets $\{x, x'\}$ of two elements each. They are used to define a fixed-point free involution σ over V_6 such that $\sigma(x) = x'$ and $\sigma(x') = x$.

By construction, σ satisfies also

$$S_i(\sigma(x)) \oplus S_i(x) = \beta$$

for all $x \in V_6$. ***QED***

Acknowledgments

The author thanks Professor James Davis, from the University of Richmond, for his help on constructions of *G*-difference sets [4] and Assistant Professor Cyril Prissette, from the University of South Toulon-Var, for the anatomical study of the S-boxes of the DES [11].

References

[1] E. Biham a,nd A. Shamir. Differential cryptanalysis of des-like cryptosystems. *Journal of cryptology*, 4(1):3-72, 1991.

[2] F. Chabaud and S. Vaudenay. Links between differential and linear cryptanalysis. In *Advances in cryptology – Eurocrypt'94*, volume 950 of *Lecture Notes in Computer Science*, pages 356-365, 1994.

[3] J. F. Dillon. *Elementary Hadamard difference sets*. PhD thesis, University of Maryland, 1974.

[4] J. Davis and L Poinsot. The Hyperplane construction. Private communication, April 2005.

[5] G. Lachaud and J. Wolfmann. The weights of the orthogonal of the extended quadratic binary Goppa codes. *IEEE transactions on information theory*, 36:686-692, 1990.

[6] M. Matsui. Linear cryptanalysis for DES cipher. In *Advances in cryptology – Eurocrypt'93*, volume 765 of *Lecture Notes in Computer Science*, pages 386-397, 1994.

[7] K. Nyberg. Perfect nonlinear S-boxes. In *Advances in cryptology – Eurocrypt'92*, volume 547 of *Lecture Notes in Computer Science*, pages 378-386, 1992.

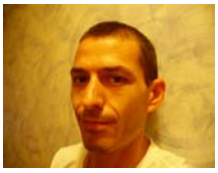
[8] K. Nyberg. Differentially uniform mappings for cryptography. In *Advances in cryptology – Eurocrypt'93*, volume 765 of *Lecture Notes in Computer Science*, pages 55-64, 1994.

[9] L. Poinsot and S. Harari. Generalized Boolean bent functions. In *Progress in cryptology – Indocrypt 2004*, volume 3348 of *Lecture Notes in Computer Science*, pages 107-119, 2004.

[10] L. Poinsot and S. Harari. Group actions based perfect nonlinearity. *GEST international transactions on computer science and engineering*, 12(1):1-14, 2005.

[11] C. Prissette and L. Poinsot. Involution and S-box. Private communication, May 2005.

[12] O. S. Rothaus. On bent functions. *Journal of combinatorial theory* A, 20:300-365, 1976.



Laurent Poinsot received the Bachelor's degree in Mathematics from the University of South Toulon-Var in 1998. He received the Engineer's degree in Computer Science from the French National School of Civil Aviation (ENAC) in Toulouse in 2000. After working two years for the Aix-en-Provence based company Clearsy as an engineer with the technical maintenance responsibility of the automatic and interactive provers of the Atelier B software that implements the B-Method, he received the Master's degree in Discrete Mathematics and Foundations of Computer Science from the University of Mediterranea Aix-Marseille II in 2002. He received his PhD in Mathematics from the University of South Toulon-Var in 2005. Since 2005 he works as a research and teaching assistant in the department of services and communication networks of the IUT of Toulon. His research interest includes perfect nonlinear and bent functions, difference sets, group actions, harmonic analysis of finite groups and finite algebraic structures.