More Correlation-Immune and Resilient Functions over Galois Fields and Galois Rings

Claude Carlet

GREYC, Université de Caen
and
INRIA Projet Codes
Domaine de Voluceau, BP 105
78153 Le Chesnay Cedex
FRANCE
email: Claude.Carlet@inria.fr

Abstract. We show that the usual constructions of bent functions, when they are suitably modified, allow constructions of correlation-immune and resilient functions over Galois fields and, in some cases, over Galois rings.

1 Introduction

The functions used in a conventional cipher must provide both diffusion, for merging several inputs, and confusion, for hiding any structure (cf. [19]). These notions are respectively formalized through the properties of correlation-immunity [2, 3, 4, 5, 20, 22] and nonlinearity [15, 16].

Correlation-immune functions play an important role in several aspects of cryptography such as, for instance, the design of running-key generators in stream ciphers which resist the correlation attack [20] or the design of hash functions (cf. [21]). The most general definition (cf. [3]) defines them over finite alphabets (the original definition was given in [20] for binary functions): let $\mathcal{A}$ be a finite alphabet; a function f from $\mathcal{A}^n$ to $\mathcal{A}^m$ is t-th order correlation-immune if the probability distribution of the output vector $f(X_1, \ldots, X_n)$, where $X_1, \ldots, X_n$ are random input variables assuming values from $\mathcal{A}$ with independent equiprobable distributions, is unaltered when at most t of the variables $X_1, \ldots, X_n$ are fixed (i.e. replaced by constants).
In [22], Xiao Guo-Zhen and J. L. Massey give a convenient characterization of binary correlation-immune functions by means of characters. It is generalized in [3] by Camion and Canteaut to finite abelian groups. Recall that the group of characters on a finite abelian group G is isomorphic with G itself. For $x, u \in G$, we denote by $\langle x, u \rangle$ the image of x under the character associated to u via such an isomorphism. We have:

$$\sum_{x \in G} \langle x, u \rangle \neq 0 \Leftrightarrow u = 0. \tag{1}$$

W. Fumy (Ed.): Advances in Cryptology - EUROCRYPT '97, LNCS 1233, pp. 422-433, 1997.

Such an isomorphism being chosen, the characters on the group G^n ($n > 0$) are:

$$\langle x, u\rangle_n = \prod_{i=1}^{n} \langle x_i, u_i\rangle\ ,\ x = (x_1, \ldots, x_n),\ u = (u_1, \ldots, u_n).$$

A function f from G^n to G^m is t-th order correlation-immune if:

$$\forall v \in G^m,\ \forall u \in G^n,\ 1 \leq w_H(u) \leq t,\ \sum_{x \in G^n} \langle x, u\rangle_n \langle f(x), v\rangle_m = 0 \qquad (2)$$

where $w_H(u)$ denotes the Hamming weight of u.
According to property (1), the equality in (2) is satisfied for every $u \neq 0$ if $v = 0$. Thus, v may be assumed to be nonzero in (2).
f is t-resilient if it is t-th order correlation-immune and balanced. It is a simple matter to show that, thanks to the characterization above, this is equivalent to:

$$\forall v \in G^m,\ v \neq 0,\ \forall u \in G^n,\ w_H(u) \leq t,\ \sum_{x \in G^n} \langle x, u\rangle_n \langle f(x), v\rangle_m = 0. \qquad (3)$$

In [4] is given a bound on the degree relative to each variable of the algebraic normal form of a t-th order correlation-immune (resp. t-resilient) function over a finite field: in each monomial, at most $n - t$ (resp. $n - t - 1$, provided $q^m \neq 2$ or $t \neq n - m$) of the variables have (maximum) degree $q - 1$.
This bound, that generalizes Siegenthaler inequality [20], shows that the functions over finite fields are better suited than binary ones to achieve high linear complexity, given the order of their correlation-immunity.

The bent functions [5, 6, 7, 9, 11, 13, 15, 17] are those Boolean functions whose nonlinearity is maximum. The notion has been first defined for Boolean functions over $GF(2)^n$ (cf. [17], recall that n must then be even) and later generalized to functions over residue class rings (cf. [13]): let q and n be any positive integers; we denote by $\mathbf{Z}_q$ the ring $\mathbf{Z}/q\mathbf{Z}$. A function f from ${\mathbf{Z}_q}^n$ to $\mathbf{Z}_q$ is called bent if, for any vector s, the character sum:

$$\sum_{x \in {\mathbf{Z}_q}^n} {w_q}^{f(x) - x \cdot s}$$

has magnitude $q^{\frac{n}{2}}$, where $w_q = e^{2i\pi/q}$. The function f is called regular-bent if there exists a function $\tilde{f}$ such that, for any s:

$$\sum_{x \in {\mathbf{Z}_q}^n} {w_q}^{f(x) - x \cdot s} = q^{\frac{n}{2}}\, {w_q}^{\tilde{f}(s)}.$$

There exists also a generalization of the notion to functions over finite fields (cf. [1]), that is not equivalent for prime fields. These definitions can be extended to definitions of (regular-) bent functions over a Galois ring $GR(p^k, m)$ (whose

definition is recalled in subsection 2.1): the character sums to be considered in this wider framework are:

$$\sum_{x \in GR(p^k,m)^n} w_{p^k}{}^{Tr(f(x)-x\cdot s)}$$

where Tr is the trace function from $GR(p^k, m)$ to $\mathbf{Z}_{p^k}$.

These notions of correlation-immune and bent functions are very similar. The purpose of this paper is to show that various constructions of bent functions, when they are suitably modified, lead to constructions of correlation-immune functions. Some of these constructions will be primary, in the sense that they lead to new classes of correlation-immune functions without using known ones. Others, on the contrary, will be secondary constructions.

2 Primary constructions

2.1 A Maiorana-McFarland-like class

Maiorana-McFarland class (cf. [11]) is the set of all the (bent) Boolean functions on $GF(2)^n = \{(x, y), x, y \in GF(2)^{\frac{n}{2}}\}$ (n even) of the form : $f(x, y) = x \cdot \pi(y) + g(y)$ where π is any permutation on $GF(2)^{\frac{n}{2}}$ and g is any Boolean function on $GF(2)^{\frac{n}{2}}$.
In [5] is derived a construction of binary resilient functions:
let t and $n = r + s$ be any positive integers ($r > t > 0$, $s > 0$), g any boolean function on $GF(2)^s$ and ϕ a mapping from $GF(2)^s$ to $GF(2)^r$ such that every element in $\phi(GF(2)^s)$ has Hamming weight greater than t, then the function:

$$f(x, y) = x \cdot \phi(y) + g(y),\ x \in GF(2)^r,\ y \in GF(2)^s$$

is t-resilient.
We generalize this construction to any Galois ring in theorem 1. Before we state this theorem, we recall what are the definition and major properties of Galois rings.
For any prime p and any positive integers k and m, the Galois ring $GR(p^k, m)$ is the Galois extension of degree m of the ring $\mathbf{Z}_{p^k}$. When $m = 1$, $GR(p^k, m)$ is equal to $\mathbf{Z}_{p^k}$ and when $k = 1$, it is equal to the Galois field $GF(p^m)$. We refer to [14] for a general presentation of this notion and to [12] for the special case $p = k = 2$.
Galois rings share with Galois fields almost all their properties.
• Their elements can be described in two different forms by means of a primitive element ξ of order p^m:
- the "multiplicative" form (this term comes from field theory):

$$x = \sum_{i=1}^{k} p^{i-1} u_i,\ u_i \in \{0, 1, \xi, \ldots, \xi^{p^m-2}\},$$

- the "additive" form:

$$x = \sum_{r=0}^{m-1} a_r \, \xi^r, \; a_r \in \mathbf{Z}_{p^k}.$$

- They admit a Frobenius automorphism:

$$\varphi : \sum_{i=1}^{k} p^{i-1} u_i \to \sum_{i=1}^{k} p^{i-1} u_i{}^p$$

and a trace map from $GR(p^k, m)$ to $\mathbf{Z}_{p^k}$:

$$Tr : \; x \to x + \varphi(x) + \ldots + \varphi^{m-1}(x),$$

where φ^{m-1} is $m-1$ times the composition of φ by itself.
The difference between Galois fields and general Galois rings is obviously that every nonzero element of $GR(p^k, m)$ is not necessarily a unit; the units of $GR(p^k, m)$ are the elements:

$$\sum_{i=1}^{k} p^{i-1} u_i, \; u_1 \in \{1, \xi, \ldots, \xi^{p^m-2}\}, \; u_2, \ldots, u_k \in \{0, 1, \xi, \ldots, \xi^{p^m-2}\}.$$

Their number is $p^{(k-1)m} \cdot (p^m - 1) = |GR(p^k, m)| \cdot \left(\frac{p^m-1}{p^m}\right)$.
We denote again by $x \cdot y$ the expression:

$$\sum_{j=1}^{n} x_j \, y_j, \; x = (x_1, \ldots, x_n) \in GR(p^k, m)^n, \; y = (y_1, \ldots, y_n) \in GR(p^k, m)^n.$$

The characters on $GR(p^k, m)^n$ are the functions: $x \to \langle x, y \rangle_n = w_{p^k}{}^{Tr(x \cdot y)}$, where $w_{p^k} = e^{2\pi i / p^k}$.
The construction given in [5] could be extended to general finite rings. In the case of Galois rings, it is easy to state:

Theorem 1. *Let G be any Galois ring, t and $n = r + s$ any positive integers ($r > t > 0$, $s > 0$), g any function from G^s to G and ϕ a mapping from G^s to G^r such that any element in $\phi(G^s)$ has more than t coordinates that are units, then the function:*

$$f(x, y) = x \cdot \phi(y) + g(y), \; x \in G^r, \; y \in G^s$$

is a t-resilient function on G^n.

Proof:
For any nonzero element v of G and any element (u, u') of G^n ($u \in G^r$, $u' \in G^s$), we have:

$$\sum_{x \in G^r, \, y \in G^s} \langle x, u \rangle_r \langle y, u' \rangle_s \langle f(x, y), v \rangle =$$

$$\sum_{x\in G^r,\, y\in G^s} {w_{p^k}}^{Tr\left(v[x\cdot\phi(y)+g(y)]+x\cdot u+y\cdot u'\right)} =$$

$$\sum_{y\in G^s}\left(\left(\sum_{x\in G^r} {w_{p^k}}^{Tr(x\cdot[v\phi(y)+u])}\right){w_{p^k}}^{Tr(vg(y)+y\cdot u')}\right).$$

The sum:

$$\sum_{x\in G^r} {w_{p^k}}^{Tr(x\cdot[v\,\phi(y)+u])}$$

is equal to 0, unless $v\phi(y)+u=0$, according to property (1). Therefore:

$$\sum_{x\in G^r,\, y\in G^s} \langle x,u\rangle_r\langle y,u'\rangle_s\langle f(x,y),v\rangle =$$

$$|G|^r \sum_{y\in G^s \mid v\phi(y)+u=0} {w_{p^k}}^{Tr(vg(y)+y\cdot u')}.$$

If we assume that (u,u') has Hamming weight at most t, then u, whose Hamming weight is *a fortiori* at most t, cannot be equal to $-v\,\phi(y)$: according to the hypothesis on ϕ, $v\,\phi(y)$ has more than t nonzero coordinates. Thus, the sum $\sum_{x\in G^r,\, y\in G^s} \langle x,u\rangle_r\langle y,u'\rangle_s\langle f(x,y),v\rangle$ is equal to zero. f is t-resilient. □

Example: if G is a Galois field and $\phi(y)=(\phi_1(y),\ldots,\phi_r(y))$ is such that:
. the sets $E_i=\{y\in G^s \mid \phi_i(y)=0\}$, $i=1,\ldots,r$ are disjoint each others;
. a monomial in the algebraic normal form of one of the functions ϕ_i has maximum degree $q-1$ relative to each variable;
then $f({x_1}^{q-2},\ldots,{x_r}^{q-2},y_1,\ldots,y_s)$ is $(r-2)$-resilient (according to theorem 1 and to [3], prop. 9) and almost reaches the bound on the degrees recalled in the introduction.

2.2 A Partial-Spreads-like class

In [11] is also introduced the class of bent functions called $\mathcal{PS}_{ap}$ (a subclass of Partial-Spreads class), whose elements are defined the following way:
$GF(2)^{\frac{n}{2}}$ is identified to the Galois field $GF(2^{\frac{n}{2}})$; $\mathcal{PS}_{ap}$ is the set of all the functions of the form $f(x,y)=g(x\,y^{2^{\frac{n}{2}}-2})$ (i.e. $g(\frac{x}{y})$ with $\frac{x}{y}=0$ if $x=0$ or $y=0$) where g is a balanced Boolean function on $GF(2)^{\frac{n}{2}}$. We have then $\tilde{f}(x,y)=g(\frac{y}{x})$.
The idea of this construction may be used to obtain a construction of correlation-immune functions. We give this construction in its most general form (involving a Galois field $GF(q)$ where q is any prime power).
In the next theorem, we identify a power $\mathcal{F}^m$ of a Galois field $\mathcal{F}=GF(q)$ to the Galois field $GF(q^m)$. Such an identification is done the following way: we choose a basis $(\alpha_1,\ldots,\alpha_m)$ of the $\mathcal{F}$-vector space $GF(q^m)$ and we identify $x=(x_1,\ldots,x_m)\in\mathcal{F}^m$ to $\sum_{i=1}^m x_i\alpha_i\in GF(q^m)$. We know that a dot product on $\mathcal{F}^m$ is, via this identification $Tr_m(x\,y)$, where Tr_m is the trace map from

$GF(q^m)$ to $GF(q)$. But the notion of correlation-immune function depends on the choice of the dot product on $\mathcal{F}^m$. So, we assume that the basis $(\alpha_1, \ldots, \alpha_m)$ is self-dual (it is always possible to find such a basis when q is even or m is odd), so that:

$$Tr_m(x\,y) = \sum_{i=1}^{m} x_i\,y_i = x \cdot y.$$

Notice that if we do not have a self-dual basis, we still have, for any basis, $x \cdot y = Tr_m(a\,x\,y)$, $a \in GF(q^m)$.
We will use a well-known fact about linear mappings: let ϕ be a linear mapping from $GF(q^n)$ to $GF(q^m)$, there exists a linear mapping ϕ^* (called adjoint of ϕ) from $GF(q^m)$ to $GF(q^n)$ such that, for every $x \in GF(q^m)$ and every $y \in GF(q^n)$:

$$Tr_m(x\,\phi(y)) = Tr_n(\phi^*(x)\,y).$$

We state theorem 2 in the case we have self-dual basis in $GF(q^m)$ and $GF(q^n)$. It can be easily generalized to any case.

Theorem 2. *Let $\mathcal{F} = GF(q)$ $(q = p^s)$ be a finite field and tr the trace function from $\mathcal{F}$ to its prime field $GF(p)$. Let n and m be two positive integers (n, m odd if q is odd), g a function from $GF(q^m)$ to $\mathcal{F}$, ϕ a linear mapping from $GF(q^n)$ to $GF(q^m)$ and a an element of $GF(q^m)$ such that $a + \phi(y) \neq 0$, $\forall y \in GF(q^n)$. Let f be the function from $\mathcal{F}^m \times \mathcal{F}^n$ to $\mathcal{F}$ defined by:*

$$f(x,y) = g\left(\frac{x}{a+\phi(y)}\right) + Tr_n(b\,y),$$

where $b \in GF(q^n)$ and where x, y are viewed as elements of $GF(q^m)$, $GF(q^n)$ respectively.
Assume that, for every z in $GF(q^m)$ and every $v \neq 0$ in $\mathcal{F}$, $\phi^*(z)+v\,b$ has weight greater than t, then f is t-resilient.

Proof:
We have, for any (u,u') in $\mathcal{F}^m \times \mathcal{F}^n$ and any nonzero v in $\mathcal{F}$:

$$\sum_{x\in\mathcal{F}^m,\,y\in\mathcal{F}^n} \langle u,x\rangle_m \langle u',y\rangle_n \langle v, f(x,y)\rangle = \sum_{x\in\mathcal{F}^m,\,y\in\mathcal{F}^n} w_p^{\,tr\left[u\cdot x + u'\cdot y + v\,f(x,y)\right]} =$$

$$\sum_{x\in GF(q^m),\,y\in GF(q^n)} w_p^{\,tr\left[Tr_m(ux)+Tr_n(u'y)+v\,g\left(\frac{x}{a+\phi(y)}\right)+v\,Tr_n(b\,y)\right]}.$$

Since, for every y, $a + \phi(y) \neq 0$, the element $z = \frac{x}{a+\phi(y)}$ ranges over the whole field $GF(q^m)$ when x does. We deduce:

$$\sum_{x\in\mathcal{F}^m,\,y\in\mathcal{F}^n} \langle u,x\rangle_m \langle u',y\rangle_n \langle v, f(x,y)\rangle_r =$$

$$\sum_{z\in GF(q^m),\,y\in GF(q^n)} w_p^{\,tr\left[Tr_m(u(az+z\phi(y)))+Tr_n(u'y)+v\,g(z))+v\,Tr_n(b\,y)\right]} =$$

$$\sum_{z\in GF(q^m),\, y\in GF(q^n)} w_p{}^{tr\left[Tr_m(uaz)+Tr_n(y[\phi^*(uz))+u'+v\,b])+v\,g(z)\right]} =$$

$$\sum_{z\in GF(q^m)} w_p{}^{tr[Tr_m(uaz)+v\,g(z)]} \left(\sum_{y\in GF(q^n)} w_p{}^{tr\left[Tr_n(y[\phi^*(uz))+u'+v\,b])\right]} \right) =$$

$$q^n \sum_{z\in GF(q^m)\,|\,\phi^*(uz))+u'+v\,b=0} w_p{}^{tr[Tr_m(uaz)+v\,g(z)]},$$

according to property (1).
If $w_H(u,u') \leq t$, then according to the hypothesis on ϕ^*, the set

$$\{z \in GF(q^m)\,|\,\phi^*(uz)) + u' + v\,b = 0\}$$

is empty, and this sum is equal to 0. Thus, f is t-resilient. □

Example: Let E be an $\mathcal{F}$-subspace of $\mathcal{F}^n$ of maximum weight $n-t-1$ and ψ a linear mapping from $\mathcal{F}^m$ to E. Let b be a word of weight n in $\mathcal{F}^n$. Then the condition of theorem 2 is satisfied by $\phi = \psi^*$, provided that a does not belong to the image of ψ^* (which is always possible if $n < m$).

3 Secondary constructions

3.1 Modifying a correlation-immune function on a subgroup

Dillon proves in [11] that if a binary function f is bent on $GF(2)^n$ (n even) and if E is a $\frac{n}{2}$-dimensional flat on which f is constant, then, denoting by δ_E the indicator of E, the function $f + \delta_E$ is bent too.
We shall prove a similar result on correlation-immune functions.

Theorem 3. *Let G be any finite abelian group, t, m and n any positive integers and f a t-th order correlation-immune function from G^n to G^m.*
Assume there exists a subgroup E of G^n, whose minimum nonzero weight is greater than t and such that the restriction of f to the orthogonal of E (i.e. the subgroup of G^n: $E^\perp = \{u \in G^n\,|\,\forall x \in E, \langle u,x\rangle_n = 1\}$) is constant. Then f remains t-th order correlation-immune if we change its constant value on $E^\perp$ into any other one.

Proof:
Let a be the constant value of f on $E^\perp$ and b any element of G^m. Set $f'(x) = f(x)$ if $x \notin E^\perp$, $f'(x) = b$ if $x \in E^\perp$.
For any nonzero element v of G^m and any element u of G^n, we have:

$$\sum_{x\in G^n} \langle x,u\rangle_n \langle f'(x),v\rangle_m =$$

$$\sum_{x\in G^n} \langle x,u\rangle_n \langle f(x),v\rangle_m + \sum_{x\in E^\perp} \langle x,u\rangle_n \langle b,v\rangle_m - \sum_{x\in E^\perp} \langle x,u\rangle_n \langle a,v\rangle_m.$$

If u is nonzero and if its weight is at most equal to t, then:

$$\sum_{x \in G^n} \langle x, u \rangle_n \langle f'(x), v \rangle_m = \left(\sum_{x \in E^\perp} \langle x, u \rangle_n \right) \left(\langle b, v \rangle_m - \langle a, v \rangle_m \right).$$

The sum: $\sum_{x \in E^\perp} \langle x, u \rangle_n$ is equal to 0, since u does not belong to E. □

3.2 Adapting a secondary construction known for bent functions

It is known, cf. [11, 17], that if g, h, k and $g + h + k$ are bent on $GF(2)^m$ (m even), then the function defined on any element (x_1, x_2, x) of $GF(2)^{m+2}$ by:

$$f(x_1, x_2, x) =$$

$$g(x)h(x) + g(x)k(x) + h(x)k(x) + [g(x) + h(x)]x_1 + [g(x) + k(x)]x_2 + x_1 x_2$$

is bent.

Theorem 4. *Let g, h and k be three functions from $GF(2)^m$ to $GF(2)$. If g is t-resilient, h and k are $(t-1)$-resilient and $g + h + k$ is $(t-2)$-resilient, then the function on $GF(2)^{m+2}$:*

$$f(x_1, x_2, x) =$$

$$g(x)h(x) + g(x)k(x) + h(x)k(x) + [g(x) + h(x)]x_1 + [g(x) + k(x)]x_2 + x_1 x_2$$

is t-resilient (the converse is true).

Proof:
We have:

$$\sum_{x_1, x_2 \in GF(2), x \in GF(2)^m} (-1)^{f(x_1, x_2, x) + a_1 x_1 + a_2 x_2 + a \cdot x} = \sum_{x_1, x_2 \in GF(2), x \in GF(2)^m}$$

$$(-1)^{g(x) + [x_1 + g(x) + k(x) + a_2][x_2 + g(x) + h(x) + a_1] + a_1[g(x) + k(x)] + a_2[g(x) + h(x)] + a_1 a_2 + a \cdot x}.$$

Changing x_1 into $x_1 + g(x) + k(x) + a_2$ and x_2 into $x_2 + g(x) + h(x) + a_1$, we obtain:

$$\sum_{x_1, x_2 \in GF(2), x \in GF(2)^m} (-1)^{g(x) + x_1 x_2 + a_1[g(x) + k(x)] + a_2[g(x) + h(x)] + a \cdot x + a_1 a_2}$$

that is equal to:

$$2 \sum_{x \in GF(2)^m} (-1)^{g(x) + a_1[g(x) + k(x)] + a_2[g(x) + h(x)] + a \cdot x + a_1 a_2}.$$

Assume that the word (a_1, a_2, a) has Hamming weight at most t. Then if $a_1 = a_2 = 0$, we obtain:

$$2 \sum_{x \in GF(2)^m} (-1)^{g(x) + a \cdot x},$$

that is equal to zero, according to the hypothesis and since a has Hamming weight at most t. If $a_1 = 0$ and $a_2 = 1$ (resp. $a_1 = 1$ and $a_2 = 0$), we obtain: $2 \sum_{x \in GF(2)^m} (-1)^{h(x)+a \cdot x}$ (resp. $2 \sum_{x \in GF(2)^m} (-1)^{k(x)+a \cdot x}$), that is also equal to zero, since a has Hamming weight at most $t-1$. If $a_1 = a_2 = 1$, we obtain:

$$-2 \sum_{x \in GF(2)^m} (-1)^{g(x)+h(x)+k(x)+a \cdot x},$$

that is equal to zero too, since a has Hamming weight at most $t-2$.
The converse is similar. □

Example: This result may be applied to functions g, h and k chosen in Maiorana-McFarland-like class (over $GF(2)$): $g(x,y) = x \cdot \phi(y) + g_1(y)$, $h(x,y) = x \cdot \phi'(y) + h_1(y)$, $k(x,y) = x \cdot \phi''(y) + k_1(y)$, where any element of $\phi(G^s)$ (resp. $\phi'(G^s)$, $\phi''(G^s)$, $(\phi + \phi' + \phi'')(G^s)$) has more than t (resp. $t-1$, $t-1$, $t-2$) nonzero coordinates.

Remark: It is possible to extend this result to general finite fields, but the hypothesis becomes hard to satisfy.

3.3 Constructing correlation-immune functions from bent functions

The construction of bent functions that is recalled in the previous subsection is generalized in [8]:
Let m and r be two positive even integers. Let f be a Boolean function on $GF(2)^{m+r}$ such that, for any element x' of $GF(2)^r$, the function on $GF(2)^m$:

$$f_{x'} : x \to f(x, x')$$

is bent. Then f is bent if and only if for any element u of $GF(2)^m$, the function

$$\varphi_u : x' \to \widetilde{f_{x'}}(u)$$

is bent on $GF(2)^r$ ($\widetilde{f_{x'}}$ always exists: every bent function on $GF(2)$ in even dimension is regular-bent). This result generalizes to functions f over $\mathbf{Z_q}^{m+r}$ (as stated in [8]) such that for every x', the function $f_{x'}$ is regular-bent.
It leads us to a construction of resilient functions from regular-bent functions:

Theorem 5. *Let r be a positive integer, m a positive even integer and p a prime. Let f be a function from $(GF(p))^{m+r}$ to $GF(p)$ such that, for any element x' of $(GF(p))^r$, the function on $(GF(p))^m$:*

$$f_{x'} : x \to f(x, x')$$

is regular-bent.
If, for every element u of $(GF(p))^m$ of Hamming weight at most t, the function

$$\varphi_u : x' \to \widetilde{f_{x'}}(u)$$

is $(t - w_H(u))$-resilient, then f is t-resilient (the converse is true).

Proof:
For every nonzero v in $GF(p)$, and every (u,u') in $GF(p)^{m+r}$, we have:

$$\sum_{(x,x')\in GF(p)^{m+r}} \langle u,x\rangle_m \langle u',x'\rangle_r \langle v,f(x,x')\rangle =$$

$$\sum_{(x,x')\in GF(p)^{m+r}} {w_p}^{vf_{x'}(x)+u\cdot x+u'\cdot x'}. \tag{4}$$

$f_{x'}$ being regular-bent, we have:

$$\sum_{x\in GF(p)^m} {w_p}^{f_{x'}(x)+u\cdot x} = p^{\frac{m}{2}}\, {w_p}^{\widetilde{f_{x'}}(-u)},\ \forall u\in GF(p)^m. \tag{5}$$

Let us first prove that, for every nonzero v in $GF(p)$:

$$\sum_{x\in GF(p)^m} {w_p}^{vf_{x'}(x)+u\cdot x} = p^{\frac{m}{2}}\, {w_p}^{\widetilde{f_{x'}}\left(-\frac{u}{v}\right)},\ \forall u\in GF(p)^m :$$

let C_p be the cyclotomic field generated by w_p over the rationnals, i.e.

$$C_p = \mathbf{Q}(w_p);$$

we know (cf. [18], see also [13]) that its Galois group is the abelian group each element σ of which raises w_p to the v-th power, $v\in\{1,\ldots,p-1\}$ (every element of $\mathbf{Q}$ being invariant under σ). Say $\sigma=\sigma_v$.
From equality (5) and since $p^{\frac{m}{2}}\in\mathbf{Q}$, we deduce:

$$\sigma_v\left(\sum_{x\in GF(p)^m} {w_p}^{f_{x'}(x)+u\cdot x}\right) = p^{\frac{m}{2}}\,\sigma_v\left({w_p}^{\widetilde{f_{x'}}(-u)}\right),$$

thus:

$$\sum_{x\in GF(p)^m} {w_p}^{v(f_{x'}(x)+u\cdot x)} = p^{\frac{m}{2}}\, {w_p}^{v\widetilde{f_{x'}}(-u)}$$

and therefore:

$$\sum_{x\in GF(p)^m} {w_p}^{vf_{x'}(x)+u\cdot x} = p^{\frac{m}{2}}\, {w_p}^{\widetilde{vf_{x'}}\left(-\frac{u}{v}\right)}. \tag{6}$$

From equalities (4) and (6), we deduce:

$$\sum_{(x,x')\in GF(p)^{m+r}} \langle u,x\rangle_m \langle u',x'\rangle_r \langle v,f(x,x')\rangle =$$

$$p^{\frac{m}{2}} \sum_{x'\in GF(p)^r} {w_p}^{v\widetilde{f_{x'}}\left(-\frac{u}{v}\right)+u'\cdot x'} =$$

$$p^{\frac{m}{2}} \sum_{x'\in GF(p)^r} {w_p}^{v\varphi_{-\frac{u}{v}}(x')+u'\cdot x'}.$$

This completes the proof, since $w_H\left(-\frac{u}{v}\right) = w_H(u)$ and since $w_H(u,u') \leq t$ implies $w_H(u) \leq t$ and $w_H(u') \leq t - w_H(u)$. The converse is similar. □

Example: taking $f_{x'}$ in Partial Spreads class and φ_u in Partial Spreads-like class, we obtain that the function $f(x,y,x',y') = k(\frac{x}{y}, \frac{x'}{a+\phi(y')}) + Tr_n(b\,y')$, where for every x', the function $x \to k(x,x')$ is balanced, for every y', $a + \phi(y') \neq 0$, and for every z and every $v \neq 0$, $\phi^*(z) + v\,b$ has weight greater than t, is t-resilient.

Remark: Theorem 5 could be generalized to functions $f(x,x')$ over a more general Galois field $GF(q)$ such that, for every $x' \in GF(q)^r$ and every nonzero $v \in GF(q)$:
. the function $f_{x',v} : x \to vf(x,x')$ is regular-bent,
. $\widetilde{f_{x',v}} = v\,\widetilde{f_{x',1}}$.

References

1. A.S. Ambrosimov. Properties of bent functions of q-valued logic over finite fields. *Discrete Math. Appl.* vol 4, N° 4, pages 341-350 (1994)
2. J. Bierbrauer, K. Gopalakrishnan and D.R. Stinson. Bounds for resilient functions and orthogonal arrays. *Advances in Cryptology, CRYPTO'94, Lecture Notes in Computer Sciences, Springer Verlag* n° 839, pages 247-256 (1994)
3. P. Camion and A. Canteaut. Construction of t-resilient functions over a finite alphabet, *Advances in Cryptology, EUROCRYPT'96, Lecture Notes in Computer Sciences, Springer Verlag* n° 1070, pages 283-293 (1996)
4. P. Camion and A. Canteaut. Generalization of Siegenthaler inequality and Schnorr-Vaudenay multipermutations. In N. Koblitz, editor, *Advances in Cryptology - CRYPTO'96*, number 1109 in Lecture Notes in Computer Science, pages 372–386 Springer-Verlag, 1996.
5. P. Camion, C. Carlet, P. Charpin and N. Sendrier. On correlation-immune functions. *Advances in Cryptology, CRYPTO'91, Lecture Notes in Computer Sciences, Springer Verlag* n° 576, pages 86-100 (1992)
6. C. Carlet. Two new classes of bent functions. *EUROCRYPT' 93, Advances in Cryptology, Lecture Notes in Computer Science* 765, pages 77-101 (1994)
7. C. Carlet, Generalized Partial Spreads, *IEEE Transactions on Information Theory* vol 41 pages 1482-1487 (1995)
8. C. Carlet. A construction of bent functions. *Finite Fields and Applications, London Mathematical Society, Lecture Series* 233, Cambridge University Press, pages 47-58 (1996)
9. C. Carlet and P. Guillot. A characterization of binary bent functions. *Journal of Combinatorial Theory, Series A*, Vol. 76, No. 2 pages 328-335 (1996)
10. C. Carlet. Hyperbent functions. *PRAGOCRYPT'97, Czech Technical University Publishing House*, pages 145-155 (1996).
11. J. F. Dillon. Elementary Hadamard Difference sets. Ph. D. Thesis, Univ. of Maryland (1974).
12. A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé. The Z_4-linearity of Kerdock, Preparata, Goethals and related codes. *IEEE Transactions on Information Theory*, vol 40, pages 301-320, (1994)

13. P. V. Kumar, R.A. Scholtz and L.R. Welch. Generalized bent functions and their properties. *Journal of Combinatorial Theory*, Series A 40, pages 90-107 (1985)
14. B.R. MacDonald. Finite rings with identity. *Marcel Dekker*, NY, 1974
15. W. Meier and O. Staffelbach. Nonlinearity Criteria for Cryptographic Functions. *Advances in Cryptology, EUROCRYPT' 89, Lecture Notes in Computer Science* 434, pages 549-562, Springer Verlag (1990)
16. K. Nyberg. Perfect non-linear S-boxes. *Advances in Cryptology, EUROCRYPT' 91*, Lecture Notes in Computer Science 547, pages 378-386, Springer Verlag (1992)
17. O. S. Rothaus. On bent functions. *J. Comb. Theory*, 20A, pages 300- 305(1976)
18. P. Samuel. Algebraic Theory of Numbers. Boston, Houghton Mifflin, 1970
19. C. E. Shannon. Communication theory of secrecy systems. in *Bell system technical journal*, vol. 28, pages 656-715 (1949)
20. T. Siegenthaler. Correlation-Immunity of Nonlinear Combining Functions for Cryptographic Applications. *IEEE Trans. on Inf. Theory*, vol IT-30, n° 5, pages 776-780 (1984)
21. C.P. Schnorr and S. Vaudenay. Black box cryptanalysis of hash networks based on multipermutations. *Advances in Cryptology, EUROCRYPT' 94*, Lecture Notes in Computer Science 950, pages 47-57, Springer Verlag (1995)
22. Xiao Guo-Zhen and J. L. Massey. A Spectral Characterization of Correlation-Immune Combining Functions. *IEEE Trans. Inf. Theory*, Vol IT 34, n° 3, pages 569-571 (1988).