Constructions of bent functions and difference sets

KAISA NYBERG

University of Helsinki
and
Finnish Defence Forces

1. Introduction. Based on the work of Rothaus [12], Olsen, Scholtz and Welch suggested the bent functions to be used as feed-forward functions to generate binary sequences which possess high linear complexity and very nearly optimum cross-correlation properties [10]. In [7] Meier and Staffelbach discovered, that binary bent functions give a solution to the correlation problem when used as combining functions of several binary linear shiftregister sequences. One of their results is that bent functions are at maximum distance to the set of affine functions. We refer to [7] for the cryptographic background and motivation. The general theory of the bent functions from $\mathbf{Z}_q^n$ to $\mathbf{Z}_q$ was developed by Kumar, Scholtz and Welch [2].

The main purpose of this paper is to consider the cryptographic properties of generalized bent functions. In §2 we give the basic definitions and properties of bent functions. For more details we refer to [2]. Our main results are concerned with the value distributions of p-ary bent functions, p prime, and their distances to the set of affine functions, and are given in §3. In §4 a method is given to produce all binary bent functions. We also consider the relation between difference sets and bent functions and review the previous construction methods and their properties.

2. Generalized bent functions. Let q be a positive integer and denote the set of integers modulo q by $\mathbf{Z}_q$. Let

$$u = e^{i\frac{2\pi}{q}}$$

be the qth root of unity in $\mathbf{C}$, where $i = \sqrt{-1}$. Let f be a function from the set $\mathbf{Z}_q^n$ of n-tuples of integers modulo q to $\mathbf{Z}_q$. Then the *Fourier transform* of u^f is defined as follows

$$F(\mathbf{w}) = \frac{1}{\sqrt{q^n}} \sum_{\mathbf{x} \in \mathbf{Z}_q^n} u^{f(\mathbf{x}) - \mathbf{w}\cdot\mathbf{x}}, \quad \mathbf{w} \in \mathbf{Z}_q^n.$$

DEFINITION 2.1. *A function $f : \mathbf{Z}_q^n \to \mathbf{Z}_q$ is bent if $|F(\mathbf{w})| = 1$ for all $\mathbf{w} \in \mathbf{Z}_q^n$.*

Let f and g be two functions from $\mathbf{Z}_q^n$ to $\mathbf{Z}_q$. Then their *convolution* is

$$(u^f * u^g)(\mathbf{w}) = \sum_{\mathbf{x} \in \mathbf{Z}_q^n} u^{f(\mathbf{x}) + g(\mathbf{w}-\mathbf{x})},$$

I.B. Damgard (Ed.): Advances in Cryptology - EUROCRYPT '90, LNCS 473, pp. 151-160, 1991.

and their *shifted cross-correlation*

$$c(f,g)(\mathbf{w}) = \frac{1}{q^n} \sum_{\mathbf{x} \in \mathbf{Z}_q^n} u^{f(\mathbf{x}+\mathbf{w})-g(\mathbf{x})} = \frac{1}{q^n}(u^f * u^{g_r})(\mathbf{w}),$$

where $g_r(\mathbf{x}) = -g(-\mathbf{x})$.

From these definitions we easily obtain the following

THEOREM 2.1. *A function $f : \mathbf{Z}_q^n \to \mathbf{Z}_q$ is bent if and only if*

$$|c(f,L)(\mathbf{w})| = \frac{1}{\sqrt{q^n}}$$

for all linear (or affine) functions $L : \mathbf{Z}_q^n \to \mathbf{Z}_q$ and $\mathbf{w} \in \mathbf{Z}_q^n$.

Analogously to the binary case it then follows that the q-ary bent functions have the minimum correlation to the set of all affine functions (see Theorem 3.5 in [7]).

In [2] also the following result can be found.

THEOREM 2.2. *A function $f : \mathbf{Z}_q^n \to \mathbf{Z}_q$ is bent if and only if*

$$c(f,f)(\mathbf{w}) = 0, \text{ for all } \mathbf{w} \neq \mathbf{0}.$$

This is in the binary case exactly the property of perfect nonlinearity used by Meier and Staffelbach to define bent functions. We make the following generalization.

DEFINITION 2.2. *A function $f : \mathbf{Z}_q^n \to \mathbf{Z}_q$ is perfect nonlinear if for all $\mathbf{w} \in \mathbf{Z}_q^n$, $\mathbf{w} \neq$ bf 0 and $k \in \mathbf{Z}_q$*

$$f(\mathbf{x}) = f(\mathbf{x}+\mathbf{w}) + k,$$

for exactly q^{n-1} values of $\mathbf{x} \in \mathbf{Z}_q^n$.

THEOREM 2.3. *A perfect nonlinear function from $\mathbf{Z}_q^n$ to $\mathbf{Z}_q$ is bent. The converse is true if q is a prime.*

PROOF: Let f be a function from $\mathbf{Z}_q^n$ to $\mathbf{Z}_q$. If f is perfect nonlinear, then

$$c(f,f)(\mathbf{w}) = \frac{1}{q} \sum_{k \in \mathbf{Z}_q} u^k = 0,$$

for all $\mathbf{w} \in \mathbf{Z}_p^n$, hence f is bent by Theorem 2.2.

Assume now that q is prime and f is bent. Then

$$0 = \frac{1}{q^n} \sum_{\mathbf{x} \in \mathbf{Z}_q^n} u^{f(\mathbf{x}+\mathbf{w})-f(\mathbf{x})} = \frac{1}{q^n} \sum_{k \in \mathbf{Z}_q} b_k u^k,$$

where $b_k = \#\{\mathbf{x} \in \mathbf{Z}_q^n \mid f(\mathbf{x}+\mathbf{w}) - f(\mathbf{x}) = k\}$. Since $\{u, u^2, \ldots, u^{q-1}\}$ is a basis for the qth cyclotomic field over the field of rational numbers (see, e.g., [4], Theorem 2.47 and Exercise 2.53), it follows that the numbers b_k are all equal, or what is the same, f is a perfect nonlinear function.

Example. Let q be an odd integer and $f : \mathbf{Z}_q \to \mathbf{Z}_q$ be the function $f(x) = x^2 \pmod q$. Let $w \in \mathbf{Z}_q$ and take $\lambda \in \mathbf{Z}_q$ such that $w = 2\lambda \pmod q$. Then

$$F(w) = \frac{1}{\sqrt{q}} \sum_{x \in \mathbf{Z}_q} u^{x^2 - wx} = \frac{1}{\sqrt{q}} u^{-\lambda^2} \sum_{x \in \mathbf{Z}_q} u^{(x-\lambda)^2} = \frac{1}{\sqrt{q}} u^{-\lambda^2} \sum_{k \in \mathbf{Z}_q} u^{k^2}.$$

For q odd, the Gaussian quadratic sum takes the absolute value $\sqrt{q}$. Hence $|F(w)| = 1$ and f is bent. For $w \in \mathbf{Z}_q$, $w \neq 0$, the difference

$$f(x+w) - f(x) = 2wx + w^2 \pmod q$$

takes every value in $\mathbf{Z}_q$ equally many times if and only if w and q are relative primes. Consequently f is perfect nonlinear if and only if q is a prime.

3. Constructions and properties. The values of a non-constant affine function from $\mathbf{Z}_p^n$ to $\mathbf{Z}_p$ are evenly distributed when p is a prime. Since for the functions

$$f(\mathbf{x}) = f(x_1, x_2, \ldots, x_{2m}) = x_1 x_{m+1} + x_2 x_{m+2} + \cdots + x_m x_{2m}$$

or

$$f(\mathbf{x}) = f(x_1, x_2, \ldots, x_n) = x_1^2 + x_2^2 + \cdots + x_n^2$$

their difference functions

$$\mathbf{x} \mapsto f(\mathbf{x}+\mathbf{w}) - f(\mathbf{x})$$

are non-zero affine functions for all $\mathbf{w} \neq 0$, it follows that these functions are perfect nonlinear. Hence bent functions from $\mathbf{Z}_p^n$ to $\mathbf{Z}_p$ exist for every prime p when n is even, and for every prime $p \geq 3$ when n is odd.

DEFINITION 3.1. *A function $f : \mathbf{Z}_q^n \to \mathbf{Z}_q$ is a regular bent function if there is a function $g : \mathbf{Z}_q^n \to \mathbf{Z}_q$ such that*

$$F(\mathbf{w}) = u^{g(\mathbf{w})}, \text{ for all } \mathbf{w} \in \mathbf{Z}_q^n.$$

The following theorem is due to Kumar, Scholtz and Welch [2]. For $q = 2$ it was first proved by Maiorana, see [1], generalizing the construction method of Rothaus [12].

THEOREM 3.1. *Let $g : \mathbf{Z}_q^m \to \mathbf{Z}_q$ be any function and $\pi : \mathbf{Z}_q^m \to \mathbf{Z}_q^m$ any bijective transformation. Then the function*

$$f : \mathbf{Z}_q^{2m} = \mathbf{Z}_q^m \times \mathbf{Z}_q^m \to \mathbf{Z}_q,\ f(\mathrm{x}_1, \mathrm{x}_2) = \pi(\mathrm{x}_1) \cdot \mathrm{x}_2 + g(\mathrm{x}_1)$$

is a regular bent function.

Clearly, different choices of π and g yield different bent functions. Hence we have a lower bound

$$q^{q^{\frac{n}{2}}} (q^{\frac{n}{2}}!)$$

for the number of bent functions in $\mathbf{Z}_q^n$.

Because of their good correlation properties with linear functions (see Theorem 2.1) bent functions could be used to combine several independently generated sequences. Then it would be important to know what is their distance to affine functions and how well balanced their value distributions are.

Let us make the notation

$$b_k = \#\{\mathrm{x} \in \mathbf{Z}_p^n \mid f(\mathrm{x}) = k\},\ k \in \mathbf{Z}_p.$$

Then we say that the value distribution of $f : \mathbf{Z}_p^n \to \mathbf{Z}_p$ is the ordered p-tuple $(b_0, b_1, \ldots, b_{p-1})$.

THEOREM 3.2. *Let n be even and p a prime. Then the value distribution of a bent function $f : \mathbf{Z}_p^n \to \mathbf{Z}_p$ is $(b_0, b_1, \ldots, b_{p-1})$, where*

$$b_0 = p^{n-1} \pm (p-1)p^{\frac{n}{2}-1}$$
$$b_k = p^{n-1} \mp p^{\frac{n}{2}-1},\ \text{for } k = 1, 2, \ldots, p-1,$$

or its cyclic shift. Here the $\pm$ signs are taken correspondingly. Moreover, a regular bent function has the upper signs.

PROOF: According to [2], Property 8, there is an integer s such that

$$F(0) = u^{\frac{s}{2}}.$$

Hence we have

$$\sum_{k=0}^{p-1} b_k u^k = p^{\frac{n}{2}} u^{\frac{s}{2}}.$$

If s is even this equation gets the form

$$\sum_{k=0}^{p-1} b_k u^{k-r} = p^{\frac{n}{2}}$$

for some integer r. This is always the case for a regular bent function. If s is odd, we choose $r = \frac{s-p}{2}$ to have

$$u^{\frac{s}{2}-r} = u^{\frac{p}{2}} = -1.$$

In this case the equation becomes

$$\sum_{k=0}^{p-1} b_k u^{k-r} = -p^{\frac{n}{2}}$$

for some integer r. Since p is a prime it then follows that

$$b_0 \mp p^{\frac{n}{2}} = b_1 = b_2 = \cdots = b_{p-1},$$

or a cyclic shift. On the other hand $\sum_{k=0}^{p-1} b_k = p^n$, from where we obtain the solution

$$b_0 \mp p^{\frac{n}{2}} = b_1 = b_2 = \cdots = b_{p-1} = p^{n-1} \mp p^{\frac{n}{2}-1}.$$

Let us give some examples of regular bent functions:

(1) the functions given in Theorem 3.1;
(2) all binary bent functions (which exist only for even dimensions);
(3) $f(\mathrm{x}) = x_1^2 + x_2^2 + \cdots + x_n^2$ for n even and $p = 1 \pmod 4$;
(4) $f(\mathrm{x}) = x_1^2 + x_2^2 + \cdots + x_n^2$ for $n = 0 \pmod 4$ and p odd.

An example of a function having the lower signs in Theorem 3.2. (and falling in the category (2) of Theorem 3.3 below) is $f(\mathrm{x}) = x_1^2 + x_2^2 + \cdots + x_n^2$ for $n = 2 \pmod 4$ and $p = 3 \pmod 4$ and so is, more generally, the sum $f + g : \mathbf{Z}_p^n \times \mathbf{Z}_p^m \to \mathbf{Z}_p$, where $g : \mathbf{Z}_p^m \to \mathbf{Z}_p$ is a regular bent function.

THEOREM 3.3. *Let n be even and p a prime. Then the Hamming distance of a bent function $f : \mathbf{Z}_p^n \to \mathbf{Z}_p$ to the nearest affine function is either*

(1) $(p-1)(p^{n-1} - p^{\frac{n}{2}-1})$; *or*
(2) $(p-1)p^{n-1} - p^{\frac{n}{2}-1}$.

Regular bent functions have the distance (1) to the nearest affine function.

PROOF: Let $A : \mathbf{Z}_p^n \to \mathbf{Z}_p$, $A(\mathrm{x}) = \mathrm{w} \cdot \mathrm{x} + r$, be an affine function and denote

$$a_k = \#\{\mathrm{x} \in \mathbf{Z}_p^n \mid f(\mathrm{x}) - \mathrm{w} \cdot \mathrm{x} - r = k\}.$$

We now make use of [2], Property 8, for $\mathrm{w} \neq 0$ and proceed exactly as in the proof of the preceding theorem to obtain

$$a_0 \mp p^{\frac{n}{2}} = a_1 = a_2 = \cdots = a_{p-1} = p^{n-1} \mp p^{\frac{n}{2}-1}.$$

The Hamming distance of f to the affine function A is then $\sum_{k=1}^{p-1} a_k$. This is minimized over the totality of all affine functions when we choose r such that a_0 obtains its maximal value which is either

(1) $p^{n-1} + (p-1)p^{\frac{n}{2}-1}$, or
(2) $p^{n-1} + p^{\frac{n}{2}-1}$.

From this theorem and the above example it follows that for $p = 3 \pmod 4$ there are two classes of bent functions and the first one, to which the regular bent functions belong, is closer to the set of affine functions than the second one, to which the square-sum function belongs.

To study the case where n is odd we need the following lemma from the theory of cyclotomic fields.

LEMMA. *For a prime p there is a unique integer solution $(a_1, a_2, \ldots, a_{p-1})$ to the equation*

$$a_1 u + a_2 u^2 + \cdots + a_{p-1} u^{p-1} = \begin{cases} \sqrt{p}, & \text{for } p = 1 \pmod 4 \\ i\sqrt{p}, & \text{for } p = 3 \pmod 4. \end{cases}$$

This solution is

$$a_k = \left(\frac{k}{p}\right), \ k = 1, 2, \ldots, p-1.$$

PROOF: The proof is obtained by combining Gaussian quadratic sums, see, e.g., [2], formula (14), with the argument on the dimension of the pth cyclotomic field, [4], Theorem 2.47.

THEOREM 3.4. *Let n be odd and p an odd prime. The value distribution of a regular bent function from $\mathbf{Z}_p^n$ to $\mathbf{Z}_p$ is a cyclic permutation of $(b_0, b_1, \ldots, b_{p-1})$, where $b_0 = p^{n-1}$ and either*

(1) $$b_k = p^{n-1} + \left(\frac{k}{p}\right) p^{\frac{n-1}{2}}, \text{ for all } k = 1, 2, \ldots, p-1, \text{ or}$$

(2) $$b_k = p^{n-1} - \left(\frac{k}{p}\right) p^{\frac{n-1}{2}}, \text{ for all } k = 1, 2, \ldots, p-1.$$

PROOF: Let $f : \mathbf{Z}_p^n \to \mathbf{Z}_p$ be a bent function. We consider first the case $p = 1 \pmod 4$. By [2], Property 8, there is an integer s such that

$$F(0) = u^{\frac{s}{2}} = \frac{1}{\sqrt{p^n}} \sum_{k=0}^{p-1} b_k u^k.$$

Similarily as in the proof of Theorem 3.2. this equation becomes

$$b_0 + b_1 u + \cdots + b_{p-1} u^{p-1} = \pm\sqrt{p} \cdot p^{\frac{n-1}{2}}.$$

Now it follows from the preceding lemma that the solution is of the form

$$b_k = b_0 \pm \left(\frac{k}{p}\right) p^{\frac{n-1}{2}}, \ k = 1, 2, \ldots, p-1.$$

From $\sum_{k=0}^{p-1} b_k = p^n$ we then get that $b_0 = p^{n-1}$.

Assume now that $p = 3 \pmod 4$. Then by [2], Property 8, there is an integer s such that

$$F(0) = u^{\frac{2s+1}{4}}.$$

Take $r = \frac{p^2-1}{4}(2s+1)$, which is an integer. Then we have

$$F(0) = u^{p(2s+1)\cdot\frac{p}{4}-r} = \pm i \cdot u^{-r},$$

since $p(2s+1)$ is odd. Now we proceed exactly as in the first case to obtain the solution.

By repeating this proof for $w \neq 0$ we get the following

THEOREM 3.5. *For n odd and p an odd prime the Hamming distance of a bent function from $\mathbf{Z}_p^n$ to $\mathbf{Z}_p$ to the nearest affine function is*

$$(p-1)p^{n-1} - p^{\frac{n-1}{2}}.$$

4. Difference sets and constructions. From Maiorana's construction we obtain a lower bound $2^{2^{\frac{n}{2}}}(2^{\frac{n}{2}}!)$ for the number of bent functions in $\mathbf{Z}_2^n$. If f is a bent function $\mathbf{Z}_2^n \to \mathbf{Z}_2$ then so is $f \circ A + L$ for every affine bijective transformation A of $\mathbf{Z}_2^n$ and linear $L : \mathbf{Z}_2^n \to \mathbf{Z}_2$. We call two bent functions f and g equivalent if they are related to each other in this way, i.e., $g = f \circ A + L$. This equivalence relation devides the set of bent functions into disjoint equivalence classes each containing at most 2^{n^2+n} functions. The functions in a same class have the same nonlinear order which is bounded from above by $\frac{n}{2}$. It follows that for n large enough to satisfy

$$(2^{\frac{n}{2}}!)2^{2^{\frac{n}{2}}-n^2-n} > \frac{n}{2} - 1$$

i.e., for $n \geq 10$ Maiorana's construction gives non-equivalent bent functions of the same (highest) nonlinear order. For cryptographic purposes and unpredictability this is a very desirable property.

On the other hand, Rothaus made in [12] a complete list of bent functions in $\mathbf{Z}_2^6$ and also verified using a computer program that all of them of nonlinear order 3 are obtainable from each other by an affine transformation of coordinates and the addition of a linear function. To clarify the situation for $n = 8$ other construction methods, especially those that give more bent functions for small n, might be useful.

The case $n = 8$ remains open also in[11]. There is also given another construction method which yields the same number of bent functions as Maiorana's method.

The following result can be used in the construction of the set of ones of a bent function.

THEOREM 4.1. *A function $f : \mathbf{Z}_2^n \to \mathbf{Z}_2$ with $2^{n-1} - 2^{\frac{n}{2}-1}$ ones is bent if and only if for every nonconstant linear function $L : \mathbf{Z}_2^n \to \mathbf{Z}_2$ the product Lf has either 2^{n-2} or $2^{n-2} - 2^{\frac{n}{2}-1}$ ones.*

Hence to construct the set of ones of any bent function in $\mathbf{Z}_2^n$ it is enough to find n vectors of length $2^{n-1} - 2^{\frac{n}{2}-1}$ each consisting of 2^{n-2} ones and $2^{n-2} - 2^{\frac{n}{2}-1}$ zeros such that every possible sum of these vectors has exactly 2^{n-2} or $2^{n-2} - 2^{\frac{n}{2}-1}$ ones. It is an open problem whether this method of construction can be made feasible for large n.

Example. The columns of the following matrix are constructed by means of the above principle.

x_4	x_3	x_2	x_1
0	1	0	1
0	1	1	0
1	0	1	0
1	0	1	1
1	1	0	1
1	1	1	1

Hence the row vectors form the set of the ones of a bent function. This bent function is $x_1x_3 + x_2x_3 + x_2x_4$.

In the above matrix the sum of the first and the third row equals to the sixth row and adding up the second row with the fourth one gives the fifth. Hence this set of rows break up into two triples and its easily checked that these are the only existing triples. This implies that every row a can be expressed in two different ways as a difference of two other rows b and c, i.e., $\mathrm{a} = \mathrm{b} + \mathrm{c} = \mathrm{c} + \mathrm{b}$

The rows of the above matrix form an example of a specific combinatorial structure called difference set.

DEFINITION 4.1. *Let G be an additive Abelian group of order v. A subset D of G is called a (v, k, λ)–difference set if it is of order k and if every nonzero element $a \in D$ can be expressed in λ different ways as a difference $a = b - c$, where $b \in D$ and $c \in D$.*

The following result was already known to Dillon [1].

THEOREM 4.2. *A function $f : \mathbf{Z}_2^n \to \mathbf{Z}_2$ is bent if and only if it is a characteristic function of a difference set.*

Let us mention that it was proved by Mann, [5] pp.72-73, that the parameters of a difference set in $\mathbf{Z}_2^n$ are $(2^n, 2^{n-1} \pm 2^{\frac{n}{2}-1}, 2^{n-2} \pm 2^{\frac{n}{2}-1})$.

There are some previous constructions of difference sets found in the literature. In [1] Dillon proved that the constructions of Menon [8] and [9] and that of Turyn [13] are special cases of Maiorana's binary bent functions. The main result of [1] is that for $m > 3$ there exist bent functions in $\mathbf{Z}_2^{2m}$ which are not equivalent to any Maiorana's functions.

McFarland gave in 1971 the following construction of difference set. It can be easily checked that a function f is a Maiorana bent function if and only if either its set of zeros or set of ones can be constructed by the method of McFarland.

Let $H_1, H_2, \ldots, H_r$ be the totality of different hyperplanes, i.e., $(m-1)$-dimensional subspaces in $\mathbf{Z}_2^m$; then $r = 2^m - 1$. Let $\mathbf{a}_j \in \mathbf{Z}_2^m$, $j = 1, \ldots, r$, be any elements and let $\mathbf{b}_j \in \mathbf{Z}_2^m$, $j = 1, \ldots, r$, be distinct elements.

THEOREM 4.3 (MCFARLAND [6]). *The union of the r subsets in $\mathbf{Z}_2^{2m}$ of the form*

$$\{ (\mathbf{a}_j + \mathbf{x}, \mathbf{b}_j) \mid \mathbf{x} \in H_j \}, \quad j = 1, 2, \ldots, r,$$

is a difference set with parameters $(2^{2m}, 2^{2m-1} - 2^{m-1}, 2^{2m-2} - 2^{m-1})$.

In fact, when choosing the elements $\mathbf{a}_j$ the only thing that matters is whether $\mathbf{a}_j$ belongs to H_j or not. Moreover, we have the following property of McFarland's construction.

THEOREM 4.4. *The nonlinear order of a bent function constructed by McFarland's method is maximal if and only if the element $\mathbf{a}_j$ is chosen from H_j for an odd number of indices j.*

PROOF: Assume that f is a bent function whose set of ones is of the form of McFarland. Let π be a permutation which takes each element $\mathbf{b}_j$ to the nonzero element which is orthogonal to H_j. Let us define a function g such that

$$g(\mathbf{b}_j) = \begin{cases} 1, & \text{if } \mathbf{a}_j \in H_j \\ 0, & \text{if } \mathbf{a}_j \notin H_j, \end{cases}$$

and set $g(\mathbf{b}) = 0$ if $\pi(\mathbf{b}) = \mathbf{0}$. Then

$$f(\mathbf{x}_1, \mathbf{x}_2) = g(\mathbf{x}_1) + \pi(\mathbf{x}_1) \cdot \mathbf{x}_2$$

and its nonlinear order is maximal if and only if the number of ones of g is odd.

In the general p-ary case the connection between bent functions and difference sets is more complicated and remains to be studied. Let us only mention that the general constructions of McFarland do not produce difference sets in groups of order p^n. Under some conditions regular bent functions yield difference sets in $\mathbf{Z}_p^n$, n even, with parameters

$$(p^n, p^{n-1} + (p-1)p^{\frac{n}{2}-1}, p^{n-2} + (p-1)p^{\frac{n}{2}-1}).$$

also for $p > 2$.

Example. The zeros of the bent function $f : \mathbf{Z}_3^4 \to \mathbf{Z}_3$, $f(\mathbf{x}) = x_1x_2 + x_3x_4$, form a difference set with parameters (81,33,15).

Acknowledgement. I wish to thank Rainer Rueppel for bringing [2] to my attention.

REFERENCES

1. J. F. Dillon, *Elementary Hadamard difference sets*, Proceedings of the Sixth Southeastern Conference on Combinatorics, Graph Theory and Computing, Boca Raton, Florida (1975), 237–249; Congressus Numerantium No. XIV, Utilitas Math., Winnipeg, Manitoba (1975).
2. P. V. Kumar, R. A. Scholtz and L. R. Welch, *Generalized bent functions and their properties*, J. Combinatorial Theory, Ser. A 40 (1985), 90–107.
3. A. Lempel and M. Cohn, *Maximal families of bent sequences*, IEEE Trans. Inform. Theory IT-28 (1982), 865–868.
4. R. Lidl and H. Niederreiter, "Introduction to finite fields and their applications," Cambridge University Press, Cambridge, 1986.
5. H. B. Mann, "Addition theorems," John Wiley & Sons, New York, 1965.
6. R. L. McFarland, *A family of difference sets in non-cyclic groups*, J. Combinatorial Theory, Ser. A 15 (1973), 1–10.
7. W. Meier and O. Staffelbach, *Nonlinearity criteria for cryptographic functions*, Advances in Cryptology, Proceedings of Eurocrypt '89 (to appear).
8. P. K. Menon, *Difference sets in Abelian groups*, Proc. Amer. Math. Soc. 11 (1960), 368–376.
9. ———, *On difference sets whose parameters satisfy a certain relation*, Proc. Amer. Math. Soc. 13 (1962), 739–745.
10. J. D. Olsen, R. A. Scholtz and L. R. Welch, *Bent function sequences*, IEEE Trans. Inform. Theory IT-28 (1982), 858–864.
11. B. Preneel et al., Propagation characteristics of Boolean bent functions, Proceedings of Eurocrypt '90 (to appear).
12. O. S. Rothaus, *On "bent" functions*, J. Combinatorial Theory, Ser. A 20 (1976), 300–305.
13. R. J. Turyn, *Character sums and difference sets*, Pacific J. Math. 15 (1965), 319–346.

Finnish Defense Forces, Signals Section, P.O. Box 919, SF–00101 Helsinki, Finland