New Bent Mappings Suitable for Fast Implementation

Kaisa Nyberg[1]
Prinz Eugen-Straße 18/6
A-1040 Vienna, Austria
E-mail: nyberg@ict.tuwien.ac.at

13 January 1994

Abstract

The perfect nonlinear mappings and their implementations studied in [4] where based on the Maiorana-McFarland construction of bent functions. Recently Carlet [1] presented two modifications of the Maiorana-McFarland construction and obtained two new classes of bent functions. The purpose of the present work is to give nontrivial examples of Carlet's bent functions and construct new perfect nonlinear mappings admitting fast implementation.

1 Introduction

Bent functions have a great importance in cryptology and in coding techniques for spread spectrum applications. Bent functions are optimal with respect to autocorrelation and correlation with linear functions [5]. Bent mappings have bent coordinate functions and for every fixed input difference uniformly distributed output differences [4] which offers optimal resistance against differential cryptanalysis.

It is proved in [4] that bent mappings exist only if the input is at least twice as long as the output. Hence permutations or substitution transformations with input size only slightly larger than the output size cannot have uniformly distributed output differences. Recently several examples and construction methods for near bent or equivalently, almost perfect nonlinear permutations have been given principally aimed for use in DES-like block ciphers to provide resistance against differential cryptanalysis.

Much less attention have been focused on the use of bent structures in the design of stream cipher. Self-synchronizing stream cipers can be attacked using chosen ciphertext and therefore eventually a differential cryptanalysis attack can

[1] Supported by the grant 41/Mdd 292/93, Matine Board, Finland

be launched. Since the bent mappings have the minimum correlation with the affine mappings they would be most useful when designing synchronous stream ciphers resistant against correlation attacks.

In §2 we recall the basic facts of binary bent functions their construction by the Maiorana-McFarland method. Based on this method and using a linear feedback shift register to generate a suitable set of permutations an efficient implementation of bent mappings is given in [4]. In §3 we modify this basic machinery to obtain fast implementations of new bent mappings whose coordinate functions belong to the new classes of bent functions introduced in [1]. At the same time new nontrivial concrete examples of Carlet's bent functions are obtained.

2 A Previous Construction of Bent Mappings

Throughout the paper let $\mathbf{F}$ be the Galois field of order 2, and n and p positive integers with $n = 2p$.

For a definition of bent boolean function see [5] or Definition 1 (with $m = 1$) below. The following theorem is due to Maiorana (unpublished, see [2]). An equivalent method is given by McFarland in [3].

Theorem 1 *Let $g : \mathbf{F}^p \to \mathbf{F}$ be a boolean function and $\pi : \mathbf{F}^p \to \mathbf{F}^p$ a permutation. Then the function*

$$f : \mathbf{F}^n = \mathbf{F}^p \times \mathbf{F}^p \to \mathbf{F},\ f(x, y) = x \cdot \pi(y) + g(y)$$

is bent.

The following generalization of bentness is given in [4].

Definition 1 *A mapping $f : \mathbf{F}^n \to \mathbf{F}^m$ is perfect nonlinear (bent) if for every fixed non-zero $w \in \mathbf{F}^n$ the difference $f(u + w) + f(u)$ takes each value $v \in \mathbf{F}^m$ for q^{n-m} values of $u \in \mathbf{F}^n$.*

We have the following useful characterization of bent mappings.

Theorem 2 *A mapping $f : \mathbf{F}^n \to \mathbf{F}^m$ is bent if and only if every nontrivial linear combination of its coordinate functions is bent, that is, for every nonzero $c \in \mathbf{F}^m$ the function $u \mapsto c \cdot f(u)$ is bent.*

We now recall the construction of bent mapping given in [4]. Let $f : \mathbf{F}^n \to \mathbf{F}^m$ be a mapping and $f_1, f_2, \ldots, f_m$ the coordinate functions of f. Assume that every f_i, $i = 1, 2, \ldots, m$, is a Maiorana function, i.e., has the form

$$f_i(x, y) = x \cdot \pi_i(y) + g_i(y),$$

where π_i is a permutation of the space $\mathbf{F}^p$ and g_i is a boolean function in $\mathbf{F}^p$. Then it follows from Theorem 2 that $f = (f_1, f_2, \ldots, f_m)$ is bent if every nontrivial

linear combination of the permutations π_i, $i = 1, 2, \ldots, m$ is a permutation of $\mathbf{F}^p$. Note that $m \leq p$.

One way of constructing a suitable family of permutations of $\mathbf{F}^p$, is to use a binary linear feedback shift register (LFSR) of length p with a primitive feedback polynomial. Let A be the state transition mapping of the LFSR. Then A as well as the powers A^i of A are permutations of $\mathbf{F}^p$. Moreover, by the well known property of LFSR generating maximal length sequences every non-trivial linear combination of the permutations $I, A, A^2, \ldots, A^{p-1}$ is a power of A and hence a permutation.

Now an elementary implementation of a bent mapping with n binary inputs and m binary outputs, $n \geq 2m$, is obtained in the following way. Take a binary LFSR of length p with a primitive feedback polynomial. Devide the input of n bits into two halves x and y. Load the LFSR with y, or optionally, with $\pi(y)$ where π is a (nonlinear) permutation of $\mathbf{F}^p$. The first bit of the output block of length m is obtained by calculating the dot product of x and the initial contents. To obtain the second digit the shift register is shifted once and the dot product of its new contents with x is calculated. In this manner every shift of the register produces a new output digit.

This basic arrangement is very fast. If nonlinear permutation π is used or nonlinear boolean functions g_i are added to the coordinate functions, the computational complexity may increase.

Let us still consider the properties of the basic arrangement,

$$f = (f_1, f_2, \ldots, f_m),\ f_i(x, y) = x \cdot A^{i-1}(y).$$

The output of this bent mapping $f : \mathbf{F}^n \to \mathbf{F}^m$ is not uniformly distributed. The zero output is obtained for

$$2^{n-m} - 2^{p-m} + 2^p$$

different inputs. The other outputs are obtained for equally many, i.e., for

$$2^{n-m} - 2^{p-m}$$

different inputs. If it can be arranged that the the half y of the input that goes to the LFSR is never the all zero block, then the restriction the function f has uniformly distributed output. It turns out that this restriction causes only slight deviation from strict bentness. To see this let a nonzero increment w have two halves w_1 and w_2 corresponding to the division of the input. Then

$$f_i((x, y) + w) + f_i(x, y) = w_1 \cdot A^{i-1}(y) + x \cdot A^{i-1}(w_2) + w_1 \cdot A^{i-1}(w_2),$$

for every $i = 1, 2, \ldots, m$. Now we have two cases.

1° $w_2 = 0$. In this case $f((x, y) + w)) + f(x, y)$ is a linear mapping of y and takes each nonzero value for 2^{n-m} different inputs and the zero value for $2^{n-m} - 2^p$ different inputs with $y \neq 0$.

2° $w_2 \neq 0$. Then the restrictions of the differences $f_i((x, y) + w) + f_i(x, y)$ to inputs (x, y) with $y \neq 0$ are balanced.

The Maiorana-McFarland construction of bent functions and consequently, Maiorana-McFarland based construction of bent mappings has the weakness that if the second input half is kept constant, then the resulting functions and mappings are linear in the first input half. The bent functions and mappings constructed in the next section do not have this weakness.

3 New Constructions of Bent Mappings

3.1 Bent Mappings Derived from $\mathcal{D}$

The first new class of bent functions defined in [1], Definition 1, is class $\mathcal{D}$ of all boolean functions of the form

$$(x, y) \mapsto \phi_E(x, y) + x \cdot \pi(y), \ (x, y) \in \mathbf{F}^p \times \mathbf{F}^p,$$

where ϕ_E is the characteristic function of subspace $E = E_1 \times E_2$ of $\mathbf{F}^p \times \mathbf{F}^p$ of dimension p and π is a permutation of $\mathbf{F}^p$ such that $x \cdot \pi(y) = 0$ for all $(x, y) \in E$.

Assume that $n = 2p = 4s$ where s is a positive integer. We construct now a class of bent mappings from $\mathbf{F}^n \to \mathbf{F}^s$ whose coordinate functions belong to class $\mathcal{D}$. For that purpose we choose A to be the state transition mapping of a binary LFSR of length p such that the connection polynomial C is a product of two primitive polynomials of degree s which are denoted by C_1 and C_2. Then every nonzero sequence generated by the LFSR has linear complexity at least s which means that every nontrivial linear combination of the permutations $I, A, A^2, \ldots, A^{s-1}$ is a permutation of $\mathbf{F}^p$. We choose E_2 to be the subspace of $\mathbf{F}^p$ consisting of blocks of length p of the maximum length sequence generated by the LFSR with connection polynomial C_1. Then E_2 is an invariant subspace of permutation A and, moreover, of all permutations π which are linear combinations of $I = A^0, A, A^2, \ldots, A^{s-1}$. We set

$$E_1 = \pi(E_2)^\perp = E_2^\perp.$$

Then E_1 is the subspace of $\mathbf{F}_p$ spanned by the s vectors

$$\begin{aligned} e_1 &= (c_0, \ldots, c_s, 0, \ldots, 0) \\ e_2 &= (0, c_0, \ldots, c_s, 0, \ldots, 0) \\ &\vdots \\ e_s &= (0, \ldots, 0, c_0, \ldots, c_s) \end{aligned}$$

where we have denoted by $c_0, c_1, \ldots, c_s$ the coefficients of the connection polynomial C_1.

Let G be the subspace of $\mathbf{F}^p$ spanned by the s vectors starting from

$$(1, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots$$

Then the characteristic function ϕ_G defined in $\mathbf{F}^p$ has the following expression

$$\phi_G(x) = \phi_G(x_1, \ldots, x_p) = (x_{s+1} + 1)(x_{s+2} + 1) \cdots (x_p + 1)$$

Given a basis of E_1 we get its characteristic function ϕ_{E_1} as a composed functions of a linear transformation and ϕ_G. By the definition of E_2 we have

$$\phi_{E_2}(y_1, \ldots, y_p) = \prod_{j=1}^{s} (e_j \cdot y + 1)$$

Then ϕ_E is easily computed as

$$\phi_E(x, y) = \phi_{E_1 \times E_2}(x, y) = \phi_{E_1}(x)\phi_{E_2}(y)$$

for all $(x, y) \in \mathbf{F}^n$.

For $i = 1, 2, \ldots, s$ and $(x, y) \in \mathbf{F}^p \times \mathbf{F}^p$ we set

$$f_i(x, y) = \delta_i \phi_E(x, y) + x \cdot A^{i-1}(y),$$

where $\delta_i = 0$ or 1, and $f = (f_1, f_2, \ldots, f_s)$. Then f is a bent mapping from $\mathbf{F}^n$ to $\mathbf{F}^s$ whose coordinate functions and their linear combinations are in class $\mathcal{D}$.

3.2 Bent Mappings Derived from $\mathcal{C}$

Class $\mathcal{C}$ as specified in [1], Corollary 4, consists of all boolean functions on $\mathbf{F}^n$ of the form

$$(x, y) \mapsto x \cdot \pi(y) + \phi_{L^\perp}(x)$$

where L is a linear subspace of $\mathbf{F}^p$ and π is a permutation of $\mathbf{F}^p$ such that for all $\lambda \in \mathbf{F}^p$ the set $\pi^{-1}(\lambda + L)$ is a flat.

Assume first that σ is an affine permutation of $\mathbf{F}^p$. Then the the condition in the definition of class $\mathcal{C}$ is satisfied for any linear subspace L and any permutation π of the form $B \circ \sigma$, where B is a non-zero linear combination of $I, A, \ldots, A^{p-1}$ and A is the state transition mapping of a LFSR with primitive feedback polynomial as in Section 2. For $i = 1, 2, \ldots, m$, $m \leq p$, and $(x, y) \in \mathbf{F}^p \times \mathbf{F}^p$ we set

$$f_i(x, y) = x \cdot A^{i-1}(\sigma(y)) + \delta_i \phi_{L^\perp}(x)$$

where $\delta_i = 0$ or 1. Then $f = (f_1, f_2, \ldots, f_m) : \mathbf{F}^n \to \mathbf{F}^m$ is a bent mapping with coordinate functions in $\mathcal{C}$. A fast implementation of f can be obtained in the manner described in Section 2. However, this construction has the disadvantage, that if x is fixed then f is a linear mapping of y.

A second construction of bent mapping derived from $\mathcal{C}$ is obtained as follows. Let r be any integer between 1 and s and A the state transition mapping of an LFSR whose connection polynomial is a product of two primitive polynomials of degrees r and $p - r$, $r \leq \frac{p}{2}$. Let C be the polynomial of degree r and L the invariant subspace of A of dimension r which consists of blocks of length p of the sequence generated by the LFSR with polynomial C. We choose σ to be any permutation of $\mathbf{F}^p$ such that for all $\lambda \in \mathbf{F}^p$ the set $\sigma^{-1}(\lambda + L)$ is a flat. Then this condition is satisfied for all permutations π of the form $B \circ \sigma$, where B is

a non-zero linear combination of I, $A, \ldots, A^{r-1}$. For $i = 1, 2, \ldots, m$, $m \leq r$ and $(x, y) \in \mathbf{F}^p \times \mathbf{F}^p$ we set

$$f_i(x, y) = x \cdot A^{i-1}(\sigma(y)) + \delta_i \phi_{L^\perp}(x)$$

where $\delta_i = 0$ or 1. Then $f = (f_1, f_2, \ldots, f_m) : \mathbf{F}^n \to \mathbf{F}^m$ is a bent mapping with coordinate functions in $\mathcal{C}$.

References

[1] C. Carlet, *Two New Classes of Bent Functions*, Eurocrypt'93, Bergen, Norway, May 1993

[2] J. F. Dillon, *Elementary Hadamard Difference Sets*, Proceedings of the Sixth Southeastern Conference on Combinatorics, Graph Theory and Computing, Boca Raton, Florida, Congressus Numerantium No. XIV, Utilitas Math., Winnipeg, Manitoba, 1975, pp. 237-249

[3] R. L. McFarland, *A Family of Difference Sets in Non-Cyclic Groups*, J. Combinatorial Theory, Ser. A, 15, 1973, pp. 1-10

[4] K. Nyberg, *Perfect Nonlinear S-Boxes*, Advances in Cryptology, Proceedings of Eurocrypt'91, Lectures Notes in Computer Science 547, Springer-Verlag, 1992

[5] O. S. Rothaus, *On "Bent" Functions*, J. Combinatorial Theory, Ser. A, 20, 1976