On the construction of highly nonlinear permutations

KAISA NYBERG

Finnish Defence Forces
University of Helsinki
(on leave)

1. Introduction

Highly nonlinear permutations play an important role in the design of cryptographic transformations such as block ciphers, hash functions and stream ciphers. The substitution boxes of DES are relatively small in dimension and they can be generated by testing randomly chosen functions for required design criteria. Security may be increased by the use of substitution transformations of higher dimensions. But when the dimensions grow larger, analytic construction methods become necessary.

In this paper a general methodology is developed to construct permutations of a vector space over a finite field such that the nonlinearity of both the permutation itself and its inverse can be kept in control. The nonlinearity measure used is based on the Hamming distance from the set of affine functions. For quadratic functions there is a close relationship with this nonlinearity measure and the number of the so called linear structures of the function. This approach leads to a necessary and sufficient condition under which a transformation of F_q^n (n odd, $q = 2^d$, d odd), with quadratic coordinate functions, is a highly nonlinear permutation with equally highly nonlinear inverse.

Finally, we shall apply our general methodology to give a general construction of which the cubing permutation is a special case.

It was observed by Pieprzyk [6] that the coordinate functions of the cubing permutation in $GF(2^n)$, n odd, are of high nonlinearity, when considered with respect to a self-dual normal basis in $GF(2^n)$ over $GF(2)$. His measure of nonlinearity is weaker than the one given in the present work, since it only takes into account the coordinate functions of the permutation. Our nonlinearity measure involves all nontrivial linear combinations of the coordinate functions of the permutation and allows a rigorous proof of the fact that the inverse permutation is of the same nonlinearity.

The permutations of $GF(2^n)$ constructed in §4 have the property that their coordinate functions as well as the coordinate functions of their inverses are all of the same large distance from the set of affine functions independently of the choices for the bases in the input and and output spaces. This degree of nonlinearity only depends on over which subfield $GF(2^n)$ is considered as a linear space.

Current address: Prinz Eugenstraße 18/6, A-1040 Wien, Austria

R.A. Rueppel (Ed.): Advances in Cryptology - EUROCRYPT '92, LNCS 658, pp. 92-98, 1993.

2. The nonlinearity measure

Let $\mathsf{F} = \mathsf{F}_q$ be a finite field with q elements and consider a function $f : \mathsf{F}^n \to \mathsf{F}$.

DEFINITION 1. *The nonnegative integer*

$$\mathcal{N}(f) = \min_{\mathbf{u}\in\mathsf{F}^n, v\in\mathsf{F}} \#\{\mathbf{x} \in \mathsf{F}^n \mid f(\mathbf{x}) \neq \mathbf{u}^t\mathbf{x} + v\}$$

is the Hamming distance of f from affine functions.

It is easily seen that $\mathcal{N}(f)$ is independent of the choice of the basis in the linear space F^n over F.

LEMMA 1. *For all $\mathbf{u} \in \mathsf{F}^n$, $\mathbf{u} \neq 0$*

$$\mathcal{N}(f) \leq (q-1)q^{n-1} = \#\{\mathbf{x} \in \mathsf{F}^n \mid \mathbf{u}^t\mathbf{x} \neq 0\}.$$

By the help of this lemma the third equality in the following definition can be established.

DEFINITION 2. *The nonlinearity of a vector function $\mathbf{f} : \mathsf{F}^n \to \mathsf{F}^m$ is*

$$\begin{aligned}\mathcal{N}(\mathbf{f}) &= \min_{\mathbf{w}\in\mathsf{F}^m, \mathbf{w}\neq 0} \mathcal{N}(\mathbf{w}^t\mathbf{f}) \\ &= \min_{\mathbf{u}\in\mathsf{F}^n, \mathbf{w}\in\mathsf{F}^m, v\in\mathsf{F}, \mathbf{w}\neq 0} \#\{\mathbf{x} \in \mathsf{F}^n \mid \mathbf{w}^t\mathbf{f}(\mathbf{x}) \neq \mathbf{u}^t\mathbf{x} + v\} \\ &= \min_{\mathbf{u}\in\mathsf{F}^n, \mathbf{w}\in\mathsf{F}^m, v\in\mathsf{F}, \mathbf{u}\neq 0 \text{ or } \mathbf{w}\neq 0} \#\{\mathbf{x} \in \mathsf{F}^n \mid \mathbf{w}^t\mathbf{f}(\mathbf{x}) \neq \mathbf{u}^t\mathbf{x} + v\}\end{aligned}$$

PROPOSITION 1. *The nonlinearity $\mathcal{N}(\mathbf{f})$ of $\mathbf{f} : \mathsf{F}^n \to \mathsf{F}^m$ is invariant under linear permutations of the input space F^n and also under linear permutations of the output space F^m.*

This measure of nonlinearity has the following property of symmetry.

THEOREM 1. *Let $\mathbf{f} : \mathsf{F}^n \to \mathsf{F}^n$ be a permutation. Then $\mathcal{N}(\mathbf{f}^{-1}) = \mathcal{N}(\mathbf{f})$.*

PROOF:

$$\begin{aligned}\mathcal{N}(\mathbf{f}^{-1}) &= \min_{\mathbf{u},\mathbf{w}\in\mathsf{F}^n, v\in\mathsf{F}, \mathbf{u}\neq 0 \text{ or } \mathbf{w}\neq 0} \#\{\mathbf{y} \in \mathsf{F}^n \mid \mathbf{w}^t\mathbf{f}^{-1}(\mathbf{y}) \neq \mathbf{u}^t\mathbf{y} + v\} \\ &= \min_{\mathbf{u},\mathbf{w}\in\mathsf{F}^n, v\in\mathsf{F}, \mathbf{u}\neq 0 \text{ or } \mathbf{w}\neq 0} \#\{\mathbf{x} \in \mathsf{F}^n \mid \mathbf{w}^t\mathbf{x} \neq \mathbf{u}^t\mathbf{f}(\mathbf{x}) + v\} \\ &= \mathcal{N}(\mathbf{f}).\end{aligned}$$

The following result will be used later.

PROPOSITION 2. *Let* $f : \mathsf{F}^n \to \mathsf{F}$ *have nonlinearity* $\mathcal{N}(f)$. *Then the function* $g : \mathsf{F}^{n+1} \to \mathsf{F}$

$$(x_1, x_2, \ldots, x_n, x_{n+1}) \mapsto f(x_1, x_2, \ldots, x_n) + x_{n+1}$$

has nonlinearity $q\mathcal{N}(f)$.

PROOF:

$$\begin{aligned}
\mathcal{N}(g) &= \min_{\mathbf{u}\in\mathsf{F}^{n+1}, v\in\mathsf{F}} \#\{\mathbf{x} \in \mathsf{F}^{n+1} \mid g(\mathbf{x}) \neq \mathbf{u}^t\mathbf{x} + v\} \\
&= \min_{\mathbf{u}\in\mathsf{F}^n, u_{n+1}\in\mathsf{F}, v\in\mathsf{F}} \sum_{i=0}^{q-1} \#\{\mathbf{x} \in \mathsf{F}^n, x_{n+1} = i \mid f(\mathbf{x}) + i \neq \mathbf{u}^t\mathbf{x} + iu_{n+1} + v\} \\
&\geq \sum_{i=0}^{q-1} \min_{\mathbf{u}\in\mathsf{F}^n, v_i\in\mathsf{F}} \#\{\mathbf{x} \in \mathsf{F}^n \mid f(\mathbf{x}) \neq \mathbf{u}^t\mathbf{x} + v_i\} \\
&= \sum_{i=0}^{q-1} \mathcal{N}(f) = q\mathcal{N}(f),
\end{aligned}$$

and this lower bound is obtained by the choice $u_{n+1} = 1$.

The linear behaviour of a function can also be measured by the number of its linear structures.

DEFINITION 3. *A vector* $\mathbf{w} \in \mathsf{F}^n$ *is called a linear structure of a function* $f : \mathsf{F}^n \to \mathsf{F}$ *if* $f(\mathbf{x} + \mathbf{w}) - f(\mathbf{x})$ *is constant* $(= f(\mathbf{w}) - f(\mathbf{0}))$ *as* $\mathbf{x} \in \mathsf{F}^n$ *varies.*

It was shown in [2] that if F is a prime field, then the linear structures form a linear subspace on which the restriction of the function is linear. This does not hold in general for arbitrary finite fields. In the next section it shown however that the linear structures of a quadratic function of finitely many variables over any field form a linear space whose dimension determines the Hamming distance from linear functions given in Definition 1.

3. Quadratic functions

Let

$$f(x_1, x_2, \ldots, x_n) = \sum_{i,j} a_{ij} x_i x_j$$

be a quadratic form of n indeterminates over a finite field F with q elements. Then after fixing a basis in F^n we can consider f as a function, a quadratic polynomial, from F^n to F of the form

$$f(\mathbf{x}) = f(x_1, x_2, \ldots, x_n) = \mathbf{x}^t\mathbf{A}\mathbf{x},$$

where $\mathbf{A} = (a_{ij})$. Two quadratic forms $f(\mathbf{x}) = \mathbf{x}^t\mathbf{A}\mathbf{x}$ and $g(\mathbf{x}) = \mathbf{x}^t\mathbf{B}\mathbf{x}$ are called equivalent if they represent the same quadratic form, i.e., there is a linear permutation (a change of basis) $\mathbf{C}$, such that $\mathbf{A} = \mathbf{C}^t\mathbf{B}\mathbf{C}$, or what is the same, $g(\mathbf{C}\mathbf{x}) = f(\mathbf{x})$.

PROPOSITION 3. *Let $f(\mathbf{x}) = \mathbf{x}^t\mathbf{A}\mathbf{x}$ be a quadratic form of n indeterminates over F. Then the linear structures of f form a linear subspace of dimension $\mathcal{X}(f) = n - rank(\mathbf{A} + \mathbf{A}^t)$.*

PROOF: We have

$$\begin{aligned} f(\mathbf{x}+\mathbf{w}) - f(\mathbf{x}) &= (\mathbf{x}+\mathbf{w})^t\mathbf{A}(\mathbf{x}+\mathbf{w} - \mathbf{x}^t\mathbf{A}\mathbf{x} \\ &= \mathbf{x}^tA\mathbf{w} + \mathbf{w}^t\mathbf{A}\mathbf{x} + \mathbf{w}^t\mathbf{A}\mathbf{w} \\ &= \mathbf{x}^t(\mathbf{A}+\mathbf{A}^t)\mathbf{w} + f(w). \end{aligned}$$

Hence w is a linear structure of f if and only if $(\mathbf{A} + \mathbf{A}^t)\mathbf{w} = \mathbf{0}$.

The following result is a consequence of Theorem 6.30 in [4] and the preceeding proposition.

PROPOSITION 4. *Let n be odd and $q = 2^d$ and $f(\mathbf{x}) = \mathbf{x}^t\mathbf{A}\mathbf{x}$ be a quadratic form in F^n with $rank(\mathbf{A} + \mathbf{A}^t) = r$. Then r is even and f is equivalent to*

$$x_1x_2 + x_3x_4 + \cdots + x_{r-1}x_r + L(x_1, x_2, ..., x_n)$$

where L is a linear form of n indeterminates.

The quadratic form $f(x_1, x_2, \ldots, x_n) = x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n$ (for an even n) is a perfect nonlinear function from F^n to F, that is, for every fixed $\mathbf{w} \in \mathsf{F}^n$ the difference $f(\mathbf{x}+\mathbf{w}) - f(\mathbf{x})$ obtains each value in F equally many times. Hence it is also a bent function, if F is a prime field with q elements, and the distance of f to the set of affine functions is the maximum

$$\mathcal{N}(f) = (q-1)(q^{n-1} - q^{\frac{n}{2}-1}) \tag{1}$$

(see [5], Theorem 3.3). It is straightforward to check that if f is considered over $\mathsf{F} = GF(2^d)$ then the formula (1) also holds with $q = 2^d$.

Let us remark that the quadratic functions of n variables over $GF(2)$ belong to the class of partially bent functions ([1], [7]). By definition due to C. Carlet a Boolean function is partially bent if the product of the numbers of the nonzeros of the autocorrelation function and the nonzeros of the Walsh transform obtain the absolute lower bound 2^n. So partially bent functions are optimal in this sense. But since linear functions are contained in the class of partially bent functions, also high linearity has to be required of functions to be used in cryptography. For a quadratic function f this means that $\mathcal{X}(f)$ should be as small as possible. For n odd the minimum of $\mathcal{X}(f)$ is 1.

Summarizing the results of Propositions 2, 3 and 4 we obtain the following

THEOREM 2. *Let* $\mathsf{F} = GF(2^d)$ *and* $q = 2^d$. *Then every quadratic form in* F^n,

$$f(\mathbf{x}) = \mathbf{x}^t \mathbf{A} \mathbf{x}$$

with $\mathrm{rank}(\mathbf{A} + \mathbf{A}^t) = r$ *has the distance*

$$\mathcal{N}(f) = q^{n-r}(q-1)(q^{r-1} - q^{\frac{r}{2}-1})$$

from the set of affine functions.

Observe that for n odd a nondegenerate quadratic form over $GF(2^d)$ is balanced (obtains each value in F equally many times). Conversely, if $\mathbf{x}^t\mathbf{A}\mathbf{x}$ is balanced and $\mathrm{rank}(\mathbf{A} + \mathbf{A}^t) = n - 1$, then it is nondegenerate.

The special quadratic form that we shall make use of in our construction is

$$x_1x_2 + x_2x_3 + x_3x_4 + \cdots + x_{n-1}x_n + x_nx_1 = \mathbf{x}^t\mathbf{R}\mathbf{x},$$

where $\mathbf{R} : \mathsf{F}^n \to \mathsf{F}^n$ is the linear permutation

$$\mathbf{R} : (x_1, x_2, \ldots, x_n) \mapsto (x_2, x_3, \ldots, x_n, x_1),$$

i.e., the cyclic shift of the coordinates. By using the general substitution algorithm of Lemma 6.29 of [4] it is easy to verify that $\mathbf{x}^t\mathbf{R}\mathbf{x}$ in an odd number n of indeterminates over $Gf(2^d)$ is equivalent to $x_1x_2 + x_3x_4 + \cdots + x_{n-2}x_{n-1} + x_n$.

The main result of [6], which has had a strong impact on the present work, is the observation that

$$Tr(\mathbf{x}^3) = \mathbf{x}^t\mathbf{R}\mathbf{x}, \quad \mathbf{x} \in GF(2^n),$$

with respect to a self-dual normal basis in $GF(2^n)$, for n odd. Indeed, our construction contains the cubing permutation as a special case. By replacing $\mathbf{R}$ by $\mathbf{R}^i$, $i = 1, 2, ..., n-1$, in the construction in §4, we obtain classes of equally highly nonlinear permutations where the permutations $\mathbf{x} \to \mathbf{x}^{2^i+1}$, $i = 1, 2, ..., n-1$, are as special cases. Let us recall that these are exactly the permutations on which the public key cryptosystem C^* proposed in [4] is based.

4. The construction

We combine Theorems 1 and 2 to obtain the following method for constructing permutations with desired distance from linear functions.

THEOREM 3. *Let* $\mathsf{F} = GF(2^d)$ *and* $q = 2^d$. *Then the function* $\mathbf{f} = (f_1, f_2, \ldots, f_n) : \mathsf{F}^n \to \mathsf{F}^n$ *with quadratic coordinate functions* f_k, $k = 1, \ldots, n$, *is a permutation of* F^n *with*

$$\mathcal{N}(\mathbf{f}) = \mathcal{N}(\mathbf{f}^{-1}) \geq q^{n-r}(q-1)(q^{r-1} - q^{\frac{r}{2}-1})$$

if and only if every nontrivial linear combination of the coordinate functions $f_1, f_2, \ldots, f_n$ *is a balanced quadratic form* $\mathbf{x}^t\mathbf{C}\mathbf{x}$ *with* $rank(\mathbf{C}^t + \mathbf{C}) \geq r$.

The condition of the theorem on the coordinate functions can be tested for in low dimensions. In what follows we shall give an analytic construction, which is feasible also in large dimensions.

Let n and d be odd positive integers and $n \geq 3$. Then $GF(2^{nd})$ is an n-dimensional linear space over $\mathsf{F} = GF(2^d)$. Let $e_1, e_2, \ldots, e_n$ be a basis in $\mathsf{F}^n = GF(2^{nd})$ over F. Then the matrix

$$\mathbf{E}(e_1, e_2, \ldots, e_n) = \begin{pmatrix} e_1 & e_2 & \ldots & e_n \\ e_1^2 & e_2^2 & \ldots & e_n^2 \\ e_1^4 & e_2^4 & \ldots & e_n^4 \\ \vdots & \vdots & \ddots & \vdots \\ e_1^{2^{n-1}} & e_2^{2^{n-1}} & \ldots & e_n^{2^{n-1}} \end{pmatrix}$$

is a nonsingular matrix over F (see Corollary 2.38 [4]). Choose $\alpha_1, \alpha_2, \ldots, \alpha_n \in GF(2^{nd})$ such that their cubes $\alpha_1^3, \alpha_2^3, \ldots, \alpha_n^3$ are linearly independent over $GF(2^d)$. This is possible since cubing is a permutation in $GF(2^{nd})$ if nd is odd.

Set

$$\mathbf{E}_k = \mathbf{E}(\alpha_k e_1, \alpha_k e_2, \ldots, \alpha_k e_n) \text{ and } \mathbf{B}_k = \mathbf{E}_k^t \mathbf{R} \mathbf{E}_k,$$

$k = 1, 2, \ldots, n$. Then the ij^{th} entry of $\mathbf{B}_k$ equals

$$Tr_{\mathsf{F}}(\alpha_k^3 e_i e_j^2) \in GF(2^d).$$

Let $c_k \in GF(2^d)$, $k = 1, 2, \ldots, n$ not all equal to 0. Then the ij^{th} entry of $\sum_k c_k \mathbf{B}_k$ is equal to

$$Tr_{\mathsf{F}}(\sum_k c_k \alpha_k^3 e_i e_j^2) = Tr_{\mathsf{F}}(\gamma^3 e_i e_j^2)$$

for some $\gamma \in GF(2^{nd})$, $\gamma \neq 0$. Hence

$$\sum_k c_k \mathbf{B}_k = \mathbf{C}^t \mathbf{R} \mathbf{C}, \tag{2}$$

where $\mathbf{C} = \mathbf{E}(\gamma e_1, \gamma e_2, \ldots, \gamma e_n)$.

Now $\text{rank}(\mathbf{R} + \mathbf{R}^t)$ is equal to the odd number of the indeterminates minus 1 over any field over which the nondegenerate quadratic form $\mathbf{x}^t\mathbf{R}\mathbf{x}$ is considered. Since $\mathbf{B}_k = \mathbf{E}_k^t \mathbf{R} \mathbf{E}_k$, where $\mathbf{E}_k$ is a nonsingular matrix, it then follows that $\text{rank}(\mathbf{B}_k^t + \mathbf{B}) = n - 1$ and the quadratic form $f_k(\mathbf{x}) = \mathbf{x}^t \mathbf{B}_k \mathbf{x}$ is nondegenerate and hence balanced, $k = 1, 2, \ldots, n$. Due to the identity (2) the same holds for every linear combination (over $GF(2^d)$) of $f_1, f_2, \ldots, f_n$. Hence it follows from Theorem 3 that the function $\mathbf{f} = (f_1, f_2, \ldots, f_n)$ is a permutation in $GF(2^{nd}) = GF(2^d)^n$ with nonlinearity

$$\mathcal{N}(\mathbf{f}) = \mathcal{N}(\mathbf{f}^{-1}) = \mathcal{N}(f_k) = q(q-1)(q^{n-2} - q^{\frac{n-1}{2}-1}),$$

where $q = 2^d$.

Acknowledgements. The most part of this paper was written while the author was visiting Prof. J. L. Massey at ETH Zürich. His kind hospitality and interest to my work is gratefully acknowledged. I would also like to thank Prof. Z. Wan and Dr. S. Hellberg for pointing out errors in an earlier version of the paper.

References

1. C. Carlet, *Partially-bent functions*, Codes, Designs and Cryptography (to appear).
2. X. Lai, *Linear structures of functions over prime fields*, Unpublished preprint (1990).
3. R. Lidl and H. Niederreiter, "Finite fields.," Encyclopedia of Mathematics and its applications, Vol. 20. Addison-Wesley, Reading, Massachusetts, 1983.
4. T. Matsumoto and H. Imai, *Public quadratic polynomial-tuples for efficient signature-verification and message-encryption*, Advances in Cryptology Eurocrypt '88. Lecture Notes in Computer Science, Springer-Verlag, 1989.
5. K. Nyberg, *Constructions of bent functions and difference sets*, Advances in Cryptology – Proceedings of Eurocrypt '90. Lecture Notes in Computer Science **473**, Springer-Verlag, 1991.
6. J. Pieprzyk, *On bent permutations*, Technical Report CS91/11; The University of New South Wales, Department of Computer Science. Presented at the International Conference on Finite Fields, Coding Theory and Advances in Communications and Computing, Las Vegas, 1991.
7. B. Preneel et al., *Cryptographic properties of quadratic Boolean functions*, International Conference on Finite Fields, Coding Theory and advances in Communications and Computing, Las Vegas, 1991; *Boolean functions satisfying higher order propagation criteria*, Advances in Cryptology - Eurocrypt '91. Lecture Notes in Computer Science **547**, Springer-Verlag, 1991.