AAECC **8**, 363–370 (1997)

AAECC
Applicable Algebra in Engineering, Communication and Computing

Some Power Mappings with Low Differential Uniformity*

Tor Helleseth, Daniel Sandberg

Department of Informatics, University of Bergen, Høyteknologisenteret, N-5020 Bergen, Norway

Dedicated to Aimo Tietäväinen on the occasion of his 60th birthday

Received: November 4, 1996; revised version: February 14, 1997

Abstract. Differentially uniform power mappings of the form $f(x) = x^d$ over $GF(p^n)$ are considered. We construct an infinite family of 2-uniform mappings in the binary case. In the nonbinary case we give two large families of k-uniform mappings with low values of k. We also show how to construct families of sequences from differentially 1-uniform power mappings, which have parameters as good as the best presently known comparable families of sequences.

Keywords: Differential cryptanalysis, Planar permutation polynomials, Sequences with good correlations.

1 Introduction

Let $f(x)$ be a mapping $f: GF(p^n) \to GF(p^n)$. Let $N(a, b)$ denote the number of solutions $x \in GF(p^n)$ of $f(x + a) - f(x) = b$ where $a, b \in GF(p^n)$ and let

$$\Delta_f = max\{N(a, b) \mid a, b \in GF(p^n),\ a \neq 0\}.$$

Nyberg [8] defined a mapping f to be differentially k-uniform if $\Delta_f = k$. This concept is of interest in cryptography since differential and linear cryptanalysis exploit weaknesses of the uniformity of the functions which are used in DES and in many other block ciphers.

The purpose of this paper is to give some results on the differential uniformity of functions of the form $f(x) = x^d$ over $GF(p^n)$ where p is a prime. For practical applications one would like functions for which Δ_f is small. In the binary case the solutions come in pairs and therefore $\Delta_f = 2$ is the smallest possible value. Such a function is called almost perfect nonlinear (APN).

* This work was supported in part by The Norwegian Research Council under Grant Numbers 107542/410 and 107623/420
Correspondence to: T. Helleseth

It is known that in the binary case the function is APN for $d = 2^k + 1$ when $n/gcd(k, n)$ is odd and for $d = 2^n - 2$ when n is odd (Nyberg [8], Beth and Ding [1]). Cusick [4] showed that if two m-sequences of period $2^n - 1$ differ by a decimation of d and have a three level crosscorrelation function with values -1, $-1 \pm 2^{\frac{n+1}{2}}$ then the corresponding function $f(x) = x^d$ is also APN. Chabaud and Vaudenay [2] give some similar connections between differential and linear cryptanalysis. Beth and Ding [1] conjectured that $f(x) = x^d$ for $d = 2^m - 1$, $2 \leqq m \leqq n - 1$, is APN whenever n and $2^n - 1$ are primes. Numerical results show that this conjecture does not hold in general. In Theorem 1 we will, however, construct an infinite family of APN mappings of this form.

In the nonbinary case we give two examples of infinite families of k-uniform mappings with small k. It is interesting to note that a special case of one of the families for $p = 3$ gives a 1-uniform mapping which turns out to be a counterexample to a conjecture due to Dembowski and Ostrom [5] about planar permutation polynomials (see also Mullen [7]). This counterexample has also been discovered by Coulter and Matthews [3] but proved in a different way. We finally show how to construct families of sequences with good correlation properties from differentially uniform 1-mappings of the form $f(x) = x^d$. These sequences have parameters as good as the best presently known comparable sequence families.

2 Mappings with Low Differential Uniformity

In this section we construct three infinite families of mappings of the form $f(x) = x^d$ with low differential uniformity. The first is a family of APN mappings.

Theorem 1 *Let $n = 2m - 1$, $d = 2^m - 1$, $m \geqq 2$ and let $f(x) = x^d$ be a mapping over $GF(p^n)$, then $\Delta_f = 2$.*

Proof. Since $N(a, b) = N(1, \frac{b}{a^d})$ when $a \neq 0$, it is sufficient for any b to find the maximum number of solutions of

$$(x + 1)^{2^m - 1} + x^{2^m - 1} = b. \tag{1}$$

We multiply both sides by $x(x + 1)$ and obtain

$$(x + 1)^{2^m} x + x^{2^m}(x + 1) = bx(x + 1)$$

or

$$x^{2^m} = bx^2 + (b + 1)x. \tag{2}$$

Raising both sides to the 2^{m-1} power gives

$$(x^{2^m})^{2^{m-1}} = x^{2^n} = x = b^{2^{m-1}} x^{2^m} + (b^{2^{m-1}} + 1)x^{2^{m-1}}$$

and thus

$$b^{2^{m-1}} x^{2^m} + (b^{2^{m-1}} + 1)x^{2^{m-1}} + x = 0.$$

We now use (2) to obtain

$$b^{2^{m-1}+1} x^2 + (b^{2^{m-1}+1} + b^{2^{m-1}} + 1)x + (b^{2^{m-1}} + 1)x^{2^{m-1}} = 0.$$

Squaring and applying (2) again, we obtain

$$b^{2^m+2} x^4 + (b^{2^m+2} + b^{2^m+1} + b^{2^m} + b + 1)x^2 + (b^{2^m+1} + b^{2^m} + b + 1)x = 0. \tag{3}$$

This equation has at most 4 solutions, two of which are $x = 0$ and $x = 1$. If we substitute $x = 0$ and $x = 1$ into (1), we get that $b = 1$. Hence, $x = 0$ and $x = 1$ cannot be solutions of (1) except when $b = 1$, and therefore (1) has at most 2 solutions if $b \neq 1$. If $b = 1$, then it follows from (3) that (1) has the two solutions $x = 0$ and $x = 1$. We therefore conclude that the maximum number of solutions of (1) for any $b \in GF(2^n)$ is 2, i.e., $\Delta_f = 2$. □

In the following two theorems we will present a family of nonbinary functions with low differential uniformity, based upon properties of the quadratic character. Let QR denote the set of quadratic residues of $GF(p^n)$ and let QNR denote the set of quadratic non-residues. We define the quadratic character of $GF(p^n)$ by

$$\chi(\xi) = \begin{cases} 0 & \text{if } \xi \text{ is } 0 \\ 1 & \text{if } \xi \text{ is a QR} \\ -1 & \text{if } \xi \text{ is a QNR.} \end{cases}$$

Theorem 2 *Let p be a prime, $p^n \equiv 3 \pmod 4$, $d = \frac{p^n - 1}{2} - 1$ and let $f(x) = x^d$ be a mapping over $GF(p^n)$. Then for $p^n > 7$,*

$$\Delta_f = \begin{cases} 1 & \text{if } p^n = 27 \\ 2 & \text{if } \chi(5) = -1 \text{ (i.e., } p \equiv 3, 7 \pmod{20}) \\ 3 & \text{if } \chi(5) = 1 \text{ (i.e., } p \equiv 11, 19 \pmod{20}). \end{cases}$$

Proof. We consider the equation

$$(x+1)^d - x^d = b.$$

Since d is even, $x = 0$ and $x = -1$ contribute to $b = 1$ and $b = -1$ respectively. We next assume that $x \neq 0$ and $x \neq -1$. From $\chi(x) = x^{\frac{p^n-1}{2}}$, we obtain

$$\chi(x+1)\frac{1}{x+1} - \chi(x)\frac{1}{x} = b,$$

which gives

$$bx^2 + (b - \chi(x+1) + \chi(x))x + \chi(x) = 0.$$

Depending on the values of $(\chi(x), \chi(x+1))$ we have four possible equations. Solving the equations and computing $x_i(x_i + 1)$, $i = 1, 2$, and $x_1 x_2$ for the roots of the second degree equations one verifies that the following holds, where $b' = \frac{1}{b}$.

	$\chi(x)$	$\chi(x+1)$	Equation	x	$x+1$	x_1x_2	$x(x+1)$
I	1	1	$bx^2 + bx + 1 = 0$	$\frac{-1 \pm \sqrt{1-4b'}}{2}$	$\frac{1 \pm \sqrt{1-4b'}}{2}$	$\frac{1}{b}$	$-\frac{1}{b}$
II	1	−1	$bx^2 + (b+2)x + 1 = 0$	$\frac{-1-2b' \pm \sqrt{1+4b'^2}}{2}$	$\frac{1-2b' \pm \sqrt{1+4b'^2}}{2}$	$\frac{1}{b}$	–
III	−1	1	$bx^2 + (b-2)x - 1 = 0$	$\frac{-1+2b' \pm \sqrt{1+4b'^2}}{2}$	$\frac{1+2b' \pm \sqrt{1+4b'^2}}{2}$	$-\frac{1}{b}$	–
IV	−1	−1	$bx^2 + bx - 1 = 0$	$\frac{-1 \pm \sqrt{1+4b'}}{2}$	$\frac{1 \pm \sqrt{1+4b'}}{2}$	$-\frac{1}{b}$	$\frac{1}{b}$

It is important to note that $\chi(-1) = -1$ since $p^n \equiv 3 \pmod 4$. In order for I to have a solution x it is necessary that $\chi(x(x+1)) = \chi(-\frac{1}{b}) = 1$ i.e., $\chi(b) = -1$. Observe that I has at most one solution since $\chi(x_1x_2) = \chi(\frac{1}{b}) = -1$. Similarly, IV can only have a solution when $\chi(b) = 1$ and in this case IV has at most one solution.

Therefore for any $b \in GF(p^n)\backslash\{0\}$, I and IV can not give solutions simultaneously, and hence they contribute at most one solution altogether.

Suppose x_1 and x_2 are the two solutions of II (resp. III), then direct calculations give

$$x_1(x_1+1)x_2(x_2+1) = -b'^2$$

and therefore

$$\chi(x_1(x_1+1)x_2(x_2+1)) = -1$$

which implies that II (resp. III) has at most one solution each.

Let x_1 be a solution of II and y_1 a solution of III. Then

$$\chi(x_1) = 1, \quad \chi(x_1+1) = -1 \quad \text{and} \quad \chi(y_1) = -1, \quad \chi(y_1+1) = 1.$$

Let x_2 and y_2 be the other solution of II and III respectively, when we discard the condition on $\chi(x_2)$, $\chi(x_2+1)$, $\chi(y_2)$ and $\chi(y_2+1)$. Note that $x_1 = -(y_2+1)$ and $x_2 = -(y_1+1)$. Since $x_1x_2 = \frac{1}{b}$ and $\chi(x_1) = 1$ we have $\chi(b) = \chi(x_2) = \chi(-(y_1+1)) = -1$. On the other hand, since $y_1y_2 = -\frac{1}{b}$ and $\chi(y_1) = -1$ we have $\chi(b) = \chi(y_2) = \chi(-(x_1+1)) = 1$, which is a contradiction. Hence, for any $b \in GF(p^n)\backslash\{0\}$, II and III can not give solutions simultaneously and therefore they contribute at most one solution altogether.

In the case $b = 0$ the number of solutions in $GF(p^n)$ of $(x+1)^d = x^d$ is $gcd(d, p^n - 1) - 1 = 1$. Since $x = 0$ and $x = -1$ contribute to $b = 1$ and $b = -1$ respectively, we have to check whether the four equations I–IV contribute 2 solutions to the cases $b = 1$ or $b = -1$. It is straightforward to verify that these cases give exactly 2 solutions when $\chi(5) = 1$ and 0 solutions otherwise.

It follows that $\Delta_f = 3$ when $\chi(5) = 1$ and $\Delta_f \leqq 2$ otherwise. To show that $\Delta_f = 2$ when $\chi(5) = -1$ it is sufficient to find an element $b' \in GF(p^n)\backslash\{0\}$ such that $\chi(b') = 1$, $\chi(1+4b') = 1$ and $\chi(1+4b'^2) = 1$ since this will lead to a solution of IV and one solution of either II or III. Such an element can be found by standard methods (character sums and computer search) when $p^n > 7$ except for $p^n = 27$. □

Theorem 3 *Let p be an odd prime, $d = \frac{p^n-1}{2} + 2$ and let $f(x) = x^d$, then*

$$\Delta_f \leqq \begin{cases} 1 & \text{if } p = 3 \text{ and } n \text{ even} \\ 3 & \text{if } p \neq 3 \text{ and } p^n \equiv 1 \pmod 4 \\ 4 & \text{otherwise.} \end{cases}$$

Proof. Since $d = \frac{p^n-1}{2} + 2$, we have

$$(x+1)^{\frac{p^n-1}{2}+2} - x^{\frac{p^n-1}{2}+2} = b.$$

We assume that $x \neq 0$ and $x \neq -1$ since they contribute to $b = 1$ and $b = (-1)^{d+1}$ respectively. Further, since $\chi(x) = x^{\frac{p^n-1}{2}}$, we obtain

$$\chi(x+1)(x^2+2x+1) - \chi(x)x^2 = b$$

and therefore

$$(\chi(x+1) - \chi(x))x^2 + 2\chi(x+1)x + \chi(x+1) - b = 0.$$

Depending on the values of $(\chi(x), \chi(x+1))$ we have four possible equations. Solving the equations and computing $x_1(x_1+1)(= x_2(x_2+1))$ and x_1x_2 for the roots of the second degree equations one verifies that the following holds:

	$\chi(x)$	$\chi(x+1)$	Equation	x	$x+1$	$x(x+1)$	x_1x_2
I	1	1	$2x+1-b=0$	$\frac{-1+b}{2}$	$\frac{1+b}{2}$	–	–
II	1	-1	$-2x^2-2x-1-b=0$	$\frac{-1\pm\sqrt{-1-2b}}{2}$	$\frac{1\pm\sqrt{-1-2b}}{2}$	$\frac{-1-b}{2}$	$\frac{1+b}{2}$
III	-1	1	$2x^2+2x+1-b=0$	$\frac{-1\pm\sqrt{-1+2b}}{2}$	$\frac{1\pm\sqrt{-1+2b}}{2}$	$\frac{-1+b}{2}$	$\frac{1-b}{2}$
IV	-1	-1	$-2x-1-b=0$	$\frac{-1-b}{2}$	$\frac{1-b}{2}$	–	–

It is important to observe that in order for II (resp. III) to have solutions it is necessary that $\chi(\frac{-1-b}{2})=\chi(x(x+1))=-1$ and $\chi(-1-2b)\neq -1$ (resp. $\chi(\frac{-1+b}{2})=-1$ and $\chi(-1+2b)\neq -1$). Further, if a solution of II (resp. III) exists then the solution is unique whenever $\chi(\frac{1+b}{2})=\chi(x_1x_2)=-1$ (resp. $\chi(\frac{1-b}{2})=\chi(x_1x_2)=-1$).

We first assume that $-1\in QR$, i.e., $\chi(-1)=1$. We consider four possible cases depending on the values of the elements $\chi(\frac{-1+b}{2})$ and $\chi(\frac{1+b}{2})$.

Case 1. $(\chi(\frac{-1+b}{2})=1, \chi(\frac{1+b}{2})=1)$. In this case there is clearly a solution of I while IV has no solution since $\chi(\frac{-1-b}{2})=\chi(\frac{1+b}{2})=1$. There is no solution of II (resp. III) since a solution x would lead to $-1=\chi(x(x+1))=\chi(\frac{-1-b}{2})=1$ (resp. $-1=\chi(x(x+1))=\chi(\frac{-1+b}{2})=1$) which is impossible.

Case 2. $(\chi(\frac{-1+b}{2})=1, \chi(\frac{1+b}{2})=-1)$. Since $\chi(\frac{1+b}{2})=-1$, there is no solution of I. Further, $\chi(\frac{-1+b}{2})=1$ and $\chi(\frac{1-b}{2})=1$ implies that there are no solutions of III and IV respectively. Since $\chi(\frac{1+b}{2})=-1$ there is at most one solution of II.

Case 3. $(\chi(\frac{-1+b}{2})=-1, \chi(\frac{1+b}{2})=1)$. It follows as in the previous case that there are no solutions of I, II and IV and that III contains at most one solution.

Case 4. $(\chi(\frac{-1+b}{2})=-1, \chi(\frac{1+b}{2})=-1)$. In this case there is no solution of I while IV has a solution. Since $\chi(\frac{-1-b}{2})=\chi(\frac{-1+b}{2})=-1$, there is exactly one solution of II when $\chi(-1-2b)\neq -1$ and exactly one solution of III when $\chi(-1+2b)\neq -1$ and no solutions otherwise. Note that in the case $p=3$ we have $-1-2b=\frac{1-b}{2}$ and $-1+2b=\frac{1+b}{2}$. Hence, when $p=3$, this case gives no solutions of II and III.

Hence, if $-1\in QR$, i.e., $p^n\equiv 1 \pmod 4$, we have showed the following:

Case	$\chi(\frac{-1+b}{2})$	$\chi(\frac{1+b}{2})$	I	II	III	IV	$p\neq 3$	$p=3$
1	1	1	1	0	0	0	1	1
2	1	-1	0	$\leqq 1$	0	0	$\leqq 1$	1
3	-1	1	0	0	$\leqq 1$	0	$\leqq 1$	1
4	-1	-1	0	$\leqq 1$	$\leqq 1$	1	$1\leqq \# \leqq 3$	1

We next consider the case $-1\in QNR$, i.e., $\chi(-1)=-1$.

Case 1. $(\chi(\frac{-1+b}{2})=1, \chi(\frac{1+b}{2})=1)$. In this case I has a solution. Since $\chi(\frac{-1-b}{2})=\chi(\frac{1-b}{2})=-1$ also IV has a solution. There is no solution of III since $\chi(\frac{-1+b}{2})=1$. Further, II has at most two solutions.

Case 2. $(\chi(\frac{-1+b}{2})=1, \chi(\frac{1+b}{2})=-1)$. Since $\chi(\frac{1+b}{2})=-1$, $\chi(\frac{-1-b}{2})=1$, $\chi(\frac{-1+b}{2})=1$ and $\chi(\frac{-1-b}{2})=1$, there are no solutions of I, II, III and IV respectively.

Case 3. $(\chi(\frac{-1+b}{2})=-1, \chi(\frac{1+b}{2})=1)$. Since $\chi(\frac{-1+b}{2})=-1$ and $\chi(\frac{1-b}{2})=1$, there are no solutions of I and IV respectively, while II and III contain at most two solutions each.

Case 4. $(\chi(\frac{-1+b}{2})=-1, \chi(\frac{1+b}{2})=-1)$. Since $\chi(\frac{-1+b}{2})=-1$, $\chi(\frac{-1-b}{2})=1$, and $\chi(\frac{1-b}{2})=1$, it follows that there are no solutions of I, II and IV respectively, while III has at most two solutions.

Thus if $-1 \in QNR$, i.e., $p^n \equiv 3 \pmod 4$, we have shown the results listed in the table below:

Case	$\chi(\frac{-1+b}{2})$	$\chi(\frac{1+b}{2})$	I	II	III	IV	
1	1	1	1	$\leqq 2$	0	1	$2 \leqq \# \leqq 4$
2	1	-1	0	0	0	0	0
3	-1	1	0	$\leqq 2$	$\leqq 2$	0	$\leqq 4$
4	-1	-1	0	0	$\leqq 2$	0	$\leqq 2$

It is also straightforward to verify that the cases $b=1$ and $b=-1$ never contribute more solutions than the cases I–IV. In conclusion, we have therefore shown that $\Delta_f = 1$ when $p=3$ and that $\Delta_f \leqq 3$ when $p \neq 3$ and $p^n \equiv 1 \pmod 4$ and that $\Delta_f \leqq 4$, otherwise. □

It is also straightforward to decide when equality holds. For instance, to show that $\Delta_f = 3$ in the case $p \neq 3$ and $p^n \equiv 1 \pmod 4$ it is sufficient to find an element $b \in GF(p^n)$ such that $\chi(\frac{-1-b}{2})=\chi(\frac{1-b}{2})=-1$, $\chi(-1-2b)=1$ and $\chi(-1+2b)=1$. In particular, if $p^n \equiv 5 \pmod 8$, $b=0$ has this property since $2 \in QNR$. In the case $p^n \equiv 1 \pmod 8$, standard methods i.e., exponential sums for the quadratic character can be applied to find such an element for p^n sufficiently large and then a computer search can settle small values of p^n. It turns out that $\Delta_f = 3$ whenever $p^n \neq 17$. Similarly, we may settle when $\Delta_f = 4$ in the remaining case.

It is of interest to observe that in the special case $p=3$ and n even in Theorem 3, the function is differentially 1-uniform. In the literature this is called a planar permutation polynomial. It has been conjectured [5] that all planar permutation polynomials are of the form $f(x)=\sum_{i,j} a_{i,j} x^{p^i+p^j}$. The case $p=3$ and n even is a counterexample to this conjecture, since $f(x)=x^d$ is not of this form when $d=\frac{3^n-1}{2}+2$. This counterexample and several others have also been proved by Coulter and Matthews [3] by a different method using Chebyshev polynomials. Their result states that $f(x)=x^d$, where $d=\frac{3^s+1}{2}$, is a planar permutation polynomial when $gcd(s,n)=1$ and s is odd.

3 Sequences with Good Correlations

Based on any differentially 1-uniform mapping $f(x) = x^d$ one can construct a family of sequences with good correlation properties. Let ω be a complex pth root of unity and let $Tr(x) = \sum_{i=0}^{n-1} x^{p^i}$ denote the trace mapping. Then for any differentially 1-uniform mapping $f(x) = x^d$,

$$\sum_{x \in GF(p^n)} \omega^{f(x+a)-f(x)} = \sum_{b \in GF(p^n)} \omega^b = 0$$

for all $a \in GF(p^n) \backslash \{0\}$. Let $c \neq 0$ and

$$S(c, \lambda) = \sum_{x \in GF(p^n)} \omega^{Tr(cf(x)+\lambda x)}$$

then

$$\begin{aligned} |S(c,\lambda)|^2 &= \sum_{x,y \in GF(p^n)} \omega^{Tr(c(f(x)-f(y))+\lambda(x-y))} \\ &= \sum_{y,z \in GF(p^n)} \omega^{Tr(c(f(y+z)-f(y))+\lambda z)} \\ &= p^n + \sum_{z \in GF(p^n)\backslash\{0\}} \omega^{Tr(\lambda z)} \sum_{b \in GF(p^n)} \omega^{Tr(cb)} \\ &= p^n. \end{aligned}$$

It follows that

$$|S(c,\lambda)| = \left| \sum_{x \in GF(p^n)} \omega^{Tr(cf(x)+\lambda x)} \right| = \sqrt{p^n}$$

for all $\lambda \in GF(p^n)$ whenever $c \neq 0$.

Let α be a primitive $(p^n - 1)$th root of unity in $GF(p^n)$. Let $\{s_c(t)\}$ be the sequence of period $p^n - 1$ defined by

$$s_c(t) = Tr(c\alpha^{dt} + \alpha^t).$$

Then

$$\mathscr{F} = \{\{s_c(t)\} \mid c \in GF(p^n)\}$$

is a family of p^n cyclically distinct sequences with maximum correlation bounded by $1 + \sqrt{p^n}$ in magnitude. This follows since,

$$\begin{aligned} \theta(\tau) &= \sum_{t=0}^{p^n-2} \omega^{s_{c_1}(t+\tau)-s_{c_2}(t)} \\ &= \sum_{t=0}^{p^n-2} \omega^{Tr((c_1\alpha^{d\tau}-c_2)\alpha^{dt}+(\alpha^\tau-1)\alpha^t)} \\ &= -1 + \sum_{x \in GF(p^n)} \omega^{Tr(cx^{dt}+\lambda x)}, \end{aligned}$$

where $c = c_1\alpha^{d\tau} - c_2$ and $\lambda = \alpha^{\tau} - 1$. Hence, $|\theta(\tau)| \leqq 1 + \sqrt{p^n}$, except when $c_1 = c_2$ and $\tau = 0$. Thus, family $\mathscr{F}$ has the same parameters as the best presently known families of sequences found in Kumar and Moreno [6]. It is perhaps interesting to note that these sequences correspond to $d = 2$ or $d = p^k + 1$ where $n/gcd(n, k)$ is odd. Observe that $f(x) = x^2$ and $f(x) = x^{p^k+1}$ are also planar permutation polynomials.

4 Conclusions

We have found some binary APN mappings of the form $f(x) = x^d$ as well as families of nonbinary mappings with low differential uniformity. We have given examples of sequences with good correlation properties based upon differentially 1-uniform mappings of the form $f(x) = x^d$. Similar techniques lead to several other families of mappings with low differential uniformity that will be the topic for a future paper.

Acknowledgements. The authors thank P. V. Kumar for useful discussions during the preparation of this paper.

References

1. Beth, T., Ding, C.: On almost perfect nonlinear permutations, In: Helleseth, T. (ed.), Advances in cryptology – EUROCRYPT'93. Lecture Notes in Computer Science, Vol. 765, pp. 65–76. Berlin Heidelberg New York: Springer 1994
2. Chabaud, F., Vaudenay, S.: Links between differential and linear cryptanalysis. In: DeSantis, A. (ed.) Advances in cryptology – EUROCRYPT'94. Lecture Notes in Computer Science, Vol. 950, pp. 356–365. Berlin Heidelberg New York: Springer 1995
3. Coulter, R. S., Matthews, R. W.: Planar functions and planes of the Lenz-Barlotti class II. Designs, codes and cryptography **10**, 167–184 (1997)
4. Cusick, T. W.: Constructing differentially uniform permutations via cross-correlation functions. Unpublished manuscript
5. Dembowski, P., Ostrom, T. G.: Planes of order n with collineation groups of order n^2. Math. Z. **103**, 239–258 (1968)
6. Kumar, P., Moreno, O.: Prime-phase sequences with periodic correlation properties better than binary sequences, IEEE Trans. Inform. Theory **IT-37**, 603–616 (1991)
7. Mullen, G. L.: Permutation polynomials over finite fields, In: Mullen, G. L., Shiue, P. (eds.) Finite fields, coding theory, and advances in communications and computing. Lecture Notes in Pure and Applied Mathematics, Vol. 141, pp. 131–151. New York Basel Hong Kong: Dekker 1993
8. Nyberg, K.: Differentially uniform mappings for cryptography, In: T. Helleseth (ed.) Advances in cryptology – EUROCRYPT'93. Lecture Notes in Computer Science, Vol. 765, pp. 55–64. Berlin Heidelberg New York: Springer 1994
9. Nyberg, K., Knudsen, L. R.: Provable security against a differential attack. J. Cryptol. **8**, 27–37 (1995)