Differential Spectrum of Non-binary Kasami Power Functions and Related Topics

Tor Helleseth

Selmer Center
Department of Informatics
University of Bergen
Bergen, Norway

The Kasami part is joint work with H. Yan, Z. Zhou, J. Weng, J. Wen and Q. Wang

June 17, 2019

Outline

1. Introduction

2. Sequences and APN/PN functions

3. Differential spectrum of the Kasami case

4. Functions with low uniformity from the 1990s

5. PN power functions and optimal sequences

Introduction

Delta uniform functions

Let $f\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ and $N_f(a,b) = \#\{x \in \mathbb{F}_{p^n} \mid f(x+a) - f(x) = b\}$.

Definition

The differential uniformity of f is defined as

$$\delta_f = \max_{a \neq 0, b \in \mathbb{F}_{p^n}} N_f(a,b)$$

Definition

A function $f\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is δ - uniform if

$$\delta_f = \delta$$

- If $\delta_f = 1$ then f is called perfect nonlinear (PN)
- If $\delta_f = 2$ then f is called almost perfect nonlinear (APN)
- APN functions have optimal resistance against the differential attack

Early history of differential uniform functions

The motivation of δ-uniformity comes from differential (and linear) cryptanalysis. Early influential papers motivating research on differential uniformity in cryptography are:

Early history

- Eurocrypt'91 - K. Nyberg, Perfect Nonlinear S-boxes.
- Eurocrypt'92 - K. Nyberg, On the Construction of Highly Nonlinear Permutations.
- Crypto'92 - K. Nyberg and L. R. Knudsen, Provable security against differential cryptanalysis,. (Section 3: Almost Perfect Nonlinear Permutations).
- Eurocrypt'93 - K. Nyberg, Differential Uniform Mappings for Cryptography.
- Eurocrypt'93 - T. Beth and C. Ding, On Almost Perfect Nonlinear Permutations.
- FFA 1995 - R. Coulter and R. Matthews found the polynomial x^d, $d = (3^k + 1)/2$, k odd and $\gcd(n, k) = 1$ i.e., $f(x) = x^d$ is PN.

Sequences and APN functions

My own interest in PN and APN functions

My interest in the problem

- Studied m-sequences $\{s_t\}$ and $\{s_{dt}\}$ with 3-valued crosscorrelation.
- Apparent similarities between values d giving 3-valued correlations and $f(x) = x^d$ giving APN functions.
- In 1995 my masterstudent Daniel Sandberg performed a computer search of the δ-uniformity of power functions for many values of d, n and p.
- His master thesis (1997) solved several cases and provided open cases in the 1990s. This inspired other researchers (Hans Dobbertin, Alexander Pott etc.) to work on some of the open problems (and some problems are still open).

Crosscorrelation of m-sequences

Crosscorrelation of binary m-sequences

- Let $\{s_t\}$ be a binary m-sequence of period $2^n - 1$.
- Let $\{s_{dt}\}$ be a decimated m-sequence i.e., $gcd(d, 2^n - 1) = 1$.
- The crosscorrelation between the two m-sequences is

$$C_d(\tau) = \sum_{t=0}^{2^n-2} (-1)^{s_{dt} - s_{t+\tau}} = -1 + \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(x^d + ax)}$$

where α is a primitive element in $\mathbb{F}_{2^n}$ and $a = \alpha^\tau$.

- In the case $d = 2^i \pmod{2^n - 1}$ then $C_d(\tau)$ is two-valued (autocorrelation).
- In all other cases at least three values occur.

Gold and Kasam: Three-Valued Crosscorrelation

Theorem (Gold(1968) , Kasami (1968) , Welch(1960s))

Let $d = 2^k + 1$ or $d = 2^{2k} - 2^k + 1$ and $e = gcd(n,k)$ where $\frac{n}{gcd(n,k)}$ is odd. Then $C_d(\tau)$ has three-valued crosscorrelation with distribution:

$$\begin{array}{cccc} -1 + 2^{\frac{n+e}{2}} & \textit{occurs} & 2^{n-e-1} - 2^{\frac{n-e-2}{2}} & \textit{times} \\ -1 & \textit{occurs} & 2^n - 2^{n-e} - 1 & \textit{times} \\ -1 - 2^{\frac{n+e}{2}} & \textit{occurs} & 2^{n-e-1} + 2^{\frac{n-e-2}{2}} & \textit{times} \end{array}$$

In particular when n is odd and $gcd(k,n) = 1$ then the values of

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(x^d + ax)}$$

belong to $\{0, \pm 2^{\frac{n+1}{2}}\}$.

The function $f(x) = x^d$ s called almost bent (AB).

Three-valued crosscorrelation of binary m-sequences

The crosscorrelation $C_d(\tau)$ is known to be three-valued in the cases:

- (Gold 1968): $d = 2^k + 1$, $\frac{n}{gcd(n,k)}$ odd.
- (Kasami 1968), (Welch 1960's): $d = 2^{2k} - 2^k + 1$, $\frac{n}{gcd(n,k)}$ odd.
- Welch's conjecture: (Canteaut, Charpin, Dobbertin (2000)) $d = 2^{\frac{n-1}{2}} + 3$, n odd.
- Niho's conjecture: (Hollmann and Xiang (2001), Dobbertin (1999))

$$\begin{aligned} d &= 2^{\frac{n-1}{2}} + 2^{\frac{n-1}{4}} - 1 \text{ when } n = 1 \pmod 4 \\ &= 2^{\frac{n-1}{2}} + 2^{\frac{3n-1}{4}} - 1 \text{ when } n = 3 \pmod 4. \end{aligned}$$

- Cusick and Dobbertin (1996)

$$\begin{aligned} d &= 2^{\frac{n}{2}} + 2^{\frac{n+2}{2}} + 1 \text{ when } n = 2 \pmod 4 \\ &= 2^{\frac{n+2}{2}} + 3 \qquad \text{ when } n = 2 \pmod 4. \end{aligned}$$

Three-valued crosscorrelation of non-binary m-sequences

Known 3-valued Correlation Function $C_d(\tau)$ over $\mathbb{F}_{p^n}$

No.	d-Decimation	Condition	Remarks
1	$(p^{2k}+1)/2$	$n/\gcd(n,k)$ odd	Trachtenberg, 1970
2	$p^{2k}-p^k+1$	$n/\gcd(n,k)$ odd	Trachtenberg, 1970
3	$2\cdot 3^{(n-1)/2}+1$	n odd	Dobbertin et al., 2001
4	$2\cdot 3^{(n-1)/4}+1$	$n \equiv 1 \pmod 4$	Katz and Langevin 2013
5	$2\cdot 3^{(3n-1)/4}+1$	$n \equiv 3 \pmod 4$	Katz and Langevin 2013

Remarks: (1) Nos. 1 and 2 are due to Helleseth for even n; (2) The 3-valued correlation function in No. 4 and No. 5 was conjectured by Dobbertin et al. in 2001.

Open Problems

- Show that the table contains all decimations with 3-valued correlation function for $p > 3$.

APN Power Functions

Table 1a. Known APN power functions x^d on $\mathbb{F}_{2^n}$

Functions	Exponents d	Conditions
Gold	$2^i + 1$	$\gcd(i, n) = 1$
Kasami	$2^{2i} - 2^i + 1$	$\gcd(i, n) = 1$
Welch	$2^t + 3$	$n = 2t + 1$
Niho	$2^t + 2^{\frac{t}{2}} - 1,$ t even $2^t + 2^{\frac{3t+1}{2}} - 1,$ t odd	$n = 2t + 1$
Inverse	$2^{2t} - 1$	$n = 2t + 1$
Dobbertin	$2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$	$n = 5i$

The Walsh Transform

The nonlinearity $NL(F)$ of an (n, m) function F can be expressed by means of the Walsh transform. The Walsh transform of F at $(\alpha, \beta) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ is defined by

$$W_F(\alpha, \beta) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^m(\beta F(x)) + Tr_1^n(\alpha x)}$$

and the Walsh spectrum of F is the set

$$\{W_F(\alpha, \beta) : \alpha \in \mathbb{F}_{2^n}, \beta \in \mathbb{F}_{2^m}^*\}.$$

Then

$$NL(F) = 2^{n-1} - \frac{1}{2} \max_{\alpha \in \mathbb{F}_{2^n}, \beta \in \mathbb{F}_{2^m}^*} |W_F(\alpha, \beta)|.$$

The Walsh spectrum of AB functions consists of three values $0, \pm 2^{\frac{n+1}{2}}$. The Walsh spectrum of a bent function is $\{\pm 2^{\frac{n}{2}}\}$.

AB Power Functions

Table 1b. Known AB power functions x^d on $\mathbb{F}_{2^n}$

Functions	Exponents d	Conditions
Gold	$2^i + 1$	$\gcd(i, n) = 1$
Kasami	$2^{2i} - 2^i + 1$	$\gcd(i, n) = 1$
Welch	$2^t + 3$	$n = 2t + 1$
Niho	$2^t + 2^{\frac{t}{2}} - 1$, t even $2^t + 2^{\frac{3t+1}{2}} - 1$, t odd	$n = 2t + 1$

Connections between (APN) and (AB) Functions

Theorem (Chabaud and Vaudenay (1994))

Any AB function is APN.

A short proof for this fact for power functions is:

Proof.

Let $\theta(a,b) = \sum_{a,b\in\mathbb{F}_{2^n}} (-1)^{Tr(bx^d+ax)}$. Then

$$\sum_{a,b\in\mathbb{F}_{2^n}} (\theta(a,b))^4 = 2^{2n} \sum_{u,v\in\mathbb{F}_{2^n}} N(u,v)^2$$

where $N(u,v)$ is the number of solutions of $f(x+u)+f(x)=v$ □

Using the three-valued crosscorrelation distribution for AB functions gives a relation

$$\sum_{v\in\mathbb{F}_{2^n}} N(1,v)^2 = 2^{n+1} \text{ and } \sum_{v\in\mathbb{F}_{2^n}} N(1,v) = 2^n$$

it follows that x^d is APN since $N(1,v)=0$ or $N(1,v)\geq 2$.

Differential Spectrum of Power Functions

Differential spectrum of a power function

Let $f(x) = x^d$ be a power function. Then $N(a, b)$ is the number of solutions of

$$(x + a)^d - x^d = b \text{ for } x \in \mathbb{F}_{p^n}$$

or

$$(\frac{x}{a} + 1)^d - \frac{x}{a^d} = \frac{b}{a^d} \text{ for } x \in \mathbb{F}_{p^n}$$

In particular, $N(a, b) = N(1, b/a^d)$

Definition

Let $w_i = |\{b \in \mathbb{F}_{p^n} | N(1, b) = i\}|$.
The differential spectrum is defined to be the multiset

$$S = \{w_i | 0 \leq i \leq n\}.$$

Theorem

Let f be a power function over $\mathbb{F}_{p^n}$. The differential spectrum of f is
1) $S = \{\ w_1 = p^n\}$ if p is odd and f is PN.
2) $S = \{\ w_0 = 2^{n-1}, w_2 = 2^{n-1}\}$ if $p = 2$ is odd and f is APN.

Binary power functions with known differential spectrum

Binary power functions x^d with known differential spectrum

p	d	condition	δ
2	$2^s + 1$	$\gcd(s, n) = 2$	4
2	$2^{2s} - 2^s + 1$	$\gcd(s, n) = 2$	4
2	$2^n - 2$	n even	4
2	$2^{2k} + 2^k + 1$	$n = 4k$, k odd	4
2	$2^{2k} + 2^k + 1$	$n = 4k$	4
2	$2^t - 1$	$t = 3, n - 2$	6
2	$2^t - 1$	$t = (n-1)/2, (n+3)/2, n$ odd	6 or 8
2	$2^m + 2^{(m+1)/2} + 1$	$n = 2m, m \geq 5$ odd	8
2	$2^{m+1} \ + 3$	$n = 2m, m \geq 5$ odd	8

APN Power Functions

Non-binary power functions x^d with known differential spectrum

p	d	condition	δ
odd	$(p^k+1)/2$	$e = gcd(s,n)$	$(p^e-1)/2$ or p^e+1
odd	$\frac{p^n+1}{p^m+1}+(p^n-1)/2$	$p \equiv 3 \mod 4, n$ odd $m\|n$	$(p^m+1)/2$
odd	$p^{2k}-p^k+1$	n odd, $\gcd(k,n)=1$	$p+1$

The last case is the result of this talk from the recent paper.

Haode Yan, Zhengchun Zhou, Jian Weng, Jinming Wen, Tor Helleseth and Qi Wang,
Differential Spectrum og Kasami Power Permutations Over Odd Characteristic Finite Fields,
IEEE Transactions on Information Theory 2019 (to appear).

The Differential Spectrum of Kasami Power Functions

The Differential Spectrum of Kasami power function

Conjecture (G. Xu, X. Cao, and S. Xu (2016))

Let n be odd and k be an integer with $\gcd(k, n) = 1$. Then the power function $f(x) = x^d$, $d = 3^{2k} - 3^k + 1$ over $\mathbb{F}_{3^n}$ satisfies $\delta \leq 4$.

This was proved by the authors above in the special case $k = 1$.

Theorem (Yan, Zhou, Weng, Wen, Helleseth and Wang (2019))

Let p be an odd prime and $d = p^{2k} - p^k + 1$ where $gcd(k, n) = 1$. Then the power function $f(x) = x^d$ is $(p + 1)$-uniform with the following differential spectrum:

$$S = \{w_0 = \frac{p^{n+2} - p^{n+1} - p^n + 1}{p^2 - 1}, w_{p-1} = \frac{p^n - p}{2(p-1)}, w_p = 1, w_{p+1} = \frac{p^n - p}{2(p+1)}\}$$

Note that the conjecture above follows as a special case of the theorem.

The distribution of $S(\gamma, \delta)$

The differential spectrum distribution depends on the following exponential sum. Let p be a prime and ω a complex p-th root of unity and define,

$$S(\gamma, \delta) = \sum_{x \in \mathbb{F}_{p^n}} \omega^{Tr(\gamma x^{p^k+1} + \delta x^{p^{3k}+1})}.$$

Theorem (X. Zheng, L. Hu, W. Jiang, Q. Yue, X. Cao (2010))

Let n be odd and $\gcd(n, k) = 1$. Then the distribution of $S(\gamma, \delta)$ is given by:

p^n	*occurs*	1	*time*
$\sqrt{(-1)^{(p-1)/2}}p^{\frac{n}{2}}$	*occurs*	$\frac{(p^{n+2}-p^{n+1}-p^n+p^2)(p^n-1)}{2(p^2-1)}$	*times*
$-\sqrt{(-1)^{(p-1)/2}}p^{\frac{n}{2}}$	*occurs*	$\frac{(p^{n+2}-p^{n+1}-p^n+p^2)(p^n-1)}{2(p^2-1)}$	*times*
$p^{\frac{n+1}{2}}$	*occurs*	$\frac{(p^{n-1}+p^{\frac{n-1}{2}})(p^n-1)}{2}$	*times*
$-p^{\frac{n+1}{2}}$	*occurs*	$\frac{(p^{n-1}-p^{\frac{n-1}{2}})(p^n-1)}{2}$	*times*
$\sqrt{(-1)^{(p-1)/2}}p^{\frac{n+2}{2}}$	*occurs*	$\frac{(p^{n-1}-1)(p^n-1)}{2(p^2-1)}$	*times*
$-\sqrt{(-1)^{(p-1)/2}}p^{\frac{n+2}{2}}$	*occurs*	$\frac{(p^{n-1}-1)(p^n-1)}{2(p^2-1)}.$	*times*

The fourth power sum of $S(\gamma, \delta)$

The differential spectrum distribution depends on the following 4-th power sum of:

$$S(\gamma, \delta) = \sum_{x \in \mathbb{F}_{p^n}} \omega^{Tr(\gamma x^{p^k+1} + \delta x^{p^{3k}+1})}$$

Theorem

The fourth power sum is

$$\sum_{\gamma, \delta \in \mathbb{F}_{p^n}} (S(\gamma, \delta))^4 = p^{2n} N_\epsilon$$

where N_ϵ, $\epsilon \in \{1, \lambda\}$, λ a non-square, is the number of solutions to

$$\begin{aligned} y^{p^k+1} - \epsilon z^{p^k+1} + u^{p^k+1} - \epsilon v^{p^k+1} &= 0 \\ y^{p^{3k}+1} - \epsilon z^{p^{3k}+1} + u^{p^{3k}+1} - \epsilon v^{p^{3k}+1} &= 0 \end{aligned}$$

which is

$$N_\epsilon = 2p^{2n+1} + 2p^{2n} - p^{n+2} - 2p^{n+1} - p^n + p^2$$

Alternative expression for N_ϵ

Let M_ϵ be the number of solutions of:

$$\begin{aligned} y^{p^k+1} - \epsilon z^{p^k+1} &= \alpha \\ y^{p^{3k}+1} - \epsilon z^{p^{3k}+1} &= \beta \end{aligned}$$

Then,

$$N_\epsilon = \sum_{(\alpha,\beta)\in\mathbb{F}^2_{p^n}} M_\epsilon(\alpha,\beta) M_\epsilon(-\alpha,-\beta)$$

Technical calculations and the alternative expression for N_ϵ one can determine distribution of $M_\epsilon(\alpha,\beta)$. Let χ_p be the quadratic character. Then for example:

Lemma

Let b run through $\mathbb{F}_{p^n} \setminus \{0\}$, then the value distribution of $M_\epsilon(1,b)$ is given by:

$$\begin{array}{ccc} 2(p-\chi_p(\epsilon)) & occurs & \dfrac{p^n-p}{2(p-\chi_p(\epsilon))} \; times, \\ & 0 \quad otherwise. & \end{array}$$

Details of the Kasami differential spectrum

- Let $f(x) = (x+1)^d - x^d$
- $f^{-1}(b) = \{\ x \in \mathbb{F}_{p^n} \mid f(x) = b\ \}$
- S_0 denotes the set of squares in $\mathbb{F}_{p^n}$
- S_1 denotes the set of non-squares in $\mathbb{F}_{p^n}$
- $C_{i,j} = \{\ x \in \mathbb{F}_{p^n} \mid x \in S_i, x+1 \in S_j\}$
- $Im(f) = \{\ f(x) \mid x \in \mathbb{F}_{p^n}\}$
- $Im(f)|_{C_{i,j}} = \{f(x) \mid x \in C_{i,j}\ \}$

Lemma

(1) $\#\ f^{-1}(b) = p+1$ *for any* $b \in Im(f)|_{C_{1,0}}$ *and* $\#\ Im(f)|_{C_{1,0}} = \frac{p^n-p}{2(p+1)}$
(2) $\#\ f^{-1}(b) = p-1$ *for any* $b \in Im(f)|_{C_{0,0}}$ *and* $\#\ Im(f)|_{C_{0,0}} = \frac{p^n-p}{2(p-1)}$
(3) $\#\ f^{-1}(1) = p$

Differential Uniformity of Power Functions from the 1990s

The first non-binary result in 1997

Let QR (resp. QNR) denote the set of quadratic residues (quadratic non residues) in $\mathbb{F}_{p^n}$ The quadratic character of x is defined by:

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

Theorem (Helleseth and Sandberg 1997)

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

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

The second non-binary result in 1997

Theorem (Helleseth and Sandberg 1997)

Let p be a prime, $p \equiv 3 \mod 4$, $d = \frac{p^n-1}{2} + 2$ and let $f(x) = x^d$ be a mapping over $\mathbb{F}_{p^n}$. Then for $p^n > 7$

$$\delta = \begin{cases} 1 & \textit{if} \quad p = 3 \textit{ and } n \textit{ even} \\ 3 & \textit{if} \quad p \neq 3 \textit{ and } p^n \equiv 1 \pmod 4 \\ 4 & \textit{otherwise} . \end{cases}$$

Some non-binary result from 1999

Theorem (Helleseth and Sandberg 1999)

Let p be a prime and let $f(x) = x^d$ be a mapping over $\mathbb{F}_{p^n}$. Then $f(x)$ is an APN mapping for $p^n > 7$ when

$$d = \begin{cases} \frac{p^n+1}{4} + \frac{p^n-1}{2} & \text{if} \quad p^n = 3 \pmod 8 \\ \frac{p^n+1}{4} & \text{if} \quad p^n = 7 \pmod 8) \end{cases}$$

Theorem (Helleseth and Sandberg 1999)

Let p be a prime and let $f(x) = x^d$, $d = p^n - 3$ be a mapping over $\mathbb{F}_{p^n}$.

- *For any odd prime then $1 \leq \delta \leq 5$.*
- *If $n > 1$ and $p = 3$ then $\delta = 2$.*

Proof first 1999 result above

Proof for the case $2d = (p^n+1)/2 \pmod{p^n-1}$.

Let $u_x = x^d$, then $u_x^2 = \chi(x)x$ and $(x+1)^d - x^d = b$ implies

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

	$\chi(x+1)$	$\chi(x)$	u_x	u_{x+1}	$u_{x_i}u_{x_i+1}$	$u_{x_1}u_{x_2}$
1)	1	1	$\frac{1-b^2}{2b}$	$\frac{1+b^2}{2b}$		
2)	1	-1	$\frac{-b\pm\sqrt{-2-b^2}}{2}$	$\frac{b\pm\sqrt{-2-b^2}}{2}$	$\frac{-1-b^2}{2b}$	$\frac{1+b^2}{2b}$
3)	1	-1	$\frac{-b\pm\sqrt{2-b^2}}{2}$	$\frac{b\pm\sqrt{2-b^2}}{2}$	$\frac{1-b^2}{2b}$	$\frac{-1+b^2}{2b}$
4)	1	1	$\frac{-1-b^2}{2b}$	$\frac{-1+b^2}{2b}$		

- Each class has at most one solution in u_x giving a unique x
- Class 1) and 2) as well as Class 3) and 4) cannot both have solutions
- At most two classes can have solution simultaneously

Considering contribution from $x = 0$ and $= 1$ gives $\delta \leq 2$.
Showing the existing of a case with solution in two classes complete the proof.

Some binary APN functions found in 1990s

Some binary APN functions found in 1990s

p	n	d	δ
2	6	3	2
2	7	5	2
2	7	9	2
2	7	11	2
2	7	13	2
2	7	15	2
2	7	23	2
2	7	27	2
2	7	29	2
2	7	43	2
2	7	63	2
2	8	3	2
2	8	9	2
2	8	39 *	2

Some non-binary APN functions found in 1990s

Some non-binary APN functions found in 1990s

p	n	d	δ
3	3	2	2
3	5	26	2
3	5	40	2
3	5	62	2
3	5	80	2
3	5	134 *	2
3	5	152 *	2
3	7	40 *	2
3	7	80	2
3	7	224 *	2
3	7	274 *	2
3	7	364	2
3	7	548	2
3	7	728	2

PN Power Functions and Optimal Sequences

PN power functions

Three known classes of PN power mappings:

Power PN mappings

- $d = 2$.
- $d = p^k + 1$, where $n/\gcd(k, n)$ is odd.
- $d = (3^k + 1)/2$, where $p = 3$, k is odd and $\gcd(n, k) = 1$.

The first two classes have been used to construct sequences with optimal correlation properties.

Any PN power function $f(x)$ can be used to construct optimal sequences.

Sequences from PN power functions

Let ω be a complex p-th root of unity and let $Tr(x) = \sum_{x=0}^{n-1} x^{p^i}$. Then for a PN function $f(x)$

$$\sum_{x \in \mathbb{F}_{p^n}} \omega^{Tr(f(x+a)-f(x))} = 0 \text{ for any } \ a \neq 0.$$

Let α be a primitive element in $\mathbb{F}_{p^n}$. Let $c \in \mathbb{F}_{p^n}$ and let $\{s_c(t)\}$ be the sequence of period $p^n - 1$ defined by

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

Then the family of sequences

$$\mathcal{F} \ = \{\{s_c(t)\} \mid c \in \mathbb{F}_{p^n}\}$$

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

An exponential sum from PN functions

Theorem

Let $f(x)$ be a PN function. Let $S(c,\lambda) = \sum_{x \in \mathbb{F}_{p^n}} \omega^{Tr(cf(x)-\lambda x)}$. Then,

$$|S(c,\lambda)|^2 = p^n.$$

Proof.

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

□

Correlation of sequences from PN power functions

Theorem

Let $s_c(t) = Tr(c\alpha^{dt} + \alpha^t)$ where $f(x) = x^d$ is a PN power function. Then the magnitude of the crosscorrelation of $\{s_{c_1}(t)\}$ and $\{s_{c_2}(t)\}$ is at most $1 + \sqrt{p^n}$

Proof.

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

Hence, $|\theta(\tau)| \leq 1 + \sqrt{p^n}$. □

Thank You!

Questions? Comments? Suggestions?