Is χ_n a power function?

Jan Schoone

Radboud University

13 July 2023

Introduction

Introduction to χ_n

Definition 1 (χ_n)

The map $\chi_n \colon \mathbb{F}_2^n \to \mathbb{F}_2^n,\ x \mapsto y$ is given by:

$$y_i = x_i + (x_{i+1} + 1)x_{i+2} \qquad i \in \mathbb{Z}/n\mathbb{Z}.$$

Introduction to χ_n

Definition 1 (χ_n)

The map $\chi_n \colon \mathbb{F}_2^n \to \mathbb{F}_2^n,\ x \mapsto y$ is given by:

$$y_i = x_i + (x_{i+1} + 1)x_{i+2} \qquad i \in \mathbb{Z}/n\mathbb{Z}.$$

We have: x_i is followed by $x_{i+1} = 0$ and $x_{i+2} = 1$ if and only if $y_i = x_i + 1$.

Introduction to χ_n

Definition 1 (χ_n)

The map $\chi_n \colon \mathbb{F}_2^n \to \mathbb{F}_2^n,\ x \mapsto y$ is given by:

$$y_i = x_i + (x_{i+1} + 1)x_{i+2} \qquad i \in \mathbb{Z}/n\mathbb{Z}.$$

We have: x_i is followed by $x_{i+1} = 0$ and $x_{i+2} = 1$ if and only if $y_i = x_i + 1$.

Keccak-f, the SHA-3 standard: χ_5.

Introduction to χ_n

Definition 1 (χ_n)

The map $\chi_n \colon \mathbb{F}_2^n \to \mathbb{F}_2^n,\ x \mapsto y$ is given by:

$$y_i = x_i + (x_{i+1} + 1)x_{i+2} \qquad i \in \mathbb{Z}/n\mathbb{Z}.$$

We have: x_i is followed by $x_{i+1} = 0$ and $x_{i+2} = 1$ if and only if $y_i = x_i + 1$.

KECCAK-f, the SHA-3 standard: χ_5.

ASCON, the Lightweight Cryptography winner: χ_5.

Properties of χ_n

- χ_n has (algebraic) degree 2:
  $y_i = x_i + x_{i+1}x_{i+2} + x_{i+2}$;

Properties of χ_n

- χ_n has (algebraic) degree 2:
  $y_i = x_i + x_{i+1}x_{i+2} + x_{i+2}$;
- χ_n is shift invariant:
  $\chi_n(x \ll 1) = \chi_n(x) \ll 1$;

Properties of χ_n

- χ_n has (algebraic) degree 2:
  $y_i = x_i + x_{i+1}x_{i+2} + x_{i+2}$;
- χ_n is shift invariant:
  $\chi_n(x \lll 1) = \chi_n(x) \lll 1$;
- χ_n is invertible if and only if n is odd:
  $(01)^n \mapsto 0^{2n} \mapsfrom (10)^n$;

Properties of χ_n

- χ_n has (algebraic) degree 2:
  $y_i = x_i + x_{i+1}x_{i+2} + x_{i+2}$;
- χ_n is shift invariant:
  $\chi_n(x \ll 1) = \chi_n(x) \ll 1$;
- χ_n is invertible if and only if n is odd:
  $(01)^n \mapsto 0^{2n} \leftarrow\!\!\dashv (10)^n$;
- $\mathrm{ord}(\chi_n) = 2^{\lfloor \lg n \rfloor}$.

Univariate polynomials

$$\begin{array}{ccc} \mathbb{F}_2^n & \xrightarrow{\chi_n} & \mathbb{F}_2^n \\ \downarrow \phi & & \downarrow \phi \\ \mathbb{F}_{2^n} & \xrightarrow[\widehat{\chi_n}]{} & \mathbb{F}_{2^n} \end{array}$$

$$\phi(\vec{x}) = \sum_{i=0}^{n-1} x_i \beta^{q^i}$$

Univariate polynomials

$$\begin{array}{ccc} \mathbb{F}_2^n & \xrightarrow{\chi_n} & \mathbb{F}_2^n \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi} \\ \mathbb{F}_{2^n} & \xrightarrow[\widehat{\chi_n}]{} & \mathbb{F}_{2^n} \end{array} \qquad \phi(\vec{x}) = \sum_{i=0}^{n-1} x_i \beta^{q^i}$$

Definition 2 (Normal basis)

Consider $\mathbb{F}_2 \subset \mathbb{F}_{2^n}$. Then $\beta \in \mathbb{F}_{2^n}$ is called a *normal element* of $\mathbb{F}_{2^n}$ if the set $\{\beta, \beta^2, \beta^{2^2}, \ldots, \beta^{2^{n-1}}\}$ is a linear independent set. This set is then called a *normal basis* of $\mathbb{F}_{2^n}$.

Univariate polynomials

$$\begin{array}{ccc} \mathbb{F}_2^n & \xrightarrow{\chi_n} & \mathbb{F}_2^n \\ \phi \downarrow & & \downarrow \phi \\ \mathbb{F}_{2^n} & \xrightarrow[\widehat{\chi_n}]{} & \mathbb{F}_{2^n} \end{array}$$

$$\phi(\vec{x}) = \sum_{i=0}^{n-1} x_i \beta^{q^i}$$

Definition 2 (Normal basis)

Consider $\mathbb{F}_2 \subset \mathbb{F}_{2^n}$. Then $\beta \in \mathbb{F}_{2^n}$ is called a *normal element* of $\mathbb{F}_{2^n}$ if the set $\{\beta, \beta^2, \beta^{2^2}, \ldots, \beta^{2^{n-1}}\}$ is a linear independent set. This set is then called a *normal basis* of $\mathbb{F}_{2^n}$.

Theorem 3

If $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is shift invariant and the isomorphism ϕ is induced by a normal element, then $\widehat{F}$ has coefficients in $\mathbb{F}_2$.

Univariate polynomials

$$\begin{array}{ccc} \mathbb{F}_2^n & \xrightarrow{\chi_n} & \mathbb{F}_2^n \\ \downarrow \phi & & \downarrow \phi \\ \mathbb{F}_{2^n} & \xrightarrow[\widehat{\chi_n}]{} & \mathbb{F}_{2^n} \end{array}$$

$$\phi(\vec{x}) = \sum_{i=0}^{n-1} x_i \beta^{q^i}$$

Example 2

Consider the map χ_3. Let $\mathbb{F}_{2^3} := \mathbb{F}_2(\alpha) = \mathbb{F}_2[X]/(X^3 + X + 1)$. Then α^3 is a normal element. We define $\widehat{\chi_3} := \phi \circ \chi_3 \circ \phi^{-1}$. By using Lagrange interpolation we find that $\widehat{\chi_3}(t) = t^6$.

Power functions

Definition 3 (Power functions)

A *power function* is a polynomial function that can be represented by a single monomial in $\mathbb{F}_{2^n}[X]$. We write $*^e \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ for a power function, here $e \geq 0$.

Power functions

Definition 3 (Power functions)

A *power function* is a polynomial function that can be represented by a single monomial in $\mathbb{F}_{2^n}[X]$. We write $*^e\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ for a power function, here $e \geq 0$.

A power function $*^e\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is invertible if and only if $\gcd(e, 2^n - 1) = 1$.

Power functions

Definition 3 (Power functions)

A *power function* is a polynomial function that can be represented by a single monomial in $\mathbb{F}_{2^n}[X]$. We write $*^e\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ for a power function, here $e \geq 0$.

A power function $*^e\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is invertible if and only if $\gcd(e, 2^n - 1) = 1$.

The order of an invertible power function $*^e$ is given by the (multiplicative) order of e in $\mathbb{Z}/(2^n - 1)\mathbb{Z}$.

Power functions

Definition 3 (Power functions)

A *power function* is a polynomial function that can be represented by a single monomial in $\mathbb{F}_{2^n}[X]$. We write $*^e\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ for a power function, here $e \geq 0$.

A power function $*^e\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is invertible if and only if $\gcd(e, 2^n - 1) = 1$.

The order of an invertible power function $*^e$ is given by the (multiplicative) order of e in $\mathbb{Z}/(2^n - 1)\mathbb{Z}$.

Why power functions?

Question, answer and small results

Is χ_n a power function (for *any* choice of (normal) basis)?

Question, answer and small results

Is χ_n a power function (for *any* choice of (normal) basis)?

No!

Question, answer and small results

Is χ_n a power function (for *any* choice of (normal) basis)?

No! (For $n \neq 1, 3$.)

Question, answer and small results

Is χ_n a power function (for *any* choice of (normal) basis)?

No! (For $n \neq 1, 3$.)

Proposition 1

For any even n, there is no (normal) basis representation such that $\widehat{\chi_n}$ is a power function.

Question, answer and small results

Is χ_n a power function (for *any* choice of (normal) basis)?

No! (For $n \neq 1, 3$.)

Proposition 1

For any even n, there is no (normal) basis representation such that $\widehat{\chi_n}$ is a power function.

Proof.

Suppose that it does exist. Since $\chi_n((01)^{n/2}) = 0^n$, there needs to exist some nonzero $\alpha \in \mathbb{F}_{2^n}$ with $\alpha^s = 0$ for some integer s. □

Question, answer and small results

Is χ_n a power function (for *any* choice of (normal) basis)?

No! (For $n \neq 1, 3.$)

Proposition 1 (Excluding Mersenne-exponents)

If $n > 3$ is such that $2^n - 1$ is a prime number, then there exists no (normal) basis representation of χ_n such that $\widehat{\chi_n}$ is a power function.

Question, answer and small results

Is χ_n a power function (for *any* choice of (normal) basis)?

No! (For $n \neq 1, 3$.)

Proposition 1 (Excluding Mersenne-exponents)

If $n > 3$ is such that $2^n - 1$ is a prime number, then there exists no (normal) basis representation of χ_n such that $\widehat{\chi_n}$ is a power function.

Proof.

Since $2^n - 1$ is a prime number, $\varphi(2^n - 1) = 2^n - 2$. The order of χ_n is divisible by 4 for all $n > 3$. The expression $2^n - 2$ has only one factor 2 . □

Historical attempts

State diagrams

Definition 4 (State diagram)

Let S be a set. The *state diagram* for a map $F\colon S \to S$ is a directed graph (V, A), where $V = S$ and $A = \{(a, F(a)) \mid a \in S\}$.

State diagrams

Definition 4 (State diagram)

Let S be a set. The *state diagram* for a map $F\colon S \to S$ is a directed graph (V, A), where $V = S$ and $A = \{(a, F(a)) \mid a \in S\}$.

The state diagram of χ_n consists of cycles of length $1, 2, 4, 8, \ldots, \operatorname{ord}(\chi_n)$.

State diagrams

Definition 4 (State diagram)

Let S be a set. The *state diagram* for a map $F\colon S \to S$ is a directed graph (V, A), where $V = S$ and $A = \{(a, F(a)) \mid a \in S\}$.

The state diagram of χ_n consists of cycles of length $1, 2, 4, 8, \ldots, \operatorname{ord}(\chi_n)$.
Each length occurs at least once!

State diagrams

Definition 4 (State diagram)

Let S be a set. The *state diagram* for a map $F\colon S \to S$ is a directed graph (V, A), where $V = S$ and $A = \{(a, F(a)) \mid a \in S\}$.

The state diagram of χ_n consists of cycles of length $1, 2, 4, 8, \ldots, \mathrm{ord}(\chi_n)$.
Each length occurs at least once!

Theorem 5 (Ahmad's Theorem)

Let m, q be positive integers with $q = p^n$ for some prime number p and $n \geq 1$. Let $*^e\colon \mathbb{F}_q^* \to \mathbb{F}_q^*,\ x \mapsto x^e$ be a power function. Then $*^e$ has a cycle of length precisely m if and only if there exists some $t \mid q-1$ such that the order of e modulo t is equal to m.

State diagrams

Definition 4 (State diagram)

Let S be a set. The *state diagram* for a map $F\colon S \to S$ is a directed graph (V, A), where $V = S$ and $A = \{(a, F(a)) \mid a \in S\}$.

The state diagram of χ_n consists of cycles of length $1, 2, 4, 8, \ldots, \mathrm{ord}(\chi_n)$.
Each length occurs at least once!

Theorem 5 (Ahmad's Theorem)

Let m, q be positive integers with $q = p^n$ for some prime number p and $n \geq 1$. Let $*^e\colon \mathbb{F}_q^* \to \mathbb{F}_q^*,\ x \mapsto x^e$ be a power function. Then $*^e$ has a cycle of length precisely m if and only if there exists some $t \mid q-1$ such that the order of e modulo t is equal to m.

Not every length necessarily occurs!

Corollary

Theorem 6 (Necessary conditions for χ_n to be a power function)

Let $n > 3$ be an odd integer. Write $o := \operatorname{ord}(\chi_n) = 2^{\lfloor \lg(n) \rfloor}$. Then χ_n can only be a power function if $2^n - 1$ factors as

$$2^n - 1 = p_1^{e_1} \cdots p_r^{e_r},$$

such that there exists some permutation $\sigma \in S_r$ with

$$\begin{aligned} \varphi(p_{\sigma(1)}^{e_{\sigma(1)}}) & \text{ is a multiple of } o \\ \varphi(p_{\sigma(2)}^{e_{\sigma(2)}}) & \text{ is a multiple of } \frac{o}{2} \\ & \vdots \\ \varphi(p_{\sigma(t)}^{e_{\sigma(t)}}) & \text{ is a multiple of } 2 \end{aligned}$$

for some $t < r$.

Results

Using these conditions, we can verify[1] that χ_n is not a power function for any $n \leq 1115$, except for $n = 63$ and $n = 441$.

[1] Using MAGMA in under 2 minutes!

Results

Using these conditions, we can verify[1] that χ_n is not a power function for any $n \leq 1115$, except for $n = 63$ and $n = 441$.

Remaining cases:

- $n = 63$:
  - $\approx 2^{12.59}$ out of $\approx 2^{62.742}$ possible e;

[1] Using MAGMA in under 2 minutes!

Results

Using these conditions, we can verify[1] that χ_n is not a power function for any $n \leq 1115$, except for $n = 63$ and $n = 441$.

Remaining cases:

- $n = 63$:
  - $\approx 2^{12.59}$ out of $\approx 2^{62.742}$ possible e;
  - Algebraic degree of power function is $\mathrm{wt}_2(e)$;

[1] Using MAGMA in under 2 minutes!

Results

Using these conditions, we can verify[1] that χ_n is not a power function for any $n \leq 1115$, except for $n = 63$ and $n = 441$.

Remaining cases:

- $n = 63$:
  - $\approx 2^{12.59}$ out of $\approx 2^{62.742}$ possible e;
  - Algebraic degree of power function is $\mathrm{wt}_2(e)$;
  - None have algebraic degree 2.

[1] Using MAGMA in under 2 minutes!

Results

Using these conditions, we can verify[1] that χ_n is not a power function for any $n \leq 1115$, except for $n = 63$ and $n = 441$.

Remaining cases:

- $n = 63$:
  - $\approx 2^{12.59}$ out of $\approx 2^{62.742}$ possible e;
  - Algebraic degree of power function is $\mathrm{wt}_2(e)$;
  - None have algebraic degree 2.
- $n = 441$:[2]
  - $2^{35.322}$ out of $\approx 2^{440.742}$ possible e;

[1] Using MAGMA in under 2 minutes!

[2] This takes way longer to compute...

Results

Using these conditions, we can verify[1] that χ_n is not a power function for any $n \leq 1115$, except for $n = 63$ and $n = 441$.

Remaining cases:

- $n = 63$:
  - $\approx 2^{12.59}$ out of $\approx 2^{62.742}$ possible e;
  - Algebraic degree of power function is $\mathrm{wt}_2(e)$;
  - None have algebraic degree 2.
- $n = 441$:[2]
  - $2^{35.322}$ out of $\approx 2^{440.742}$ possible e;
  - None have algebraic degree 2.

[1] Using MAGMA in under 2 minutes!

[2] This takes way longer to compute...

Proof technique

Differential distributions

Definition 7 (Differential probability (Biham, Shamir))

Let $f\colon G \to H$ be a map between finite groups G and H. Let $g \in G$ and $h \in H$ be arbitrary. Then we define the *differential probability of f at (g, h)* as

$$\mathrm{DP}_f(g,h) = \#\{x \in G \mid f(x) - f(x-g) = h\}/|G|.$$

Differential distributions

Definition 7 (Differential probability (Biham, Shamir))

Let $f\colon G \to H$ be a map between finite groups G and H. Let $g \in G$ and $h \in H$ be arbitrary. Then we define the *differential probability of f at (g,h)* as

$$\mathrm{DP}_f(g,h) = \#\{x \in G \mid f(x) - f(x-g) = h\}/|G|.$$

input difference

output difference

χ_3	000	001	010	011	100	101	110	111
000	1	-	-	-	-	-	-	-
001	-	$^1/_4$	-	$^1/_4$	-	$^1/_4$	-	$^1/_4$
010	-	-	$^1/_4$	$^1/_4$	-	-	$^1/_4$	$^1/_4$
011	-	$^1/_4$	$^1/_4$	-	-	$^1/_4$	$^1/_4$	-
100	-	-	-	-	$^1/_4$	$^1/_4$	$^1/_4$	$^1/_4$
101	-	$^1/_4$	-	$^1/_4$	$^1/_4$	-	$^1/_4$	-
110	-	-	$^1/_4$	$^1/_4$	$^1/_4$	$^1/_4$	-	-
111	-	$^1/_4$	$^1/_4$	-	$^1/_4$	-	-	$^1/_4$

Differential distribution for χ

Proposition 2 (Differential probabilities for χ (Daemen))

Let $n > 1$ be an arbitrary odd integer. Let $a \in \mathbb{F}_2^n$ be arbitrary. Then for any compatible $b \in \mathbb{F}_2^n$ we have $\mathrm{DP}_{\chi_n}(a, b) = 2^{-w(a)}$, where

$$w(a) = \begin{cases} n - 1 & \text{if } a = 1^n; \\ \mathrm{wt}(a) + r & \text{else}, \end{cases}$$

where r is the number of (cyclic) 001-substrings in a.

Differential distribution for χ

Proposition 2 (Differential probabilities for χ (Daemen))

Let $n > 1$ be an arbitrary odd integer. Let $a \in \mathbb{F}_2^n$ be arbitrary. Then for any compatible $b \in \mathbb{F}_2^n$ we have $\mathrm{DP}_{\chi_n}(a, b) = 2^{-w(a)}$, where

$$w(a) = \begin{cases} n - 1 & \textit{if } a = 1^n; \\ \mathrm{wt}(a) + r & \textit{else,} \end{cases}$$

where r is the number of (cyclic) 001-substrings in a.

Let $n > 3$ be odd.

- $a = 110^{n-2} \implies$

Differential distribution for χ

Proposition 2 (Differential probabilities for χ (Daemen))

Let $n > 1$ be an arbitrary odd integer. Let $a \in \mathbb{F}_2^n$ be arbitrary. Then for any compatible $b \in \mathbb{F}_2^n$ we have $\mathrm{DP}_{\chi_n}(a, b) = 2^{-w(a)}$, where

$$w(a) = \begin{cases} n - 1 & \text{if } a = 1^n; \\ \mathrm{wt}(a) + r & \text{else,} \end{cases}$$

where r is the number of (cyclic) 001-substrings in a.

Let $n > 3$ be odd.

- $a = 110^{n-2} \implies \mathrm{DP}_{\chi_n}(a, b) = \frac{1}{8}$;

Differential distribution for χ

Proposition 2 (Differential probabilities for χ (Daemen))

Let $n > 1$ be an arbitrary odd integer. Let $a \in \mathbb{F}_2^n$ be arbitrary. Then for any compatible $b \in \mathbb{F}_2^n$ we have $\mathrm{DP}_{\chi_n}(a, b) = 2^{-w(a)}$, where

$$w(a) = \begin{cases} n - 1 & \text{if } a = 1^n; \\ \mathrm{wt}(a) + r & \text{else,} \end{cases}$$

where r is the number of (cyclic) 001-substrings in a.

Let $n > 3$ be odd.

- $a = 110^{n-2} \implies \mathrm{DP}_{\chi_n}(a, b) = \frac{1}{8}$;
- $a' = 10^{n-1} \implies$

Differential distribution for χ

Proposition 2 (Differential probabilities for χ (Daemen))

Let $n > 1$ be an arbitrary odd integer. Let $a \in \mathbb{F}_2^n$ be arbitrary. Then for any compatible $b \in \mathbb{F}_2^n$ we have $\mathrm{DP}_{\chi_n}(a, b) = 2^{-w(a)}$, where

$$w(a) = \begin{cases} n - 1 & \text{if } a = 1^n; \\ \mathrm{wt}(a) + r & \text{else,} \end{cases}$$

where r is the number of (cyclic) 001-substrings in a.

Let $n > 3$ be odd.

- $a = 110^{n-2} \implies \mathrm{DP}_{\chi_n}(a, b) = \frac{1}{8}$;
- $a' = 10^{n-1} \implies \mathrm{DP}_{\chi_n}(a', b) = \frac{1}{4}$.

Invariant

Proposition 3 (Differential probabilities under linear isomorphisms)

Let $G \overset{\varphi}{\cong} H$ be isomorphic groups. Let $f \colon G \to G$ be a map and let $\hat{f} \colon H \to H$ be the map induced through the isomorphism. Then $\mathrm{DP}_{\hat{f}}(g, h) = \mathrm{DP}_f(\varphi^{-1}(g), \varphi^{-1}(h))$ for all $g, h \in H$.

Invariant

Proposition 3 (Differential probabilities under linear isomorphisms)

Let $G \overset{\varphi}{\cong} H$ *be isomorphic groups. Let* $f\colon G \to G$ *be a map and let* $\hat{f}\colon H \to H$ *be the map induced through the isomorphism. Then* $\mathrm{DP}_{\hat{f}}(g,h) = \mathrm{DP}_f(\varphi^{-1}(g), \varphi^{-1}(h))$ *for all* $g, h \in H$.

Proposition 4 (Differential probabilities for power functions (Blondeau, Canteaut, Charpin))

Let $0 \le e \le 2^n - 1$ *and let* $f = *^e\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *be a power function. Then* $\mathrm{DP}_f(a,b) = \mathrm{DP}_f(ya, y^e b)$ *for all* $y \in \mathbb{F}_{2^n}^*$.

Invariant

Proposition 3 (Differential probabilities under linear isomorphisms)

Let $G \overset{\varphi}{\cong} H$ *be isomorphic groups. Let* $f\colon G \to G$ *be a map and let* $\hat{f}\colon H \to H$ *be the map induced through the isomorphism. Then* $\mathrm{DP}_{\hat{f}}(g,h) = \mathrm{DP}_f(\varphi^{-1}(g), \varphi^{-1}(h))$ *for all* $g, h \in H$*.*

Proposition 4 (Differential probabilities for power functions (Blondeau, Canteaut, Charpin))

Let $0 \le e \le 2^n - 1$ *and let* $f = *^e\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *be a power function. Then* $\mathrm{DP}_f(a,b) = \mathrm{DP}_f(ya, y^e b)$ *for all* $y \in \mathbb{F}_{2^n}^*$*.*

Proof.

Substitute $x := yy^{-1}x = yx'$ in
$\mathrm{DP}_f(ya, y^e b) = \#\{x \in \mathbb{F}_{2^n} \mid x^e + (x+ya)^e = y^e b\}/2^n$. □

Invariant

Proposition 3 (Differential probabilities under linear isomorphisms)

Let $G \overset{\varphi}{\cong} H$ *be isomorphic groups. Let* $f\colon G \to G$ *be a map and let* $\hat{f}\colon H \to H$ *be the map induced through the isomorphism. Then* $\mathrm{DP}_{\hat{f}}(g, h) = \mathrm{DP}_f(\varphi^{-1}(g), \varphi^{-1}(h))$ *for all* $g, h \in H$*.*

Proposition 4 (Differential probabilities for power functions (Blondeau, Canteaut, Charpin))

Let $0 \leq e \leq 2^n - 1$ *and let* $f = *^e\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *be a power function. Then* $\mathrm{DP}_f(a, b) = \mathrm{DP}_f(ya, y^e b)$ *for all* $y \in \mathbb{F}_{2^n}^*$*.*

Proof.

Substitute $x := yy^{-1}x = yx'$ in

$\mathrm{DP}_f(ya, y^e b) = \#\{x \in \mathbb{F}_{2^n} \mid x^e + (x + ya)^e = y^e b\}/2^n$. □

Thus, we have that the rows of the DDT all have the same number of occurrences of $0, 2, 4, \ldots$.

Conclusion and corollary

Theorem 8

Let $n \neq 1, 3$ be a positive integer. Then $\widehat{\chi_n}$ is not a power function.

Conclusion and corollary

Theorem 8

Let $n \neq 1, 3$ be a positive integer. Then $\widehat{\chi_n}$ is not a power function.

Corollary 9

There is no function F_n that is extended affine equivalent to χ_n ($AF_nB + C = \chi_n$), such that $\widehat{F_n}$ is a power function.

Conclusion and corollary

Theorem 8

Let $n \neq 1, 3$ be a positive integer. Then $\widehat{\chi_n}$ is not a power function.

Corollary 9

There is no function F_n that is extended affine equivalent to χ_n ($AF_nB + C = \chi_n$), such that $\widehat{F_n}$ is a power function.

Thank you for your attention!