Insights into the Algebraic Structure of χ

Björn Kriepke Gohar Kyureghyan

University of Rostock, Germany

PBC 2025, May 4

The map χ

- First introduced by Joan Daemen[1].
- χ is a permutation on n bits if and only if n is odd [1].
- χ is shift-invariant.
- χ is quadratic, i.e. algebraic degree 2.
- χ^{-1} has algebraic degree $(n+1)/2$.
- An explicit formula for the inverse is known[2].

[1] Joan Daemen. "Cipher and hash function design strategies based on linear and differential cryptanalysis". PhD thesis. Doctoral Dissertation, March 1995, KU Leuven, 1995.

[2] Fukang Liu, Santanu Sarkar, Willi Meier, and Takanori Isobe. "The inverse of χ and its applications to Rasta-like ciphers". In: *Journal of Cryptology* 35.4 (2022), p. 28.

χ in practice

Cryptographic algorithm	Length
SHA-3 (Keccak)	$n = 5$
ASCON	$n = 5$
Subterranean	$n = 257$
Rasta/Dasta/Agrasta	several options for n

The map χ

Definition

$\chi : \mathbb{F}_2^n \to \mathbb{F}_2^n, x \mapsto y = \chi(x)$ given by

$$y_i = x_i + x_{i+2}(1 + x_{i+1})$$

where the indices are taken modulo n.

The map χ

Definition

$\chi : \mathbb{F}_2^n \to \mathbb{F}_2^n, x \mapsto y = \chi(x)$ given by

$$y_i = x_i + x_{i+2}(1 + x_{i+1})$$

where the indices are taken modulo n.

When does χ change the bit x_i?

The map χ

Definition

$\chi : \mathbb{F}_2^n \to \mathbb{F}_2^n, x \mapsto y = \chi(x)$ given by

$$y_i = x_i + x_{i+2}(1 + x_{i+1})$$

where the indices are taken modulo n.

When does χ change the bit x_i?
$y_i = x_i + 1$

The map χ

Definition

$\chi : \mathbb{F}_2^n \to \mathbb{F}_2^n, x \mapsto y = \chi(x)$ given by

$$y_i = x_i + x_{i+2}(1 + x_{i+1})$$

where the indices are taken modulo n.

When does χ change the bit x_i?

$y_i = x_i + 1 \iff x_{i+2}(1 + x_{i+1}) = 1$

The map χ

Definition

$\chi : \mathbb{F}_2^n \to \mathbb{F}_2^n, x \mapsto y = \chi(x)$ given by

$$y_i = x_i + x_{i+2}(1 + x_{i+1})$$

where the indices are taken modulo n.

When does χ change the bit x_i?

$y_i = x_i + 1 \iff x_{i+2}(1 + x_{i+1}) = 1 \iff (x_{i+1}, x_{i+2}) = (0, 1).$

The map χ

Definition

$\chi : \mathbb{F}_2^n \to \mathbb{F}_2^n, x \mapsto y = \chi(x)$ given by

$$y_i = x_i + x_{i+2}(1 + x_{i+1})$$

where the indices are taken modulo n.

When does χ change the bit x_i?
$y_i = x_i + 1 \iff x_{i+2}(1 + x_{i+1}) = 1 \iff (x_{i+1}, x_{i+2}) = (0, 1)$.
$\rightsquigarrow$ χ flips the bit x_i if and only if x_i is followed by the pattern 01.

The map χ

Definition

$\chi : \mathbb{F}_2^n \to \mathbb{F}_2^n, x \mapsto y = \chi(x)$ given by

$$y_i = x_i + x_{i+2}(1 + x_{i+1})$$

where the indices are taken modulo n.

When does χ change the bit x_i?
$y_i = x_i + 1 \iff x_{i+2}(1 + x_{i+1}) = 1 \iff (x_{i+1}, x_{i+2}) = (0, 1)$.
$\rightsquigarrow$ χ flips the bit x_i if and only if x_i is followed by the pattern 01.

Definition

χ is given by the complementing landscape $*01$.

The map χ, an example

Example

$n = 9$.

$$x = 1\ 1\ 0\ 1\ 1\ 0\ 1\ 0\ 0$$

$$\chi(x) =$$

The map χ, an example

Example

$n = 9$.

$$\begin{array}{rcccccccccc} x & = & 1 & & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ & & \downarrow & & & & & & & & & \\ \chi(x) & = & 1 & & & & & & & & & \end{array}$$

The map χ, an example

Example

$n = 9$.

$$\begin{array}{rcccccccccc} x & = & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ & & & \downarrow & & & & & & & \\ \chi(x) & = & 1 & 0 & & & & & & & \end{array}$$

The map χ, an example

Example

$n = 9$.

$$
\begin{array}{rcccccccccc}
x & = & 1 & & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
 & & & & & & & & & \downarrow & \\
\chi(x) & = & 1 & & 0 & 0 & 1 & 0 & 0 & 1 & 1
\end{array}
$$

The map χ, an example

Example

$n = 9$.

$$\begin{array}{rcccccccccc} x & = & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ & & & & & & & & & & \downarrow \\ \chi(x) & = & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \end{array}$$

Iterates of χ

We are interested in the iterates of χ, i.e. what is

$$\chi^k(x) = \chi(\chi(\ldots\chi(x)\ldots))$$

for $k \geq 1$.

Warm-up

Let $x = x^{(0)} \in \mathbb{F}_2^n$ and denote $x^{(k)} = \chi^k(x^{(0)})$. Then

$$x_i^{(0)} = x_i$$

Warm-up

Let $x = x^{(0)} \in \mathbb{F}_2^n$ and denote $x^{(k)} = \chi^k(x^{(0)})$. Then

$$x_i^{(0)} = x_i$$
$$x_i^{(1)} = \chi(x)_i = x_i + x_{i+2}(1 + x_{i+1})$$

Warm-up

Let $x = x^{(0)} \in \mathbb{F}_2^n$ and denote $x^{(k)} = \chi^k(x^{(0)})$. Then

$$
\begin{aligned}
x_i^{(0)} &= x_i \\
x_i^{(1)} &= \chi(x)_i = x_i + x_{i+2}(1 + x_{i+1}) \\
x_i^{(2)} &= \chi(x^{(1)})_i = x_i^{(1)} + x_{i+2}^{(1)}(1 + x_{i+1}^{(1)})
\end{aligned}
$$

Warm-up

Let $x = x^{(0)} \in \mathbb{F}_2^n$ and denote $x^{(k)} = \chi^k(x^{(0)})$. Then

$$
\begin{aligned}
x_i^{(0)} &= x_i \\
x_i^{(1)} &= \chi(x)_i = x_i + x_{i+2}(1 + x_{i+1}) \\
x_i^{(2)} &= \chi(x^{(1)})_i = x_i^{(1)} + x_{i+2}^{(1)}(1 + x_{i+1}^{(1)}) \\
&= x_i + x_{i+2}(1 + x_{i+1}) \\
&\quad + (x_{i+2} + x_{i+4}(1 + x_{i+3})) \cdot (1 + x_{i+1} + x_{i+3}(1 + x_{i+2}))
\end{aligned}
$$

Warm-up

Let us focus on that last product.

$$(x_{i+2} + x_{i+4}(1 + x_{i+3})) \cdot ((1 + x_{i+1}) + x_{i+3}(1 + x_{i+2}))$$

Warm-up

Let us focus on that last product.

$$(x_{i+2} + x_{i+4}(1 + x_{i+3})) \cdot ((1 + x_{i+1}) + x_{i+3}(1 + x_{i+2}))$$

Because we are in $\mathbb{F}_2$ we have $x_i \cdot (1 + x_i) = 0$.

Warm-up

Let us focus on that last product.

$$(x_{i+2} + x_{i+4}(1 + x_{i+3})) \cdot ((1 + x_{i+1}) + x_{i+3}(1 + x_{i+2}))$$

Because we are in $\mathbb{F}_2$ we have $x_i \cdot (1 + x_i) = 0$. In particular:

$$x_{i+2}x_{i+3}(1 + x_{i+2}) = 0,$$
$$x_{i+4}(1 + x_{i+3})x_{i+3}(1 + x_{i+2}) = 0.$$

Warm-up

Let us focus on that last product.

$$(x_{i+2} + x_{i+4}(1 + x_{i+3})) \cdot ((1 + x_{i+1}) + x_{i+3}(1 + x_{i+2}))$$

Because we are in $\mathbb{F}_2$ we have $x_i \cdot (1 + x_i) = 0$. In particular:

$$x_{i+2}x_{i+3}(1 + x_{i+2}) = 0,$$
$$x_{i+4}(1 + x_{i+3})x_{i+3}(1 + x_{i+2}) = 0.$$

After multiplying out we get

$$x_{i+2}(1 + x_{i+1}) + x_{i+4}(1 + x_{i+3})(1 + x_{i+1}).$$

Warm-up

After simplifying we are left with

$$x_i^{(2)} = x_i + x_{i+4}(1 + x_{i+3})(1 + x_{i+1}).$$

Warm-up

Similarly,

$$\begin{aligned} x_i^{(3)} = x_i &+ x_{i+2} \cdot (1 + x_{i+1}) \\ &+ x_{i+4} \cdot (1 + x_{i+3}) \cdot (1 + x_{i+1}) \\ &+ x_{i+6} \cdot (1 + x_{i+5}) \cdot (1 + x_{i+3}) \cdot (1 + x_{i+1}) \end{aligned}$$

Warm-up

Similarly,

$$\begin{aligned} x_i^{(3)} = x_i &+ x_{i+2} \cdot (1 + x_{i+1}) \\ &+ x_{i+4} \cdot (1 + x_{i+3}) \cdot (1 + x_{i+1}) \\ &+ x_{i+6} \cdot (1 + x_{i+5}) \cdot (1 + x_{i+3}) \cdot (1 + x_{i+1}) \end{aligned}$$

and

$$x_i^{(4)} = x_i + x_{i+8} \cdot (1 + x_{i+7}) \cdot (1 + x_{i+5}) \cdot (1 + x_{i+3}) \cdot (1 + x_{i+1}).$$

Warm-up

We define $\gamma_{2k} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ given by

$$\gamma_{2k}(x)_i = x_{i+2k} \cdot (1 + x_{i+2k-1}) \cdot (1 + x_{i+2k-3}) \cdots (1 + x_{i+1}).$$

Warm-up

We define $\gamma_{2k} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ given by

$$\gamma_{2k}(x)_i = x_{i+2k} \cdot (1 + x_{i+2k-1}) \cdot (1 + x_{i+2k-3}) \cdots (1 + x_{i+1}).$$

With that notation we have

$$\begin{aligned}
\chi^0(x) &= x \\
\chi^1(x) &= x + \gamma_2(x) \\
\chi^2(x) &= x + \gamma_4(x) \\
\chi^3(x) &= x + \gamma_2(x) + \gamma_4(x) + \gamma_6(x) \\
\chi^4(x) &= x + \gamma_8(x).
\end{aligned}$$

What is the general pattern?

Explicit form of χ^k

Definition

The notation $j \preceq k$ means that any power of 2 occuring in the binary expansion of j also appears in the binary expansion of k. We say that j is covered by k.

Example

$$4 = (100)_2 \preceq (101)_2 = 5$$
$$9 = (1001)_2 \preceq (1011)_2 = 11$$
$$27 = (11011)_2 \preceq (11111)_2 = 31$$

Explicit form of χ^k

Theorem

Let $k \geq 1$. Then

$$\chi^k = \sum_{j=0}^{\min\{k,(n-1)/2\}} a_j \gamma_{2j}$$

with $a_j = 1$ if and only if $j \preceq k$.

Explicit form of χ^k

Theorem

Let $k \geq 1$. Then

$$\chi^k = \sum_{j=0}^{\min\{k,(n-1)/2\}} a_j \gamma_{2j}$$

with $a_j = 1$ if and only if $j \preceq k$.

This is very surprising:

1. It is unlikely in general to find any closed form for iterates of functions.

Explicit form of χ^k

Theorem

Let $k \geq 1$. Then

$$\chi^k = \sum_{j=0}^{\min\{k,(n-1)/2\}} a_j \gamma_{2j}$$

with $a_j = 1$ if and only if $j \preceq k$.

This is very surprising:

1. It is unlikely in general to find any closed form for iterates of functions.
2. It is surprising that the iterates are always linear combinations of γ_{2k}.

Explicit form of χ^k

Theorem

Let $k \geq 1$. Then

$$\chi^k = \sum_{j=0}^{\min\{k,(n-1)/2\}} a_j \gamma_{2j}$$

with $a_j = 1$ if and only if $j \preceq k$.

This is very surprising:

1. It is unlikely in general to find any closed form for iterates of functions.
2. It is surprising that the iterates are always linear combinations of γ_{2k}.
3. The coefficients are easy to compute.

New notation

Our previous notation is difficult to use for our purposes.
For example

$$x_{i+1} \circ (x_{i+2} \cdot (1 + x_{i+1})) = x_{i+3} \cdot (1 + x_{i+2}).$$

On the left the x_{i+1} means "add 1 to every index" while on the right x_{i+1} means "(i+1)th entry of x".
$\rightsquigarrow$ We want notation that is better suited for compositions.

New notation

We introduce the cyclic left-shift operator $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$ given by

$$S(x_1, \ldots, x_n) = (x_2, x_3, \ldots, x_n, x_1)$$

and the Hadamard-product $\odot$ given by

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \odot \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 y_1 \\ x_2 y_2 \\ \vdots \\ x_n y_n \end{pmatrix}.$$

New notation

Remember, χ is given by

$$\chi(x)_i = x_i + x_{i+2}(1 + x_{i+1}).$$

In vector form:

$$\chi(x) = \begin{pmatrix} x_1 + x_3(1 + x_2) \\ x_2 + x_4(1 + x_3) \\ x_3 + x_5(1 + x_2) \\ \vdots \\ x_n + x_2(1 + x_1) \end{pmatrix}.$$

New notation

This can also be written as

$$\chi(x) = \begin{pmatrix} x_1 + x_3(1 + x_2) \\ x_2 + x_4(1 + x_3) \\ x_3 + x_5(1 + x_2) \\ \vdots \\ x_n + x_2(1 + x_1) \end{pmatrix}$$

$$= \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} x_3 \\ x_4 \\ x_5 \\ \vdots \\ x_2 \end{pmatrix} \odot \left[\begin{pmatrix} 1 \\ 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} + \begin{pmatrix} x_2 \\ x_3 \\ x_4 \\ \vdots \\ x_1 \end{pmatrix} \right]$$

New notation

This can also be written as

$$\chi(x) = \begin{pmatrix} x_1 + x_3(1+x_2) \\ x_2 + x_4(1+x_3) \\ x_3 + x_5(1+x_2) \\ \vdots \\ x_n + x_2(1+x_1) \end{pmatrix}$$

$$= \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} x_3 \\ x_4 \\ x_5 \\ \vdots \\ x_2 \end{pmatrix} \odot \left[\begin{pmatrix} 1 \\ 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} + \begin{pmatrix} x_2 \\ x_3 \\ x_4 \\ \vdots \\ x_1 \end{pmatrix} \right]$$

$$= x + S^2(x) \odot (\mathbb{1} + S(x)).$$

New notation

Now we can write it as

$$\chi = \mathrm{id} + S^2 \odot (\mathbb{1} + S) = \gamma_0 + \gamma_2$$

where id is the identity function and $\mathbb{1} = (1, 1, \ldots, 1) \in \mathbb{F}_2^n$. Furthermore,

$$\gamma_{2k} = S^{2k} \odot (\mathbb{1} + S^{2k-1}) \odot (\mathbb{1} + S^{2k-3}) \odot \ldots \odot (\mathbb{1} + S)$$

and $\gamma_0 := \mathrm{id}$.

New notation

This notation is better suited for our purposes, for example

$$S \circ (S^2 \odot (\mathbb{1} + S)) = S(S^2 \odot (\mathbb{1} + S)) = S^3 \odot (\mathbb{1} + S^2)$$

compared to

$$x_{i+1} \circ (x_{i+2} \cdot (1 + x_{i+1})) = x_{i+3} \cdot (1 + x_{i+2}).$$

Goal

Goal:

- Study the functions γ_{2k}.
- Obtain results about compositions of the functions γ_{2k}.
- Apply the results to $\chi = \gamma_0 + \gamma_2$.

Basic fact about γ_{2k}

$$\gamma_{2k} = S^{2k} \odot (\mathbb{1} + S^{2k-1}) \odot (\mathbb{1} + S^{2k-3}) \odot \ldots \odot (\mathbb{1} + S)$$

- γ_{2k} is shift-invariant.
- γ_{2k} has algebraic degree $k + 1$ if $2k < n$.

Basic fact about γ_{2k}

Let n be odd.

Lemma

$\gamma_{2k} = 0$ *for* $2k > n$.

Basic fact about γ_{2k}

Let n be odd.

Lemma

$\gamma_{2k} = 0$ *for* $2k > n$.

Proof.

We have $S^{2k} = S^{2k-n}$ and $2k - n$ is odd.

$$\gamma_{2k} = S^{2k} \odot (\mathbb{1} + S^{2k-1}) \odot \ldots \odot (\mathbb{1} + S^{2k-n}) \odot \ldots \odot (\mathbb{1} + S)$$

Basic fact about γ_{2k}

Let n be odd.

Lemma

$\gamma_{2k} = 0$ *for* $2k > n$.

Proof.

We have $S^{2k} = S^{2k-n}$ and $2k - n$ is odd.

$$\begin{aligned}\gamma_{2k} &= S^{2k} \odot (\mathbb{1} + S^{2k-1}) \odot \ldots \odot (\mathbb{1} + S^{2k-n}) \odot \ldots \odot (\mathbb{1} + S) \\ &= S^{2k-n} \odot (\mathbb{1} + S^{2k-n}) \odot (\ldots) = 0.\end{aligned}$$

Basic fact about γ_{2k}

Let n be odd.

Lemma

$\gamma_{2k} = 0$ *for* $2k > n$.

Proof.

We have $S^{2k} = S^{2k-n}$ and $2k - n$ is odd.

$$\begin{aligned}\gamma_{2k} &= S^{2k} \odot (\mathbb{1} + S^{2k-1}) \odot \ldots \odot (\mathbb{1} + S^{2k-n}) \odot \ldots \odot (\mathbb{1} + S) \\ &= S^{2k-n} \odot (\mathbb{1} + S^{2k-n}) \odot (\ldots) = 0.\end{aligned}$$

□

We will revisit this later for n even.

Compositions of the functions γ_{2k}

Key Lemma

It holds that

$$\gamma_{2m}\left(\gamma_0 + \sum_{i=1}^{k} a_i \gamma_{2i}\right) = \sum_{i=0}^{k} a_i \gamma_{2i+2m}.$$

Compositions of the functions γ_{2k}

Key Lemma

It holds that

$$\gamma_{2m}\left(\gamma_0 + \sum_{i=1}^{k} a_i \gamma_{2i}\right) = \sum_{i=0}^{k} a_i \gamma_{2i+2m}.$$

If γ_0 is not included, then the result does not hold. For example

$$\gamma_2 \circ \gamma_2 = S^4 \odot (\mathbb{1} + S^3)$$

is not a linear combination of γ_{2k}.

Generalized χ-maps

Definition

Let G denote the set

$$G = \gamma_0 + \text{span}\{\gamma_2, \gamma_4, \ldots, \gamma_{n-1}\}.$$

Note that $\chi = \gamma_0 + \gamma_2 \in G$. We call the maps in G generalized χ-maps.

Generalized χ-maps

Definition

Let G denote the set

$$G = \gamma_0 + \text{span}\{\gamma_2, \gamma_4, \ldots, \gamma_{n-1}\}.$$

Note that $\chi = \gamma_0 + \gamma_2 \in G$. We call the maps in G generalized χ-maps.

The Key Lemma implies:

Theorem

G is closed under composition. In other words, $(G, \circ)$ is a monoid.

Compositions of the functions γ_{2k}

Key Lemma

It holds that

$$\gamma_{2m}\left(\gamma_0 + \sum_{i=1}^{k} a_i \gamma_{2i}\right) = \sum_{i=0}^{k} a_i \gamma_{2i+2m}.$$

Example

$$\gamma_2 \circ (\gamma_0 + \gamma_4) = \gamma_2 + \gamma_6$$

Compositions of the functions γ_{2k}

Key Lemma

It holds that

$$\gamma_{2m}\left(\gamma_0+\sum_{i=1}^{k}a_i\gamma_{2i}\right)=\sum_{i=0}^{k}a_i\gamma_{2i+2m}.$$

Example

$$\gamma_2\circ(\gamma_0+\gamma_4)=\gamma_2+\gamma_6$$
$$\gamma_4\circ(\gamma_0+\gamma_2+\gamma_6)=\gamma_4+\gamma_6+\gamma_{10}.$$

Compositions of the functions γ_{2k}

Key Lemma

It holds that

$$\gamma_{2m}\left(\gamma_0 + \sum_{i=1}^{k} a_i \gamma_{2i}\right) = \sum_{i=0}^{k} a_i \gamma_{2i+2m}.$$

Example

$$\gamma_2 \circ (\gamma_0 + \gamma_4) = \gamma_2 + \gamma_6$$
$$\gamma_4 \circ (\gamma_0 + \gamma_2 + \gamma_6) = \gamma_4 + \gamma_6 + \gamma_{10}.$$

This looks like polynomial multiplication!

Polynomial interpretation

This looks like polynomial multiplication!

Example

$$\gamma_2 \circ (\gamma_0 + \gamma_4) = \gamma_2 + \gamma_6$$
$$X^2 \cdot (1 + X^4) = X^2 + X^6$$

and

$$\gamma_4 \circ (\gamma_0 + \gamma_2 + \gamma_6) = \gamma_4 + \gamma_6 + \gamma_{10}$$
$$X^4 \cdot (1 + X^2 + X^6) = X^4 + X^6 + X^{10}.$$

Polynomial interpretation

This looks like polynomial multiplication!

Example

$$\gamma_2 \circ (\gamma_0 + \gamma_4) = \gamma_2 + \gamma_6$$
$$X^2 \cdot (1 + X^4) = X^2 + X^6$$

and

$$\gamma_4 \circ (\gamma_0 + \gamma_2 + \gamma_6) = \gamma_4 + \gamma_6 + \gamma_{10}$$
$$X^4 \cdot (1 + X^2 + X^6) = X^4 + X^6 + X^{10}.$$

Observation: γ_{2k} seems to behave like X^{2k}.

Polynomial interpretation

We remove the factor of 2 in the exponent of the polynomials.

Example

$$\gamma_2 \circ (\gamma_0 + \gamma_4) = \gamma_2 + \gamma_6$$
$$X \cdot (1 + X^2) = X + X^3$$

and

$$\gamma_4 \circ (\gamma_0 + \gamma_2 + \gamma_6) = \gamma_4 + \gamma_6 + \gamma_{10}$$
$$X^2 \cdot (1 + X + X^3) = X^2 + X^3 + X^5.$$

Polynomial interpretation

We remove the factor of 2 in the exponent of the polynomials.

Example

$$\gamma_2 \circ (\gamma_0 + \gamma_4) = \gamma_2 + \gamma_6$$
$$X \cdot (1 + X^2) = X + X^3$$

and

$$\gamma_4 \circ (\gamma_0 + \gamma_2 + \gamma_6) = \gamma_4 + \gamma_6 + \gamma_{10}$$
$$X^2 \cdot (1 + X + X^3) = X^2 + X^3 + X^5.$$

Do we get a map

$$\sum_{i=0}^{k} a_i \gamma_{2i} \mapsto \sum_{i=0}^{k} a_i X^i ?$$

Polynomial interpretation

We saw before: $\gamma_{2k} = 0$ for $2k > n$, in particular $\gamma_{n+1} = 0$.

Polynomial interpretation

We saw before: $\gamma_{2k} = 0$ for $2k > n$, in particular $\gamma_{n+1} = 0$.

If we want that the correspondence $\gamma_{2i} \mapsto X^i$ makes sense, we therefore need $X^{(n+1)/2} = 0$.

Polynomial interpretation

We saw before: $\gamma_{2k} = 0$ for $2k > n$, in particular $\gamma_{n+1} = 0$.

If we want that the correspondence $\gamma_{2i} \mapsto X^i$ makes sense, we therefore need $X^{(n+1)/2} = 0$.

Hence, consider the polynomials modulo $X^{(n+1)/2}$, i.e. in the quotient ring $R = \mathbb{F}_2[X]/(X^{(n+1)/2})$. We denote by $[f]$ the coset $f + (X^{(n+1)/2})$.

Polynomial interpretation

We saw before: $\gamma_{2k} = 0$ for $2k > n$, in particular $\gamma_{n+1} = 0$.

If we want that the correspondence $\gamma_{2i} \mapsto X^i$ makes sense, we therefore need $X^{(n+1)/2} = 0$.

Hence, consider the polynomials modulo $X^{(n+1)/2}$, i.e. in the quotient ring $R = \mathbb{F}_2[X]/(X^{(n+1)/2})$. We denote by $[f]$ the coset $f + (X^{(n+1)/2})$.

We obtain a map $\varphi : \mathrm{span}\{\gamma_0, \gamma_2, \ldots, \gamma_{n-1}\} \to R$ defined by

$$\sum_{i=0}^{k} a_i \gamma_{2i} \mapsto \left[\sum_{i=0}^{k} a_i X^i \right].$$

Polynomial interpretation

What is $\varphi(G)$?

Polynomial interpretation

What is $\varphi(G)$?

Denote

$$M = \left\{ \left[1 + \sum_{i=1}^{k} a_i X^i \right] : a_i \in \mathbb{F}_2 \right\} \subseteq R.$$

Polynomial interpretation

What is $\varphi(G)$?

Denote

$$M = \left\{ \left[1 + \sum_{i=1}^{k} a_i X^i \right] : a_i \in \mathbb{F}_2 \right\} \subseteq R.$$

Lemma

M is an Abelian monoid, i.e. M is closed under polynomial multiplication. $\varphi : G \to M$ is a monoid isomorphism. In particular, $G \cong M$ as monoids and G is also an Abelian monoid.

Polynomial interpretation

Lemma

M is an Abelian monoid, i.e. M is closed under polynomial multiplication. $\varphi : G \to M$ is a monoid isomorphism. In particular, $G \cong M$ as monoids and G is also an Abelian monoid.

What does that mean?

Polynomial interpretation

Lemma

M is an Abelian monoid, i.e. M is closed under polynomial multiplication. $\varphi : G \to M$ is a monoid isomorphism. In particular, $G \cong M$ as monoids and G is also an Abelian monoid.

What does that mean?

It means that the composition in G behaves like the multiplication in M.

But the multiplication in M is polynomial multiplication which we understand very well.

It gets even better.

Polynomial interpretation

Definition

The multiplicative invertible elements of a ring R are called units. They form a group, called the unit group R^*.

Lemma

Let $f(X) \in \mathbb{F}_2[X]$ be a polynomial. The unit group of the ring $\mathbb{F}_2[X]/(f(X))$ is given by

$$(\mathbb{F}_2[X]/(f(X)))^* = \{[g(X)] : \gcd(f(X), g(X)) = 1\}.$$

The inverse of $[g(X)]$ can be found by the Extended Euclidean Algorithm.

Polynomial interpretation

In our case $f(X) = X^{(n+1)/2}$ and $\gcd(f(X), g(X)) = 1$ if and only if $g(0) = 1$, in other words, g has constant term 1.

Polynomial interpretation

In our case $f(X) = X^{(n+1)/2}$ and $\gcd(f(X), g(X)) = 1$ if and only if $g(0) = 1$, in other words, g has constant term 1.

Those are exactly the elements of M.

Lemma

M is the unit group of R.

Polynomial interpretation

As M is a group, it follows that G is a group.

Theorem

$G = \gamma_0 + \text{span}\{\gamma_2, \gamma_4, \ldots, \gamma_{n-1}\} \cong M$ is an Abelian group under composition.

Before we go back to studying χ, we look at a few consequences of this theorem.

Implications

Theorem

$G = \gamma_0 + \text{span}\{\gamma_2, \gamma_4, \ldots, \gamma_{n-1}\} \cong M$ *is an Abelian group under composition.*

Let $f \in G$ be arbitrary. Then it holds:

Implications

Theorem

$G = \gamma_0 + \text{span}\{\gamma_2, \gamma_4, \ldots, \gamma_{n-1}\} \cong M$ *is an Abelian group under composition.*

Let $f \in G$ be arbitrary. Then it holds:

1. f is shift-invariant.

Implications

Theorem

$G = \gamma_0 + \text{span}\{\gamma_2, \gamma_4, \ldots, \gamma_{n-1}\} \cong M$ *is an Abelian group under composition.*

Let $f \in G$ be arbitrary. Then it holds:

1. f is shift-invariant.
2. f is a permutation of $\mathbb{F}_2^n$.

Implications

Theorem

$G = \gamma_0 + \text{span}\{\gamma_2, \gamma_4, \ldots, \gamma_{n-1}\} \cong M$ *is an Abelian group under composition.*

Let $f \in G$ be arbitrary. Then it holds:

1. f is shift-invariant.
2. f is a permutation of $\mathbb{F}_2^n$.
3. f^{-1} can be computed using the Extended Euclidean algorithm.

Implications

Theorem

$G = \gamma_0 + \text{span}\{\gamma_2, \gamma_4, \ldots, \gamma_{n-1}\} \cong M$ *is an Abelian group under composition.*

Let $f \in G$ be arbitrary. Then it holds:

1. f is shift-invariant.
2. f is a permutation of $\mathbb{F}_2^n$.
3. f^{-1} can be computed using the Extended Euclidean algorithm.
4. The algebraic degrees of f and f^{-1} are easy to determine.

Implications

We can now easily construct shift-invariant permutations of $\mathbb{F}_2^n$:

Implications

We can now easily construct shift-invariant permutations of $\mathbb{F}_2^n$:

1. Pick any algebraic degree $d \leq (n+1)/2$.

Implications

We can now easily construct shift-invariant permutations of $\mathbb{F}_2^n$:

1. Pick any algebraic degree $d \leq (n+1)/2$.
2. Choose any polynomial $p = \left[1 + \sum_{i=1}^{d-1} a_i X^i\right] \in \mathbb{F}_2[X]/(X^{(n+1)/2})$ of degree $d-1$.

Implications

We can now easily construct shift-invariant permutations of $\mathbb{F}_2^n$:

1. Pick any algebraic degree $d \leq (n+1)/2$.
2. Choose any polynomial $p = \left[1 + \sum_{i=1}^{d-1} a_i X^i\right] \in \mathbb{F}_2[X]/(X^{(n+1)/2})$ of degree $d-1$.
3. The map $f = \gamma_0 + \sum_{i=1}^{d-1} a_i \gamma_{2^i}$ is a shift-invariant permutation of algebraic degree d.

Implications

We can now easily construct shift-invariant permutations of $\mathbb{F}_2^n$:

1. Pick any algebraic degree $d \leq (n+1)/2$.
2. Choose any polynomial $p = \left[1 + \sum_{i=1}^{d-1} a_i X^i\right] \in \mathbb{F}_2[X]/(X^{(n+1)/2})$ of degree $d-1$.
3. The map $f = \gamma_0 + \sum_{i=1}^{d-1} a_i \gamma_{2^i}$ is a shift-invariant permutation of algebraic degree d.
4. Let $q = \left[1 + \sum_{i=1}^{k} b_i X^i\right]$ be the inverse of p.

Implications

We can now easily construct shift-invariant permutations of $\mathbb{F}_2^n$:

1. Pick any algebraic degree $d \leq (n+1)/2$.
2. Choose any polynomial $p = \left[1 + \sum_{i=1}^{d-1} a_i X^i\right] \in \mathbb{F}_2[X]/(X^{(n+1)/2})$ of degree $d-1$.
3. The map $f = \gamma_0 + \sum_{i=1}^{d-1} a_i \gamma_{2^i}$ is a shift-invariant permutation of algebraic degree d.
4. Let $q = \left[1 + \sum_{i=1}^{k} b_i X^i\right]$ be the inverse of p.
5. Then $f^{-1} = \gamma_0 + \sum_{i=1}^{k} b_i \gamma_{2^i}$ has algebraic degree $k+1$.

From here: Study other properties of f and f^{-1}.

The case n even

What happens for n even?

The case n even

What happens for n even?

We go through the last slides and highlight the differences.

The case n even

$$\gamma_{2k} = S^{2k} \odot (\mathbb{1} + S^{2k-1}) \odot (\mathbb{1} + S^{2k-3}) \odot \ldots \odot (\mathbb{1} + S)$$

- γ_{2k} is shift-invariant.
- γ_{2k} has algebraic degree $k+1$ if $2k < n$ and algebraic degree $n/2+1$ for $2k \geq n$.

The case n even

Let n be even.

Lemma

$\gamma_{2k} = \gamma_{2k-n}$ *for* $k \geq n$.

The case n even

Let n be even.

Lemma

$\gamma_{2k} = \gamma_{2k-n}$ *for* $k \geq n$.

Proof.

Similar as before, however now $2k - n$ is still even. □

The case n even

Key Lemma

It holds that

$$\gamma_{2m}\left(\gamma_0 + \sum_{i=1}^{k} a_i \gamma_{2i}\right) = \sum_{i=0}^{k} a_i \gamma_{2i+2m}.$$

The case n even

Definition

Let G denote the set

$$G = \gamma_0 + \text{span}\{\gamma_2, \gamma_4, \ldots, \gamma_n, \ldots, \gamma_{2n-2}\}.$$

Note that $\chi = \gamma_0 + \gamma_2 \in G$. We call the maps in G generalized χ-maps.

The case n even

Definition

Let G denote the set

$$G = \gamma_0 + \text{span}\{\gamma_2, \gamma_4, \ldots, \gamma_n, \ldots, \gamma_{2n-2}\}.$$

Note that $\chi = \gamma_0 + \gamma_2 \in G$. We call the maps in G generalized χ-maps.

The Key Lemma implies:

Theorem

G is closed under composition. In other words, $(G, \circ)$ is a monoid.

The case n even

Example

$$\gamma_2 \circ (\gamma_0 + \gamma_4) = \gamma_2 + \gamma_6$$
$$X \cdot (1 + X^2) = X + X^3$$

and

$$\gamma_4 \circ (\gamma_0 + \gamma_2 + \gamma_6) = \gamma_4 + \gamma_6 + \gamma_{10}$$
$$X^2 \cdot (1 + X + X^3) = X^2 + X^3 + X^5.$$

Do we get a map

$$\sum_{i=0}^{k} a_i \gamma_{2i} \mapsto \sum_{i=0}^{k} a_i X^i ?$$

The case n even

We saw before: $\gamma_{2k} + \gamma_{2k-n} = 0$ for $k \geq n$, in particular $\gamma_{2n} + \gamma_n = 0$.

If we want that the correspondence $\gamma_{2i} \mapsto X^i$ makes sense, we therefore need $X^n + X^{n/2} = 0$.

Hence, consider the polynomials modulo $X^n + X^{n/2}$, i.e. in the quotient ring $R = \mathbb{F}_2[X]/(X^n + X^{n/2})$. We denote by $[f]$ the coset $f + (X^n + X^{n/2})$.

We obtain a map $\varphi : \mathrm{span}\{\gamma_0, \gamma_2, \ldots, \gamma_n, \ldots, \gamma_{2n-2}\} \to R$ defined by

$$\sum_{i=0}^{k} a_i \gamma_{2i} \mapsto \left[\sum_{i=0}^{k} a_i X^i \right].$$

The case n even

What is $\varphi(G)$?

Denote

$$M = \left\{ \left[1 + \sum_{i=1}^{k} a_i X^i \right] : a_i \in \mathbb{F}_2 \right\} \subseteq R.$$

Lemma

M is an Abelian monoid, i.e. M is closed under polynomial multiplication. $\varphi : G \to M$ is a monoid isomorphism. In particular, $G \cong M$ as monoids and G is also an Abelian monoid.

The case n even

For n odd we had:
$f(X) = X^{(n+1)/2}$ and $\gcd(f(X), g(X)) = 1$ if and only if $g(0) = 1$.

The case n even

For n odd we had:
$f(X) = X^{(n+1)/2}$ and $\gcd(f(X), g(X)) = 1$ if and only if $g(0) = 1$.

Now for n even we have:
$f = X^n + X^{n/2} = X^{n/2}(1 + X^{n/2})$ and the condition $\gcd(f(X), g(X)) = 1$ now does *not* have such a simple characterization.

The case n even

For n odd we had:
$f(X) = X^{(n+1)/2}$ and $\gcd(f(X), g(X)) = 1$ if and only if $g(0) = 1$.

Now for n even we have:
$f = X^n + X^{n/2} = X^{n/2}(1 + X^{n/2})$ and the condition $\gcd(f(X), g(X)) = 1$ now does *not* have such a simple characterization.

Lemma

The unit group of R is a proper subset of M.

The case n even

Theorem

A proper subset of $G = \gamma_0 + \text{span}\{\gamma_2, \gamma_4, \ldots, \gamma_n, \ldots, \gamma_{2n-2}\} \cong M$ *is an Abelian group under composition.*

Example

We know that $\chi = \gamma_0 + \gamma_2$ is not a permutation. Why?
$\varphi(\chi) = [1 + X]$ is not invertible in $\mathbb{F}_2[X]/(X^n + X^{n/2})$ because $\gcd(1 + X, X^n + X^{n/2}) = 1 + X \neq 1$.

The case n even

We can now easily construct shift-invariant permutations of $\mathbb{F}_2^n$:

1. Pick any algebraic degree $d \leq n/2 + 1$.
2. Choose any invertible polynomial $p = \left[1 + \sum_{i=1}^{m} a_i X^i\right] \in \mathbb{F}_2[X]/(X^n + X^{n/2})$ of degree $m = d - 1$ or if $d = n/2 + 1$, then arbitrary degree $m \geq d - 1$.
3. The map $f = \gamma_0 + \sum_{i=1}^{d-1} a_i \gamma_{2i}$ is a shift-invariant permutation of algebraic degree d.
4. Let $q = \left[1 + \sum_{i=1}^{k} b_i X^i\right]$ be the inverse of p.
5. Then $f^{-1} = \gamma_0 + \sum_{i=1}^{k} b_i \gamma_{2i}$ has algebraic degree $\min(k + 1, n/2 + 1)$.

From here: Study other properties of f and f^{-1}.

The case n even

Example

The polynomial $[1 + X + X^2] \in \mathbb{F}_2[X]/(X^n + X^{n/2})$ is invertible if and only if n is not a multiple of 6.

This gives a shift-invariant permutation $f = \gamma_0 + \gamma_2 + \gamma_4 = \chi + \gamma_4$ of algebraic degree 3.

Due to the similarity to χ this map might be interesting from a cryptographic perspective.

The case n even

A special case is $n = 2^k$.

We have $f(X) = X^{2^k} + X^{2^{k-1}} = X^{2^{k-1}}(1+X)^{2^{k-1}}$. In particular:

$\gcd(f(X), g(X)) = 1$ iff $g(0) = g(1) = 1$. In other words, g has constant coefficient 1 and an odd number of terms.

Theorem

Let $n = 2^k$. Any map $f \in \gamma_0 + \mathrm{span}\{\gamma_2, \ldots, \gamma_{2n-2}\}$ with an odd number of terms is a permutation of $\mathbb{F}_2^n$.

Iterates of χ

Let n be odd again.

We return to our study of χ.

We started this talk by looking at the iterates χ^k of χ.

How can we now use the previously discovered tools?

Iterates of χ

We have $\varphi(\chi) = [1 + X] \in \mathbb{F}_2[X]/(X^{(n+1)/2})$ and therefore $\varphi(\chi^k) = [1 + X]^k$.

Iterates of χ

We have $\varphi(\chi) = [1 + X] \in \mathbb{F}_2[X]/(X^{(n+1)/2})$ and therefore $\varphi(\chi^k) = [1 + X]^k$.

By the Binomial Theorem we have

$$[1 + X]^k = \left[\sum_{j=0}^{k} \binom{k}{j} X^j \right].$$

Iterates of χ

We have $\varphi(\chi) = [1 + X] \in \mathbb{F}_2[X]/(X^{(n+1)/2})$ and therefore $\varphi(\chi^k) = [1 + X]^k$.

By the Binomial Theorem we have

$$[1 + X]^k = \left[\sum_{j=0}^{k} \binom{k}{j} X^j\right].$$

From Lucas's Theorem we know $\binom{k}{j}$ is odd if and only if $j \preceq k$. Therefore

$$[1 + X]^k = \left[\sum_{j=0}^{k} \binom{k}{j} X^j\right] = \left[\sum_{j=0}^{k} a_j X^j\right] = \left[\sum_{j=0}^{\min\{k,(n-1)/2\}} a_j X^j\right].$$

Iterates of χ

Theorem

Let $k \geq 1$. Then

$$\chi^k = \sum_{j=0}^{\min\{k,(n-1)/2\}} a_j \gamma_{2j}$$

with $a_j = 1$ if and only if $j \preceq k$.

Iterates of χ

We saw previously:

$$
\begin{aligned}
\chi^0(x) &= x \\
\chi^1(x) &= x + \gamma_2(x) \\
\chi^2(x) &= x \qquad\qquad + \gamma_4(x) \\
\chi^3(x) &= x + \gamma_2(x) + \gamma_4(x) + \gamma_6(x) \\
\chi^4(x) &= x \qquad\qquad\qquad\qquad\qquad + \gamma_8(x).
\end{aligned}
$$

Iterates of χ

We saw previously:

$$\begin{aligned}
\chi^0(x) &= x \\
\chi^1(x) &= x + \gamma_2(x) \\
\chi^2(x) &= x + \gamma_4(x) \\
\chi^3(x) &= x + \gamma_2(x) + \gamma_4(x) + \gamma_6(x) \\
\chi^4(x) &= x + \gamma_8(x).
\end{aligned}$$

We now have the explanation:

$$\begin{aligned}
(1+X)^0 &= 1 \\
(1+X)^1 &= 1 + X \\
(1+X)^2 &= 1 + X^2 \\
(1+X)^3 &= 1 + X + X^2 + X^3 \\
(1+X)^4 &= 1 + X^4.
\end{aligned}$$

Further implications?

Is it possible to use these tools to attack one of the primitives using χ?

We have an idea but we need help from experts!

We are happy to discuss.

An attack?

The following are known:

- The order of χ is 2^m with $2^m < n+1 \leq 2^{m+1}$.[3]
- The algebraic degree of χ^{-1} is $(n+1)/2$.

How are these connected?

[3] Jan Schoone and Joan Daemen. "The state diagram of χ". In: *Designs, Codes and Cryptography* 92 (2024), pp. 1393–1421. DOI: 10.1007/s10623-023-01349-8.

An attack?

χ having order 2^m means that $\chi^{2^m} = \mathrm{id}$.

In other words, for any fixed $x \in \mathbb{F}_2^n$ we have $\chi^{2^m}(x) = x$. This means $\chi^{2^m-1}(\chi(x)) = x$. Therefore $\chi^{2^m-1} = \chi^{-1}$ is the inverse of χ.

An attack?

Let $x \in \mathbb{F}_2^n$ be fixed. We have the following sequence:

$$\begin{aligned} x &\mapsto \chi(x) \\ &\mapsto \chi(\chi(x)) \\ &\mapsto \dots \\ &\mapsto \underbrace{\chi(\dots(\chi(x)))}_{2^m \text{ times}} = x \end{aligned}$$

When is the first time (after the beginning) that x appears in that sequence?

An attack?

Suppose that

$$x \mapsto \chi(x) \mapsto \ldots \mapsto \underbrace{\chi(\ldots(\chi(x)))}_{k \text{ times}} = x$$

with minimal k. We say that x has order k under χ. x is included in a cycle of length k in the cycle structure of χ.

An attack?

Suppose that

$$x \mapsto \chi(x) \mapsto \ldots \mapsto \underbrace{\chi(\ldots(\chi(x)))}_{k \text{ times}} = x$$

with minimal k. We say that x has order k under χ. x is included in a cycle of length k in the cycle structure of χ.

It holds that

$$\chi^{k-1}(\chi(x)) = x.$$

In other words, for this fixed x the map χ^{k-1} is inverting χ.

If k is fixed, then how many elements of order k are there?

An attack?

Define

$$C_{k,n} = \{x \in \mathbb{F}_2^n \setminus \{0\} : \gamma_{2k}(x) = 0\}$$

and $c(k, n) = |C_{k,n}|$.

Lemma

All cycles of χ have length $k = 2^s$ for some $0 \leq s \leq m$. The number of nonzero elements of order $\leq 2^s$ is given by $c(2^s, n)$.

An attack?

We can show that the generating function of $c(k,n)$ equals

$$\sum_{n\geq 0} c(k,n)x^n = \frac{xB_k'(x)}{1-B_k(x)}$$

where $B_k(x) = x + 2x^3 + 4x^5 + \ldots + 2^{k-1}x^{2k-1}$.
An explicit formula for $c(k,n)$ is given by

$$c(k,n) = \sum_{N=0}^{n\cdot\frac{k-1}{2k-1}} \frac{n2^N}{n-2N} \sum_{q=0}^{N/k} (-1)^q \binom{n-2N}{q} \binom{n-N-qk-1}{n-2N-1}.$$

An attack?

Let $n = 257$.

k	$c(k, n)$	$c(k, n)/2^n$	$(2^n - c(k, n))/2^n$
1	1.000	4.318e-78	1.000
2	8.659e58	3.739e-19	1.000
4	3.139e74	0.001355	0.9986
8	1.645e77	0.7104	0.2896
16	2.313e77	0.9987	0.001307
32	2.316e77	1.000	1.995e-8
64	2.316e77	1.000	4.644e-18
128	2.316e77	1.000	3.776e-37
256	2.316e77	1.000	4.318e-78

An attack?

Let $n = 257$.

k	$c(k, n)$	$c(k, n)/2^n$	$(2^n - c(k, n))/2^n$
8	1.645e77	0.7104	0.2896
16	2.313e77	0.9987	0.001307

- Over 71% of elements of $\mathbb{F}_2^{257}$ have order ≤ 8.
- Over 99% of elements of $\mathbb{F}_2^{257}$ have order ≤ 16.

What does that mean?

An attack?

- Over 71% of elements of $\mathbb{F}_2^{257}$ have order ≤ 8.
- Over 99% of elements of $\mathbb{F}_2^{257}$ have order ≤ 16.

Let $x \in \mathbb{F}_2^n$ be arbitrary.

- With $\approx 71\%$ probability we have $\chi^7(\chi(x)) = x$, i.e. we can invert χ with χ^7 which has degree 8.
- With $> 99\%$ probability we have $\chi^{15}(\chi(x)) = x$, i.e. we can invert χ with χ^{15} which has degree 16.

Meanwhile, χ^{-1} has degree 129.

How significant is that for an algebraic attack?

Source

For more details:

- n odd: Björn Kriepke and Gohar Kyureghyan. "Algebraic Structure of the Iterates of χ". In: *Advances in Cryptology – CRYPTO 2024*. Ed. by Leonid Reyzin and Douglas Stebila. Cham: Springer Nature Switzerland, 2024, pp. 412–424. ISBN: 978-3-031-68385-5
- n even: In preparation

Thank you for your attention.