Algebraic Structure of the Iterates of χ

Björn Kriepke Gohar Kyureghyan

University of Rostock, Germany

CRYPTO 2024, August 19

The map χ

- First introduced by 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

Let n be odd.

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

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

where the indices are taken modulo n.

The map χ

Let n be odd.

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

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

where the indices are taken modulo n.

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

$\rightsquigarrow \chi$ flips the bit x_i if and only if x_i is followed by the pattern 01.

The map χ

Let n be odd.

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

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

where the indices are taken modulo n.

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

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

The map χ, an example

Example $n = 9$.

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

$$\chi(x) =$$

The map χ, an example

Example $n = 9$.

$$\begin{array}{ccccccccccc} x & = & {\color{red}1} & {\color{green}1} & {\color{green}0} & 1 & 1 & 0 & 1 & 0 & 0 \\ & & \downarrow & & & & & & & & \\ \chi(x) & = & 1 & & & & & & & & \end{array}$$

The map χ, an example

Example $n = 9$.

$$\begin{array}{ccccccccccc} x & = & 1 & {\color{red}1} & {\color{green}0} & {\color{green}1} & 1 & 0 & 1 & 0 & 0 \\ & & & \downarrow & & & & & & & \\ \chi(x) & = & 1 & 0 & & & & & & & \end{array}$$

The map χ, an example

Example $n = 9$.

$$
\begin{array}{ccccccccccc}
x & = & \color{green}{1} & 1 & 0 & 1 & 1 & 0 & 1 & \color{red}{0} & \color{green}{0} \\
 & & & & & & & & & \downarrow & \\
\chi(x) & = & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 &
\end{array}
$$

The map χ, an example

Example $n = 9$.

$$\begin{array}{ccccccccccc} x & = & {\color{green}1} & {\color{green}1} & 0 & 1 & 1 & 0 & 1 & 0 & {\color{red}0} \\ & & & & & & & & & & \downarrow \\ \chi(x) & = & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \end{array}$$

Iterates of χ

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

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

for $j \geq 1$.

Warm-up

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

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

Warm-up

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

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

Warm-up

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

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

Warm-up

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

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

Warm-up

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

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

Warm-up

Similarly,

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

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

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

What is the general pattern?

New notation

Our previous notation is ill-suited for our purposes.
For example

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

$\rightsquigarrow$ 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

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

This can also be written as

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

New notation

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

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

Compositions of the functions γ_{2k}

Goal:

- Study how the composition of the functions γ_{2k} and their linear combination works.
- Apply the results to $\chi = \gamma_0 + \gamma_2$.

Compositions of the functions γ_{2k}

Key Lemma. It holds that

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

It is very surprising that such a composition is again a linear combination of the functions γ_{2k}.

Compositions of the functions γ_{2k}

Key Lemma. It holds that

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

It is very surprising that such a composition is again a linear combination of the functions γ_{2k}.

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

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

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

Compositions of the functions γ_{2k}

Key Lemma, 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, 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!

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

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

This looks like polynomial multiplication!

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

and

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

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

Polynomial interpretation

γ_{n+1} is the zero map, so $X^{(n+1)/2}$ should also be zero.

Polynomial interpretation

γ_{n+1} is the zero map, so $X^{(n+1)/2}$ should also be zero.

$\rightsquigarrow$ Consider the polynomials modulo $X^{(n+1)/2}$, i.e. in the quotient ring $R = \mathbb{F}_2[X]/(X^{(n+1)/2})$.

Polynomial interpretation

γ_{n+1} is the zero map, so $X^{(n+1)/2}$ should also be zero.

$\rightsquigarrow$ Consider the polynomials modulo $X^{(n+1)/2}$, i.e. in the quotient ring $R = \mathbb{F}_2[X]/(X^{(n+1)/2})$.

Lemma. The composition of functions in G behaves exactly like polynomial multiplication for polynomials of the form $1 + \sum_{i=1}^{k} a_i X^i$ in the ring $R = \mathbb{F}_2[X]/(X^{(n+1)/2})$.

Polynomial interpretation

Lemma. The composition of functions in G behaves exactly like polynomial multiplication for polynomials of the form $1 + \sum_{i=1}^{k} a_i X^i$ in the ring $R = \mathbb{F}_2[X]/(X^{(n+1)/2})$.

Polynomial interpretation

Lemma. The composition of functions in G behaves exactly like polynomial multiplication for polynomials of the form $1 + \sum_{i=1}^{k} a_i X^i$ in the ring $R = \mathbb{F}_2[X]/(X^{(n+1)/2})$.

The polynomials of the form $1 + \sum_{i=1}^{k} a_i X^i$ are all multiplicatively invertible in R, in fact they form the unit group of R.
Furthermore, clearly polynomial multiplication is commutative.

Polynomial interpretation

Lemma. The composition of functions in G behaves exactly like polynomial multiplication for polynomials of the form $1 + \sum_{i=1}^{k} a_i X^i$ in the ring $R = \mathbb{F}_2[X]/(X^{(n+1)/2})$.

The polynomials of the form $1 + \sum_{i=1}^{k} a_i X^i$ are all multiplicatively invertible in R, in fact they form the unit group of R.
Furthermore, clearly polynomial multiplication is commutative.

Theorem. G is an Abelian group under composition, in particular **every** function in G is a permutation.

Iterates of χ

We can now apply these results to $\chi = \gamma_0 + \gamma_2$, which behaves like $1 + X$.

Composition of χ corresponds to exponentiation of $1 + X$.

Iterates of χ

We saw previously:

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

Iterates of χ

We saw previously:

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

We now have the explanation:

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

Thank you for your attention.