How to Find and Prove the Inverse of χ

Fukang Liu[1], Santanu Sarkar[2], Willi Meier[3], Takanori Isobe[4,5]

[1]Tokyo Institute of Technology, Tokyo, Japan

[2]Indian Institute of Technology Madras, Chennai, India

[3]FHNW, Windisch, Switzerland

[4]University of Hyogo, Hyogo, Japan

[5]NICT, Tokyo, Japan

PBC 2023

Overview

The χ_n Operation

- Invented by Joan Daemen (Ph.D. thesis)
- Implementation: easy to mask & high performance
- Applications: Keccak, Ascon, Rasta, Subterranean 2.0

Definition 1

For an odd integer $n \geq 3$, the n-bit nonlinear transform $\chi_n : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ is defined as

$$y_i = x_i + \overline{x_{i+1}} x_{i+2}, \ \ i \in [0, n-1] \tag{1}$$

where $X = (x_0, \ldots, x_{n-1})$ and $Y = (y_0, \ldots, y_{n-1})$ are input and output bits, respectively.

The Inverse of χ_n

- Proof of invertibility: **seed-and-leap** (Daemen's thesis)
  - **Seed**: Find an index j such that $y_{j+1} = 1$. Then, $x_j = y_j$.
  - **Leap**: If x_j is known, x_{j-2} can be found. Since n is an odd number, all $(x_i)_{0 \le i \le n-1}$ can be found by repeating this step.

- Correctness (from an algebraic perspective):

$$\begin{aligned} y_{j-2} &= x_{j-2} + \overline{x_{j-1}} x_j, \\ y_{j-1} &= x_{j-1} + \overline{x_j} x_{j+1}, \\ y_j &= x_j + \overline{x_{j+1}} x_{j+2}, \\ y_{j+1} &= x_{j+1} + \overline{x_{j+2}} x_{j+3}, \end{aligned}$$

Seed: $\overline{x_{j+1}} = \overline{x_{j+2}} x_{j+3}$ if $y_{j+1} = 1 \rightarrow \overline{x_{j+1}} x_{j+2} = 0$

The Inverse of χ_n

Degree of χ_n^{-1} : $(n+1)/2$ (AC 2014[1], Biryukov et al.)

1: $(x_0, x_1, \ldots, x_{n-1}) \leftarrow (y_0, y_1, \ldots, y_{n-1})$
2: **for** $0 \le i < \frac{3(n-1)}{2}$ **do**
3: $\quad x_{(n-2)i} \leftarrow x_{(n-2)i} + x_{(n-2)i+2} \cdot \overline{x_{(n-2)i+1}}$
4: **end for**
5: return $(x_0, x_1, \ldots, x_{n-1})$

[1] Cryptographic Schemes Based on the ASASA Structure: Black-box, White-box, and Public-key

The Inverse of χ_n

A small example for χ_9^{-1}:

$$
\begin{aligned}
i = 0: &\qquad x_0 = y_0 + y_2\overline{y_1}, \\
i = 1: &\qquad x_7 = y_7 + x_0\overline{y_8}, \\
i = 2: &\qquad x_5 = y_5 + x_7\overline{y_6}, \\
i = 3: &\qquad x_3 = y_3 + x_5\overline{y_4}.
\end{aligned}
$$

Hence, the expression of x_3 in terms of Y is

$$x_3 = y_3 + (y_5 + (y_7 + (y_0 + y_2\overline{y_1})\overline{y_8})\overline{y_6})\overline{y_4}.$$

The Inverse of χ_n

How the algorithm ends for χ_9^{-1}:

$$\begin{aligned}
i = 4: &\qquad x_1 = y_1 + x_3\overline{y_2},\\
i = 5: &\qquad x_8 = y_8 + x_1\overline{x_0},\\
i = 6: &\qquad x_6 = y_6 + x_8\overline{x_7},\\
i = 7: &\qquad x_4 = y_4 + x_6\overline{x_5},\\
i = 8: &\qquad x_2 = y_2 + x_4\overline{x_3},\\
i = 9: &\qquad x_0 = y_0 + x_2\overline{x_1},\\
i = 10: &\qquad x_7 = y_7 + x_0\overline{x_8},\\
i = 11: &\qquad x_5 = y_5 + x_7\overline{x_6}.
\end{aligned}$$

The order to compute $(x_0, \ldots, x_8)$:

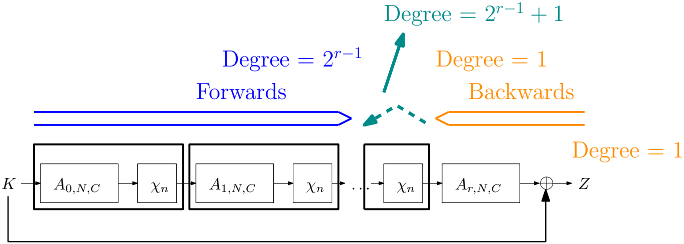
$$x_3 \to x_1 \to x_8 \to x_6 \to \cdots \to x_7 \to x_5.$$

The Inverse of χ_n

No explicit formula and the corresponding proof.

Too long to write down? (degree: $(n+1)/2$)

Motivation



An efficient way to find low-degree equations for r-round Rasta[2]:

$$P(Y) + \sum_{j=0}^{n-1} x_j L_j(Y) + c = 0,$$

where $Deg(P) \leq 2^{r-1} + 1$, $Deg(L_j) \leq 1$ and $c \in \mathbb{F}_2$ is a constant.

[2] Algebraic Attacks on Rasta and Dasta Using Low-Degree Equations

Observations

Low-degree equations found via experiments/observations:

$$
\begin{aligned}
0 &= x_i + \overline{y_{i+1}} x_{i+2} + y_i, \\
0 &= y_{i+1}(x_i + y_i), \\
0 &= y_{i+3}(x_i + y_i + y_{i+2}\overline{y_{i+1}}), \\
0 &= y_{i+5}(x_i + x_{i+2} + y_i + y_{i+1}y_{i+2} + y_{i+1}\overline{y_{i+3}}y_{i+4}), \\
0 &= y_{i+7}(x_i + y_i + y_{i+6}\overline{y_{i+5}}\ \overline{y_{i+3}}\ \overline{y_{i+1}} + y_{i+4}\overline{y_{i+3}}\ \overline{y_{i+1}} + y_{i+2}\overline{y_{i+1}}).
\end{aligned}
$$

Observations

Observation 1

All these 5 polynomials belong to the ideal $\mathcal{I} = \langle f_0, \dots, f_{n-1} \rangle$, where

$$f_i = y_i + x_i + \overline{y_{i+1}} x_{i+2}. \tag{2}$$

Note that $f_i = 0$ is a low-degree equation, i.e. $f_i = 0$ holds for all (X, Y) satisfying $Y = \chi_n(X)$.

More such (linearly independent) polynomials in $\mathcal{I}$?

Observations

Why do we need these polynomials?

Note 1

Note that for a polynomial $p_i \in \mathcal{I}$, by definition of an ideal, there must exist polynomials $h_0, \ldots, h_{n-1} \in \mathbb{F}_2[X, Y]$ such that

$$p_i = \sum_{i=0}^{n-1} h_i f_i$$

and hence $p_i = 0$ holds for all (X, Y) satisfying $Y = \chi_n(X)$.

Especially, if p_i is also of the following form

$$P(Y) + \sum_{j=0}^{n-1} x_j L_j(Y) + c,$$

it can be used for attacks on Rasta.

Observations

Initial Idea

Consider $x_i y_{i+j}$ and use the division algorithm to compute the remainder of $x_i y_{i+j} / \langle f_0, \ldots, f_{n-1} \rangle$.

- case 1: $j = 2t$.
- case 2: $j = 2t + 1$.

Observations

Small examples (case 2): $i = 0, j = 2t + 1 = 7$

$$x_0 y_7 / \langle f_0, f_1, \ldots, f_{n-1} \rangle, \;\; n \geq 9.$$

The procedure[3] is to iteratively compute N_{i+1} and R_i:

$$N_i \;\; = \;\; Q_i D_i + N_{i+1} + R_i,$$

where

$$N_0 = x_0 y_7, \;\; D_i \in \{f_0, \ldots, f_{n-1}\}, \;\; R_i \in \mathbb{F}_2[y_0, y_1, \ldots, y_{n-1}].$$

Then, we know $N_0 + \sum_{j=0}^{i} R_j \in \mathcal{I}$ if finally $N_{i+1} = 0$, i.e. we expect that the remainder will finally be in $\mathbb{F}_2[y_0, y_1, \ldots, y_{n-1}]$.

[3] N_i : numerator, D_i : divisor, Q_i: quotient, $N_{i+1} + R_i$: remainder

Observations

i	N_i	D_i	Q_i	R_i
0	$x_0 y_7$	$f_0 = x_0 + x_2 y_1 + x_2 + y_0$	y_7	$y_0 y_7$
1	$x_2 y_1 y_7 + x_2 y_7$	$f_2 = x_2 + x_4 y_3 + x_4 + y_2$	$y_1 y_7$	$y_1 y_2 y_7$
2	$x_2 y_7 + x_4 y_1 y_3 y_7 + x_4 y_1 y_7$	$f_2 = x_2 + x_4 y_3 + x_4 + y_2$	y_7	$y_2 y_7$
3	$x_4 y_1 y_3 y_7 + x_4 y_1 y_7$ $+ x_4 y_3 y_7 + x_4 y_7$	$f_4 = x_4 + x_6 y_5 + x_6 + y_4$	$y_1 y_3 y_7$	$y_1 y_3 y_4 y_7$
4	$x_4 y_1 y_7 + x_4 y_3 y_7 + x_4 y_7$ $+ x_6 y_1 y_3 y_5 y_7 + x_6 y_1 y_3 y_7$	$f_4 = x_4 + x_6 y_5 + x_6 + y_4$	$y_1 y_7$	$y_1 y_4 y_7$
5	$x_4 y_3 y_7 + x_4 y_7 + x_6 y_1 y_3 y_5 y_7$ $+ x_6 y_1 y_3 y_7 + x_6 y_1 y_5 y_7 + x_6 y_1 y_7$	$f_4 = x_4 + x_6 y_5 + x_6 + y_4$	$y_3 y_7$	$y_3 y_4 y_7$
6	$x_4 y_7 + x_6 y_1 y_3 y_5 y_7 + x_6 y_1 y_3 y_7$ $+ x_6 y_1 y_5 y_7 + x_6 y_1 y_7$ $+ x_6 y_3 y_5 y_7 + x_6 y_3 y_7$	$f_4 = x_4 + x_6 y_5 + x_6 + y_4$	y_7	$y_4 y_7$
7	$x_6 y_1 y_3 y_5 y_7 + x_6 y_1 y_3 y_7$ $+ x_6 y_1 y_5 y_7 + x_6 y_1 y_7 + x_6 y_3 y_5 y_7$ $+ x_6 y_3 y_7 + x_6 y_5 y_7 + x_6 y_7$	$f_6 = x_6 + x_8 y_7 + x_8 + y_6$	$y_1 y_3 y_5 y_7$	$y_1 y_3 y_5 y_6 y_7$

Observations

i	N_i	D_i	Q_i	R_i
8	$x_6y_1y_3y_7$ $+x_6y_1y_5y_7+x_6y_1y_7+x_6y_3y_5y_7$ $+x_6y_3y_7+x_6y_5y_7+x_6y_7$	$f_6=x_6+x_8y_7+x_8+y_6$	$y_1y_3y_7$	$y_1y_3y_6y_7$
9	$x_6y_1y_5y_7+x_6y_1y_7+x_6y_3y_5y_7$ $+x_6y_3y_7+x_6y_5y_7+x_6y_7$	$f_6=x_6+x_8y_7+x_8+y_6$	$y_1y_5y_7$	$y_1y_5y_6y_7$
10	$x_6y_1y_7+x_6y_3y_5y_7$ $+x_6y_3y_7+x_6y_5y_7+x_6y_7$	$f_6=x_6+x_8y_7+x_8+y_6$	y_1y_7	$y_1y_6y_7$
11	$x_6y_3y_5y_7$ $+x_6y_3y_7+x_6y_5y_7+x_6y_7$	$f_6=x_6+x_8y_7+x_8+y_6$	$y_3y_5y_7$	$y_3y_5y_6y_7$
12	$x_6y_3y_7+x_6y_5y_7+x_6y_7$	$f_6=x_6+x_8y_7+x_8+y_6$	y_3y_7	$y_3y_6y_7$
13	$x_6y_5y_7+x_6y_7$	$f_6=x_6+x_8y_7+x_8+y_6$	y_5y_7	$y_5y_6y_7$
14	x_6y_7	$f_6=x_6+x_8y_7+x_8+y_6$	y_7	y_6y_7
15	0			

Observations

$$
\begin{aligned}
x_0 y_7 &= y_7 f_0 \\
&+ (y_1 y_7 + y_7) f_2 \\
&+ (y_1 y_3 y_7 + y_1 y_7 + y_3 y_7 + y_7) f_4 \\
&+ (y_1 y_3 y_5 y_7 + y_1 y_3 y_7 + y_1 y_5 y_7 + y_1 y_7 + y_3 y_5 y_7 + y_3 y_7 \\
&+ y_5 y_7 + y_7) f_6 + r_n,
\end{aligned}
$$

where

$$
\begin{aligned}
r_n &= y_7 y_0 \\
&= (y_1 y_7 + y_7) y_2 \\
&+ (y_1 y_3 y_7 + y_1 y_7 + y_3 y_7 + y_7) y_4 \\
&+ (y_1 y_3 y_5 y_7 + y_1 y_3 y_7 + y_1 y_5 y_7 \\
&+ y_1 y_7 + y_3 y_5 y_7 + y_3 y_7 + y_5 y_7 + y_7) y_6 .
\end{aligned}
$$

Observations

Small examples (case 1): $i = 1, j = 2t = 4$

$$x_1 y_5 / \langle f_0, f_1, \ldots, f_6 \rangle$$

i	N_i	D_i	Q_i	R_i
0	$x_1 y_5$	$f_1 = x_1 + x_3\overline{y_2} + y_1$	y_5	$y_1 y_5$
1	$x_3\overline{y_2}y_5$	$f_3 = x_3 + x_5\overline{y_4} + y_3$	$\overline{y_2}y_5$	$\overline{y_2}y_3y_5$
2	$x_5\overline{y_2}\ \overline{y_4}y_5$	$f_5 = x_5 + x_0\overline{y_6} + y_5$	$\overline{y_2}\ \overline{y_4}y_5$	$\overline{y_2}\ \overline{y_4}y_5$
3	$x_0\overline{y_2}\ \overline{y_4}y_5\overline{y_6}$	$f_0 = x_0 + x_2\overline{y_1} + y_0$	$\overline{y_2}\ \overline{y_4}y_5\overline{y_6}$	$y_0\overline{y_2}\ \overline{y_4}y_5\overline{y_6}$
4	$x_2\overline{y_1}\ \overline{y_2}\ \overline{y_4}y_5\overline{y_6}$	$f_2 = x_2 + x_4\overline{y_3} + y_2$	$\overline{y_1}\ \overline{y_2}\ \overline{y_4}y_5\overline{y_6}$	0
5	$x_4\overline{y_1}\ \overline{y_2}\ \overline{y_3}\ \overline{y_4}y_5\overline{y_6}$	$f_4 = x_4 + x_6\overline{y_5} + y_4$	$\overline{y_1}\ \overline{y_2}\ \overline{y_3}\ \overline{y_4}y_5\overline{y_6}$	0
6	0			

$$\begin{aligned} x_1 y_5 &= y_1 y_5 + \overline{y_2}y_3y_5 + \overline{y_2}\ \overline{y_4}y_5 + y_0\overline{y_2}\ \overline{y_4}y_5\overline{y_6} \\ &= y_5\left(y_1 + \overline{y_2}y_3 + \overline{y_4}y_5 + y_0\overline{y_2}\ \overline{y_4}\ \overline{y_6}\right) \end{aligned}$$

Observations

- Studying the remainder of $x_i y_{i+2t+1}/\langle f_0, \ldots, f_{n-1}\rangle$ may give us the formula of low-degree equations for Rasta.
- Studying the remainder of $x_i y_{i+2t}/\langle f_0, \ldots, f_{n-1}\rangle$ may give us the formula of χ_n^{-1}.

If the formula of χ_n^{-1} is known, we should be able to know what $x_i y_j$ exactly is for any (i, j).

Lemma

Lemma 1

For a given pair (i, j) satisfying $i, j \in [0, n-1]$, if there exist $n+1$ polynomials $r_{0,i}, \ldots, r_{n,i} \in \mathbb{F}_2[y_0, y_2, \ldots, y_{n-1}]$ such that

$$x_i y_j \quad = \quad \sum_{k=0}^{n-1} r_{k,i} f_k + r_{n,i},$$

there must exist $n+1$ polynomials
$r_{0,i+1}, \ldots, r_{n,i+1} \in \mathbb{F}_2[y_1, y_2, \ldots, y_n]$ such that

$$x_{i-2} y_j \quad = \quad \sum_{k=0}^{n-1} r_{k,i+1} f_k + r_{n,i+1}.$$

Proof

construct the term $x_{i-2}y_j$:

$$
\begin{aligned}
f_{i-2} &= x_{i-2} + x_i\overline{y_{i-1}} + y_{i-2}, \\
x_{i-2}y_j &= y_j f_{i-2} + x_i y_j \overline{y_{i-1}} + y_{i-2}y_j, \\
&= y_j f_{i-2} + \overline{y_{i-1}}\left(\sum_{k=0}^{n-1} r_{k,i} f_k + r_{n,i}\right) + y_{i-2}y_j, \\
&= (y_j + \overline{y_{i-1}} r_{i-2,i}) f_{i-2} + \sum_{k=0, k\neq i-2}^{n-1} \overline{y_{i-1}} r_{k,i} f_k \\
&+ \overline{y_{i-1}} r_{n,i} + y_{i-2}y_j.
\end{aligned}
$$

Therefore, Lemma 1 is proved and we have

$$
r_{n,i+1} = \overline{y_{i-1}} r_{n,i} + y_{i-2}y_j.
$$

Finding χ_n^{-1}

Let

$$h = (n-1)/2. \tag{3}$$

Consider

$$x_{i-1}y_i/f_{i-1}. \tag{4}$$

Since

$$f_{i-1} \quad = \quad x_{i-1} + x_{i+1}\overline{y_i} + y_{i-1},$$

we have

$$f_{i-1}y_i \quad = \quad x_{i-1}y_i + y_{i-1}y_i.$$

Finding χ_n^{-1}

Satisfy the condition of Lemma 1:

$$x_{i-1}y_i = x_{i+2h}y_i = y_i f_{i-1} + y_{i-1}y_i.$$

So, the remainder of

$$x_{i+2h-2}y_i, \ldots, x_{i+2(h-j)}y_i, \ldots, x_{i+2(h-h-t)}y_i = x_{i-2}y_i$$

divided by $\langle f_0, f_1, \ldots, f_{n-1} \rangle$ must be polynomials only in Y.

Finding χ_n^{-1}

Let

$$x_{i+2(h-j)}y_i \quad = \quad \sum_{k=0}^{n-1} r_{k,j} f_k + r_{n,j}, \ \ j \in [0, h+t]$$

The recursive relation in the Lemma:

$r_{n,j+1} = \overline{y_{i+2(h-j)-1}} r_{n,j} + y_{i+2(h-j)-2} y_i = \overline{y_{i-2j-2}} r_{n,j} + y_{i-2j-3} y_i$

where

$$r_{n,0} = y_{i-1} y_i.$$

Finding χ_n^{-1}

- On the degree of $r_{n,j}$:
  - $Deg(r_{n,0}) = 2,\ Deg(r_{n,1}) = 3,\ \ldots,\ Deg(r_{n,j}) = 2 + j$
- Low-degree equations are found:

$$\begin{aligned}
0 &= x_{i+2(h-j)}y_i + r_{n,j} = x_{i-1-2j}y_i + r_{n,j}, \\
r_{n,j} &= (y_{i-1-2j} + \sum_{u=1}^{j} y_{i-2u+1} \prod_{k=u}^{j} \overline{y_{i-2k}})y_i.
\end{aligned}$$

Finding χ_n^{-1}

$$x_{i-1-2j}y_i = (y_{i-1-2j} + \sum_{u=1}^{j} y_{i-2u+1} \prod_{k=u}^{j} \overline{y_{i-2k}})y_i.$$

So,

$$x_{i-1-2j} = y_{i-1-2j} + \sum_{u=1}^{j} y_{i-2u+1} \prod_{k=u}^{j} \overline{y_{i-2k}} \text{ ???}$$

When will the formula become stable ???

Finding χ_n^{-1}

$$x_{i-1-2j} = y_{i-1-2j} + \sum_{u=1}^{j} y_{i-2u+1} \prod_{k=u}^{j} \overline{y_{i-2k}}$$

When $j = (n-1)/2 = h$, we have

$$\begin{aligned} & x_{i-1-2h} = y_{i-1-2h} + \sum_{u=1}^{h} y_{i-2u+1} \prod_{k=u}^{h} \overline{y_{i-2k}} \\ \rightarrow \quad & x_i = y_i + \sum_{u=1}^{h} y_{i-2u+1} \prod_{k=u}^{h} \overline{y_{i-2k}}. \end{aligned}$$

Finding χ_n^{-1}

$$x_i = y_i + \sum_{u=1}^{h} y_{i-2u+1} \prod_{k=u}^{h} \overline{y_{i-2k}}$$

- initial analysis: $Deg(r_{n,j})$ becomes stable when $j \geq h$, i.e. $Deg(r_{n,j}) = h + 1 = (n+1)/2$ for $j \geq h$.
- this is the inverse of χ_n with a very high probability!

Finding χ_n^{-1}

- Why do we need to prove the correctness?
  - Is the above deduction not tight?

Current Status

We proved that for any (X, Y) satisfying $Y = \chi_n(X)$, there is:

$$x_i y_{i+2t} = (y_i + \sum_{u=1}^{h} y_{i-2u+1} \prod_{k=u}^{h} \overline{y_{i-2k}}) y_{i+2t}. \tag{5}$$

We do not know whether

$$x_i = (y_i + \sum_{u=1}^{h} y_{i-2u+1} \prod_{k=u}^{h} \overline{y_{i-2k}}) \tag{6}$$

will always hold. At least, it is not so obvious.

Proof Idea

Consider two equation systems E_1 and E_2 in terms of (X, Y):

$$\begin{aligned} E_1 : y_i &= x_i + \overline{x_{i+1}} x_{i+2},\ i \in [0, n-1], \\ E_2 : x_i &= y_i + \sum_{u=1}^{h} y_{i-2u+1} \prod_{k=u}^{h} \overline{y_{i-2k}},\ i \in [0, n-1]. \end{aligned}$$

If $V(E_1) = V(E_2)$ where $V(E_1)$ and $V(E_2)$ denotes the set of solutions to E_1 and E_2, the correctness is proved.

Trivial observations:

- $|V(E_1)| = |V(E_2)| = 2^n$ (size is the same).
- If $V(E_1) = V(E_2)$, the invertibility is also proved.
- If proved, $Deg(\chi_n^{-1}) = h + 1 = (n+1)/2$.

Proof Idea

A common two-step proof:

- Step 1: prove $V(E_1) \subseteq V(E_2)$
- Step 2: prove $V(E_2) \subseteq V(E_1)$

■ Direct proof: difficult

- introduce another equation system E_3:

$$E_3 : x_i + y_i + \overline{y_{i+1}} x_{i+2} = 0, \ \ i \in [0, n-1].$$

- our finding: $V(E_1) = V(E_3) \backslash \{1^n, 0^n\}$, i.e. $V(E_1) \subseteq V(E_3)$
- step 2: prove $V(E_2) \subseteq V(E_3)$ due to $\{1^n, 0^n\} \notin V(E_2)$.
- step 1: prove $V(E_1) \subseteq V(E_2)$.

Proving $V(E_2) \subseteq V(E_3)$

For any $(X, Y) \in V(E_2)$, we have

$$\begin{aligned}
x_i &= y_i + \sum_{u=1}^{h} y_{i-2u+1} \prod_{k=u}^{h} \overline{y_{i-2k}}, \\
x_{i+2} &= y_{i+2} + \sum_{u=1}^{h} y_{i-2(u-1)+1} \prod_{k=u}^{h} \overline{y_{i-2(k-1)}} \\
&= y_{i+2} + \sum_{u=0}^{h-1} y_{i-2u+1} \prod_{k=u}^{h-1} \overline{y_{i-2k}}
\end{aligned}$$

Proving $V(E_2) \subseteq V(E_3)$

$$\begin{aligned}
x_{i+2}\overline{y_{i+1}} &= y_{i+2}\overline{y_{i+1}} + \overline{y_{i+1}} \sum_{u=0}^{h-1} y_{i-2u+1} \prod_{k=u}^{h-1} \overline{y_{i-2k}} \\
&= y_{i-2h+1}\overline{y_{i-2h}} + \overline{y_{i-2h}} \sum_{u=0}^{h-1} y_{i-2u+1} \prod_{k=u}^{h-1} \overline{y_{i-2k}} \\
&= \sum_{u=0}^{h} y_{i-2u+1} \prod_{k=u}^{h} \overline{y_{i-2k}} \\
&= y_{i+1} \prod_{k=0}^{h} \overline{y_{i-2k}} + \sum_{u=1}^{h} y_{i-2u+1} \prod_{k=u}^{h} \overline{y_{i-2k}} \\
&= x_i + y_i.
\end{aligned}$$

$*2h = n-1 \rightarrow i+2 = i-2h+1 \mod n, i+1 = i-2h \mod n.$

Proving $V(E_1) \subseteq V(E_2)$

The proof is a bit long. Basically, it is based on the proof by induction and proof by contradiction.

Conclusion

- The formula of χ_n^{-1} is found and can be written down in only one line:

$$x_i = y_i + \sum_{u=1}^{h} y_{i-2u+1} \prod_{k=u}^{h} \overline{y_{i-2k}}.$$

- Finding and proving χ_n^{-1} highly relies on the ideal $\mathcal{I} = \langle f_0, \ldots, f_{n-1} \rangle$. Underlying reasons? (unclear to me)
- Potential attacks based on this formula?