Massive Superpoly Recovery with Nested Monomial Predictions

Kai Hu, Siwei Sun, Yosuke Todo, Meiqin Wang, Qingju Wang

ASIACRYPT 2021

December 7, 2021

Introduction

- Stream and Block cipher
- Degree Evaluations, Cube Attacks
- Division Properties,Integral Attack

Contribution

- Propose a new technique called monomial prediction,can be regarded as a new language for describing the division properties
- Apply this technique to Degree Evaluations and Cube Attacks

Preliminaries

Boolean Function

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function whose algebraic normal form (ANF) is

$$f(\boldsymbol{x}) = f(x_0, x_1, ..., x_{n-1}) = \bigoplus_{\boldsymbol{u} \in \mathbb{F}_2^n} a_{\boldsymbol{u}} \prod_{i=0}^{n-1} x_i^{u_i}$$

where $a_{\boldsymbol{u} \in \mathbb{F}_2}$ and

$$\boldsymbol{x}^{\boldsymbol{u}} = \pi_{\boldsymbol{u}}(\boldsymbol{x}) = \prod_{i=0}^{n-1} x_i^{u_i} = \begin{cases} x_i, if & u_i = 1, \\ 1, if & u_i = 0, \end{cases}$$

Example 1

Let $f(x_0, x_1) = x_0 x_1 \oplus x_0 \oplus 1$,then we have

$$x_0 x_1 \to f, x_0 \to f, 1 \to f, x_1 \not\to f$$

Vectorial Boolean Function

$\boldsymbol{f}: \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a vectorial Boolean function with $\boldsymbol{y} = (y_0, y_1, ..., y_{m-1}) = \boldsymbol{f}(\boldsymbol{x}) = (f_0(\boldsymbol{x}), ..., f_{n-1}(\boldsymbol{x}))$. For $\boldsymbol{x} \in \mathbb{F}_2^n$,we use $\boldsymbol{y}^{\boldsymbol{v}}$ to denote the product of some coordinates of $\boldsymbol{y}$:

$$\boldsymbol{y}^v = \prod_{i=0}^{m-1} y_i^{v_i} = \prod_{i=0}^{m-1} (f_i(\boldsymbol{x}))^{v_i}$$

Monomial Prediction

Let $\boldsymbol{f} : \mathbb{F}_2^{n_0} \rightarrow \mathbb{F}_2^{n_r}$ be a composite vectorial Boolean function of a sequence of r smaller function $\boldsymbol{f}^i : \mathbb{F}_2^{n_i} \rightarrow \mathbb{F}_2^{n_{i+1}}, 0 \leq i \leq r-1$ as

$$\boldsymbol{f} = \boldsymbol{f}^{(r-1)} \circ \boldsymbol{f}^{(r-2)} \circ \cdots \circ \boldsymbol{f}^{(0)} \tag{1}$$

Definition 1 (Monomial Trail)

Let $\boldsymbol{x}^{(i+1)} = \boldsymbol{f}^{(i)}(\boldsymbol{x}^{(i)})$ for $0 \leq i < r$.We call a sequence of monomails $(\pi_{\boldsymbol{u}^{(0)}}(\boldsymbol{x}^{(0)}), \pi_{\boldsymbol{u}^{(1)}}(\boldsymbol{x}^{(1)}), \ldots, \pi_{\boldsymbol{u}^{(r)}}(\boldsymbol{x}^{(r)}))$ an r-round monomial trail connecting $\pi_{\boldsymbol{u}^{(0)}}(\boldsymbol{x}^{(0)})$ and $\pi_{\boldsymbol{u}^{(r)}}(\boldsymbol{x}^{(r)})$ with respect to the composite function $\boldsymbol{f} = \boldsymbol{f}^{(r-1)} \circ \boldsymbol{f}^{(r-2)} \circ \cdots \circ \boldsymbol{f}^{(0)}$ if

$$\pi_{\boldsymbol{u}^{(0)}}(\boldsymbol{x}^{(0)}) \rightarrow \pi_{\boldsymbol{u}^{(1)}}(\boldsymbol{x}^{(1)}) \rightarrow \cdots \rightarrow \pi_{\boldsymbol{u}^{(r)}}(\boldsymbol{x}^{(r)})$$

If there is at least one monomial trail connecting $\pi_{\boldsymbol{u}^{(0)}}(\boldsymbol{x}^{(0)})$ and $\pi_{\boldsymbol{u}^{(r)}}(\boldsymbol{x}^{(r)})$,we write $\pi_{\boldsymbol{u}^{(0)}}(\boldsymbol{x}^{(0)}) \rightsquigarrow \pi_{\boldsymbol{u}^{(r)}}(\boldsymbol{x}^{(r)})$. Otherwise,$\pi_{\boldsymbol{u}^{(0)}}(\boldsymbol{x}^{(0)}) \not\rightsquigarrow \pi_{\boldsymbol{u}^{(r)}}(\boldsymbol{x}^{(r)})$

Example 2

Let $\boldsymbol{z} = (z_0, z_1) = \boldsymbol{f}^{(0)}(y_0, y_1) = (y_0 y_1, y_0 \oplus y_1), \boldsymbol{y} = (y_0, y_1) = \boldsymbol{f}^{(0)}(x_0, x_1, x_2) = (x_0 \oplus x_1 \oplus x_2, x_0 x_1 \oplus x_0 \oplus x_2)$ and $\boldsymbol{f} = \boldsymbol{f}^{(0)} \boldsymbol{f}^{(1)}$.Consider $(x_0, x_1, x_2)^{(1,0,0)} = x_0$

$$(y_0, y_1)^{(0,0)} = 1, (y_0, y_1)^{(1,0)} = y_0 = \underline{x_0} \oplus x_1 \oplus x_2, (y_0, y_1)^{(0,1)} = y_1 = x_0 x_1 \oplus \underline{x_0} \oplus x_2,$$

$$(y_0, y_1)^{(1,1)} = y_0 y_1 = x_0 x_1 x_2 \oplus x_0 x_1 \oplus x_1 x_2 \oplus \underline{x_0} \oplus x_2.$$

Then

$$x_0 \to y_0, x_0 \to y_1, x_0 \to y_0 y_1$$

Similarly

$$(z_0, z_1)^{(0,0)} = 1, (z_0, z_1)^{(1,0)} = z_0 = y_0 y_1, (z_0, z_1)^{(0,1)} = z_1 = y_0 \oplus y_1, (z_0, z_1)^{(1,1)} = z_0 z_1 = 0$$

Then connecting x_0 and monomials of z:

$$x_0 \to y_0 \to z_1, x_0 \to y_1 \to z_1, x_0 \to y_0 y_1 \to z_0$$

Lemma 1

$\pi_{\boldsymbol{u}^{(0)}}(\boldsymbol{x}^{(0)}) \rightsquigarrow \pi_{\boldsymbol{u}^{(r)}}(\boldsymbol{x}^{(r)})$. if $\pi_{\boldsymbol{u}^{(0)}}(\boldsymbol{x}^{(0)}) \rightarrow \pi_{\boldsymbol{u}^{(r)}}(\boldsymbol{x}^{(r)})$,and thus $\pi_{\boldsymbol{u}^{(0)}}(\boldsymbol{x}^{(0)}) \not\rightsquigarrow \pi_{\boldsymbol{u}^{(r)}}(\boldsymbol{x}^{(r)})$ implies $\pi_{\boldsymbol{u}^{(0)}}(\boldsymbol{x}^{(0)}) \not\rightarrow \pi_{\boldsymbol{u}^{(r)}}(\boldsymbol{x}^{(r)})$

Considering Example 2, although $x_0 \rightsquigarrow z_1$,we have $x_0 \not\rightarrow z_1$ since

$$z_1 = y_0 \oplus y_1 = \underline{x_0} \oplus x_1 \oplus x_2 \oplus x_0x_1 \oplus \underline{x_0} \oplus x_2 = x_0x_1 \oplus x_1.$$

Definition 2 (Monomial Hull)

For $\boldsymbol{f}$ with a specific composition sequence, the monomial hull of $\pi_{\boldsymbol{u}^{(0)}}(\boldsymbol{x}^{(0)})$ and $\pi_{\boldsymbol{u}^{(r)}}(\boldsymbol{x}^{(r)})$, denoted by $\pi_{\boldsymbol{u}^{(0)}}(\boldsymbol{x}^{(0)}) \bowtie \pi_{\boldsymbol{u}^{(r)}}(\boldsymbol{x}^{(r)})$,is the set of all monomial trails connecting them. The number of trails in the monomial hull is called the **size** of the hull and is denoted by $|\pi_{\boldsymbol{u}^{(0)}}(\boldsymbol{x}^{(0)}) \bowtie \pi_{\boldsymbol{u}^{(r)}}(\boldsymbol{x}^{(r)})|$.

Example 3

Consider Example 2, the monomial hull of x_0 and z_1 is the set

$$x_0 \bowtie z_1 = \{x_0 \to y_0 \to z_1, x_0 \to y_1 \to z_1\}$$

Thus the size of $x_0 \bowtie z_1$ is 2. Furthermore, since $x_0 \not\rightsquigarrow z_0 z_1$, $x_0 \bowtie z_0 z_1 = \emptyset$ and $|x_0 \bowtie z_0 z_1| = 0$.

Theorem 1

Let $\boldsymbol{f} = \boldsymbol{f}^{(r-1)} \circ \boldsymbol{f}^{(r-2)} \circ \cdots \circ \boldsymbol{f}^{(0)}$ defined as above. $\pi_{\boldsymbol{u}^{(0)}}(\boldsymbol{x}^{(0)}) \to \pi_{\boldsymbol{u}^{(r)}}(\boldsymbol{x}^{(r)})$ if and only if

$$|\pi_{\boldsymbol{u}^{(0)}}(\boldsymbol{x}^{(0)}) \bowtie \pi_{\boldsymbol{u}^{(r)}}(\boldsymbol{x}^{(r)}) \equiv 1 \pmod 2.$$

Propation rules

Rule 1(Copy)

Let $\boldsymbol{x} = (x_0, x_1, ..., x_{n-1})$ and $\boldsymbol{y} = (x_0, x_0.x_1, ..., x_{n-1})$ be the input and ouput vector of a Copy function.Consider a monomial of $\boldsymbol{x}$ as $\boldsymbol{x}^{\boldsymbol{u}}$,the monomial $\boldsymbol{y}^{\boldsymbol{v}}$ of $\boldsymbol{y}$,$\boldsymbol{x}^{\boldsymbol{u}} \rightarrow \boldsymbol{y}^{\boldsymbol{v}}$

$$\boldsymbol{v} = \begin{cases} (0, u_1, ..., u_{n-1}) \Rightarrow_{copy} (0, 0, u_1, ...u_{n-1}), \\ (1, u_1, ..., u_{n-1}) \Rightarrow_{copy} (1, 0, u_1, ...u_{n-1}) \ or \ (0, 1, u_1, ...u_{n-1}) \ or \ (1, 1, u_1, ...u_{n-1}) \end{cases}$$

Rule 2(Xor)

Let $\boldsymbol{x} = (x_0, x_1, ..., x_{n-1})$ and $\boldsymbol{y} = (x_0 \oplus x_1, ..., x_{n-1})$ be the input and ouput vector of a XOR function.Consider a monomial of $\boldsymbol{x}$ as $\boldsymbol{x}^{\boldsymbol{u}}$,the monomial $\boldsymbol{y}^{\boldsymbol{v}}$ of $\boldsymbol{y}$,$\boldsymbol{x}^{\boldsymbol{u}} \rightarrow \boldsymbol{y}^{\boldsymbol{v}}$

$$\boldsymbol{v} = (u_0 + u_1, ..., u_{n-1}), (u_0, u - 1) \in \{(0,0), (0,1), (1,0)\}$$

Rule 3(And)

Let $\boldsymbol{x} = (x_0, x_1, ..., x_{n-1})$ and $\boldsymbol{y} = (x_0 \wedge x_1, ..., x_{n-1})$ be the input and ouput vector of a XOR function.Consider a monomial of $\boldsymbol{x}$ as $\boldsymbol{x}^{\boldsymbol{u}}$,the monomial $\boldsymbol{y}^{\boldsymbol{v}}$ of $\boldsymbol{y}$,$\boldsymbol{x}^{\boldsymbol{u}} \rightarrow \boldsymbol{y}^{\boldsymbol{v}}$

$$\boldsymbol{v} = (u_0, u_2, ..., u_{n-1}), (u_0, u - 1) \in \{(0,0), (1,1)\}$$

Degree Evaluation

The degree of a Boolean function f is defined as follows,

$$deg(f) = max_{\pi_{\boldsymbol{u}}(\boldsymbol{x}^{(0)}) \rightarrow f} wt(\boldsymbol{u}^{(0)})$$

1. Find a monomial $\pi_{\boldsymbol{u}}(\boldsymbol{x}^{(0)}) \rightsquigarrow f$ with $wt(\boldsymbol{u}) = d$ and prove $\pi_{\hat{\boldsymbol{u}}}(\boldsymbol{x}^{(0)}) \not\rightarrow f$ for any $wt(\hat{\boldsymbol{u}}) > d$
2. Compute $|\pi_{\boldsymbol{u}^{(0)}}(\boldsymbol{x}^{(0)}) \bowtie f|$,if the value is odd, then the $deg(f) = d$,else,repeat the process until we find a desired monomial of f.

MILP-based approach to search for the monomials of f.In this MILP model, the objective function of the model is to maximize $wt(\boldsymbol{u}^{(0)})$.

Cube Attack

For a cipher with a secret key $\boldsymbol{k} = (k_0, ..., k_{m-1}) \in \mathbb{F}_2^m$ and a public input $\boldsymbol{v} = (v_0, ...v_{n-1}) \in \mathbb{F}_2^n$, a Boolean function $f(\boldsymbol{v}, \boldsymbol{k})$

$$f(\boldsymbol{v}, \boldsymbol{k}) = p(\boldsymbol{v}[\hat{\boldsymbol{u}}], \boldsymbol{k}) \cdot \boldsymbol{v}^{\boldsymbol{u}} + q(\boldsymbol{v}, \boldsymbol{k})$$

Let $\mathbb{C}_u = \boldsymbol{v} \in \mathbb{F}_2^n : \boldsymbol{v} \preceq \boldsymbol{u}, wt(\boldsymbol{u}) \leq n$,

$$\bigoplus_{\boldsymbol{v} \in \mathbb{C}_u} f(\boldsymbol{v}, \boldsymbol{k}) = \bigoplus_{\boldsymbol{v} \in \mathbb{C}_u} (p \cdot \boldsymbol{v}^{\boldsymbol{u}} + q(\boldsymbol{v}, \boldsymbol{k})) = p$$

It is easy to check that the superpoly of $\mathbb{C}_u$ is just the coeffcient of $\boldsymbol{x}^{\boldsymbol{u}}$ in the parameterized Boolean function $f(\boldsymbol{v}, \boldsymbol{k})$

$$p(\boldsymbol{v}[\hat{\boldsymbol{u}}], \boldsymbol{k}) = Coe(f(\boldsymbol{v}, \boldsymbol{k}), \boldsymbol{v}^{\boldsymbol{u}}).$$

Example

We suppose a stream cipher has input $\boldsymbol{v} = (v_0, v_1, v_2, v_3) \in \mathbb{F}_2^4$ and $\boldsymbol{k} = (k_0, k_1, k_2) \in \mathbb{F}_2^3$,

$$f(\boldsymbol{v}, \boldsymbol{k}) = v_0 v_1 v_2 (v_3 k_0 + k_2) + v_0 v_2 (k_1 k_2) + v_0 + k_0$$

then we chose $\mathbb{C}_u = (v_0, v_1, v_2)$,and calculate

$$\bigoplus_{\boldsymbol{v} \in \mathbb{C}_u} f(\boldsymbol{v}, \boldsymbol{k}) = \bigoplus_{\boldsymbol{v} \in \mathbb{C}_u} (p \cdot \boldsymbol{v}^{\boldsymbol{u}} + q(\boldsymbol{v}, \boldsymbol{k})) = (v_3 k_0 + k_2)$$

or we chose $\mathbb{C}_u = (v_0, v_2)$,and the superpoly will be

$$v_1 (v_3 k_0 + k_2) + k_1 k_2$$

Key-Recovery Attacks with Superpolies

Offline

We have recovered the exact ANF of superpoly $p(\boldsymbol{f})$ for the cube term $\boldsymbol{x}^{\boldsymbol{u}}$ (the corresponding cube is denoted by $\mathbb{C}_{\boldsymbol{u}}$).

Online

In the online phase, we first call the cipher oracle to encrypt all elements in the cube and get the value of the superpoly with time complexity $2^{wt(\boldsymbol{u})}$.

Next,we try to obtain some information of the secret key from the equation:

$$p(\boldsymbol{k}) = \bigoplus_{\boldsymbol{x} \in \mathbb{C}_{\boldsymbol{u}}} f_{\boldsymbol{k}}(\boldsymbol{x}).$$

Thank You