Coefficient Grouping for Complex Affine Layers

Fukang Liu[1], Lorenzo Grassi[2], Clémence Bouvier[3,4], Willi Meier[5], Takanori Isobe[6]

[1]Tokyo Institute of Technology, Tokyo, Japan
liufukangs@gmail.com

[2]Ruhr University Bochum, Bochum, Germany

[3]Sorbonne University, Paris, France

[4]Inria, Paris, France

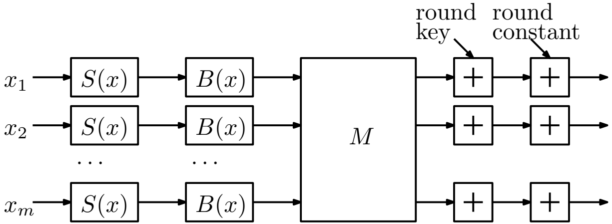
[5]FHNW, Windisch, Switzerland

[6]University of Hyogo, Hyogo, Japan

Aug 23, CRYPTO 2023

SPN Ciphers over $\mathbb{F}_{2^n}^m$

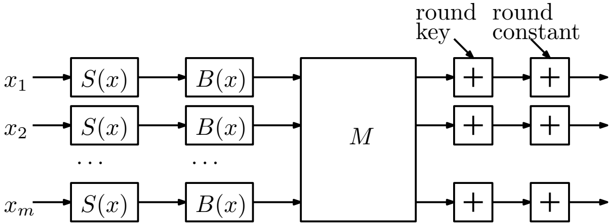
- Target: SPN ciphers over $\mathbb{F}_{2^n}$
  - $S(x) = x^d$ (power map)
  - $B(x) = c_0 + \sum_{i=1}^{w} c_i x^{2^{h_i}}$ (w : density of $B(x)$)
  - M : any matrix



- Examples: MiMC, Chaghri, RAIN, AES

SPN Ciphers over $\mathbb{F}_{2^n}^m$

- Specific target:
  - $S(x) = x^{2^d+1}$ (of algebraic degree 2)
  - $B(x) = c_0 + \sum_{i=1}^{w} c_i x^{2^{h_i}}$ $(h_1 < h_2 < \cdots < h_w)$
  - M : any matrix



- Examples: MiMC, Chaghri

Description of the Problem

The General Problem

Let the m inputs be linear polynomials in a variable x, i.e.

$$x_i = P_{i,0}(x) = u_{i,1} \cdot x + u_{i,0},$$

where $u_{i,0}, u_{i,1}$ are randomly chosen constants. **Find the upper bound δ_r on the algebraic degree of the polynomials of the internal states after r rounds.**

- Note 1: the algebraic degree of a polynomial in $\mathbb{F}_{2^n}[x]$ is defined by the maximal Hamming weight of the exponents of monomials with nonzero coefficients.
- Examples:

$$Deg(X^{2^3+2^4} + x^{2^5}) = 2, \quad Deg(X^{2^3+2^4} + x^{2^1+2^2+2^3}) = 3.$$

Specific Problems

- Note 2: For simplicity, we treat the coefficients of all possible monomials in x as 1, i.e.

$$x_i = P_0(x) = x + 1.$$

  Moreover, the polynomial in x of the internal state after r rounds is denoted by $P_r(x)$.

Studied problems:

1. How does w influence the growth of δ_r?
2. How to efficiently find $(h_1, \ldots, h_w)$ with the smallest w to ensure the fastest growth of δ_r?
3. How to efficiently upper bound δ_r for any $(h_1, \ldots, h_w)$?

Finding Properties of $P_r(x)$

Let

$$P_r(x) = (B \circ S)^r(P_0(x)), \qquad P_r^S(x) = S(P_{r-1}(x)).$$

- Note 3: we omit the influence of $M(\cdot)$, i.e., ignore the influence of cancellations in monomials.
- Note 4: Studying the algebraic degree of $P_r^S(x)$ is enough as $B(x)$ is linear over $\mathbb{F}_2$, i.e. $Deg(P_r(x)) = Deg(P_r^S(x))$

Finding Properties of $P_r(x)$

Studying $P_r(x)$ for small r:

$r = 0$:

$$P_0(x) = x + 1$$

$r = 1$:

$$\begin{aligned} P_1^S(x) &= (x+1)^{2^d}(x+1) = x^{2^d} + x^{2^d+1} + x + 1, \\ P_1(x) &= 1 + \sum_{i=1}^{w} \left(P_1^S(x)\right)^{2^{h_i}} = 1 + \sum_{i=1}^{w} x^{2^{d+h_i}} + x^{2^{d+h_i}+2^{h_i}} + x^{2^{h_i}}. \end{aligned}$$

Observations:

Only $\left\{x^{2^d}, x^{2^d+1}, x, x^0\right\}$ will appear in $P_0^S(x)$.

Only $\left\{x^{2^{d+h_i}}, x^{2^{d+h_i}+2^{h_i}}, x^{2^{h_i}}, x^0 \mid 1 \le i \le w\right\}$ will appear in $P_1(x)$.

Finding Properties of $P_r(x)$

Describing $P_r(x)$ by its exponents:

$$\begin{aligned} \mathcal{W}_r &= \{e \in \mathbb{N} \mid x^e \text{ is a monomial of } P_r(x)\}, \\ \mathcal{W}_r^S &= \{e \in \mathbb{N} \mid x^e \text{ is a monomial of } P_r^S(x)\}. \end{aligned}$$

For the cases $r = 0, 1$:

$$\begin{aligned} \mathcal{W}_0 &= \{0, 1\}, \\ \mathcal{W}_1^S &= \left\{2^d, 2^d + 1, 1, 0\right\} = \left\{a_{1,1}2^d + a_{1,2} \mid 0 \leq a_{1,1}, a_{1,2} \leq 1\right\} \\ \mathcal{W}_1 &= \left\{2^{d+h_i}, 2^{h_i} + 2^{d+h_i}, 2^{h_i}, 0 \mid 1 \leq i \leq w\right\} \\ &= \left\{a_{1,1}2^{d+h_i} + a_{1,2}2^{h_i} \mid 0 \leq a_{1,1}, a_{1,2} \leq 1, 1 \leq i \leq w\right\}, \end{aligned}$$

How to compute $\mathcal{W}_2^S$?

Finding Properties of $P_r(x)$

From $\mathcal{W}_1$ to $\mathcal{W}_2^S$:

We have $y^{2^d+1} = y^{2^d} \cdot y$ where y **is a polynomial whose monomials can always be represented as** $x^{a_{1,1}2^{d+h_i}+a_{1,2}2^{h_i}}$.

Left part in $y^{2^d} \cdot y$, i.e. y^{2^d}: we can choose any possible monomial $x^{a_{1,1}2^{d+h_{i_0}}+a_{1,2}2^{h_{i_0}}}$ for y, and compute $y^{2^d} = (x^{a_{1,1}2^{d+h_{i_0}}+a_{1,2}2^{h_{i_0}}})^{2^d} = x^{a'_{1,1}2^{2d+h_{i_0}}+a'_{1,2}2^{d+h_{i_0}}}$.

Right part in $y^{2^d} \cdot y$, i.e. y: we can also independently choose any possible monomial $x^{a''_{1,1}2^{d+h_{i_1}}+a''_{1,2}2^{h_{i_1}}}$ for y.

Consequence: $x^{a'_{1,1}2^{2d+h_{i_0}}+a'_{1,2}2^{d+h_{i_0}}+a''_{1,1}2^{d+h_{i_1}}+a''_{1,2}2^{h_{i_1}}}$ is a possible monomial in $y^{2^d+1} = y^{2^d} \cdot y$.

Finding Properties of $P_r(x)$

For the case $r = 2$:

$$\mathcal{W}_2^S = \Big\{ a_{2,1}2^{2d+h_{i_0}} + a_{2,2}2^{d+h_{i_0}} + a_{2,3}2^{d+h_{i_1}} + a_{2,4}2^{h_{i_1}} \;\Big|\; 0 \le a_{2,j} \le 1, 1 \le i_0, i_1 \le w, 1 \le j \le 4 \Big\},$$

$$\mathcal{W}_2 = \Big\{ a_{2,1}2^{2d+h_{i_0}+h_{i_2}} + a_{2,2}2^{d+h_{i_0}+h_{i_2}} + a_{2,3}2^{d+h_{i_1}+h_{i_2}} + a_{2,4}2^{h_{i_1}+h_{i_2}} \;\Big|\; 0 \le a_{1,j} \le 1, 1 \le i_0, i_1, i_2 \le w, 1 \le j \le 4 \Big\},$$

From $\mathcal{W}_2^S$ to $\mathcal{W}_2$: easy

Finding Properties of $P_r(x)$

For each $r \geq 1$, let $\mathcal{V}_{r,w}$ be the set defined as

$$\mathcal{V}_{r,w} = \left\{ e \in \mathbb{N} \mid e = \sum_{i=1}^{w} b_i h_i, \sum_{i=1}^{w} b_i = r-1, b_i \geq 0 \right\}, \qquad (1)$$

which represents all possible values by summing up $r-1$ elements from the set $\{h_1, \ldots, h_w\}$.

■ Examples:

$$\begin{aligned} \mathcal{V}_{2,w} &= \left\{ e \in \mathbb{N} \mid e = \sum_{i=1}^{w} b_i h_i, \sum_{i=1}^{w} b_i = 1, b_i \geq 0 \right\} \\ &= \{h_i \mid 1 \leq i \leq w\} \\ \mathcal{V}_{3,w} &= \{ e \in \mathbb{N} \mid e = \sum_{i=1}^{w} b_i h_i, \sum_{i=1}^{w} b_i = 2, b_i \geq 0 \} \\ &= \{h_i + h_j \mid 1 \leq i, j \leq w\}. \end{aligned}$$

Finding Properties of $P_r(x)$

Theorem

Given $\mathcal{V}_{r,w}$, the set $\mathcal{W}_r^S$ can be represented as follows:

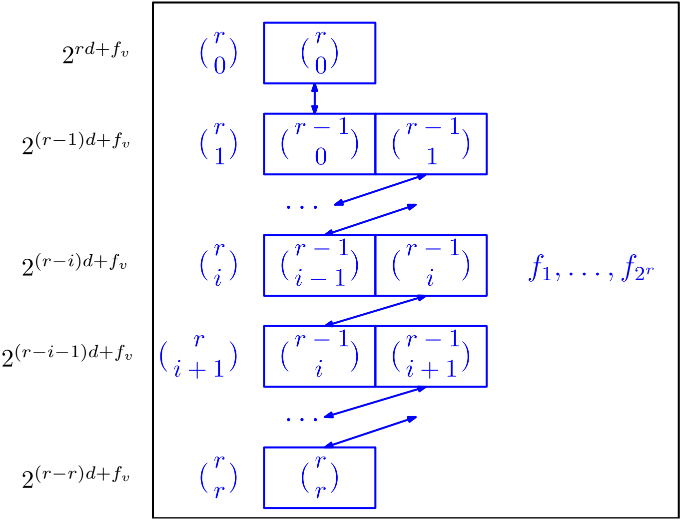
$$\mathcal{W}_r^S = \left\{ \sum_{i=0}^{r} \sum_{j=1}^{\binom{r}{i}} a_{r,v} 2^{(r-i)d + f_v}, \right. \\ \left. v = j + \binom{r}{\leq i-1}, 0 \leq a_{r,v} \leq 1, f_v \in \mathcal{V}_{r,w} \right\}$$

where

$$f_{\binom{r}{\leq i}+\ell} = f_{\binom{r}{\leq i}-\binom{r-1}{i}+\ell} \quad \text{for } 0 \leq i \leq r-1, 1 \leq \ell \leq \binom{r-1}{i}.$$

Finding Properties of $P_r(x)$

Graphic illustration:



Implications of the Theorem

For each valid assignment to $(f_1, \ldots, f_{2^r})$, we obtain a subset $\mathcal{W}_r^{S,f} \subseteq \mathcal{W}_r^S$:

$$\mathcal{W}_r^{S,f} = \left\{ \sum_{i=0}^{r} \sum_{j=1}^{\binom{r}{i}} a_{r,v} 2^{(r-i)d+f_v}, v = j + \binom{r}{\leq i-1}, 0 \leq a_{r,v} \leq 1 \right\}.$$

Our Goals

- Study the properties of $\mathcal{W}_r^{S,f}$ under all possible assignments.
- Find the common features inside all possible $\mathcal{W}_r^{S,f}$.

Implications of the Theorem

For each $W_r^{S,f}$, we can find the element with the maximal Hamming weight by first converting it into a vector of integers denoted by $\nu_r = (\nu_{r,n-1}, \ldots, \nu_{r,0})$:

procedure CONVERSION_SUBSET(ν_r, r, n)
    initialize $(\nu_{r,n-1}, \ldots, \nu_{r,0})$ as all 0
    $v = 1$
    for all $i \in [0, r]$ **do**
        for all $j \in [1, \binom{r}{i}]$ **do**
            $u = ((r - i) \times d + f_v)\%n$
            $\nu_{r,u} = \nu_{r,u} + 1$
            $v = v + 1$
        end for
    end for
end procedure

Implications of the Theorem

- reduced to a well-structured optimization problem:

$$\begin{aligned} &\text{maximize}\,\mathrm{Hw}\left(M_n\left(\sum_{i=0}^{n-1} 2^i \alpha_i\right)\right), \\ &\text{subject to } \ 0 \le \alpha_i \le \nu_{r,i} \ \text{ for } \ i \in [0, n-1], \end{aligned}$$

where

$$M_n(x) := \begin{cases} 2^n - 1 & \text{if } 2^n - 1 \mid x \text{ and } x \ge 2^n - 1, \\ x\%(2^n - 1) & \text{otherwise.} \end{cases}$$

Implications of the Theorem

If $w = 1$, we have $\mathcal{V}_{r,1} = \{(r-1)h_1\}$ and hence

$$\mathcal{W}_r^S = \left\{ \sum_{i=0}^{r} a_i 2^{(r-i)d+(r-1)h_1}, 0 \leq a_i \leq \binom{r}{i} \right\}.$$

Based on $\mathrm{Hw}(M_n(a+b)) \leq \mathrm{Hw}(M_n(a)) + \mathrm{Hw}(M_n(b))$, we have

$$\begin{aligned}
\mathrm{Hw}\left(M_n \left(\sum_{i=0}^{n-1} 2^i \alpha_i \right) \right) &\leq \sum_{i=0}^{n-1} \mathrm{Hw}\left(M_n(2^i \alpha_i) \right) \\
&\leq \sum_{i=0}^{n-1} \mathrm{Hw}(\alpha_i) \leq \sum_{i=0}^{n-1} \lfloor \log_2(\nu_{r,i}+1) \rfloor, \\
&\leq \sum_{j=0}^{r} \log_2 \left(\binom{r}{j} + 1 \right) \leq r^2 - 2r + 3
\end{aligned}$$

At most quadratic increase for $w = 1$.

Exponential Growth

Necessary condition on the exponential growth of δ_r

There should exist a valid assignment to $(f_1, \ldots, f_{2^r})$ such that the following 2^r elements are different:

$$
\begin{aligned}
&\underbrace{(rd + f_1)\%n}_{i=0},\\
&\underbrace{((r-1)d + f_{1+1})\%n, \ldots, ((r-1)d + f_{1+\binom{r}{1}})\%n}_{i=1},\\
&\ldots,\\
&\underbrace{((r-i)d + f_{\binom{r}{\le i-1}+1})\%n, \ldots, ((r-i)d + f_{\binom{r}{\le i-1}+\binom{r}{i}})\%n}_{i},\\
&\ldots, \underbrace{f_{2^r}\%n}_{i=r}.
\end{aligned}
$$

Tokyo Tech

Exponential Growth

Necessary condition on the exponential growth of δ_r

$\mathcal{B}_{r,w} = \{(b_1, \ldots, b_w) | \sum_{i=1}^{w} b_i = r, b_i \geq 0\}$ should satisfy $|\mathcal{B}_{r-1,w}| \geq \binom{r}{\lceil \frac{r}{2} \rceil}$, i.e. $|\mathcal{B}_{r-1,w}|$ is an upper bound on $|\{f_1, \ldots, f_{2^r}\}|$.

Applications:

$$|\mathcal{B}_{2,2}| = 3 \geq \binom{3}{2} = 3, \qquad |\mathcal{B}_{3,2}| = 4 < \binom{4}{2} = 6,$$

$$|\mathcal{B}_{5,3}| = 21 \geq \binom{6}{3} = 20, \qquad |\mathcal{B}_{6,3}| = 28 < \binom{7}{4} = 35,$$

$$|\mathcal{B}_{8,4}| = 165 \geq \binom{9}{5} = 126, \qquad |\mathcal{B}_{9,4}| = 220 < \binom{10}{5} = 252,$$

Implications:

- The sharp exponential growth can be achieved for at most the first 3, 6 and 9 rounds when $w = 2, 3, 4$, respectively.

Efficiently Checking the Necessary Condition

Problem reduction

Given w and $(h_1, \ldots, h_w)$, we compute $r+1$ arrays $A_1, \ldots, A_{r+1}$:

$$
\begin{aligned}
&\text{Set } A_{i+1} \text{ as all zero} \\
&\text{for all } u \in \mathcal{V}^R_{r,w}: \\
&\quad j = ((r-i) \times d + u)\%n \\
&\quad A_{i+1}[j] = 1
\end{aligned}
$$

where $\mathcal{V}^R_{r,w} = \{e\%n \mid e \in \mathcal{V}_{r,w}\}$. **We should be able to choose $\binom{r}{i} = \binom{r-1}{i-1} + \binom{r-1}{i}$ different indices of A_{i+1} such that**

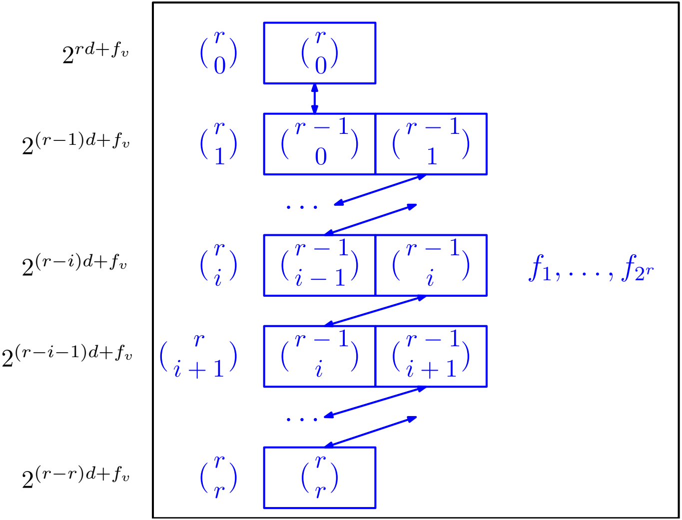
- the values in A_{i+1} at these indices are all 1;
- for a set of $\binom{r-1}{i-1}$ indices $\mathcal{J}$ chosen for A_{i+1}, the set of indices $\{(j+d)\%n \mid j \in \mathcal{J}\}$ has to be chosen for A_i.

It can be converted into a MILP problem and efficiently solved.

Tokyo Tech

Efficiently Checking the Necessary Condition

Graphic illustration:



Upper Bounding δ_r for arbitrary $B(x)$

Common features in ν_r

For all possible subsets $W_r^{S,f}$, we find that the corresponding vectors ν_r share the following three common features:

$$\begin{aligned} \sum_{i=0}^{n-1} \nu_{r,n-1} &= 2^r; \\ |\,\{i \mid \nu_{r,i} \neq 0,\ 0 \leq i \leq n-1\}\,| &\leq \beta; \\ \{i \mid \nu_{r,i} \neq 0,\ 0 \leq i \leq n-1\} &\subseteq \mathcal{Z}, \end{aligned}$$

where the constant β and the set $\mathcal{Z}$ are fixed for given $(n, d, h_1, \ldots, h_w)$, and they can be efficiently precomputed.

Tokyo Tech

Upper Bounding δ_r for arbitrary $B(x)$

Problem reduction

Let

$$\mathcal{Z} = \{p_1, \ldots, p_{|\mathcal{Z}|}\}.$$

Upper bounding δ_r can be converted into solving the following optimization problem:

$$\begin{aligned} \text{maximize } & \mathrm{Hw}\left(M_n\left(\sum_{i=1}^{|\mathcal{Z}|} 2^{p_i}\alpha_{p_i}\right)\right), \\ \text{subject to } & \alpha_{p_i} \geq 0 \ \forall i \in [1, |\mathcal{Z}|], \\ & \sum_{i=1}^{|\mathcal{Z}|} \alpha_{p_i} \leq 2^r, \\ & \mid \{p_i \mid \alpha_{p_i} \neq 0\} \mid \leq \beta. \end{aligned}$$

Upper Bounding δ_r for arbitrary $B(x)$

Experiments for $w = 2$ (problems solved in less than 1 minute):

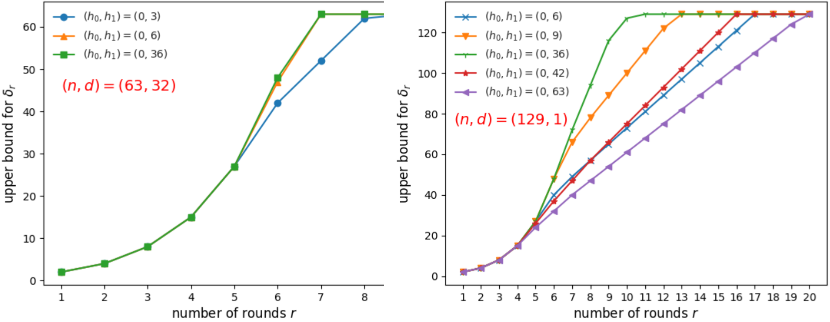


Figure: Graphic illustration of the growth of the algebraic degree

Conclusion

The considered SPN ciphers:

$$S(x) = x^{2^d+1}, \quad B(x) = c_0 + \sum_{i=1}^{w} c_i x^{2^{h_i}},$$

- The growth of the algebraic degree is below the quadratic growth $r^2 - 2r + 3$ for $w = 1$.
- Build the theory to explain the relation between w and the growth of the algebraic degree.
- Efficiently check whether the exponential growth can be achieved for given $(n, d, h_1, \ldots, h_w)$.
- Efficiently find the upper bound on the algebraic degree for arbitrary $(n, d, h_1, \ldots, h_w)$.

Tokyo Tech