Coefficient Grouping: A New Algebraic Degree Evaluation Technique and Its Applications

Fukang Liu

Tokyo Institute of Technology, Tokyo, Japan

ASK 2023

Outline

Background

The talks are based on three papers:

- Coefficient Grouping: Breaking Chaghri and More
- Coefficient Grouping for Complex Affine layers
- An $\mathcal{O}(n)$ Algorithm for Coefficient Grouping

Special thanks to my collaborators:

- Ravi Anand (University of Hyogo, Japan)
- Libo Wang (University of Hyogo, Japan)
- Willi Meier (FHNW, Switzerland)
- Lorenzo Grassi (Ruhr University Bochum, Germany)
- Clémence Bouvier (Sorbonne University & Inria, France)
- Takanori Isobe (University of Hyogo & NICT, Japan)

The Chaghri Primitive

- Proposed at ACM CCS 2022
- FHE-friendly block cipher
- Outperforms AES (in FHE setting) by 65%
- Over a large finite field $\mathbb{F}_{2^{63}}^3$

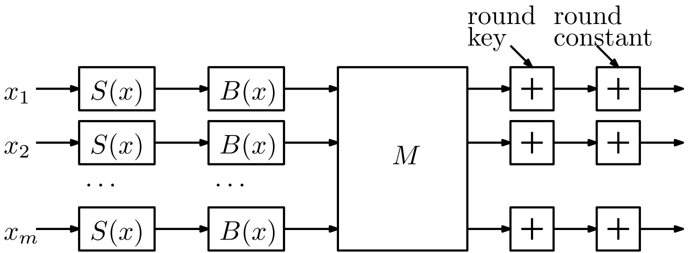
Description of Chaghri

- The round function:

$$S(x) = x^{2^{32}+1}, \quad B(x) = c_0 x^{2^3} + c_1.$$

- State transitions:

$$(z_{0,1}, z_{0,2}, z_{0,3}) \to (z_{1,1}, z_{1,2}, z_{1,3}) \to \cdots \to (z_{r,1}, z_{r,2}, z_{r,3})$$



Higher-order Differential Attack over $\mathbb{F}_{2^n}$

Algebraic degree of a univariate polynomial $\mathcal{F}(X)$ in $\mathbb{F}_{2^n}[X]$

Let

$$\mathcal{F}(X) = \sum_{i=0}^{2^n-1} u_i X^i.$$

Then, its algebraic degree $D_{\mathcal{F}}$ is defined as:

$$D_{\mathcal{F}} \quad = \quad \max\{H(i) : i \in [0, 2^n - 1], u_i \neq 0\},$$

where $H(i)$ denotes the hamming weight of the integer i, i.e., the number of "1" in its binary representation.

Example

For $\mathcal{F} = X^{2^{30}+2^{31}} + X^{2^1+2^3+2^4}$, we have $D_{\mathcal{F}} = 3$.

Degree Evaluation for Chaghri via Enumeration

Our very naive idea:

- Step 1: set the input as a univariate polynomial in X:

$$\begin{aligned} z_{0,1} &= A_{0,1}X + B_{0,1}, \\ z_{0,2} &= A_{0,2}X + B_{0,2}, \\ z_{0,3} &= A_{0,3}X + B_{0,3}. \end{aligned}$$

  - $z_{r,i}$ is always a univariate polynomial $P_{r,i}(X) \in \mathbb{F}_{2^n}[X]$.

- Step 2: trace the evolution of $P_{r,i}$.
- Step 3: compute all possible exponents in $P_{r,i}$. (practical???)
- Step 4: find the exponent with the maximal hamming weight

Degree Evaluation for Chaghri via Enumeration

Step 2: trace the evolution of polynomials

- New representation for $(z_{r,1}, z_{r,2}, z_{r,3})$

$$z_{r,1} = \sum_{i=1}^{|w_r|} A_{r,i} X^{w_{r,i}},\ z_{r,2} = \sum_{i=1}^{|w_r|} B_{r,i} X^{w_{r,i}}, z_{r,3} = \sum_{i=1}^{|w_r|} C_{r,i} X^{w_{r,i}}$$

- The set of all possible exponents after r rounds:

$$w_r = \{w_{r,1}, w_{r,2}, \ldots, w_{r,|w_r|}\} \subseteq \mathbb{N}, \quad w_0 = \{0, 1\}.$$

- Goal: find a relation between w_r and w_{r+1} to compute w_r iteratively.

Degree Evaluation for Chaghri via Enumeration

Step 2: trace the evolution of polynomials

- Through $S(x) = x^{2^{32}+1}$:

$$
\begin{aligned}
S(z_{r,1}) &= \left(\sum_{i=1}^{|w_r|} A_{r,i} X^{w_{r,i}}\right)^{2^{32}+2^0} \\
&= \left(\sum_{i=1}^{|w_r|} A_{r,i} X^{w_{r,i}}\right)^{2^{32}} \times \left(\sum_{i=1}^{|w_r|} A_{r,i} X^{w_{r,i}}\right)^{2^0} \\
&= \sum_{i=1}^{|w_r|} \sum_{j=1}^{|w_r|} A_{r,i,j} X^{2^{32} w_{r,i} + 2^0 w_{r,j}}.
\end{aligned}
$$

where $A_{r,i,j} \in \mathbb{F}_{2^n}$ are key-dependent coefficients.

Degree Evaluation for Chaghri via Enumeration

Step 2: trace the evolution of polynomials

- Through $B(x) = x^{2^3}$:

$$
\begin{aligned}
B \circ S(z_{r,1}) &= c_0 \left(\sum_{i=1}^{|w_r|} \sum_{j=1}^{|w_r|} A_{r,i,j} X^{(2^{32} w_{r,i} + 2^0 w_{r,j})} \right)^{2^3} + c_1 \\
&= \sum_{i=1}^{|w_r|} \sum_{j=1}^{|w_r|} A'_{r,i,j} X^{2^{35} w_{r,i} + 2^3 w_{r,j}}.
\end{aligned}
$$

- The matrix M does not affect this representation:

$$
z_{r+1,1} = \sum_{i=1}^{|w_r|} \sum_{j=1}^{|w_r|} A_{r+1,i,j} X^{2^{35} w_{r,i} + 2^3 w_{r,j}}
$$

Degree Evaluation for Chaghri via Enumeration

Step 2: trace the evolution of polynomials

- The relation between w_r and w_{r+1} is obtained as

$$w_{r+1} = \{\mathcal{M}_{63}(e) | e = 2^{35} w_{r,i} + 2^3 w_{r,j}, 1 \leq i, j \leq |w_r|\},$$

where we define

$$\mathcal{M}_n(x) = \begin{cases} 2^n - 1 \text{ if } 2^n - 1 | x, x \geq 2^n - 1, \\ x\%(2^n - 1) \text{ otherwise.} \end{cases}$$

due to

$$\begin{cases} x^{2^n} = x \ \forall x \in \mathbb{F}_{2^n}, \\ x^{2^n - 1} = 1 \ \forall x \in \mathbb{F}_{2^n} \text{ and } x \neq 0. \end{cases}$$

- Why previous methods failed: they can not handle the modular addition!!!

Degree Evaluation for Chaghri via Enumeration

Step 2: trace the evolution of polynomials

- The relation between w_r and w_{r+2} is obtained as

$$
\begin{aligned}
w_{r+1} &= \{\mathcal{M}_{63}(e) \mid e = 2^{35} w_{r,i} + 2^{3} w_{r,j}, 1 \leq i, j \leq |w_r|\}, \\
w_{r+2} &= \{\mathcal{M}_{63}(e) \mid e = 2^{35}(2^{35} w_{r,i} + 2^{3} w_{r,j}) + 2^{3}(2^{35} w_{r,s} + 2^{3} w_{r,t}), 1 \leq i, j, s, t \leq |w_r|\}, \\
&= \{\mathcal{M}_{63}(e) \mid e = 2^{38}(w_{r,i} + w_{r,s}) + 2^{7} w_{r,j} + 2^{6} w_{r,t}, 1 \leq i, j, s, t \leq |w_r|\},
\end{aligned}
$$

- Why we consider w_{r+2}: 2 rounds are treated as 1 round in Chaghri.

Throughout this slide, we have

$$w_r = \left\{w_{r,1}, w_{r,2}, \ldots, w_{r,|w_r|}\right\}.$$

Degree Evaluation for Chaghri via Enumeration

Step 3: Compute w_r

- Initial set:

$$w_0 = \{0, 1\}.$$

- Compute w_{r+2} with

$$\begin{aligned} w_{r+2} &= \{\mathcal{M}_{63}(e) \mid e = 2^{38}(w_{r,i} + w_{r,s}) + 2^7 w_{r,i} + 2^6 w_{r,t}, \\ &\quad 1 \le i, j, s, t \le |w_r|\}. \end{aligned}$$

- Naive enumeration quickly becomes impractical as $|w_r|$ is too large even for small r.

Coefficient Grouping Technique

Motivation

- Do we really need to compute w_r round by round?
- Can we have a more elegant and general method that can work for any

$$S(x) = x^{2^{k_0}+2^{k_1}}, B(x) = c_1 x^{2^{k_2}} + c_2$$

and a general finite field $\mathbb{F}_{2^n}$?

Coefficient Grouping Technique

Using $S(x) = x^{2^{k_0}+2^{k_1}} \in \mathbb{F}_{2^n}[x], \quad B(x) = c_1 x^{2^{k_2}} + c_2 \in \mathbb{F}_{2^n}[x]$

- Relation between w_r and w_{r+1}:

$$w_{r+1} = \{\mathcal{M}_n(e) \mid e = 2^{k_0+k_2} w_{r,i} + 2^{k_1+k_2} w_{r,j}, 1 \leq i,j \leq |w_r|\}$$

- Relation between w_r and w_{r+2}:

$$\begin{aligned} & w_{r+2} \\ = \quad & \{\mathcal{M}_n(e) \mid e = 2^{k_0+k_2}(2^{k_0+k_2} w_{r,i} + 2^{k_1+k_2} w_{r,j}) + 2^{k_1+k_2}(2^{k_0+k_2} w_{r,s} + 2^{k_1+k_2} w_{r,t}), \\ & 1 \leq i,j,s,t \leq |w_r|\} \\ = \quad & \{\mathcal{M}_n(e) \mid e = 2^{2k_0+2k_2} w_{r,i} + 2^{k_0+k_1+2k_2}(w_{r,j} + w_{r,s}) + 2^{2k_1+2k_2} w_{r,t}, \\ & 1 \leq i,j,s,t \leq |w_r|\}. \end{aligned}$$

Coefficient Grouping Technique

Using $S(x) = x^{2^{k_0}+2^{k_1}} \in \mathbb{F}_{2^n}[x], \quad B(x) = c_1 x^{2^{k_2}} + c_2 \in \mathbb{F}_{2^n}[x]$

- Three important properties for $\mathcal{M}_n(x)$, i.e. mod $2^n - 1$:

$$\begin{aligned} \mathcal{M}_n(2^i) &= 2^{i \mod n}, \\ \mathcal{M}_n(x+y) &= \mathcal{M}_n(x) + \mathcal{M}_n(y), \\ \mathcal{M}_n(x \cdot y) &= \mathcal{M}_n\Big(\mathcal{M}_n(x) \cdot \mathcal{M}_n(y)\Big) \end{aligned}$$

Coefficient Grouping Technique

Using $S(x) = x^{2^{k_0}+2^{k_1}} \in \mathbb{F}_{2^n}[x], \quad B(x) = c_1 x^{2^{k_2}} + c_2 \in \mathbb{F}_{2^n}[x]$

- Relation between w_r and $w_{r+\ell}$:

$$w_{r+\ell} = \quad \{\mathcal{M}_n(e) \mid e = \sum_{i=1}^{N_{n-1}} 2^{n-1} w_{r,d_{i,n-1}} + \sum_{i=1}^{N_{n-2}} 2^{n-2} w_{r,d_{i,n-2}} + \ldots + \sum_{i=1}^{N_0} 2^0 w_{r,d_{i,0}}, \text{ where } 1 \le d_{i,j} \le |w_r| \text{ for } 0 \le j \le n-1\}.$$

- Group all possible N_j coefficients sharing the same factor 2^j:

$$w_{r,d_{1,j}}, w_{r,d_{2,j}}, \ldots, w_{r,d_{N_j,j}} \in w_r \ (r = 0, \ w_0 = \{0,1\}),$$

i.e., in the formula of e, $2^j w_{r,d_{i,j}}$ is possible to appear

- $w_{r+\ell}$ is fully described by a vector $(N_{n-1}, \ldots, N_0)$ and w_r.

Coefficient Grouping Technique

New representation of w_r

- $r = 0$:

$$\begin{aligned} w_0 &= \{0,1\} = \{\mathcal{M}_n(e) \mid e = 2^0 w_{0,i}, 1 \le i \le 2 = |w_0|\}, \\ &\rightarrow (N^0_{n-1}, \ldots, N^0_1) = (0, \ldots, 0), \quad N^0_0 = 1. \end{aligned}$$

- Relation between w_r and w_{r+1}:

$$w_{r+1} = \{\mathcal{M}_n(e) \mid e = 2^{k_0+k_2} w_{r,i} + 2^{k_1+k_2} w_{r,j}, 1 \le i,j \le |w_r|\}$$

- Find $(N^r_{n-1}, \ldots, N^r_0)$ to represent w_r:

$$N^{r+1}_i = N^r_{(i-(k_1+k_2))\%n} + N^r_{(i-(k_0+k_2))\%n} \text{ for } 0 \le i \le n-1.$$

- $(N^r_{n-1}, \ldots, N^r_0)$ can be computed in time $O(n)$.

Coefficient Grouping Technique

Finding two representations of w_r

- Representation 1 of w_r:

$$w_r = \Big\{ \mathcal{M}_n(e) \mid e = \sum_{i=1}^{N_{n-1}^r} 2^{n-1} w_{0,d_{i,n-1}} + \sum_{i=1}^{N_{n-2}^r} 2^{n-2} w_{0,d_{i,n-2}} + \ldots + \sum_{i=1}^{N_0^r} 2^0 w_{0,d_{i,0}}, \\ \text{where } 1 \le d_{i,j} \le |w_0| \text{ for } 0 \le j \le n-1 \text{ and } w_0 = \{0,1\} \Big\}.$$

- For each term 2^j, there are N_j^r possible coefficients

$$w_{0,d_{1,j}}, w_{0,d_{2,j}}, \ldots, w_{0,d_{N_j,j}} \in w_0 = \{0,1\},$$

which implies $\sum_{i=1}^{N_j^r} 2^j w_{0,d_{i,j}} \in \{2^j \gamma_j \mid 0 \le \gamma_j \le N_j^r\}$.

Coefficient Grouping Technique

Finding $e \in w_r$ with $H(e)$ maximal

- Representation 2 of w_r:

$$w_r = \{\mathcal{M}_n(e) \mid e = \sum_{i=0}^{n-1} 2^i \gamma_i,\ 0 \le \gamma_i \le N_i^r\}.$$

- Problem reduction (optimization problem):

$$\begin{aligned} \text{maximize} \quad & H\left(\mathcal{M}_n(\sum_{i=0}^{n-1} 2^i \gamma_i)\right), \\ \text{subject to} \quad & 0 \le \gamma_i \le N_i^r \text{ for } i \in [0, n-1]. \end{aligned}$$

- Solved in time $O(n)$!!! or by blackbox solvers.
  - finding and proving the $O(n)$ algorithm require significant additional work

The $\mathcal{O}(n)$ Algorithm

Goal: Reduce $(N^i_{n-1}, \ldots, N^i_0)$ to an equivalent $(N'^i_{n-1}, \ldots, N'^i_0)$.
Idea: 1. Find nonzero $N^i_j = 2a + b$ where $b \in \{1, 2\}$.
2. Let $N'^i_{j+1} = N^i_{j+1} + a$ and $N'^i_j = b$.

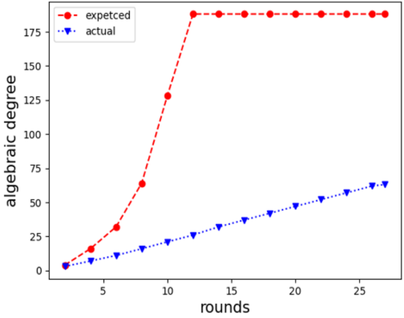
$$
\begin{aligned}
& (N^i_4, N^i_3, N^i_2, N^i_1, N^i_0) \\
= \quad & (0, 6, 7, 0, 0) \\
\to \quad & (0, 6, 7, 0, 0) \\
\to \quad & (0, 6, 7, 0, 0) \text{ [as } 7 = 2 \times 3 + 1] \\
\to \quad & (0, 6 + 3, 1, 0, 0) = (0, 9, 1, 1, 0) \text{ [as } 9 = 2 \times 4 + 1] \\
\to \quad & (0 + 4, 1, 1, 0, 0) = (4, 1, 1, 0, 0) \text{ [as } 2 = 2 \times 1 + 2] \\
\to \quad & (2, 1, 1, 0, 0 + 1) = (2, 1, 1, 0, 1) \text{ [as } 1 = 2 \times 0 + 1] \\
= \quad & (N'^i_4, N'^i_3, N'^i_2, N'^i_1, N'^i_0)
\end{aligned}
$$

The solution to the optimization problem is 4 (4 nonzero elements in the reduced vector.).

Breaking Chaghri and even More rounds

Table: The upper bounds of the algebraic degree for Chaghri

r	0	2	4	6	8	10	12	14	16	18	20	22	24	25	26
deg	1	3	7	12	17	22	27	32	37	42	47	52	58	60	63



Rescuing Chaghri

Achieving an (almost) exponential degree growth

- The slow growth is mainly caused by a sparse polynomial of $B(x)$, i.e. $B(x) = c_0 x^{2^3} + c_1$
- Reason: the growth of the number of possible monomials is highly related to the density of $B(x)$
  - requires significant additional work
- Intuition: more possible monomials, higher probability that a monomial with $\deg = 2^r$ appears
- Use $B(x) = c_0 x^{2^8} + c_1 x^{2^2} + c_2 x + c_3$ instead

Further Evolution

Let us consider $S(x) = x^{2^d+1}$ and $B(x) = c_0 + \sum_{i=1}^{w} c_i x^{2^{h_i}}$

Motivation

1. What is the generic upper bound if $w = 1$?
2. How to establish theoretic relations between w and the growth of the algebraic degree?
3. How to efficiently find $(h_1, \ldots, h_w)$ to achieve the exponential growth where w is as small as possible?
4. How to upper bound the algebraic degree for arbitrary $B(x)$?

Our Results

- If $w = 1$, there is an absolute upper bound:

$$r^2 - 2r + 3,$$

  i.e. at most quadratic increase!!!

- General influence of w: for $w = 2/3/4$, the exponential growth can never be achieved at the 4th/7th/10th rounds, i.e. the algebraic degree can never be $2^4/2^7/2^{10}$ at these rounds. For other w, we can deduce similar conclusions.

Our Results

- Finding $(h_1, \ldots, h_w)$ to achieve the exponential growth: reduced to the feasibility to select 2^r different elements from $r+1$ sets of integers under some constraints.
- Efficiently find upper bounds for arbitrary $B(x)$, though they may be loose sometimes.

Our Results

Degree evaluation for arbitrary $B(x)$ at round r

$$
\begin{aligned}
\text{maximize } & H\left(\mathcal{M}_n\left(\sum_{i=1}^{|Z|} 2^{z_i}\gamma_{z_i}\right)\right), \\
\text{subject to } & \gamma_{z_i} \geq 0; \\
& \sum_{i=1}^{|Z|} \gamma_{z_i} \leq 2^r; \\
& \left|\{z_i \mid \gamma_{z_i} \neq 0\}\right| \leq t.
\end{aligned}
$$

where the set $Z = \{z_1, \ldots, z_{|Z|}\} \subseteq \{0, 1, \ldots, n-1\}$ and the integer $t \in [0, n-1]$ can be efficiently computed in advance.

Efficient ad-hoc algorithms?

Our Results

Example:

$$n = 20, \quad Z = \{1, 3, 5, 8, 10, 14\}, \quad t = 5, \quad r = 15$$

Optimization problem:

$$\begin{aligned}
\text{maximize} \;\; & H\left(\mathcal{M}_{20}\left(2\gamma_1 + 2^3\gamma_3 + 2^5\gamma_5 + 2^8\gamma_8 + 2^{10}\gamma_{10} + 2^{14}\gamma_{14}\right)\right), \\
\text{subject to} \;\; & \gamma_1, \gamma_3, \gamma_5, \gamma_8, \gamma_{10}, \gamma_{14} \geq 0; \\
& \gamma_2 + \gamma_3 + \gamma_5 + \gamma_8 + \gamma_{10} + \gamma_{14} \leq 2^{15}; \\
& |\{i \mid \gamma_i \neq 0\}| \leq 5, \;\; \forall i \in \{1, 3, 5, 8, 10, 14\}
\end{aligned}$$

Conclusion

- An efficient degree evaluation technique in time $O(n)$ for a special cipher over $\mathbb{F}_{2^n}$
- Be careful of the symmetric-key primitive design over a large finite field! (less understood)
- Open problems:
  - Further improve our method for arbitrary $B(x)$.
  - Study the influence of the matrix M.
  - Develop other novel cryptanalytic techniques for ciphers over a large finite field