Coefficient Grouping: Breaking **Chaghri** and More

Fukang Liu[1], Ravi Anand[1], Libo Wang[1], Willi Meier[4], Takanori Isobe[1,2,3]

[1]University of Hyogo, Japan
[2]NICT, Japan
[3]PRESTO, Japan,
[4]FHNW, Switzerland

willimeier48@gmail.com

FrisiaCrypt 2022, September 26, 2022

Overview

Background of **Chaghri**

- **Chaghri**: FHE-friendly block cipher, designed by Ashur, Mahzoun, and Toprakhisar (to appear at ACM CCS 2022).
- SPN network.
- Defined over large field $\mathbb{F}_{2^{63}}$.
- About 65% faster than AES.
- Block consists of 3 words of size 63 bits; 8 rounds. Each round has two steps.
- Designed to have low multiplicative depth.

Description of **Chaghri**

State of **Chaghri**: $a = (a_1, a_2, a_3) \in \mathbb{F}_{2^{63}}^3$.

Round function $\mathtt{R}(a)$ of its decryption is described in next Algorithm.

Consider decryption because designers choose the secure number of rounds by mainly analyzing the security of decryption, and their aim was to optimize decryption.

Description of **Chaghri**

Round function of **Chaghri** at the $(j+1)^{st}$ round where $0 \leq j \leq 7$:

$a_i = G(a_i)$ for $i \in \{1,2,3\}$
$a_i = B(a_i)$ for $i \in \{1,2,3\}$
$a = M \cdot (a_1, a_2, a_3)^T$
$a_i = a_i + RK[2j+1]_i$ for $i \in \{1,2,3\}$
$a_i = G(a_i)$ for $i \in \{1,2,3\}$
$a_i = B(a_i)$ for $i \in \{1,2,3\}$
$a = M \cdot (a_1, a_2, a_3)^T$
$a_i = a_i + RK[2j+2]_i$ for $i \in \{1,2,3\}$

Round key $RK[j] = (RK[j]_1, RK[j]_2, RK[j]_3) \in \mathbb{F}_{2^{63}}^3$ is generated from a master key $K = (K_1, K_2, K_3) \in \mathbb{F}_{2^{63}}^3$. Whitening key is $RK[0] = (RK[0]_1, RK[0]_2, RK[0]_3)$.

Description of **Chaghri**

Components G, B and M used in round function:

Nonlinear function $G(x) : \mathbb{F}_{2^{63}} \to \mathbb{F}_{2^{63}}$**.** $G(x)$ is defined as $G(x) = x^{2^{32}+1}$.

Affine transform $B(x) : \mathbb{F}_{2^{63}} \to \mathbb{F}_{2^{63}}$**.** $B(x)$ is defined as $B(x) = c_1 x^{2^3} + c_2$ where $c_1, c_2 \in \mathbb{F}_{2^{63}}$ are constants.

Linear transform $M : \mathbb{F}_{2^{63}}^3 \to \mathbb{F}_{2^{63}}^3$**.** M is a 3×3 MDS matrix. M not specified by designers. Our attacks apply to any choice of M.

Definition of one step. According to the round function described in the Algorithm, the round function is $\mathtt{R}(a) = AK \circ M \circ B \circ S \circ AK \circ M \circ B \circ S(a)$. One step of **Chaghri** is defined as $AK \circ M \circ B \circ S(a)$. Call it the step function of **Chaghri**.

Description of **Chaghri**

Notation for the internal state. Denote the internal state after i steps by $(z_{i,1}, z_{i,2}, z_{i,3})$.

For example, the input state is $(z_{0,1}, z_{0,2}, z_{0,3})$, the internal state after 1 step is $(z_{1,1}, z_{1,2}, z_{1,3})$, and the internal state after 1 round is $(z_{2,1}, z_{2,2}, z_{2,3})$.

Consider R steps of **Chaghri**. Total number of steps is 16. However, our attack can even apply if $R > 16$. Do not restrict the maximal value of R.

On finite fields

For a prime number p and a positive integer n, the finite field $\mathbb{F}_{p^n}$ consists of a set of p^n numbers.

Let α be a primitive element of $\mathbb{F}_{p^n}$. Then each element x in the finite field $\mathbb{F}_{p^n}$ can be written as

$$x = \sum_{i=0}^{n-1} \beta_i \alpha^i,$$

where $\beta_i \in [0, p-1]$. Moreover, the set $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is said to be a polynomial basis of $\mathbb{F}_{p^n}$. For the element $x \in \mathbb{F}_{p^n}$,

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

On finite fields

For two monomials X^a and X^b in the polynomial ring $\mathbb{F}_{2^n}[X]$, one has $X^a \cdot X^b = X^{\mathcal{M}_n(a+b)}$, where $\mathcal{M}_n(x)$ $(x \geq 0)$ is defined as:

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

By the definition of $\mathcal{M}_n(x)$, we have $\mathcal{M}_n(x_1 + x_2) = \mathcal{M}_n(\mathcal{M}_n(x_1) + \mathcal{M}_n(x_2))$, $\mathcal{M}_n(2^i) = 2^{i\%n}$ and $\mathcal{M}_n(2^i x) = \mathcal{M}_n(2^{i\%n}\mathcal{M}_n(x))$ for $i \geq 0$.

Furthermore

$$(x + y)^{p^i} = x^{p^i} + y^{p^i}$$

for $\forall x, y \in \mathbb{F}_{p^n}$ and $i \geq 0$.

Higher-Order Differentials in $\mathbb{F}_{2^n}$

For a given function $\mathcal{F} : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, there always exists a vectorial Boolean function $\mathcal{G} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ such that

$$\begin{aligned} \sigma : \sum_{i=0}^{n-1} \beta_i \alpha^i &\mapsto (\beta_0, \beta_1, \ldots, \beta_{n-1}) \in \mathbb{F}_2^n, \\ \sigma(\mathcal{F}(x)) &= \mathcal{G}(\sigma(x)) \ \forall x \in \mathbb{F}_{2^n}, \end{aligned}$$

where $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a polynomial basis of $\mathbb{F}_{2^n}$.

Let $\deg(\mathcal{G})$ be the algebraic degree of $\mathcal{G}$. For the higher-order differential attack, given any affine vector subspace V of dimension $\deg(\mathcal{G}) + 1$ from $\mathbb{F}_2^n$, one has $\sum_{v \in V} \mathcal{G}(v) = 0$. This implies

$$\sum_{(\beta_0, \beta_1, \ldots, \beta_{n-1}) \in V} \mathcal{F}\left(\sum_{i=0}^{n-1} \beta_i \alpha^i\right) = 0.$$

Higher-Order Differentials in $\mathbb{F}_{2^n}$

$\deg(\mathcal{G})$ is related to the univariate representation of $\mathcal{F}$: The univariate representation of $\mathcal{F}$ is

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

where $u_i \in \mathbb{F}_{2^n}$ for $i \in [0, 2^n - 1]$. The univariate degree of $\mathcal{F}$ denoted by $D^u_{\mathcal{F}}$ is defined as:

$$D^u_{\mathcal{F}} = \max\{i : i \in [0, 2^n - 1], u_i \neq 0\}.$$

Then, $\deg(\mathcal{G})$ can be computed as follows:

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

$\max\{H(i) : i \in [0, 2^n - 1], u_i \neq 0\}$ is also called the algebraic degree of $\mathcal{F}$ denoted by $D^a_{\mathcal{F}}$.

Higher-Order Differentials in $\mathbb{F}_{2^n}$

Examples. Consider two univariate polynomials $F_1, F_2 \in \mathbb{F}_{2^{63}}[X]$, where

$$F_1 = X^{2^{30}+2^{31}} + X^{2^1+2^3+2^4}, \ F_2 = X^{2^{60}+2^{31}+2^2+2^3} + X^{2^{61}+2^{31}}.$$

Then, we have

$$D^u_{F_1} = 2^{30} + 2^{31}, D^a_{F_1} = 3, \ D^u_{F_2} = 2^{61} + 2^{31}, D^a_{F_2} = 4.$$

Higher-order differential attacks can also be extended to the multivariate case.

How to Attack **Chaghri**

Previous methods for estimating degrees of iterated constructions over finite fields don't seem to suggest an attack on **Chaghri**.

Propose Coefficient Grouping for the degree evaluation of **Chaghri**.

Core idea: Describe a set of exponents with just a single vector of integers. Thus propagation of the exponents is reduced to studying the propagation of the vectors.

Efficiency of this method is due to these facts: Propagation of the vectors is deterministic and can be described in iterative manner. Time complexity to compute the vectors increases linearly in the number of attacked rounds.

After computing the vectors, bounding the algebraic degree is then reduced to a natural optimization problem, solvable with suitable solvers.

Attack Settings

Focus on its application to the univariate polynomial. But the method can be extended to the multivariate case.

A more general form of $S(x)$ and $B(x)$:

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

Consider the finite field $\mathbb{F}_{2^n}$, i.e. the internal state $a = (a_1, a_2, a_3)$ of **Chaghri** satisfies $a_i \in \mathbb{F}_{2^n}$ for $i \in [1, 3]$ (with constraints on (k_0, k_1, n) so that $S(x)$ is a permutation).

For **Chaghri**, $(k_0, k_1, k_2) = (32, 0, 3)$ and $n = 63$.

Attack Settings

Consider an input state which can be represented as univariate polynomials in the variable $X \in \mathbb{F}_{2^n}$, as shown:

$$z_{0,1} = A_{0,1}X + B_{0,1},\ z_{0,2} = A_{0,2}X + B_{0,2},\ z_{0,3} = A_{0,3}X + B_{0,3},\ (1)$$

where $A_{0,i}, B_{0,i} \in \mathbb{F}_{2^n}$ $(1 \leq i \leq 3)$ are randomly chosen constants.

In this way, after an arbitrary number of steps, each state word can be represented as a univariate polynomial in X.

Aim: Compute the upper bound $D_{r,i}$ for the algebraic degree of the univariate polynomial $P_{r,i}(X)$ where $z_{r,i} = P_{r,i}(X)$ $(1 \leq i \leq 3)$.

Attack Settings

Upper bound for the algebraic degree of r-step **Chaghri** is $D_r = \max\{D_{r,1}, D_{r,2}, D_{r,3}\}$.

Hence, if $D_r < n$, there exists a higher-order differential attack on r steps of **Chaghri** with time and data complexity 2^{D_r+1}.

Specifically, can consider an input state of the following form:

$$z_{0,1} = X_1, \ z_{0,2} = A_2, \ z_{0,3} = A_3,$$

where $A_2, A_3 \in \mathbb{F}_{2^n}$ are randomly chosen constants and X is the variable.

Tracing Polynomials

With the input form shown in (1), the state words $(z_{r,1}, z_{r,2}, z_{r,3})$ can be written as univariate polynomials of the form:

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

Here $A_{r,i}, B_{r,i}, C_{r,i} \in \mathbb{F}_{2^n}$ are constants depending on the key. The set

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

means the set of exponents for the univariate polynomials after r steps. Mention that for $r = 0$, we have

$$w_0 = \{0, 1\}, \tag{2}$$

which corresponds to the input form specified in (1).

Evolution of polynomial representations

We know that

$$D_r \leq \max\{H(w_{r,i}) : 1 \leq i \leq |w_r|\}. \tag{3}$$

How do the univariate polynomials representing $(z_{r+1,1}, z_{r+1,2}, z_{r+1,3})$ evolve through the step function?
For $G(z_{r,1})$, we have

$$\begin{aligned} G(z_{r,1}) &= (\sum_{i=1}^{|w_r|} A_{r,i} X^{w_{r,i}})^{2^{k_0}+2^{k_1}} \\ &= (\sum_{i=1}^{|w_r|} A_{r,i} X^{w_{r,i}})^{2^{k_0}} (\sum_{j=1}^{|w_r|} A_{r,j} X^{w_{r,j}})^{2^{k_1}} \\ &= \sum_{i=1}^{|w_r|} \sum_{j=1}^{|w_r|} A_{r,i,j} X^{\mathcal{M}_n(2^{k_0} w_{r,i} + 2^{k_1} w_{r,j})}. \end{aligned}$$

Evolution of polynomial representations

Here $A_{r,i,j} \in \mathbb{F}_{2^n}$ are still constants depending on the key.

For $B \circ G(z_{r,1})$, we get

$$\begin{aligned} B \circ G(z_{r,1}) &= c_1\Big(\sum_{i=1}^{|w_r|}\sum_{j=1}^{|w_r|} A_{r,i,j} X^{\mathcal{M}_n(2^{k_0} w_{r,i} + 2^{k_1} w_{r,j})}\Big)^{2^{k_2}} + c_2 \\ &= \sum_{i=1}^{|w_r|}\sum_{j=1}^{|w_r|} A'_{r,i,j} X^{\mathcal{M}_n(2^{k_0+k_2} w_{r,i} + 2^{k_1+k_2} w_{r,j})}. \end{aligned}$$

Evolution of polynomial representations

Similar expressions for the other two components, with other constants.
Therefore obtain

$$z_{r+1,1} = \sum_{i=1}^{|w_r|} \sum_{j=1}^{|w_r|} A_{r+1,i,j} X^{\mathcal{M}_n(2^{k_0+k_2} w_{r,i} + 2^{k_1+k_2} w_{r,j})}.$$

and similar for the two other components.
Hence, we obtain an iterative relation between the sets w_r and w_{r+1}:

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

Evolution of polynomial representations

Thus for each element $e \in w_{r+2}$, there must exist (i, j, s, t) where $1 \leq i, j, s, t \leq |w_r|$ such that

$$e = \mathcal{M}_n(2^{k_0+k_2}(2^{k_0+k_2} w_{r,i} + 2^{k_1+k_2} w_{r,j}) + 2^{k_1+k_2}(2^{k_0+k_2} w_{r,s} + 2^{k_1+k_2} w_{r,t})).$$

In other words,

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

Evolution of polynomial representations

For the concrete parameters of **Chaghri**:

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

Evolution of polynomial representations

There exists another general representation of the set $w_{r+\ell}$.

Each set w_r can be fully described with a vector of integers $(N^r_{n-1}, N^r_{n-1}, \ldots, N^r_0)$.

For w_0, this vector is

$$N^0_0 = 1, N^0_i = 0 \ (1 \leq i \leq n-1).$$

For the N_i's a recursive relation can be derived:

$$N^{r+1}_i = N^r_{(i-k_1-k_2)\%n} + N^r_{(i-k_0-k_2)\%n} \text{ for } 0 \leq i \leq n-1, r \geq 0. \quad (4)$$

Evolution of polynomial representations

For any w_r, the corresponding vector of integers $(N^r_{n-1}, N^r_{n-1}, \ldots, N^r_0)$ can be computed in linear time, i.e. with rn times of simple integer additions.

Then, the set w_r can be described as follows:

$$\begin{aligned} w_r \quad = \quad & \{e | e = \mathcal{M}_n(\sum_{i=1}^{N^r_{n-1}} 2^{n-1} w_{0,d_{i,n-1}} + \sum_{i=1}^{N^r_{n-2}} 2^{n-2} w_{0,d_{i,n-2}} + \quad (5) \\ & \ldots + \sum_{i=1}^{N^r_0} 2^0 w_{0,d_{i,0}}), \\ & \text{where } 1 \leq d_{i,j} \leq |w_0| \text{ for } 0 \leq j \leq n-1 \}. \quad (6) \end{aligned}$$

Application to the Chaghri Parameters

Concrete parameters of **Chaghri**:

For w_1 the corresponding $(N^1_{62}, N^1_{61}, \ldots, N^1_0)$ is

$$N^1_3 = 1, N^1_{35} = 1, N^1_i = 0 \ (i \notin \{3, 35\}, 0 \leq i \leq 62).$$

While for w_2, the corresponding $(N^2_{62}, N^2_{61}, \ldots, N^2_0)$ is

$$N^2_6 = 1, N^2_7 = 1, N^2_{38} = 2, N^2_i = 0 \ (i \notin \{6, 7, 38\}, 0 \leq i \leq 62).$$

For any w_r, we can compute the corresponding $(N^r_{62}, N^r_{61}, \ldots, N^r_0)$ in linear time.

A Natural Optimization Problem

How to compute D_r after giving the vector of integers $(N^r_{n-1}, N^r_{n-2}, \ldots, N^r_0)$?

Can interpret representation of w_r equivalently: There are in total $N^r_{n-1} + N^r_{n-2} + \ldots + N^r_0$ possible variables that can independently take values from $w_0 = \{0, 1\}$.

Hence, the problem to bound D_r becomes a natural optimization problem:

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

Can be solved by a suitable MILP problem, and with additional work in linear time (skipped here).

A Natural Optimization Problem

For each coefficient 2^i, there are N_i^r corresponding independent variables taking values from $w_0 = \{0, 1\}$.

Can choose γ_i variables taking the value 1 and the remaining $N_i^r - \gamma_i$ variables taking the value 0.

Therefore, we have the constraints $0 \leq \gamma_i \leq N_i^r$. Note that γ_i indeed represents the number of variables which take nonzero values.

Cryptanalysis of Full-round Chaghri

With the above model, the upper bounds for the degree D_r after r steps are obtained in seconds:

Table: The upper bounds for D_r

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

Can mount a higher-order differential attack on full 8 rounds of **Chaghri** with data and time complexity of 2^{38}.

There is a higher-order differential distinguisher for 12.5 rounds with time and data complexity of 2^{61}. Can refine this to a distinguisher for 13 rounds with time and data complexity of 2^{63}.

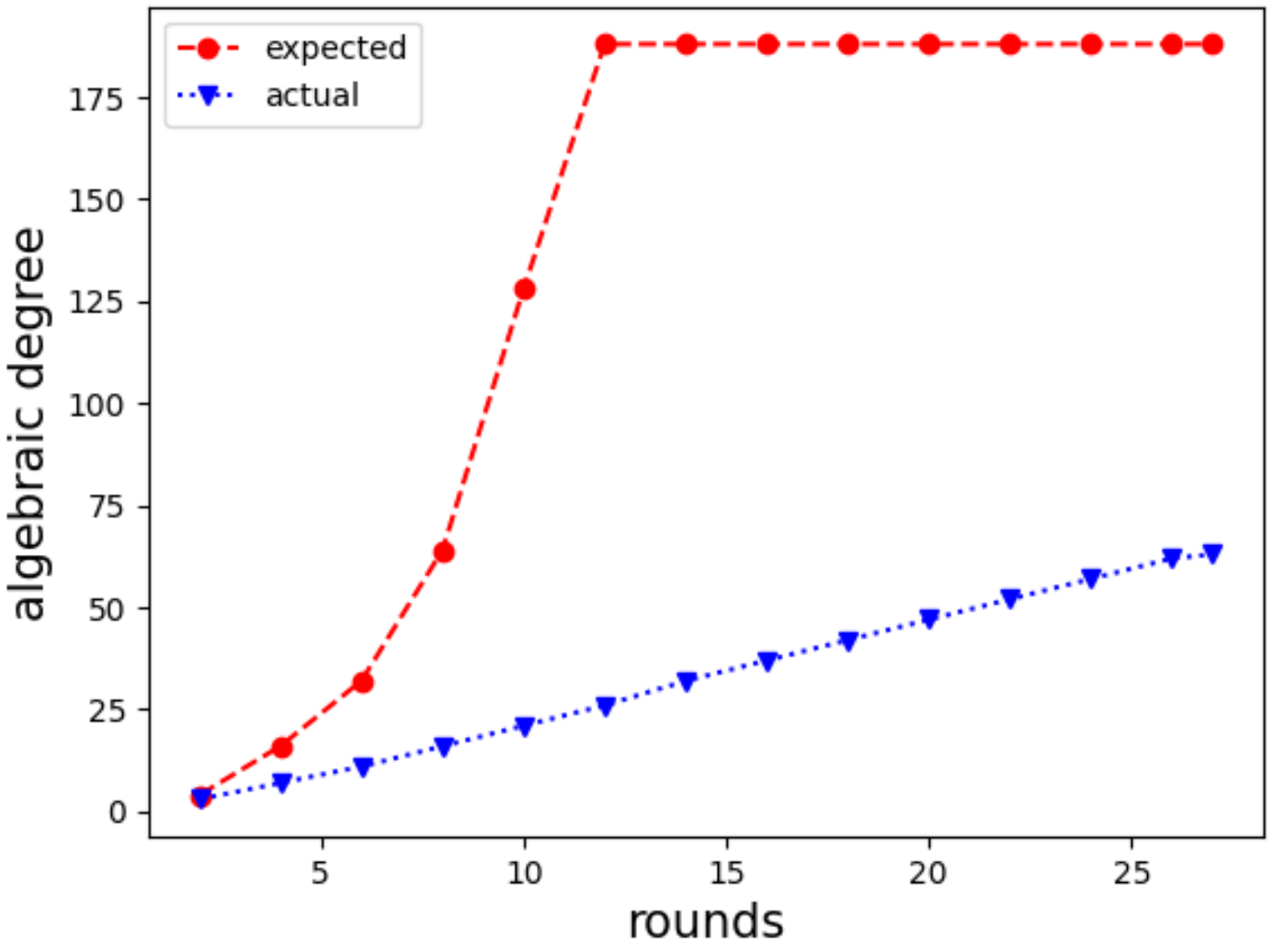
Cryptanalysis of Full-round Chaghri

Can derive a key recovery attack on 13.5 round **Chaghri** with time complexity about 2^{120} and data complexity 2^{63}.

Have considered univariate case with only one variable X. Can extend methods and degree bounds to multivariate case with more variables.

Refined degree bounds are possible. Practical experiments on up to 7 rounds show that these bounds are tight.

Cryptanalysis of Full-round Chaghri



Achieving Exponential Degree Increase

Design of (initial) **Chaghri** follows well established principles.

Which component(s) in **Chaghri** prevent(s) exponential degree increase?

For FHE-friendly ciphers, reducing the multiplicative depth is of great importance. Hence, we still keep the S-box of the form $S(x) = x^{2^{k_0}+2^{k_1}}$, which has algebraic degree 2.

Transform $B(x)$ is affine over $\mathbb{F}_{2^n}$. Almost cost-free for FHE protocols.
Can we choose a different $B(x)$ that provides an exponential increase of the algebraic degree?

Achieving (almost) exponential degree increase

In a search for secure affine transforms, consider a general form of $B(x)$:

$$B(x) = \sum_{i=1}^{|\mathcal{L}|} c'_i x^{2^{\varphi_i}},$$

where $(c'_1, c'_2, \ldots, c'_{|\mathcal{L}|})$ are constants in $\mathbb{F}_{2^{63}}$ such that $B(x)$ is a permutation and $\mathcal{L} = \{\varphi_1, \varphi_2, \ldots, \varphi_{|\mathcal{L}|}\}$. For the S-box, we keep using $S(x) = x^{2^{32}+1}$.

Application of coefficient grouping technique for this general $B(x)$ needs to adjust the general polynomial representation of $(z_{r,1}, z_{r,2}, z_{r,3})$ (and more things; skipped).

Achieving (almost) exponential degree increase

A dedicated search method for affine transforms is developed. This does not find secure candidates for $\mathcal{L}$ when $|\mathcal{L}| = 2$.

However this strategy finds that $\mathcal{L} = \{0, 2, 8\}$ is such a candidate.

With $\mathcal{L} = \{0, 2, 8\}$, for the initial input chosen with a single variable X, the algebraic degree can reach 63 after 7 steps. Therefore, for this input form, the algebraic degree can reach 63 after 8 steps.In this way, an almost exponential increase of the algebraic degree is achieved in the univariate setting.

This method can be extended to two and three input variables, respectively.

According to our findings, designers have updated their cipher **Chaghri**.

New Parameters for Chaghri

Designers of **Chaghri** have chosen the total number of rounds T with the formula

$$T = 1.5 \times \max\{5, \eta\},$$

where η is the maximal number of rounds that can be attacked with time complexity below 2^{128}. With $\mathcal{L} = \{0, 2, 8\}$, we have $\eta = 4$ and hence the total number of rounds T can be kept unchanged, i.e. $T = 8$.

We give an optional assignment to (c_1', c_2', c_3', c_4') such that $B(x) = c_1'x + c_2'x^4 + c_3'x^{256} + c_4'$ is a permutation. In their updated cipher, designers chose a different assignment.

Conclusions

- We perform an in-depth study on the increase of the algebraic degree of **Chaghri** by proposing a novel efficient technique called coefficient grouping.
- This technique is different from known methods, and can well capture how the exponents of the polynomials propagate through the round function.
- Break the full 8 rounds of **Chaghri** with a practical time and data complexity and can even break up to 13.5 rounds.
- Coefficient grouping is a generic method and potentially has other applications.
- Have not only attacked a modern cipher with it, but also describe how to use it to search for secure cryptographic components.

Thank you