

On the limits of integral attacks on block cryptographic algorithms

Anastasiia Chichaeva
Vasily Shishkin

- ▶ J. Daemen, L. Knudsen, V. Rijmen, «The block cipher Square», Fast Software Encryption: 4th International Workshop, Proceedings, Springer, 1997, 149–165.
- ▶ A. Biryukov, A. Shamir «Structural cryptanalysis of SASAS», International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2001, 395–405.
- ▶ L. Knudsen, D. Wagner «Integral cryptanalysis», International Workshop on Fast Software Encryption, FSE 2002, Springer, 2002, 112–127.
- ▶ S. Lucks «The saturation attack —a bait for Twofish». International Workshop on Fast Software Encryption, Springer, 2001, 1–15.

1. Choose a **structured set** of plaintexts.
2. **Build a distinguisher**: encrypt the set through r rounds and track the XOR of bytes to find a predictable property.

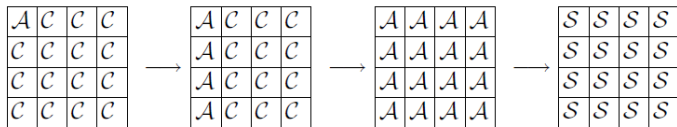


Figure: A 3-round integral distinguisher for Rijndael

1. Choose a structured set of plaintexts.
2. Build a distinguisher: encrypt the set through r rounds and track the XOR of bytes to find a predictable property.
3. Encrypt the set with the full cipher (or $r + i$ rounds) to get the real ciphertexts.

1. Choose a structured set of plaintexts.
2. Build a distinguisher: encrypt the set through r rounds and track the XOR of bytes to find a predictable property.
3. Encrypt the set with the full cipher (or $r + i$ rounds) to get the real ciphertexts.
4. Guess the last round key(s). Partially decrypt the final ciphertexts.

1. Choose a structured set of plaintexts.
2. Build a distinguisher: encrypt the set through r rounds and track the XOR of bytes to find a predictable property.
3. Encrypt the set with the full cipher (or $r + i$ rounds) to get the real ciphertexts.
4. Guess the last round key(s). Partially decrypt the final ciphertexts.
5. Check if the partially decrypted values match the expected integral property.

SKINNY-64	PRESENT	SIMON-64	AES	Kuznyechik
12	9	18	4	4

Table: Number of rounds of known integral distinguishers

- What is the maximum number of rounds for which an integral distinguisher exists?



- ▶ What is the maximum number of rounds for which an integral distinguisher exists?



The integral attack exploits a low algebraic degree to build a distinguisher.

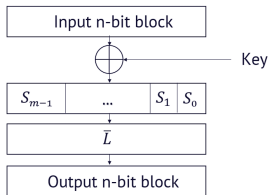
- ▶ How does the algebraic degree evolve with the number of rounds?

- ▶ $\deg(f)$ – is the degree of ANF of Boolean function $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$
- ▶ The degree of a vectorial function $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ is defined as
$$\deg(F) = \max_{i=1,\dots,m} \deg(f_i)$$
- ▶ Function $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ is balanced if each element in $\mathbb{F}_2^m$ has exactly 2^{n-m} preimages

n -bit block, s -bit S-boxes, $n = ms$

Round of the XSL-scheme:

- ▶ X is the XOR with the round key;
- ▶ S is a nonlinear transformation (concatenation of smaller S-boxes);
- ▶ L is a linear transformation.



XSL-scheme can be considered as $A(SA)^r$ scheme (A — affine function).

Algebraic degree of a composed function

A naive approach: $\deg(GF) \leq \deg(G) \cdot \deg(F)$



About $\log_t(n)$ rounds are needed to achieve full degree

Theorem (Algebraic degree of a composed function¹)

Let F be a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$ corresponding to the concatenation of m smaller balanced S -boxes, $S_1, \dots, S_m$, defined over $\mathbb{F}_2^s$. Then, for any function $G : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^\ell$, we have:

$$\deg(GF) \leq n - \frac{n - \deg(G)}{s - 1}.$$

Moreover, if $s \geq 3$ and all S -boxes have degree at most $s - 2$, we have:

$$\deg(GF) \leq n - \frac{n - \deg(G)}{s - 2}.$$

¹C. Boura, A. Canteaut, C. De Cannière «Higher-order differential properties of Keccak and Luffa», FSE 2011, Springer, 2011, 252–269.

Theorem (C. Carlet²)

For every permutation $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ and every $G : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^\ell$, we have:

$$\deg(GF) \leq n - \left\lceil \frac{n - \deg(G)}{\deg(F^{-1})} \right\rceil.$$

²C. Carlet «Graph indicators of vectorial functions and bounds on the algebraic degree of composite functions», IEEE Transactions on Information Theory, 66:12 (2020), 7702–7716

Algebraic degree of XSL-scheme with S-Boxes, that have maximum algebraic degree $s - 1$, is considered in the paper:

- ▶ A. Biryukov, D. Khovratovich, L. P. Perrin «Multiset-algebraic cryptanalysis of reduced Kuznyechik, Khazad, and secret SPNs», IACR Transactions on Symmetric Cryptology 2016:2

Theorem

Let A be an affine function, S – a function corresponding to the concatenation of m smaller balanced S -boxes, defined over $\mathbb{F}_2^s$ ($S, A : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$). S has degree t ($t \leq s - 2$). Let $d = \min(\deg(S^{-1}), s - 2)$. For all $\ell \leq \lfloor \log_t(n) \rfloor$, $r \leq \lfloor \log_d(n) \rfloor$ it holds that:

$$\deg(A(SA)^{\ell+r}) \leq n - (\psi_r + \left\lfloor \frac{n}{d^r} \right\rfloor - \left\lfloor \frac{t^\ell}{d^r} \right\rfloor),$$

where

$$\psi_1 = \left\lfloor \frac{n_0 - t_0}{d} \right\rfloor, \psi_{i+1} = \left\lfloor \frac{n_i - t_i + \psi_i}{d} \right\rfloor,$$

where $n = \sum_{i=0}^{\infty} n_i d^i$ and $t^\ell = \sum_{i=0}^{\infty} t_i d^i$ – the base d expansion of n and t^ℓ .

Bound on the degree of XSL-scheme

If we need $\deg(A(SA)^{\ell+r}) < n - k$, then it is sufficient that

$$\psi_r + \lfloor \frac{n}{d^r} \rfloor - \lfloor \frac{t^\ell}{d^r} \rfloor \geq k.$$

Let's consider the case when $\ell = \lfloor \log_t(n) \rfloor$, $n \neq t^\ell$, $r = \lfloor \log_d(n) \rfloor$.

$\psi_r = \lceil \frac{n_{r-1} - t_{r-1} + \psi_{r-1}}{d} \rceil$ is equal to 0 or 1.

- ▶ If $n_{r-1} > t_{r-1}$, then $\psi_r = 1$.
- ▶ If $n_{r-1} = t_{r-1}$ and $n_r = t_r$, then $\psi_r = 1$.
- ▶ If $n_{r-1} = t_{r-1}$ and $n_r > t_r$, then $\psi_r = 1 \Leftrightarrow \psi_{r-1} = 1$.
- ▶ If $n_{r-1} < t_{r-1}$, then $\psi_r = 0$.

Bound on the degree of XSL-scheme

In order for the degree not to exceed $n - 2$, it is sufficient that

$$\psi_r + \lfloor \frac{n}{d^r} \rfloor - \lfloor \frac{t^\ell}{d^r} \rfloor \geq 2.$$

- ▶ If $\psi_r = 1$: $n_r - t_r \geq 1$.
- ▶ If $\psi_r = 0$: $n_r - t_r \geq 2$.

If $n_r - t_r \geq 2$ or $n_r - t_r = 1$ and $n_{r-1} > t_{r-1}$ then the maximum number of rounds in which it is guaranteed that the maximum degree is not reached is

$$r_s = \lfloor \log_d(n) \rfloor + \lfloor \log_t(n) \rfloor.$$

Attack on Kuznyechik³

1. Guess the key byte $K_0[0]$.
2. Let $\mathcal{P}$ be a set of 2^{127} plaintexts, where the first byte takes 2^7 values $\{S^{-1}(0) \oplus K_0[0], S^{-1}(1) \oplus K_0[0], \dots, S^{-1}(127) \oplus K_0[0]\}$, and the other bytes take all possible values.
3. Encrypt $\mathcal{P}$ under the unknown K , get set of ciphertexts $\mathcal{C}$.
4. Decrypt $\mathcal{C}$ by two rounds guessing the round keys, and check if

$$\bigoplus_{c \in \mathcal{C}} D^2(c) = 0$$

5. Test all remaining key candidates on four (plaintext, ciphertext) pairs, pick the right one.

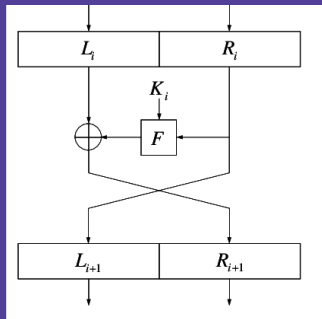
³A. Biryukov, D. Khovratovich, L. P. Perrin «Multiset-algebraic cryptanalysis of reduced Kuznyechik, Khazad, and secret SPNs»

Feistel network

$X = L \parallel R$ – input $2n$ -bit block
 $Y = Y_1 \parallel Y_2$ – output $2n$ -bit block

Round of Feistel network:

$$\begin{cases} Y_1 = R, \\ Y_2 = L \oplus f(R, K_i), \end{cases}$$



Bound on the degree of Feistel network

Theorem

For all $r \leq \ell \leq \lfloor \log_d(2n) \rfloor$, it holds that:

$$\deg(F^{\ell+r}) \leq 2n - (\psi_r + \left\lfloor \frac{2n}{d^r} \right\rfloor - \frac{d^\ell}{d^r}),$$

where

$$\psi_1 = \begin{cases} 0 & \text{if } n_{i-1} = n_{i-2} = \dots = n_0 = 0, \\ 1 & \text{otherwise,} \end{cases}$$

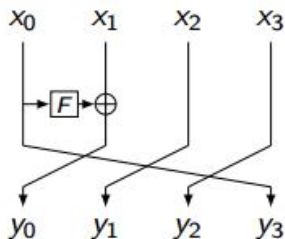
where $F : \mathbb{F}_2^{2n} \rightarrow \mathbb{F}_2^{2n}$ – function corresponding to one round of the Feistel network, in which function f is represented by a bijective XSL-transformation,
 $2n = \sum_{i=0}^{\infty} n_i d^i$ – the base d expansion of $2n$. S transformation corresponding to the concatenation of S -boxes with degree $d = s - 1$.

Corollary

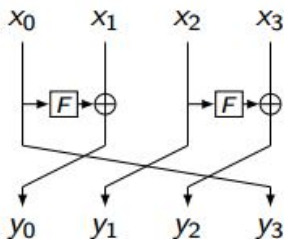
Let $\ell = \lfloor \log_d(2n) \rfloor$, $2n = \sum_{i=0}^{\infty} n_i d^i$, $d = s - 1$. Assume that there exists $i < \ell + 3$ such that $n_i \neq 0$. Then the maximum number of rounds that the degree of at least one half of the block does not exceed $2n - 2$ is

$$\begin{cases} 2\ell + 1, & \text{if } n_\ell > 1, \\ 2\ell, & \text{if } n_\ell = 1, n_{\ell-1} \geq 1, \\ 2\ell - 1, & \text{if } n_\ell = 1, n_{\ell-1} = 0, n_{\ell-2} \geq 1. \end{cases}$$

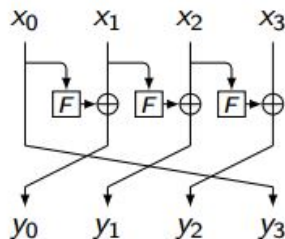
Generalized Feistel network



Type-1 (CAST-256, Lesamnta)



Type-2 (HIGHT, CLEFIA)



Type-3

Definition (Division Property⁴)

Let $\mathbb{X}$ be a multiset whose elements take values from $\mathbb{F}_2^n$ and k takes a value between 0 and n . When the multiset $\mathbb{X}$ has **division property** $\mathcal{D}_k^n$, it fulfils the following conditions:

$$\bigoplus_{x \in \mathbb{X}} \pi_u(x) = \begin{cases} \text{unknown} & \text{if } wt(u) \geq k, \\ 0 & \text{otherwise,} \end{cases}$$

where Bit Product Function $\pi_u(x)$ is defined as $\pi_u(x) := \prod_{i=1}^n x_i^{u_i}$

⁴Yosuke Todo. Structural evaluation by generalized integral property. In Elisabeth Oswald and Marc Fischlin, editors, Advances in Cryptology - EUROCRYPT 2015

MILP (Mixed Integer Linear Programming) is applied to search for Integral Distinguishers Based on the Division Property.⁵

The propagations of cryptographic properties (such division property and others) are converted into a system of linear inequalities, and these linear inequalities are sent to an **MILP solver**.

⁵Zejun Xiang, Wentao Zhang, Zhenzhen Bao, and Dongdai Lin. «Applying MILP method to searching integral distinguishers based on division property for 6 lightweight block ciphers». 2016

Division property can also be used to estimate the upper bounds on the degree of symmetric ciphers.

In the work by Chen S. et al. ⁶, it is shown that the bounds on algebraic degree obtained based on the division property and MILP are generally better than those obtained using Boura, Canteaut's and Carlet's formulas.

⁶Chen S. et al. «On the relationships between different methods for degree evaluation»
IACR Transactions on Symmetric Cryptology - 2021. – C. 411–442

Thank you for your attention!

Anastasiia Chichaeva
Vasily Shishkin



a.chichaeva@kryptonite.ru