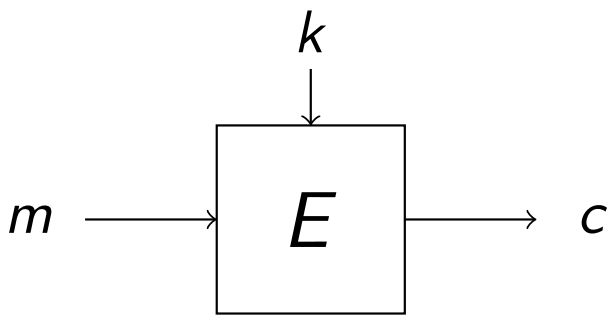
Arguments against Integral Attacks on Block Ciphers[1]

Gregor Leander

BFA 2021

[1] based on joint work with Phil Hebborn, Baptiste Lambin, Yosuke Todo

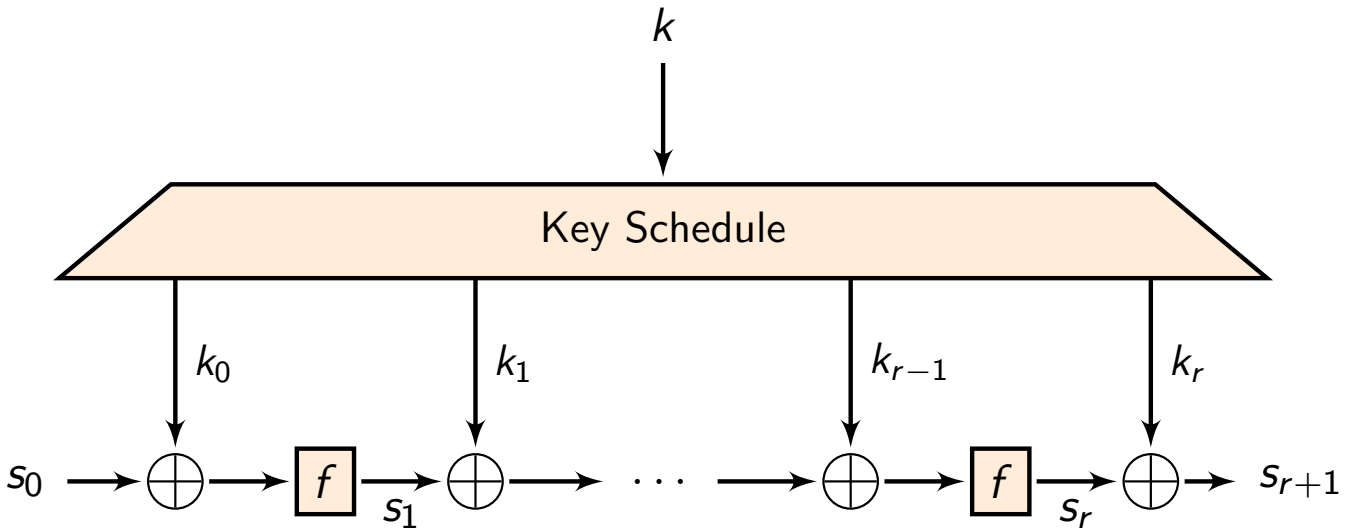
A Block Cipher



Ideal block cipher: A random selection of permutations.

$$E_k : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$$

Key-Alternating Block Cipher



Remark

Many block ciphers are key-alternating.

The Advanced Encryption Standard is one of them.

Security of Block Ciphers

Success of block ciphers: interplay of attacks and design

Security of Block Ciphers

Absence of attacks.

Many possible attack vectors, e.g.:

- Differential Attacks
- Linear Attacks
- Integral Attacks

For the first two: good understanding of security arguments.
For integral attacks: not.

Integral Attacks on Block Ciphers

Integral Attacks of Block Ciphers

Find a set M of plain-texts such that

$$\sum_{x \in M} E_k(x) = 0$$

Development:

- Invented by Lars Knudsen
- Based on δ-sets
- Link to the ANF of a cipher
- Y. Todo's division property to find M.

Similar concepts: cube-attacks, high-order differentials

Arguments against Integral Attacks on Block Ciphers

Integral Attacks of Block Ciphers

Find a set M of plain-texts such that

$$\sum_{x \in M} E_k(x) = 0$$

Main question for today

Security against Integral Attacks

How to argue that a cipher is secure?

Show that for a given cipher no such M exist!

What this means

Integral Attacks of Block Ciphers

Find a set M of plain-texts such that

$$\sum_{x \in M} E_k(x) = 0$$

The sum is key-independent.

$$\Leftrightarrow$$

The 2^n functions

$$f_x(k) = E_k(x)$$

are linear dependent

Algebraic Degree of Block Ciphers

Keyed Boolean Function

$$E_k : \mathbb{F}_2^n \to \mathbb{F}_2^n$$
$$x \mapsto \sum_{u \in \mathbb{F}_2^n} p_u(k) x^u$$

With $p_u : \mathbb{F}_2^l \to \mathbb{F}_2^n, \quad x^u = x_1^{u_1} x_2^{u_2} \dots x_n^{u_n}$

Algebraic Degree

$$\deg(E) := \max_u \{\mathrm{wt}(u) \mid p_u \neq 0\}$$

Algebraic Degree of Block Ciphers

Example I

$$E_k(x_0, x_1, x_2) = k_1x_0x_1 + k_1x_0 + x_1 + (k_1k_2 + k_3)x_2$$

$\deg(E) = 2$

Example II

$$E_k(x) = k_0x_0x_1 + k_1x_0x_2 + k_2x_1x_2 + k_2x_0 + (k_1k_4 + 1)x_1 + (k_1k_2 + k_3)x_2 + (k_1k_2k_3 + k_0)$$

$\deg(E) = 2$

Relation to Integral Attacks

How to compute the coefficients $p_u(k)$?

Moebius Transformation

Given

$$E_k(x) = \sum_{u \in \mathbb{F}_2^n} p_u(k) x^u$$

then

$$p_u(k) = \sum_{x \leq u} E_k(x)$$

Smaller? For vectors?

$$x \leq u \Leftrightarrow x_i \leq u_i$$

E.g.

$$\{x \leq (1,0,1)\} = \{(0,0,0),(1,0,0),(0,0,1),(1,0,1)\}$$

Relation to Integral Attacks

Example I

$$E_k(x_0, x_1, x_2) = k_1 x_0 x_1 + k_1 x_0 + x_1 + (k_1 k_2 + k_3) x_2$$

$$0 = p_{(0,0,0)}(k) = \sum_{x \leq (0,0,0)} E_k(x) = E_k(0)$$

Relation to Integral Attacks

Example I

$$E_k(x_0, x_1, x_2) = k_1 x_0 x_1 + k_1 x_0 + x_1 + (k_1 k_2 + k_3) x_2$$

$$p_{(1,1,0)}(k) = \sum_{x \leq (1,1,0)} E_k(x)$$

Relation to Integral Attacks

Example I

$$E_k(x_0, x_1, x_2) = k_1 x_0 x_1 + k_1 x_0 + x_1 + (k_1 k_2 + k_3) x_2$$

$$\begin{aligned} p_{(1,1,0)}(k) &= \sum_{x \leq (1,1,0)} E_k(x) \\ &= E_k(000) + E_k(100) + E_k(010) + E_k(110) \end{aligned}$$

Relation to Integral Attacks

Example I

$$E_k(x_0, x_1, x_2) = k_1 x_0 x_1 + k_1 x_0 + x_1 + (k_1 k_2 + k_3) x_2$$

$$\begin{aligned} p_{(1,1,0)}(k) &= \sum_{x \leq (1,1,0)} E_k(x) \\ &= E_k(000) + E_k(100) + E_k(010) + E_k(110) \\ &= 0 + 1 + k_1 + (k_1 + k_1 + 1) \end{aligned}$$

Relation to Integral Attacks

Example I

$$E_k(x_0, x_1, x_2) = k_1 x_0 x_1 + k_1 x_0 + x_1 + (k_1 k_2 + k_3) x_2$$

$$\begin{aligned} p_{(1,1,0)}(k) &= \sum_{x \leq (1,1,0)} E_k(x) \\ &= E_k(000) + E_k(100) + E_k(010) + E_k(110) \\ &= 0 + 1 + k_1 + (k_1 + k_1 + 1) \\ &= k_1 \end{aligned}$$

Relation to Integral Attacks

Why do integral attacks happen at all?

Degree and Integrals

If $\deg(E_k) = d$ then

$$p_u(k) = \sum_{x \leq u} E_k(x) = 0$$

for any u of weight larger than d.

$$\sum_{x \in M} E_k(x) = 0 \text{ for } M = \{x \leq u\} \quad (|M| = 2^{\mathrm{wt}(d)})$$

A *necessary* condition for the security is a high degree. Thus:

Lower bound the algebraic degree

Lower and Upper Bounds on Algebraic Degree

$$E_k(x) = \sum_{u \in \mathbb{F}_2^n} p_u(k) x^u$$

Upper bound

Upper bound d on the degree of $E \Rightarrow$ for **all** keys, **all** output bits are of degree at most d

Lower bound

Lower bound d on the degree of $E \Rightarrow$ there exists **at least one** key and **at least one** output bit which is of degree at least d

Upper Bounds well established

- Computing upper bounds on the algebraic degree is well studied
  - See e.g. paper by Boura & Canteaut
  - More recently, division property
  - only gives "at least this number of rounds for full degree"

Upper Bounds well established

- Computing upper bounds on the algebraic degree is well studied
  - See e.g. paper by Boura & Canteaut
  - More recently, division property
  - only gives "at least this number of rounds for full degree"
- Computing lower bounds is not so easy
  - Limited to computing the ANF directly
  - Only works for a very few number of rounds
  - But much more insightful for security of block ciphers

Lower Bounds (AC2020)

Lower Bounds on the Degree of Block Ciphers

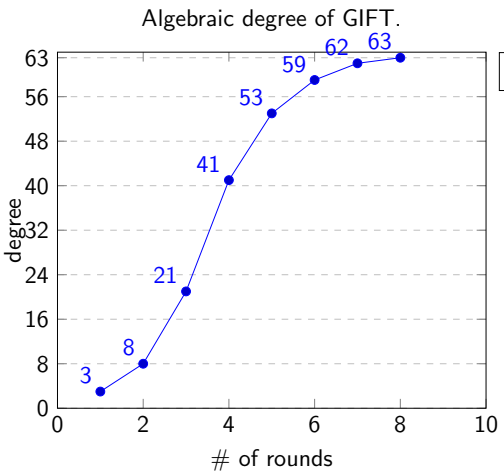
Phil Hebborn[1], Baptiste Lambin[1], Gregor Leander[1], and Yosuke Todo[1,2]

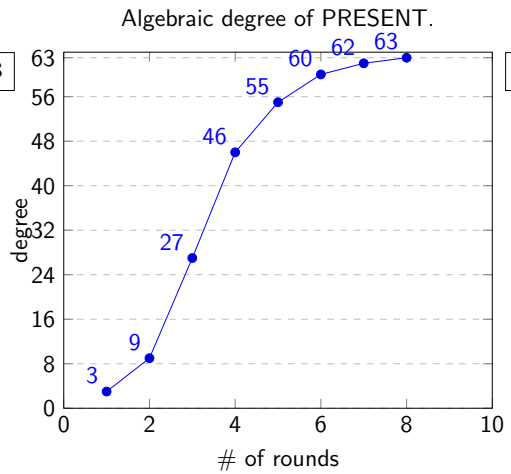
[1] Horst Görtz Institute for IT Security, Ruhr University Bochum, Bochum, Germany,
phil.hebborn@rub.de,baptiste.lambin@protonmail.com,gregor.leander@rub.de
[2] NTT Secure Platform Laboratories, Tokyo, Japan, yosuke.todo.xt@hco.ntt.co.jp

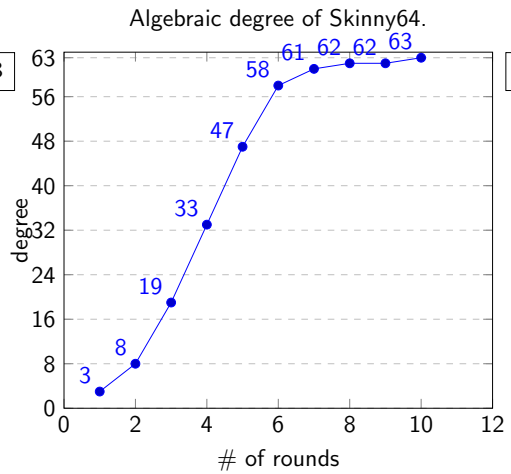
Abstract Only the method to estimate the upper bound of the algebraic degree on block ciphers is known so far, but it is not useful for the designer to guarantee the security. In this paper we provide meaningful lower bounds on the algebraic degree of modern block ciphers.

Keywords: Block cipher · Algebraic degree · Minimum degree · Lower bounds · Division property · Parity set

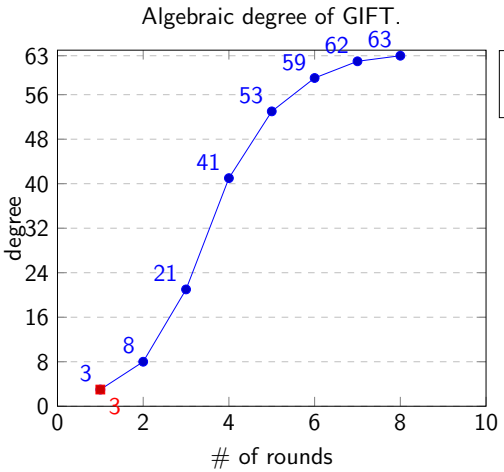
Overview

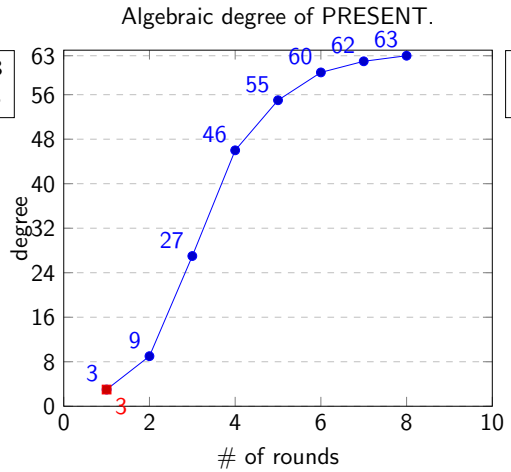

Algebraic degree of GIFT.
degree
# of rounds
UB
3
8
21
41
53
59
62
63

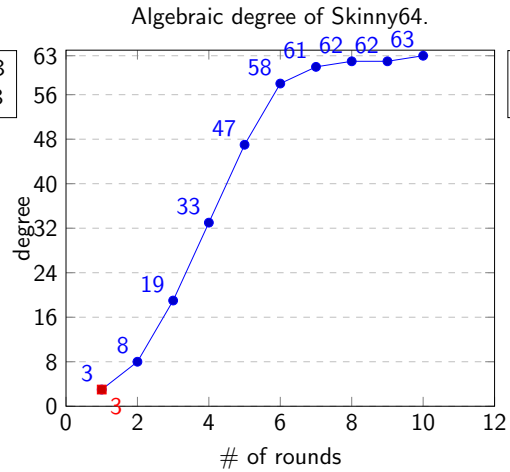

Algebraic degree of PRESENT.
degree
# of rounds
UB
3
9
27
46
55
60
62
63


Algebraic degree of Skinny64.
degree
# of rounds
UB
3
8
19
33
47
58
61
62
62
63

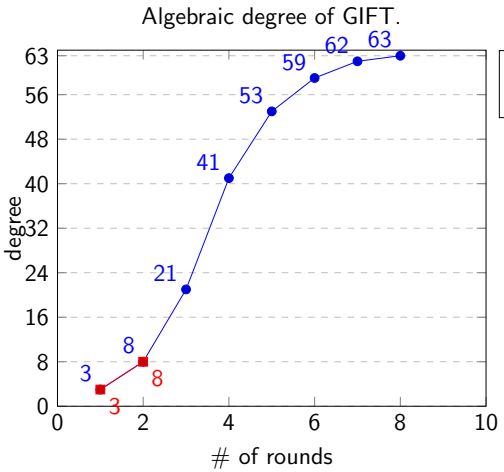
Overview

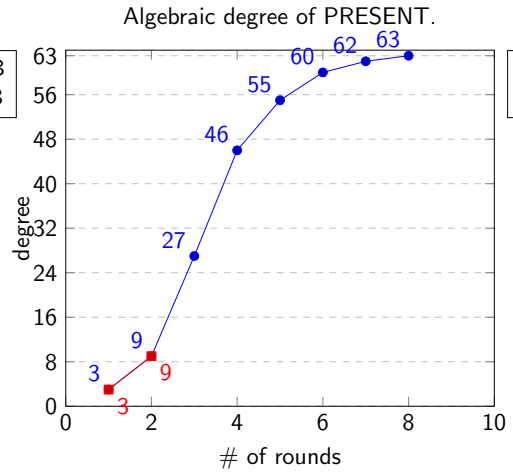

Algebraic degree of GIFT.
degree
# of rounds
UB
LB
3
8
21
41
53
59
62
63

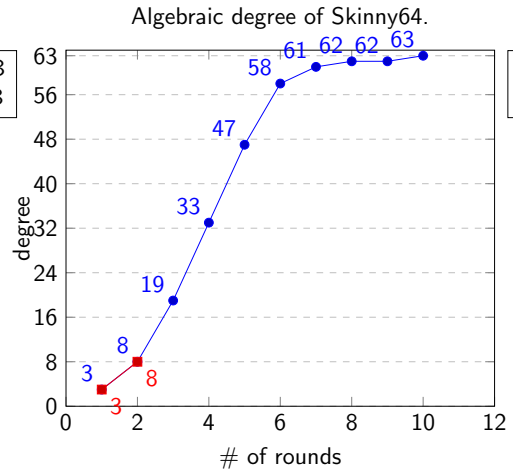

Algebraic degree of PRESENT.
degree
# of rounds
UB
LB
3
9
27
46
55
60
62
63


Algebraic degree of Skinny64.
degree
# of rounds
UB
LB
3
8
19
33
47
58
61
62
62
63

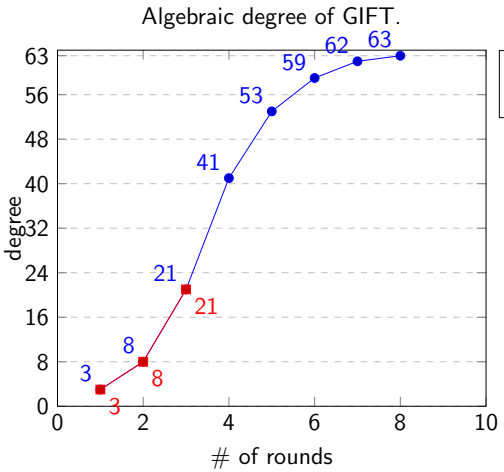
Overview

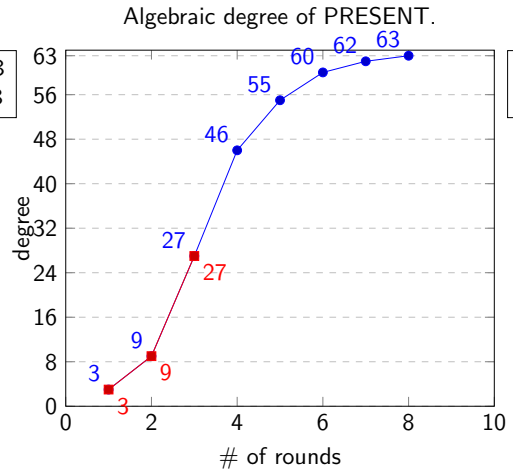

Algebraic degree of GIFT.
degree
# of rounds
UB
LB
0
8
16
24
32
40
48
56
63
0
2
4
6
8
10
3
8
21
41
53
59
62
63
3
8

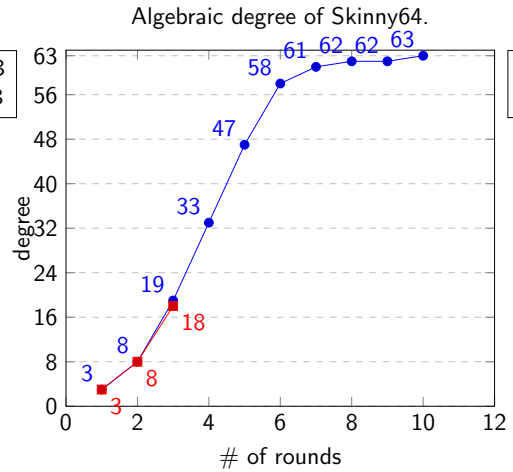

Algebraic degree of PRESENT.
degree
# of rounds
UB
LB
0
8
16
24
32
40
48
56
63
0
2
4
6
8
10
3
9
27
46
55
60
62
63
3
9


Algebraic degree of Skinny64.
degree
# of rounds
UB
LB
0
8
16
24
32
40
48
56
63
0
2
4
6
8
10
12
3
8
19
33
47
58
61
62
62
63
3
8

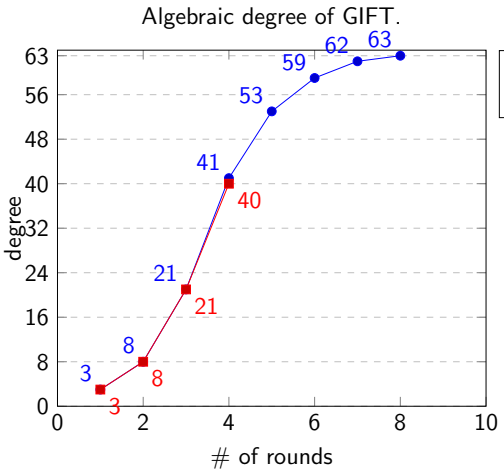
Overview

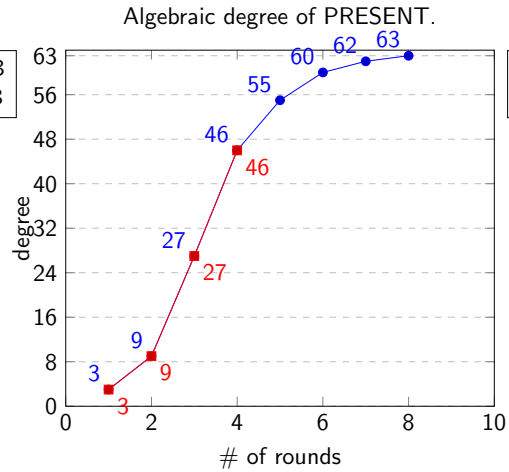

Algebraic degree of GIFT.
degree
# of rounds
UB
LB
0
8
16
24
32
40
48
56
63
0
2
4
6
8
10
3
8
21
41
53
59
62
63
3
8
21

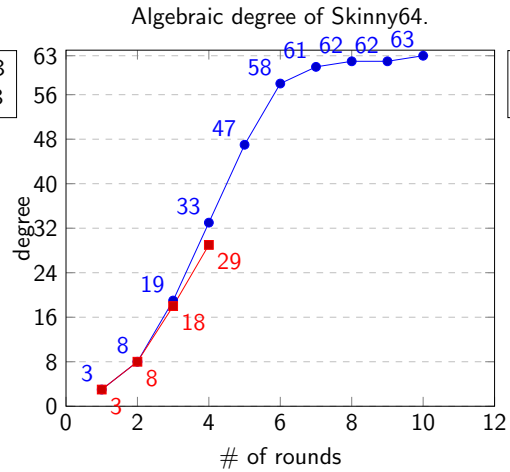

Algebraic degree of PRESENT.
degree
# of rounds
UB
LB
0
8
16
24
32
40
48
56
63
0
2
4
6
8
10
3
9
27
46
55
60
62
63
3
9
27


Algebraic degree of Skinny64.
degree
# of rounds
UB
LB
0
8
16
24
32
40
48
56
63
0
2
4
6
8
10
12
3
8
19
33
47
58
61
62
62
63
3
8
18

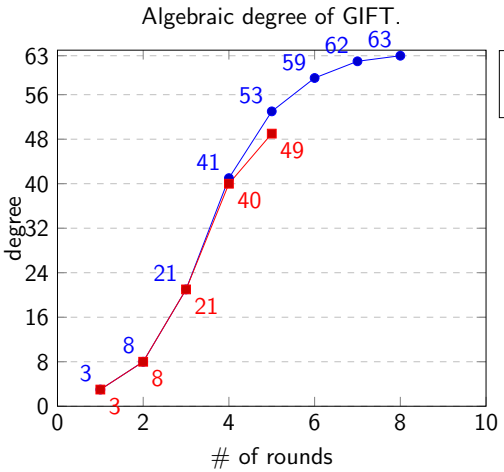
Overview

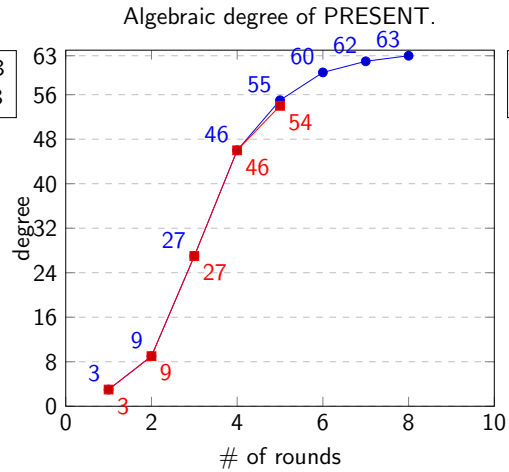

Algebraic degree of GIFT.
degree
# of rounds
UB
LB
0
8
16
24
32
40
48
56
63
0
2
4
6
8
10
3
8
21
41
53
59
62
63
3
8
21
40

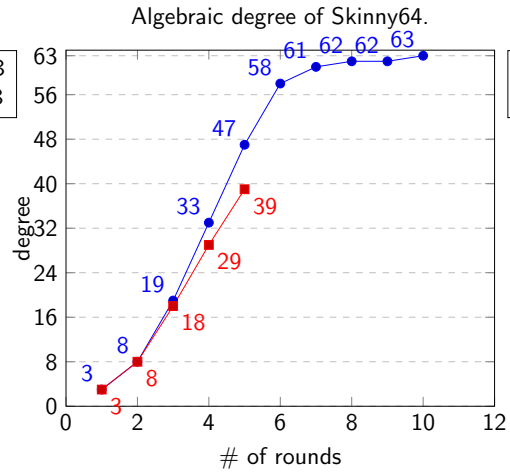

Algebraic degree of PRESENT.
degree
# of rounds
UB
LB
0
8
16
24
32
40
48
56
63
0
2
4
6
8
10
3
9
27
46
55
60
62
63
3
9
27
46


Algebraic degree of Skinny64.
degree
# of rounds
UB
LB
0
8
16
24
32
40
48
56
63
0
2
4
6
8
10
12
3
8
19
33
47
58
61
62
62
63
3
8
18
29

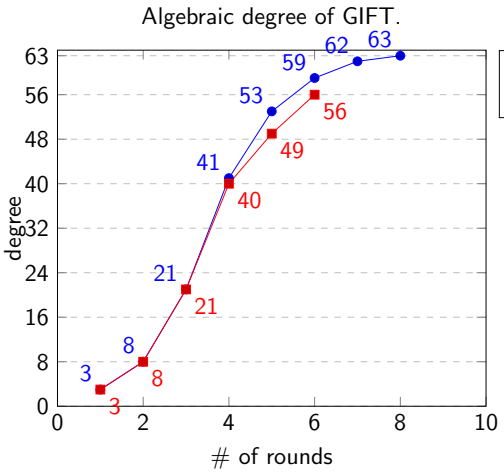
Overview

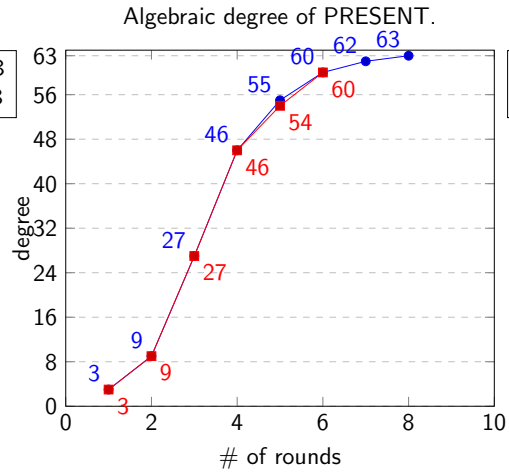

Algebraic degree of GIFT.
degree
# of rounds
UB
LB
0
8
16
24
32
40
48
56
63
0
2
4
6
8
10
3
8
21
41
53
59
62
63
3
8
21
40
49

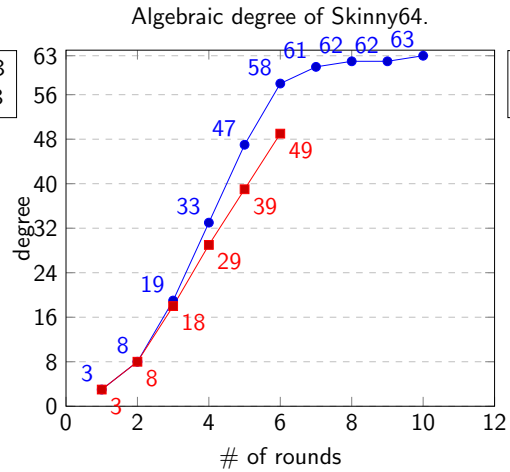

Algebraic degree of PRESENT.
degree
# of rounds
UB
LB
0
8
16
24
32
40
48
56
63
0
2
4
6
8
10
3
9
27
46
55
60
62
63
3
9
27
46
54


Algebraic degree of Skinny64.
degree
# of rounds
UB
LB
0
8
16
24
32
40
48
56
63
0
2
4
6
8
10
12
3
8
19
33
47
58
61
62
62
63
3
8
18
29
39

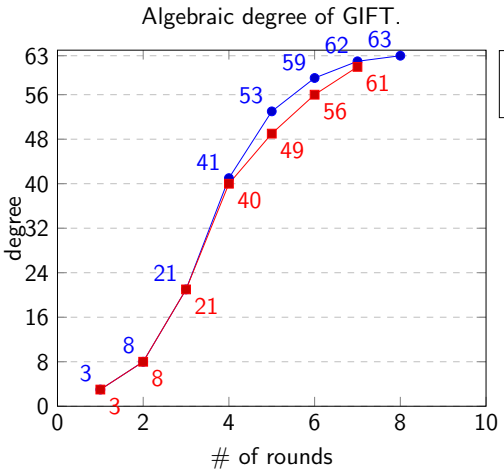
Overview

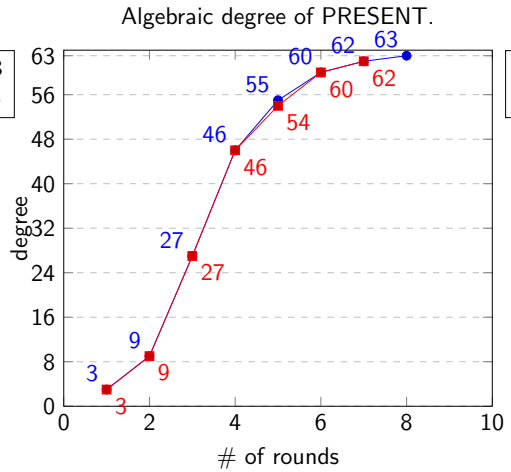

Algebraic degree of GIFT.
degree
# of rounds
UB
LB
3 8 21 41 53 59 62 63
3 8 21 40 49 56

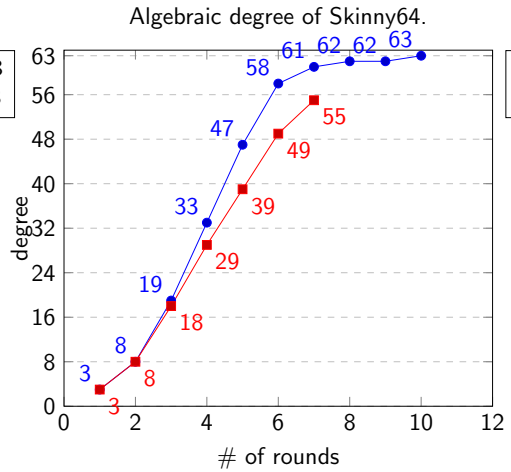

Algebraic degree of PRESENT.
degree
# of rounds
UB
LB
3 9 27 46 55 60 62 63
3 9 27 46 54 60


Algebraic degree of Skinny64.
degree
# of rounds
UB
LB
3 8 19 33 47 58 61 62 62 63
3 8 18 29 39 49

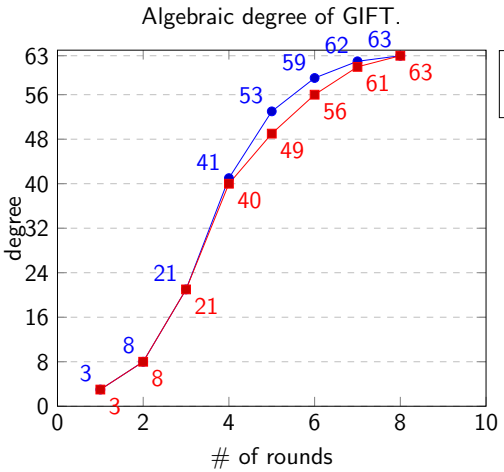
Overview

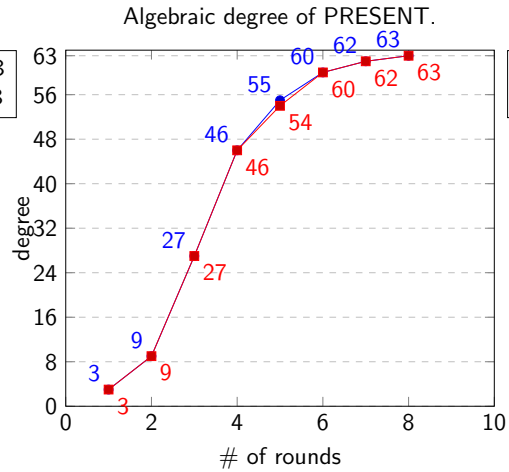

Algebraic degree of GIFT.
degree
# of rounds
UB
LB
3 8 21 41 53 59 62 63
3 8 21 40 49 56 61

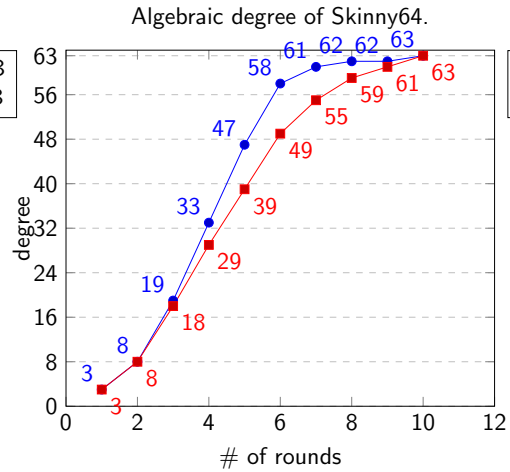

Algebraic degree of PRESENT.
degree
# of rounds
UB
LB
3 9 27 46 55 60 62 63
3 9 27 46 54 60 62


Algebraic degree of Skinny64.
degree
# of rounds
UB
LB
3 8 19 33 47 58 61 62 62 63
3 8 18 29 39 49 55

Overview


Algebraic degree of GIFT.
degree
# of rounds
UB
LB
3 8 21 41 53 59 62 63
3 8 21 40 49 56 61 63


Algebraic degree of PRESENT.
degree
# of rounds
UB
LB
3 9 27 46 55 60 62 63
3 9 27 46 54 60 62 63


Algebraic degree of Skinny64.
degree
# of rounds
UB
LB
3 8 19 33 47 58 61 62 62 63
3 8 18 29 39 49 55 59 61 63

Proving lower bounds on the degree

$$E_k(x) = \sum_{u \in \mathbb{F}_2^n} p_u(k) x^u$$

with

$$p_u(k) = \sum_{v \in \mathbb{F}_2^m} \lambda_{u,v} k^v$$

$$\deg(E) := \max_u \{\mathrm{wt}(u) \mid p_u \neq 0\}$$

Proving lower bounds on the degree

$$E_k(x) = \sum_{u \in \mathbb{F}_2^n} p_u(k) x^u$$

with

$$p_u(k) = \sum_{v \in \mathbb{F}_2^m} \lambda_{u,v} k^v$$

$$\deg(E) := \max_u \{\mathrm{wt}(u) \mid p_u \neq 0\}$$

Lower bound d on the degree $\Leftrightarrow$ Find u with $\mathrm{wt}(u) = d$ and $p_u \neq 0$

Find u with $\mathrm{wt}(u) = d$ and $p_u \neq 0$

$$E_k(x) = \sum_{u \in \mathbb{F}_2^n} p_u(k) x^u = \sum_{u \in \mathbb{F}_2^n, v \in \mathbb{F}_2^m} (\lambda_{u,v} k^v)\, x^u$$

For a given u, either :

Find u with $\mathrm{wt}(u) = d$ and $p_u \neq 0$

$$E_k(x) = \sum_{u \in \mathbb{F}_2^n} p_u(k) x^u = \sum_{u \in \mathbb{F}_2^n, v \in \mathbb{F}_2^m} (\lambda_{u,v} k^v)\, x^u$$

For a given u, either :

- Find a value $\tilde{k}$ for the key so that $p_u(\tilde{k}) \neq 0$
  (simple concept, hard in practice, can handle key schedules)

Find u with $\mathrm{wt}(u) = d$ and $p_u \neq 0$

$$E_k(x) = \sum_{u \in \mathbb{F}_2^n} p_u(k) x^u = \sum_{u \in \mathbb{F}_2^n, v \in \mathbb{F}_2^m} (\lambda_{u,v} k^v)\, x^u$$

For a given u, either :

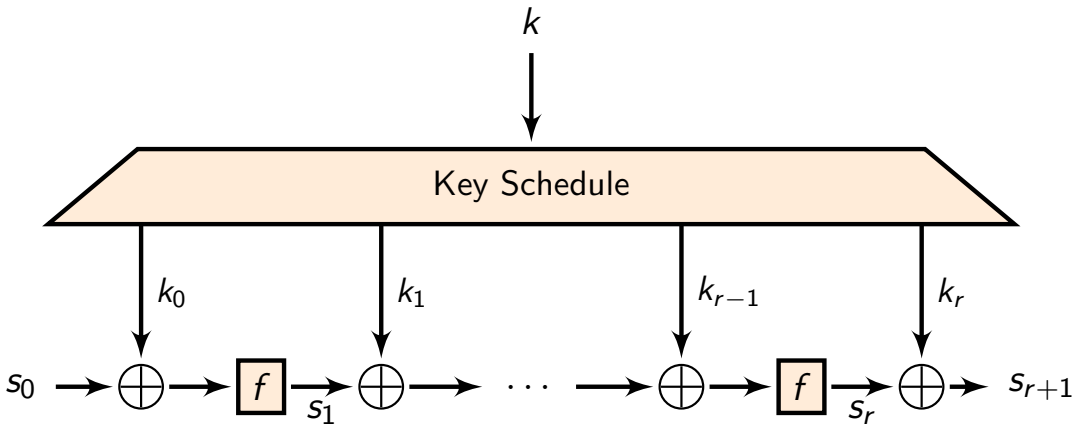
- Find a value $\tilde{k}$ for the key so that $p_u(\tilde{k}) \neq 0$
  (simple concept, hard in practice, can handle key schedules)
- Find v so that $\lambda_{u,v} \neq 0$
  (Looks harder, but easier in practice with independent round keys)

Finding v so that $\lambda_{u,v} \neq 0$

A lot of freedom for v !

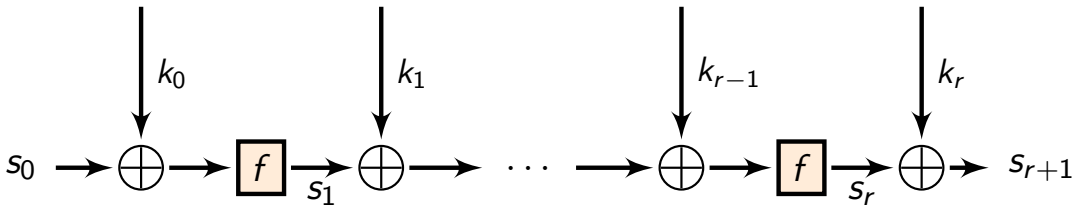
Finding v so that $\lambda_{u,v} \neq 0$

A lot of freedom for v !



Finding v so that $\lambda_{u,v} \neq 0$

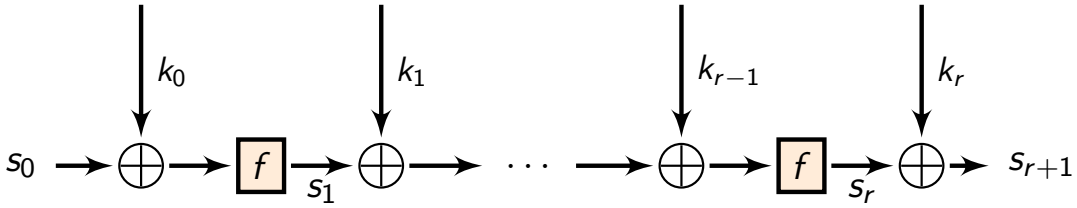
A lot of freedom for v !



With independent round keys $k^v = k_0^{v(0)} k_1^{v(1)} \ldots k_r^{v(r)}$

Finding v so that $\lambda_{u,v} \neq 0$

A lot of freedom for v !



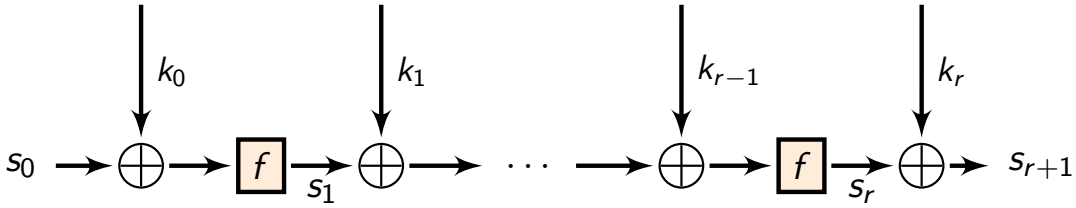
With independent round keys $k^v = k_0^{v(0)} k_1^{v(1)} \ldots k_r^{v(r)}$

Main Tasks

- How to prove $\lambda_{u,v} \neq 0$?
- How to choose each $v^{(i)}$?

Finding v so that $\lambda_{u,v} \neq 0$

A lot of freedom for v !



With independent round keys $k^v = k_0^{v^{(0)}} k_1^{v^{(1)}} \ldots k_r^{v^{(r)}}$

Main Tasks

- How to prove $\lambda_{u,v} \neq 0$? $\Rightarrow$ Hao et al. Eurocrypt'20 using Division Property
- How to choose each $v^{(i)}$? $\Rightarrow$ AC 2020

Division Property: A Powerful Technique

Introduced by Yosuke Todo

Division Property: Theory

- Consider subsets of $\mathbb{F}_2^n$
- as a vector space (with $\mathbb{X} + \mathbb{Y} := (\mathbb{X} \cup \mathbb{Y}) \setminus (\mathbb{X} \cap \mathbb{Y})$)
- in a non-standard basis $\mathbb{B} = \{\{x \leq \ell\} \mid \ell \in \mathbb{F}_2^n\}$

Division Property: A Powerful Technique

Introduced by Yosuke Todo

Division Property: Theory

- Consider subsets of $\mathbb{F}_2^n$
- as a vector space (with $\mathbb{X} + \mathbb{Y} := (\mathbb{X} \cup \mathbb{Y}) \setminus (\mathbb{X} \cap \mathbb{Y})$)
- in a non-standard basis $\mathbb{B} = \{\{x \leq \ell\} \mid \ell \in \mathbb{F}_2^n\}$

Division Property: Practice

- Trace sets through many (simple) functions
- using SAT or MILP.
- The art is to keep it efficient!

Division Property: A Powerful Technique

Introduced by Yosuke Todo

Division Property: Theory

- Consider subsets of $\mathbb{F}_2^n$
- as a vector space (with $\mathbb{X} + \mathbb{Y} := (\mathbb{X} \cup \mathbb{Y}) \setminus (\mathbb{X} \cap \mathbb{Y})$)
- in a non-standard basis $\mathbb{B} = \{\{x \leq \ell\} \mid \ell \in \mathbb{F}_2^n\}$

Division Property: Practice

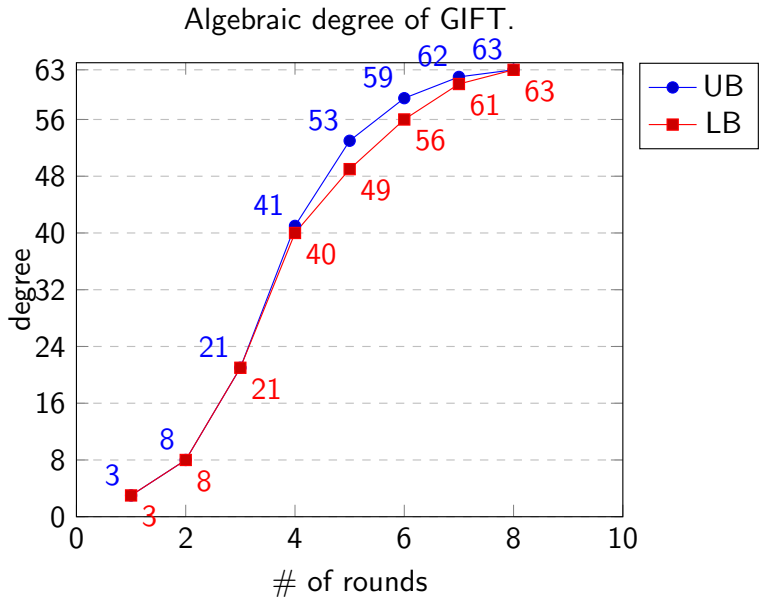
- Trace sets through many (simple) functions
- using SAT or MILP.
- The art is to keep it efficient!

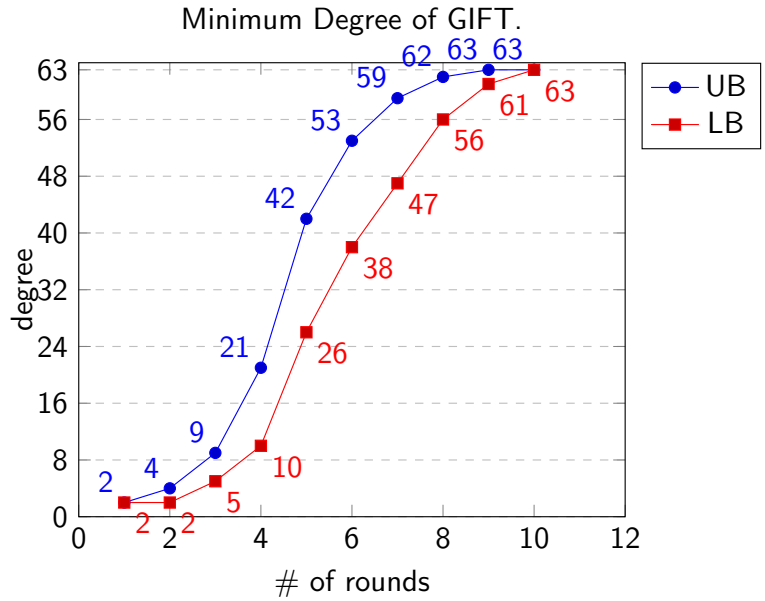
Allows to compute previously unreachable results. Here:

$$\lambda_{u,v}$$

for well choosen u and v.

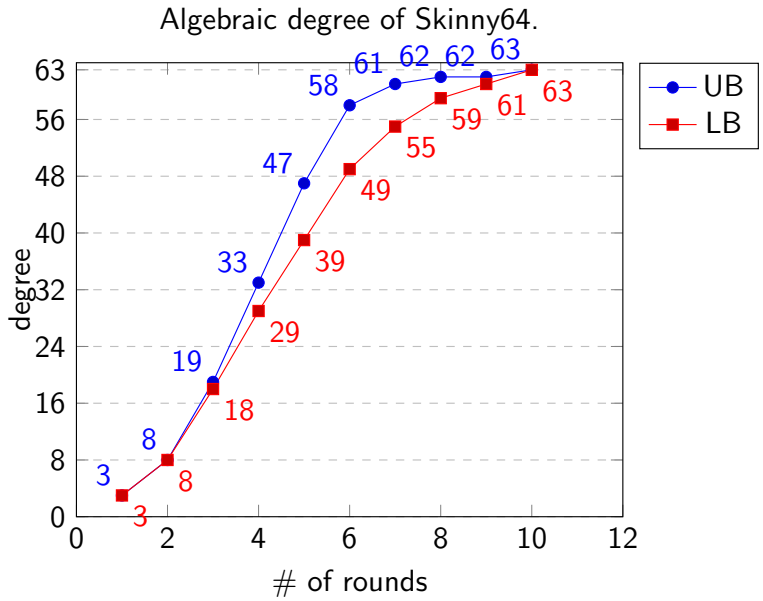
Results on GIFT-64

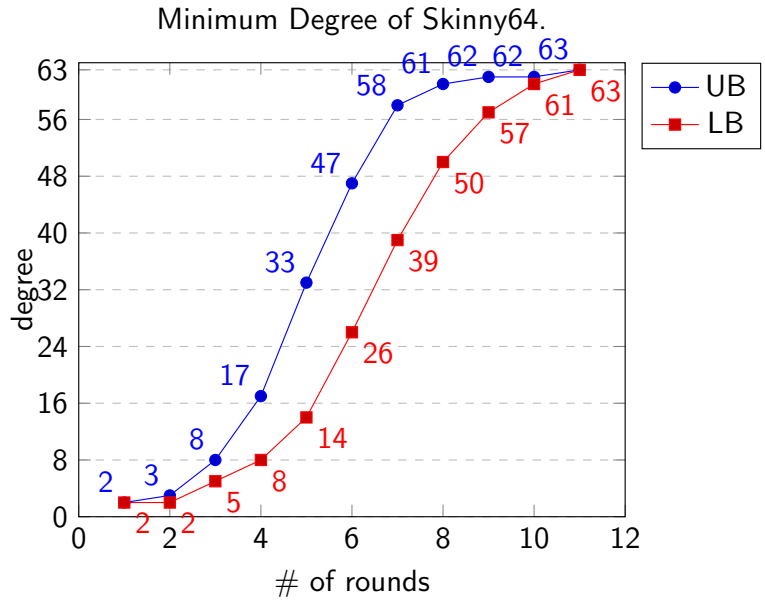




11 rounds : **all** 63-degree monomials appear in **any** component function (for at least one key each)

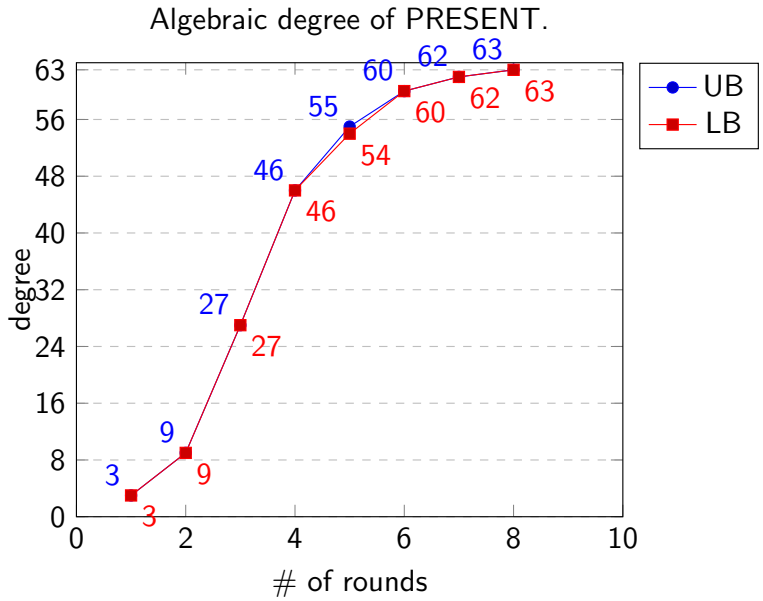
Results on SKINNY64

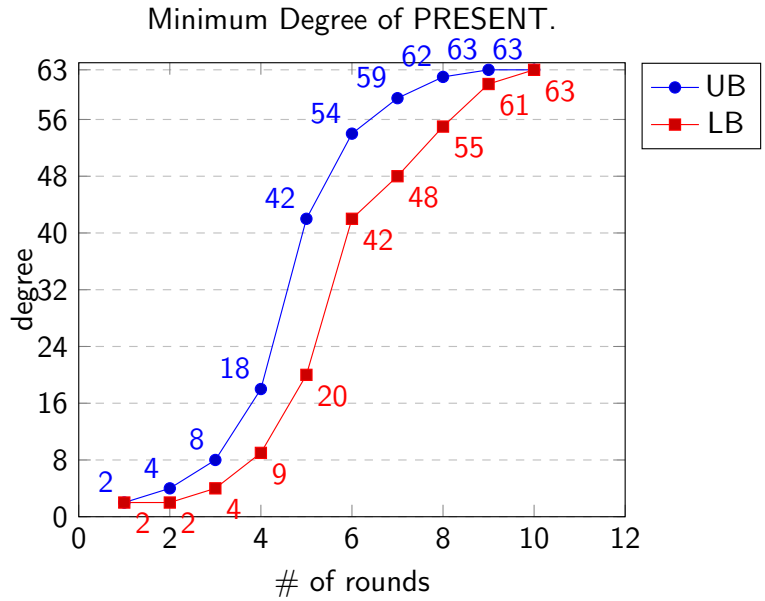




13 rounds : **all** 63-degree monomials appear in **any** component function (for at least one key each)

Results on PRESENT





11 rounds : **all** 63-degree monomials appear in **any** component function (for at least one key each)

Results on AES

For AES, much more expensive computations, but still non-trivial bounds :

- 3 rounds : Lower bound on algebraic degree (112)
- 4 rounds : Lower bound on algebraic degree (116)

Back to the original problem

The degree is a first step, but not enough.

Integral Attacks of Block Ciphers

Find a set M of plain-texts such that

$$\sum_{x \in M} E_k(x) = 0$$

We need to show that no such M exist!

Zero Coefficients Cause Problems

Example I

$$E_k(x_0, x_1, x_2) = k_1 x_0 x_1 + k_1 x_0 + x_1 + (k_1 k_2 + k_3) x_2$$

$$\begin{aligned} 0 &= p_{(0,0,0)}(k) = \sum_{x \leq (0,0,0)} E_k(x) \\ 0 &= p_{(0,1,1)}(k) = \sum_{x \leq (0,1,1)} E_k(x) \\ 0 &= p_{(1,0,1)}(k) = \sum_{x \leq (1,0,1)} E_k(x) \end{aligned}$$

$\Rightarrow p_u(k)$ must not be zero!

Equal Coefficients Cause Problems

Example II

$$E_k(x) = k_0x_0x_1 + k_1x_0x_2 + k_2x_1x_2 + k_2x_0 + (k_1k_4 + 1)x_1 + (k_1k_2 + k_3)x_2 + (k_1k_2k_3 + k_0)$$

$p_u(k)$ non-zero for all u, but

$$0 = k_2 + k_2 = p_{(0,1,1)}(k) + p_{(1,0,0)}(k) = \sum_{x \in M} E_k(x)$$

$$M = \{x \leq (0,1,1)\} \oplus \{x \leq (1,0,0)\} = \{(0,1,0), (0,0,1), (0,1,1), (1,0,0)\}$$

$$\Rightarrow p_u(k) \text{ must be pairwise different !}$$

Linear Dependent Coefficients

$$E_k(x) = \sum_{u \in \mathbb{F}_2^n} p_u(k) x^u$$

Linear Dependent Coefficients and Integral Attacks

There exist M such that $\sum_{x \in M} E_k(x) = 0$

$\Leftrightarrow$

$p_u(k)$ are linear dependent.

We need that all 2^n functions $p_u(k)$ are linear independent. Seems very hard.

Linear Dependent Coefficients

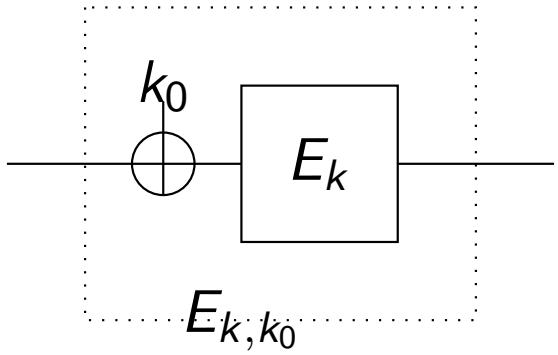
We need that all 2^n functions $p_u(k)$ are linear independent.

$$p_u(k) = \sum_{v \in \mathbb{F}_2^m} \lambda_{u,v} k^v \simeq (\lambda_{u,v})_{v \in \mathbb{F}_2^\ell}$$

Naively, would require (at least) $2^n \times 2^n$ values of $\lambda_{u,v}$.

$$M = \begin{pmatrix} \lambda_{u_1,v_1} & \cdots & \lambda_{u_1,v_t} \\ & \vdots & \\ \lambda_{u_t,v_1} & \cdots & \lambda_{u_t,v_t} \end{pmatrix}$$

Consider Whitening Keys



$$E_k(x) = \sum_{u \in \mathbb{F}_2^n} p_u(k) x^u$$

$$E_{k,k_0}(x) := E_k(x + k_0) = \sum_{v \in \mathbb{F}_2^n} q_v(k, k_0) x^v$$

Arguments Against Integral Attacks

$$E_k(x) = \sum_{u \in \mathbb{F}_2^n} p_u(k) x^u$$

$$E_{k,k_0}(x) := E_k(x + k_0) = \sum_{v \in \mathbb{F}_2^n} q_v(k, k_0) x^v$$

Theorem

If the polynomials $p_{\overline{e_i}}(k)$ are linear independent and $p_{(1,\ldots,1)}(k) = 0$, then all polynomials

$$\{q_v(k, k_0) \mid v \in \mathbb{F}_2^n \setminus \{1\}\}$$

are linear independent.

$$\overline{e_i} = (1, \ldots, 1, 0, 1, \ldots, 1)$$

Arguments Against Integral Attacks

What remains:

- Show that the n functions are $p_{\overline{e_i}}$ linear independent
- by computing enough coefficients
- using the above technique
- with several improvements.

Practical Results

Cipher	Attacked Rounds	Resistant Rounds
SKINNY64	12	13
CRAFT	13	14
GIFT-64	9	11
PRESENT	9	13
SIMON32	15	16
SIMON48	16	17
SIMON64	18	19
SIMON96	22	23
SIMON128	26	27
Simeck32	15	16
Simeck48	18	19
Simeck64	21	22

The End

Future Work

A lot of room for improvements :

- Make it faster
- Make it more useable

Thank you very much for your attention and enjoy Norway!