TAGADA:

Tool for Automatic Generation of Abstraction-based Differential Attacks

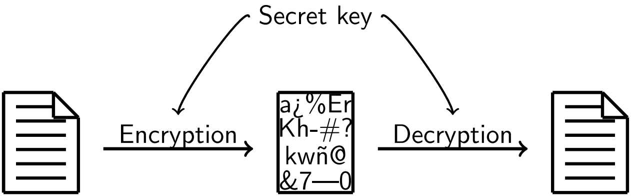
Ana Margarita Rodríguez Cordero

Université de Lorraine, CNRS, Inria, LORIA, Nancy, France
Université Clermont Auvergne, LIMOS

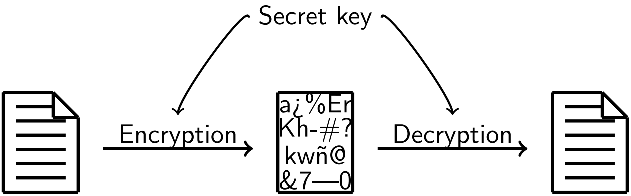
April 14, 2022

Based on work with:
Luc Libralesso – François Delobel – Pascal Lafourcade – Christine Solnon

Symmetric Cryptography

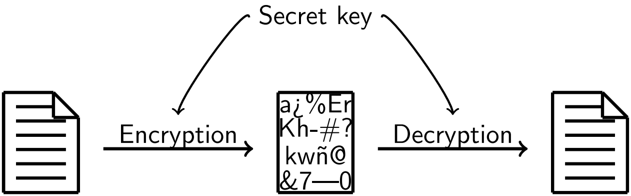


Symmetric Cryptography



- Stream ciphers
- Block ciphers

Symmetric Cryptography

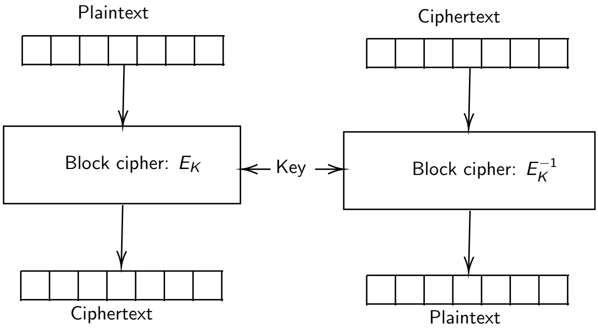


- Block ciphers

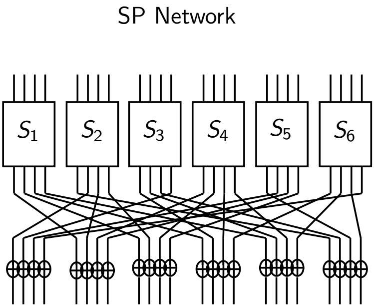
Block ciphers

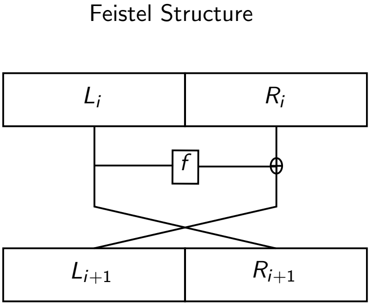
Definition

Given a key $K \in \mathbb{F}_2^m$, a message $M \in \mathbb{F}_2^N$, a *block cipher* of block size n is an invertible function E_K that encrypts the message M in blocks of size n.



SPN and Feistel cipher





x	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7
$S(x)$	0x5	0x3	0x4	0x6	0x2	0x7	0x0	0x1

Cryptanalysis

- Can we distinguish the cipher from a random permutation?
- Is the ciphertext giving us any information?
- Is there any weakness in the design?

Cryptanalysis

- Can we distinguish the cipher from a random permutation?
- Is the ciphertext giving us any information?
- Is there any weakness in the design?

Attack techniques:

- ciphertext-only
- known plaintext
- chosen plaintext

Cryptanalysis

- Can we distinguish the cipher from a random permutation?
- Is the ciphertext giving us any information?
- Is there any weakness in the design?

Attack techniques:

- ciphertext-only
- known plaintext
- chosen plaintext

Type of attacks:

- Differential attack
- Boomerang attack
- Linear attack
- Square attack
- ...

Cryptanalysis

- Can we distinguish the cipher from a random permutation?
- Is the ciphertext giving us any information?
- Is there any weakness in the design?

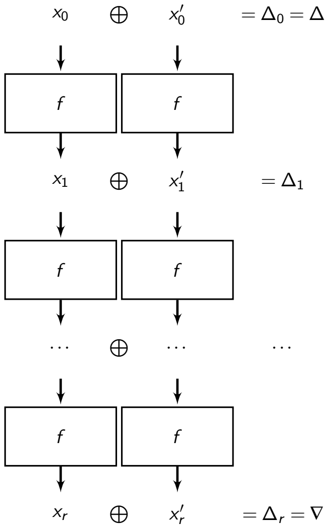
Attack techniques:

- ciphertext-only
- known plaintext
- chosen plaintext

Type of attacks:

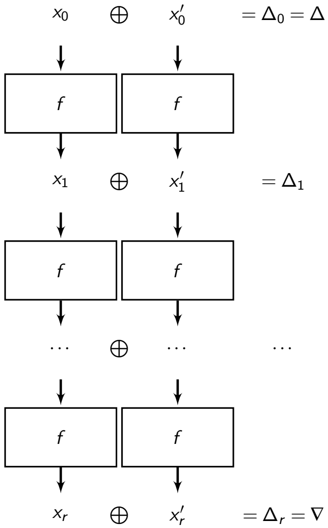
- Differential attack
- Boomerang attack
- Linear attack
- Square attack
- ...

Differential Attacks



- Δ - input difference
- ∇ - output difference
- $\nabla = E_K(X) \oplus E_K(\Delta \oplus X)$, for $X \in \mathbb{F}_2^n$
- Is $P(\Delta \rightarrow \nabla)$ high?

Differential Attacks



- Δ - input difference
- ∇ - output difference
- $\nabla = E_K(X) \oplus E_K(\Delta \oplus X)$, for $X \in \mathbb{F}_2^n$
- Is $P(\Delta \rightarrow \nabla)$ high?

Related-key differential attack: Differentials are also introduced in the key.

$$\nabla = E_K(X) \oplus E_{\Delta_K \oplus K}(\Delta \oplus X)$$

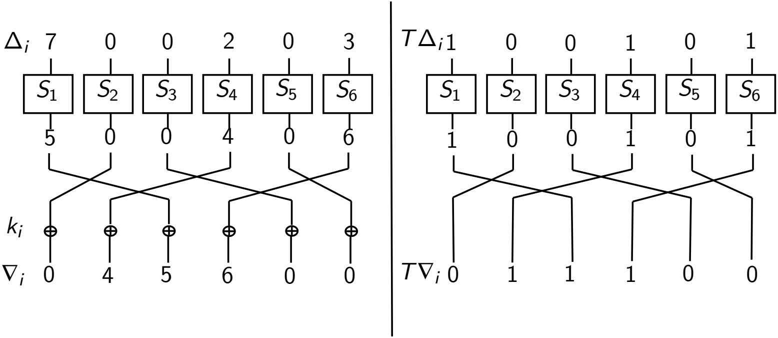
Differential Attack

- Step 1: *Abstraction*:
  - Truncated differential patterns.
  - Number of S-boxes minimized.

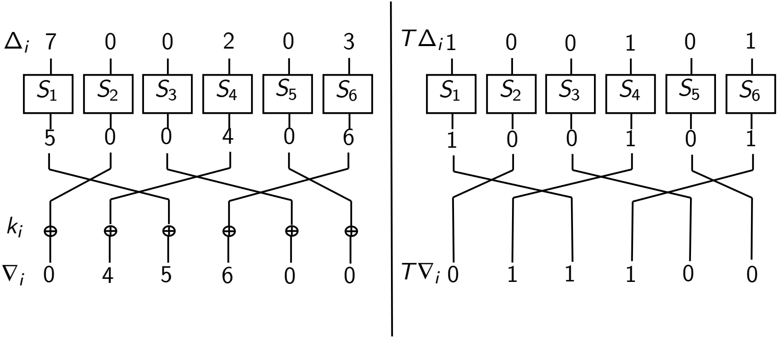
Differential Attack

- Step 1: *Abstraction*:
  - Truncated differential patterns.
  - Number of S-boxes minimized.
- Step 2: *Enumeration*:
  - Find non-abstracted differential characteristics: Distinguishers.

Step 1

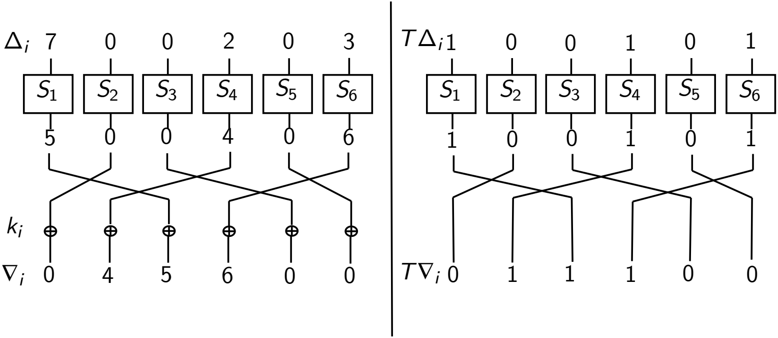

Δ_i 7 0 0 2 0 3
S_1 S_2 S_3 S_4 S_5 S_6
5 0 0 4 0 6
k_i
∇_i 0 4 5 6 0 0
$T\Delta_i$ 1 0 0 1 0 1
S_1 S_2 S_3 S_4 S_5 S_6
1 0 0 1 0 1
$T\nabla_i$ 0 1 1 1 0 0

Step 1



- Find minimum number of active S-boxes

Step 1



- Find minimum number of active S-boxes
- Find all difference patterns minimizing the active number of S-boxes

Step 2

- Find a differential characteristic that fits the truncated pattern.
- Modelling the S-box Difference Distribution Table through constraint programming:
    - MILP modelling
    - SAT modelling

Step 2

- Find a differential characteristic that fits the truncated pattern.
- Modelling the S-box Difference Distribution Table through constraint programming:
  - MILP modelling
  - SAT modelling

Difference Distribution Table:

$$DDT(\Delta_i, \nabla_o) = \#\{\mathbf{x} \in \mathbb{F}_2^n : S(\mathbf{x}) \oplus S(\mathbf{x} \oplus \Delta_i) = \nabla_o\}$$

Δ: Input difference	∇: output difference							
	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7
0x0	8	0	0	0	0	0	0	0
0x1	0	2	2	0	0	2	2	0
0x2	0	2	2	0	0	2	2	0
0x3	0	0	0	4	0	0	0	4
0x4	0	0	0	0	4	0	0	4
0x5	0	2	2	0	0	2	2	0
0x6	0	2	2	0	0	2	2	0
0x7	0	0	0	4	4	0	0	0

TAGADA

Objective:

Obtain a good differential characteristic for any cipher given in input

TAGADA

Objective:

Obtain a good differential characteristic for any cipher given in input

- Give a cipher description

TAGADA

Objective:

Obtain a good differential characteristic for any cipher given in input

- Give a cipher description
- Run TAGADA

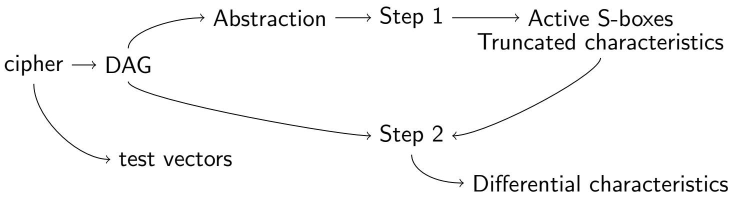
TAGADA

Objective:

Obtain a good differential characteristic for any cipher given in input

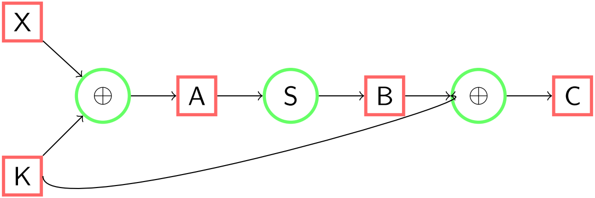
- Give a cipher description
- Run TAGADA
- Obtain an attack

TAGADA's idea



Cipher oriented language

- **State**: Internal state of the cipher at a given time (integer variable).
- **Operator**: Block used for changing from one state to another.



DAG

```
def create_cherry_dag(nb_rounds)
    # define dag and inputs
    dag = Dag.new([],[],[],[])
    x,_,_ = dag.register_block(*input_block("X", NIBBLE_RANGE, [1,4]))
    dag.set_plaintexts(x.flatten)
    k,_,_ = dag.register_block(*input_block("K", NIBBLE_RANGE, [1,4]))
    dag.set_inputs(x.flatten+k.flatten)
    dag.set_keys(k.flatten)
    a = x
    b = k
    nb_rounds.times do |round_number|
        # ARK
        a,_,_ = dag.register_block(*xor_block("ARK_#{round_number}", [a,b]))
        # pLayer
        a,_,_ = dag.register_block(*permutation_block("P_#{round_number}", a,pLayer))
        #ShiftRows
        a,_,_ = dag.register_block(*shiftrows_block("SR_#{round_number}", a,false))
        #S-box
        a,_,_ = dag.register_block(*subcell_block("S_#{round_number}", a, sbox))
        ########### key update
        b,_,_ = dag.register_block(*permutation_block("KU_#{round_number}", b, pKey))
    end
    dag.set_outputs(a.flatten)
    return dag
end
```

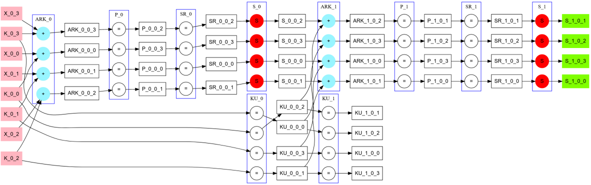


Figure: Toy cipher

Shaving

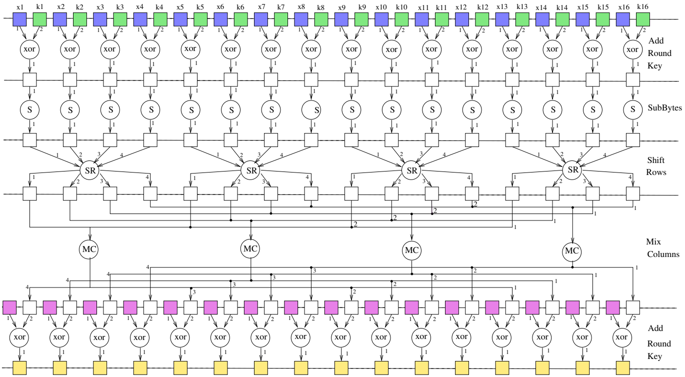


Figure: AES Directed Acyclic Graph

Shaving

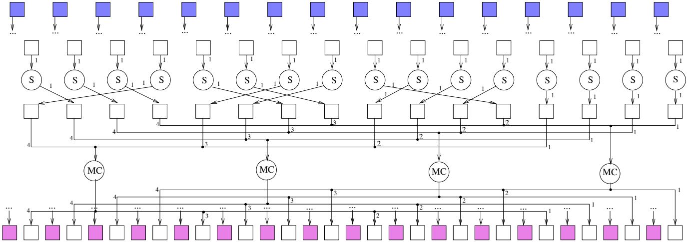


Figure: AES shaved Directed Acyclic Graph

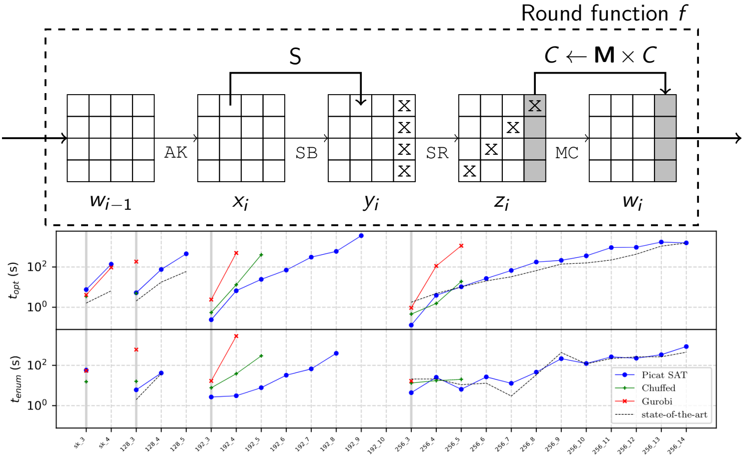
Operators

Operator description $\rightarrow$ Table of constraints

a	b	$a \oplus b$	$\rightarrow$	abstraction$(a,b,a \oplus b)$
0	0	0	$\rightarrow$	(0,0,0)
0	1	1	$\rightarrow$	(0,1,1)
...	...	...	$\rightarrow$	...
255	254	1	$\rightarrow$	(1,1,1)
255	255	0	$\rightarrow$	(1,1,0)

(0,0,0), (0,1,1), (1,0,1), (1,1,0), (1,1,1) $\Rightarrow a + b + XOR(a,b) \neq 1$

Results in AES



David Gérault – Pascal Lafourcade – Marine Minier – Christine Solnon
Revisiting AES Related-Key Differential Attacks with Constraint Programming

Results in SKINNY

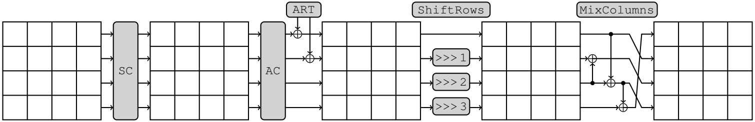
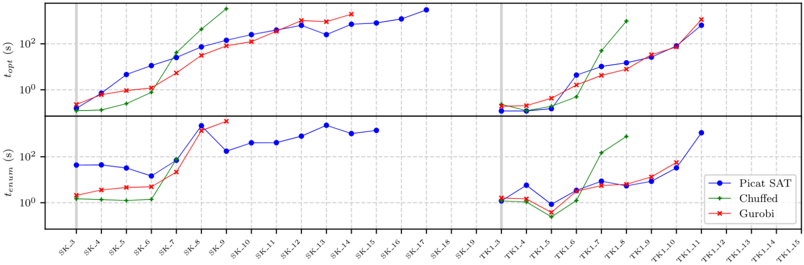


Figure: SKINNY round function

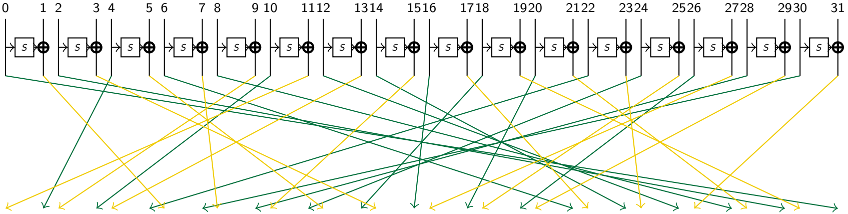


Results in SKINNY

	SKINNY *SK*					SKINNY *TK*1				
	State-of-the-art			TAGADA		State-of-the-art			TAGADA	
Rounds	#Sb	#sol	Time	#Sb	Time	#Sb	#sol	Time	#Sb	Time
3	5	4	1*s*	5	0*s*	1	12	1*s*	1	0*s*
4	8	3	1*s*	8	0*s*	2	9	1*s*	2	0*s*
5	12	2	1*s*	12	4*s*	3	2	1*s*	3	0*s*
6	16	1	1*s*	16	11*s*	6	2	1*s*	6	4*s*
7	26	4	1*s*	26	25*s*	10	2	1*s*	10	10*s*
8	36	17	1*s*	36	73*s*	13	1	1*s*	13	14*s*
9	41	2	1*s*	41	141*s*	16	1	2*s*	16	26*s*
10	46	2	1*s*	49	249*s*	23	1	5*s*	23	80*s*
11	51	2	1*s*	51	393*s*	32	2	11*s*	32	638*s*
12	55	2	1*s*	55	631*s*	38	7	24*s*	-	-
13	58	6	1*s*	58	249*s*	41	2	24*s*	-	-
14	61	2	1*s*	61	705*s*	45	3	24*s*	-	-
15	66	2	1*s*	66	800*s*	49	1	25*s*	-	-
16	75	8	1*s*	75	1197*s*	54	1	25*s*	-	-
17	82	4	1*s*	82	2967*s*	59	5	27*s*	-	-
18	88	4	1*s*	-	-	62	1	27*s*	-	-
19	92	4	1*s*	-	-	66	1	28*s*	-	-
20	96	2	1*s*	-	-	70	2	28*s*	-	-
28	105									
29	109									
30	113									

Stéphanie Delaune – Patrick Derbez – Paul Huynh – Marine Minier – Victor Mollimard, et al. :
SKINNY with Scalpel Comparing Tools for Differential Analysis. 2020

WARP


0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
S

Results in WARP

Related key results for WARP

Round	S-boxes	N-sol	Time in Gurobi (s)	Round	S-boxes	N-sol	Time in Gurobi (s)
1	1	16	0.0927	23	11	16	30.7
2	1	32	0.0901	24	12	36	29.7
3	1	48	0.0997	25	12	16	35.0
4	1	64	0.103	26	13	36	37.7
5	2	96	0.122	27	13	16	49.9
6	3	72	0.618	28	14	36	116
7	3	16	1.19	29	14	16	42.3
8	4	36	1.26	30	15	36	71.3
9	4	16	2.02	31	15	16	64.4
10	5	36	2.69	32	16	36	77.0
11	5	16	3.87	33	16	16	79.8
12	6	36	5.31	34	17	36	76.2
13	6	16	6.27	35	17	16	113
14	7	36	10.5	36	18	36	111
15	7	16	8.12	37	18	16	241
16	8	36	11.2	38	19	36	360
17	8	16	15.9	39	19	16	81.7
18	9	36	15.9	40	20	36	148
19	9	16	14.5	41	20	16	218*e*
20	10	36	28.2				
21	10	16	30.5				
22	11	36	24.9				

Conclusion

- TAGADA works with word-based ciphers.

Conclusion

- TAGADA works with word-based ciphers.
- Ciphers can be described as graphs with TAGADA.

Conclusion

- TAGADA works with word-based ciphers.
- Ciphers can be described as graphs with TAGADA.
- We obtain good resolution times compare with the state-of-the-art attacks.

Conclusion

- TAGADA works with word-based ciphers.
- Ciphers can be described as graphs with TAGADA.
- We obtain good resolution times compare with the state-of-the-art attacks.

GIFT	PRESENT	HIGHT	GIFT-COFB
Deoxys	SKINNY	ISAP	SPARKLE
WARP	CRAFT	Midori	PHOTON
Rijndeal	Simeck	Mysterion	Elephant

References

Source code:

https://gitlab.limos.fr/iia_lulibral/tagada/

Luc Libralesso and François Delobel and Pascal Lafourcade and Christine Solnon
"Automatic Generation of Declarative Models For Differential Cryptanalysis".
27th International Conference on Principles and Practice of Constraint Programming, CP 2021, Montpellier, France (Virtual Conference), October 25-29, 2021, 210: 40:1–40:18, 2021.

Thanks for your attention!