Modeling differential trail search

Marine Minier – Loria, CARAMBA Team

Joint work with C. Prud’homme, P. Derbrez, S. Delaune, P. Huynh, V. Mollimard

Codes by P. Huynh, S. Delaune and C. Prud’homme

Slides by M. Simard

Marine Minier
GDR Sécu Days | 22 June 2022 | Paris

RoadMap

- Introduction to differential cryptanalysis

- How to model that? With what?
    - Step 1
    - Step 2
    - Results

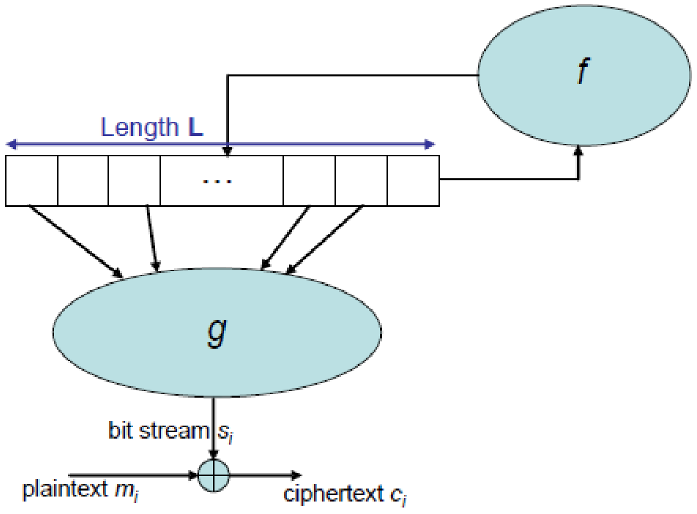
- Conclusion

Introduction

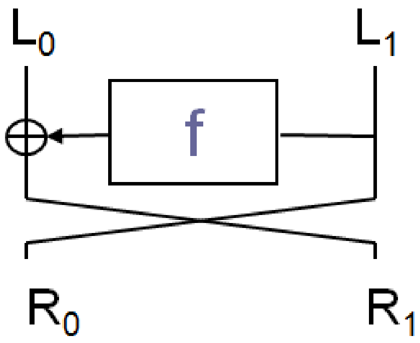
Thank you to Marc Simard for wonderful slides!

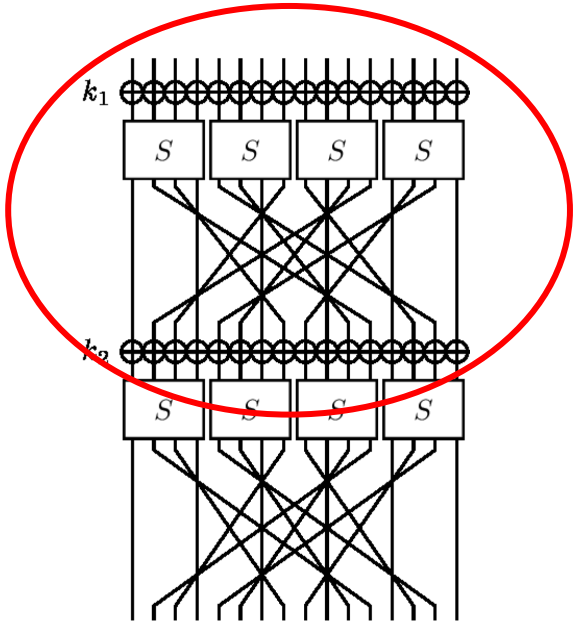
How to Cipher in symmetricc key cryptography?

- Stream Ciphers



- Block Ciphers
    - Repeat rounds many many times
    - Feistel (as DES): 1 round
    - SPN (as AES): 1 round

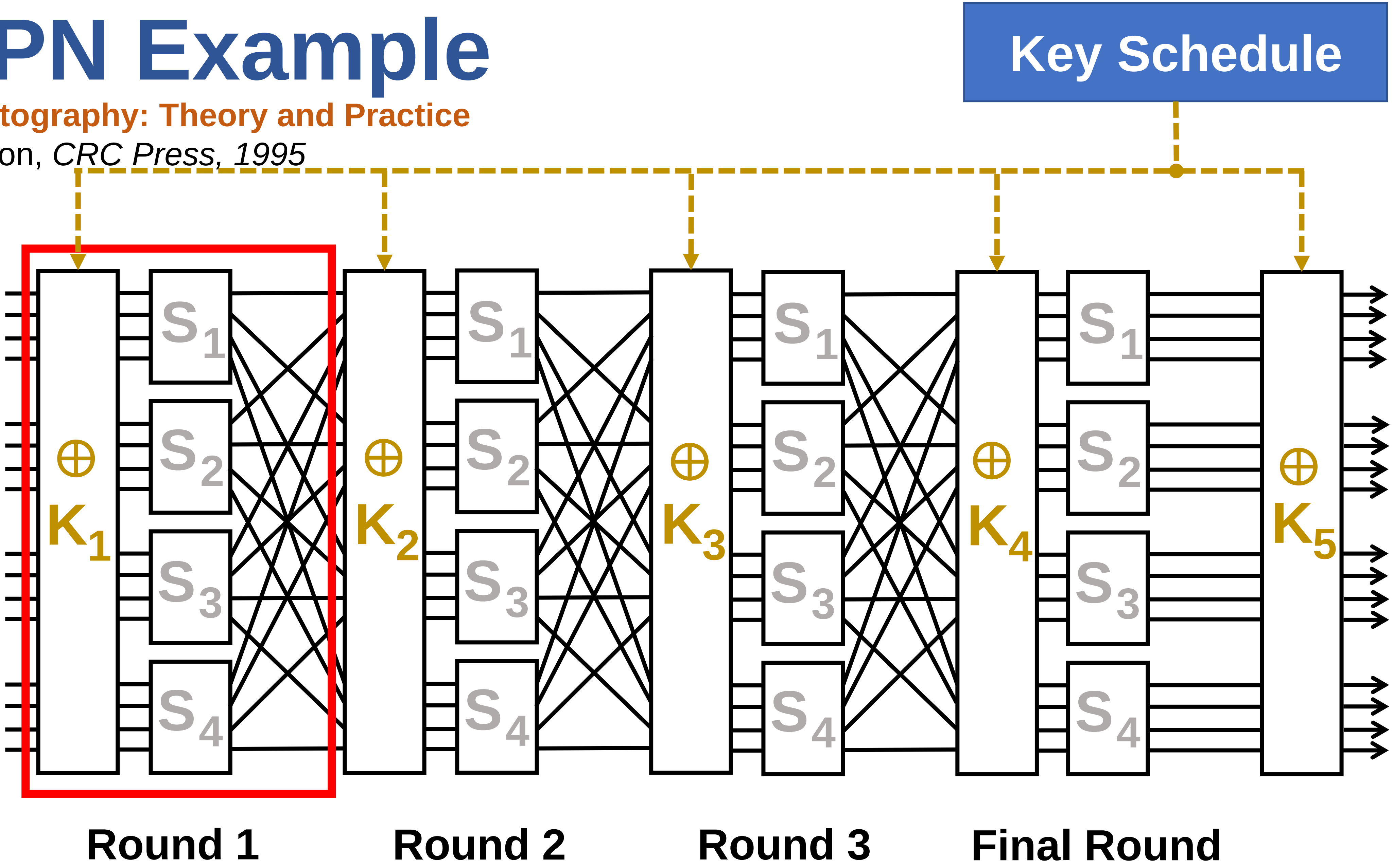




SPN Example

Cryptography: Theory and Practice

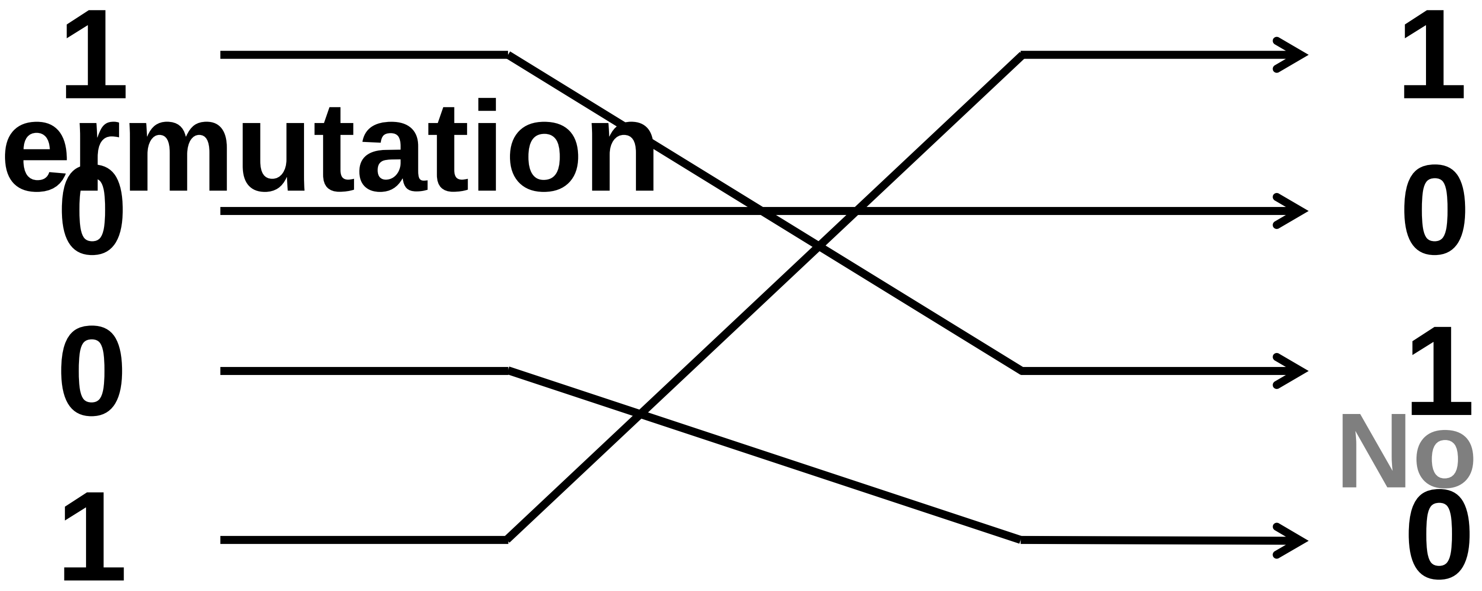
Stinson, *CRC Press, 1995*



Substitution-Permutation Network (SPN)

Elementary Operations

Linear Operation



Bits Permutation Linear

XOR Linear

S-box Non Linear

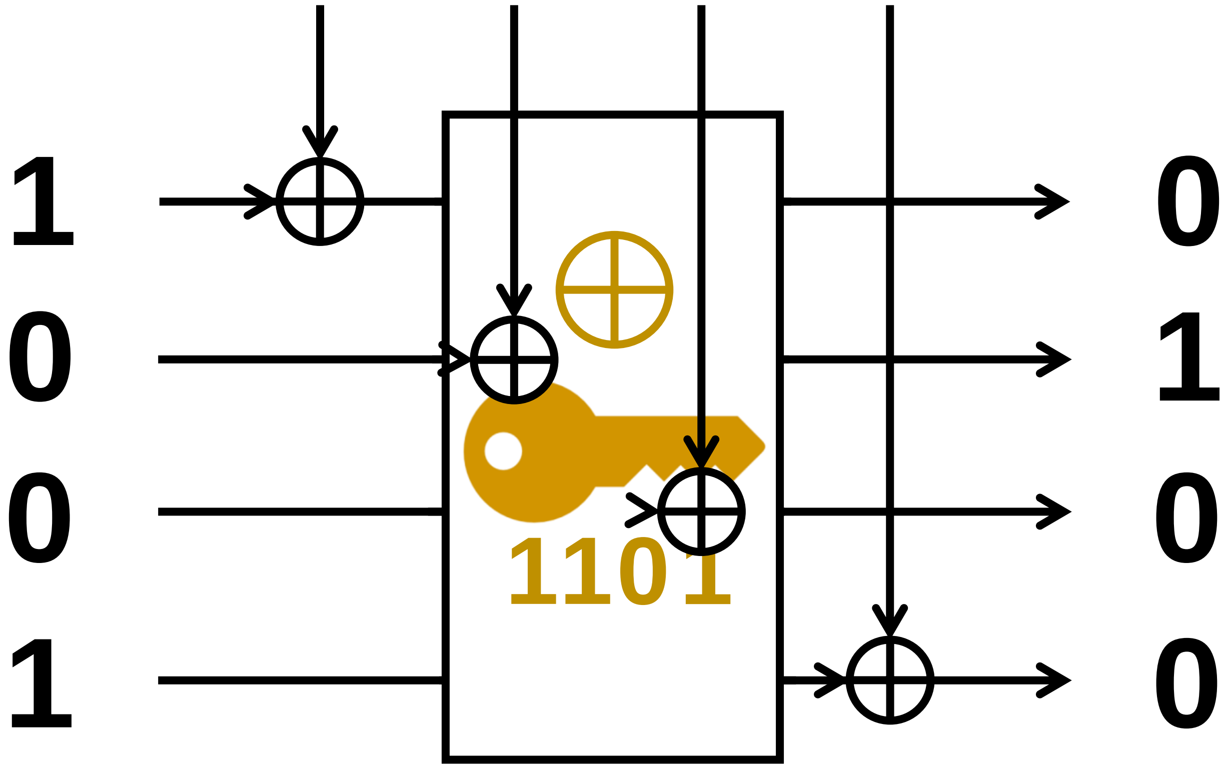
XOR

Linear Operation

A	B	$A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

$\forall \mathbf{A} \in \mathbb{F}_2$,

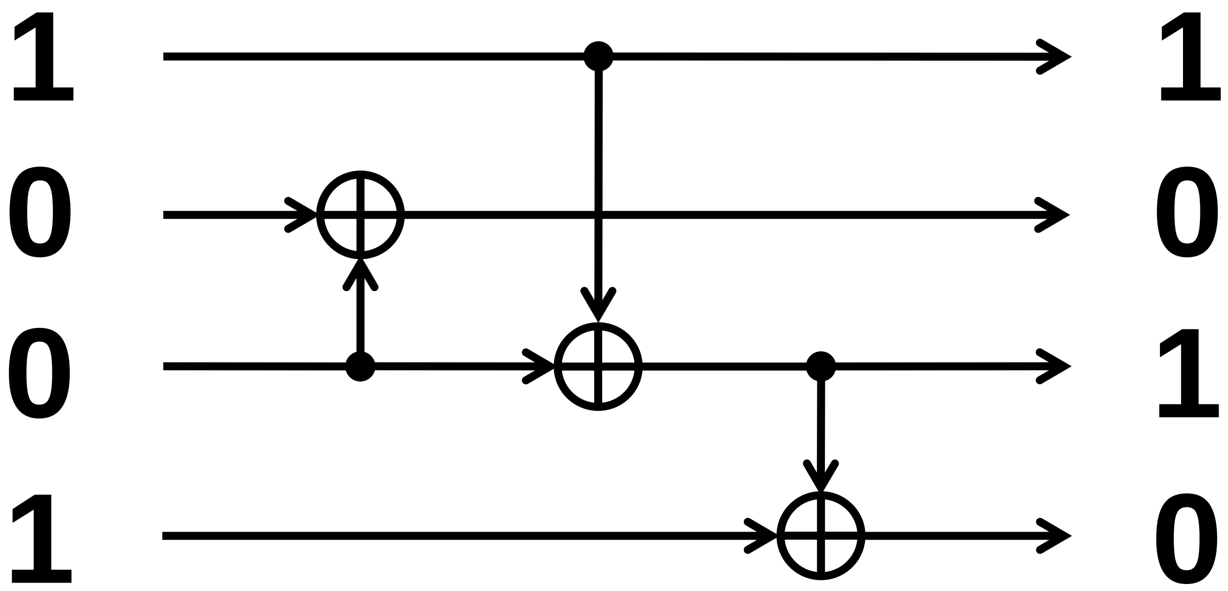
$$\mathbf{A} \oplus \mathbf{A} = 0$$



XOR

Linear Operation

A	B	A ⊕ B
0	0	0
0	1	1
1	0	1
1	1	0

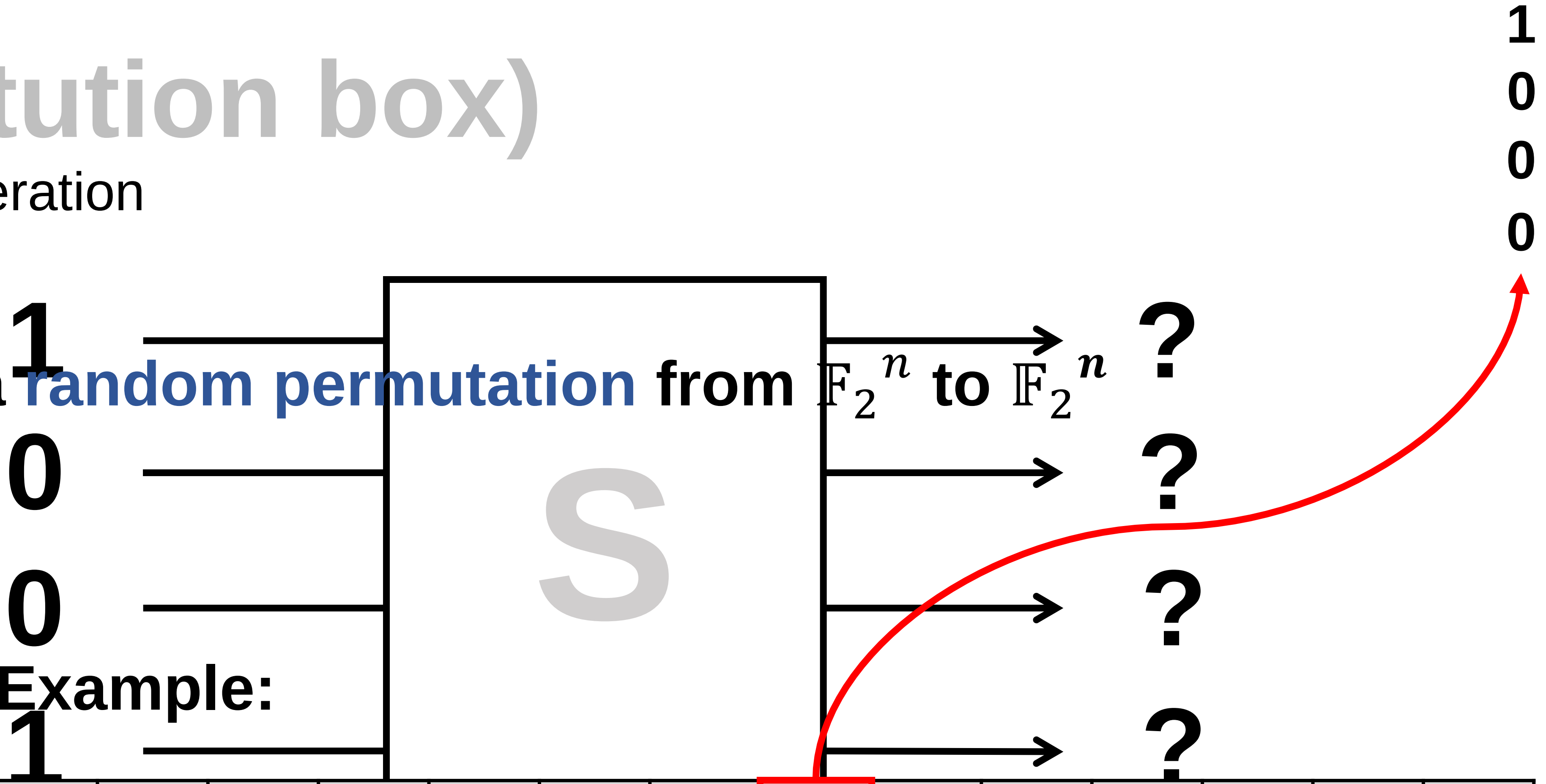


S-box (substitution box)

Non Linear Operation

Describes a random permutation from $\mathbb{F}_2{}^n$ to $\mathbb{F}_2{}^n$

4-bit S-box Example:



x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
S[x]	c	6	9	0	1	a	2	b	3	8	5	d	4	e	7	f

Cryptanalysis

We look for the plaintext, or better the used key

Linear Cryptanalysis

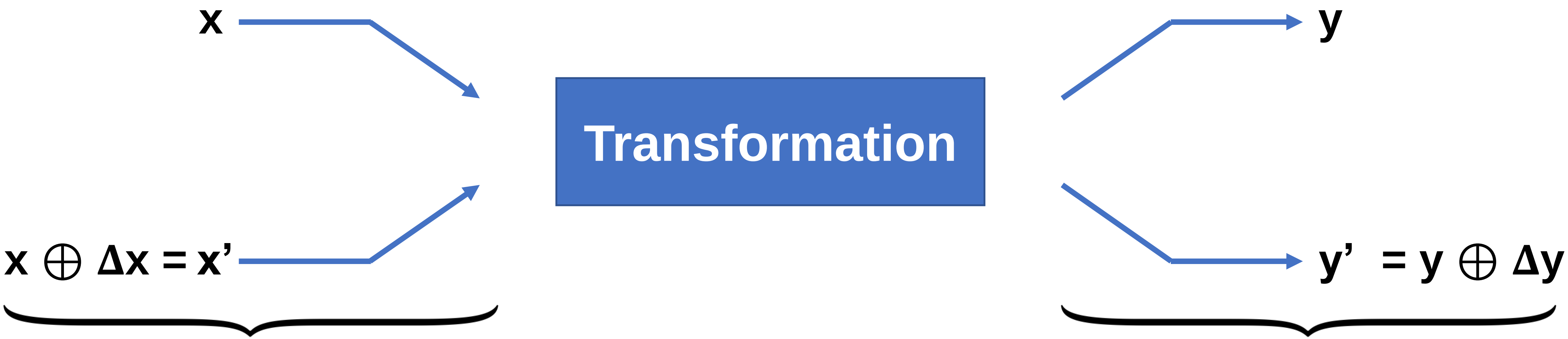
Known Plaintext Attacks

Differential Cryptanalysis

Chosen Plaintext Attacks

Differential Cryptanalysis

Elementary Principle



x

$x \oplus \Delta x = x'$

Transformation

y

$y' = y \oplus \Delta y$

Input Difference :
Δx $(= x \oplus x')$

Output Difference :
Δy $(= y \oplus y')$

We associated at each pair of differences $\Delta x \rightarrow \Delta y$ a probability p

$p (\Delta x \rightarrow \Delta y)$ is the probability to get the difference Δy as output knowing that the input difference is Δx

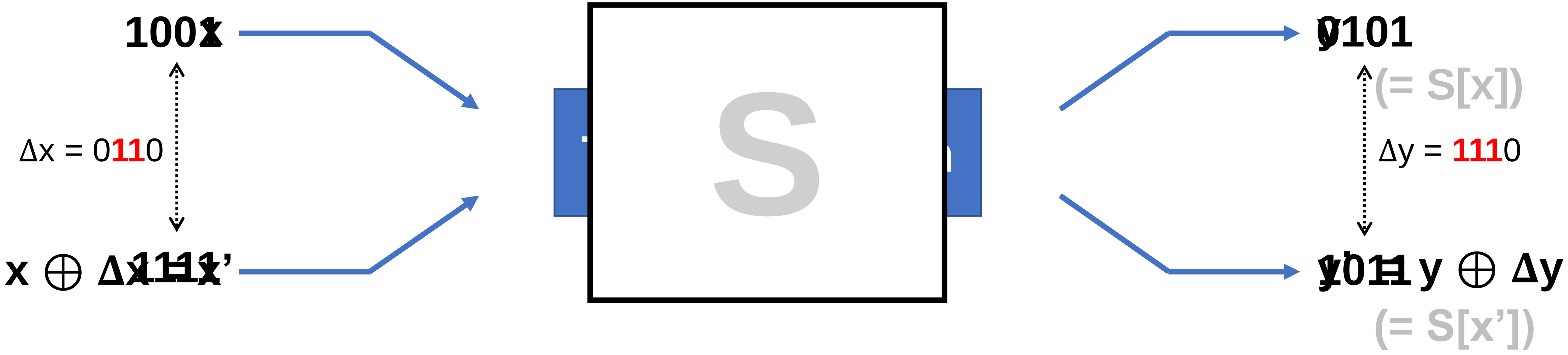
Differential Cryptanalysis

Linear / non linear

- Linear operations:
  - $L(x) \bigoplus L(x') = L(x \bigoplus x') = L(\boldsymbol{\Delta} x)$
  - with probability 1!

- Non-linear operations:
  - S-boxes
  - DDT

Differential Distribution Table (DDT)



$\forall(\Delta x,\Delta y) \in (\mathbb{F}_2^n)^2$,

Looking at all couples (x,x') having difference Δx,

$$p\,(\Delta x \rightarrow \Delta y) = \frac{\#\{(x,x') \in (\mathbb{F}_2^n)^2 \mid (x \oplus x' = \Delta x) \wedge (S[x] \oplus S[x'] = \Delta y)\}}{\#\{(x,x') \in (\mathbb{F}_2^n)^2 \mid (x \oplus x' = \Delta x)\} = 2^n}$$

Number of couples with Δx, Δy (output)

Number of possible couples in total

Thus, $p\,(0110 \rightarrow 1110) \neq 0$.

Differential Distribution Table (DDT)

4-bit S-box Example

Δy

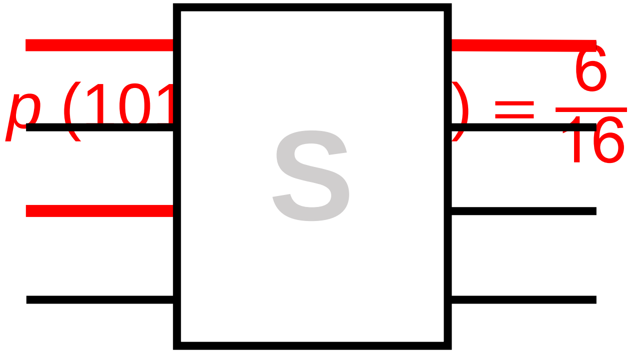
Δx

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	2	0	0	0	2	0	2	4	0	4	2	0	0
2	0	0	0	2	0	6	2	2	0	2	0	0	0	0	2	0
3	0	0	2	0	2	0	0	0	0	4	2	0	2	0	0	4
4	0	0	0	2	0	0	6	0	0	2	0	4	2	0	0	0
5	0	4	0	0	0	2	2	0	0	0	4	0	2	0	0	2
6	0	0	0	4	0	4	0	0	0	0	0	0	2	2	2	2
7	0	0	2	2	2	0	2	0	0	2	2	0	0	0	0	4
8	0	0	0	0	0	0	2	2	0	0	0	4	0	4	2	2
9	0	2	0	0	2	0	0	4	2	0	2	2	2	0	0	0
a	0	2	2	0	0	0	0	0	6	0	0	2	0	0	4	0
b	0	0	8	0	0	2	0	2	0	0	0	0	0	2	0	2
c	0	2	0	0	2	2	2	0	0	0	0	2	0	6	0	0
d	0	4	0	0	0	0	0	4	2	0	2	0	2	0	2	0
e	0	0	2	4	2	0	0	0	6	0	0	0	0	0	2	0
f	0	2	0	0	6	0	0	0	0	4	0	2	0	0	2	0

Table obtained with:

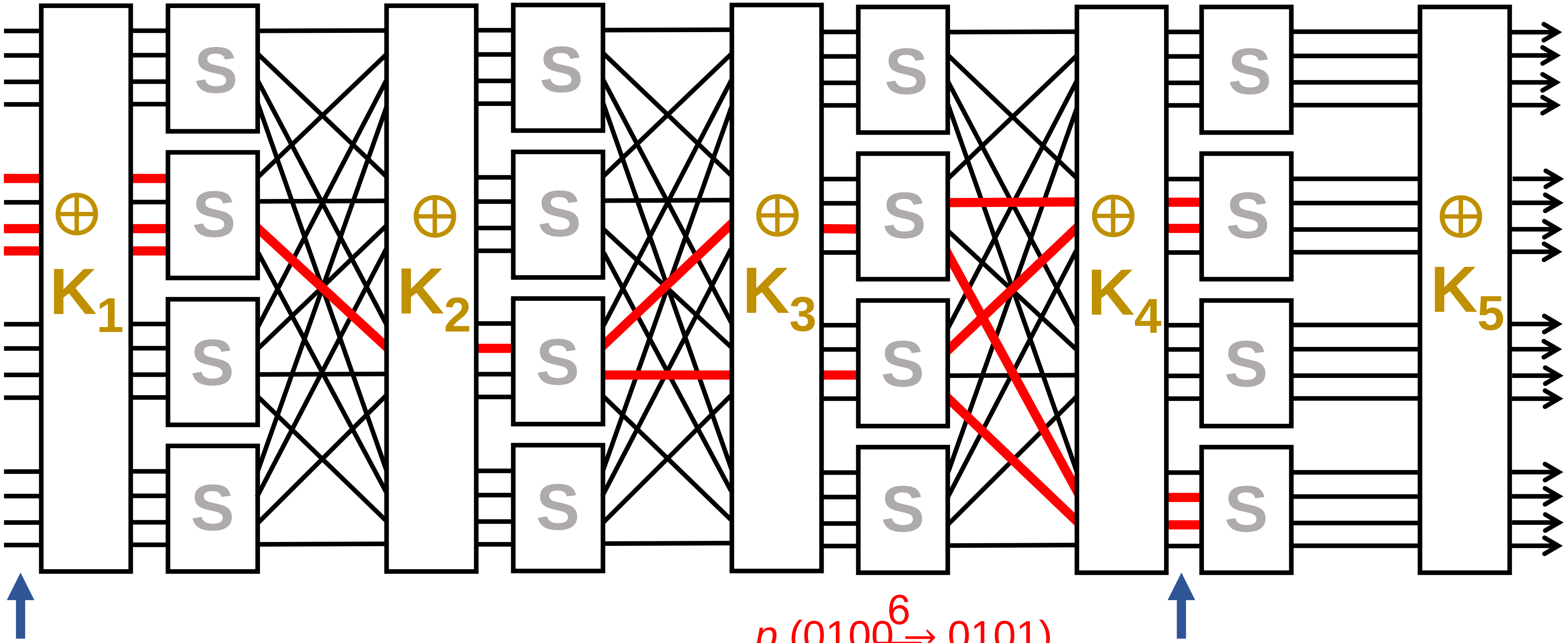
x	0	1	2	3	4	5	6	7
S[x]	e	4	d	1	2	f	b	8

x	8	9	a	b	c	d	e	f
S[x]	3	a	6	c	5	9	0	7



Differential Trail Search

Looking for the best differential characteristic

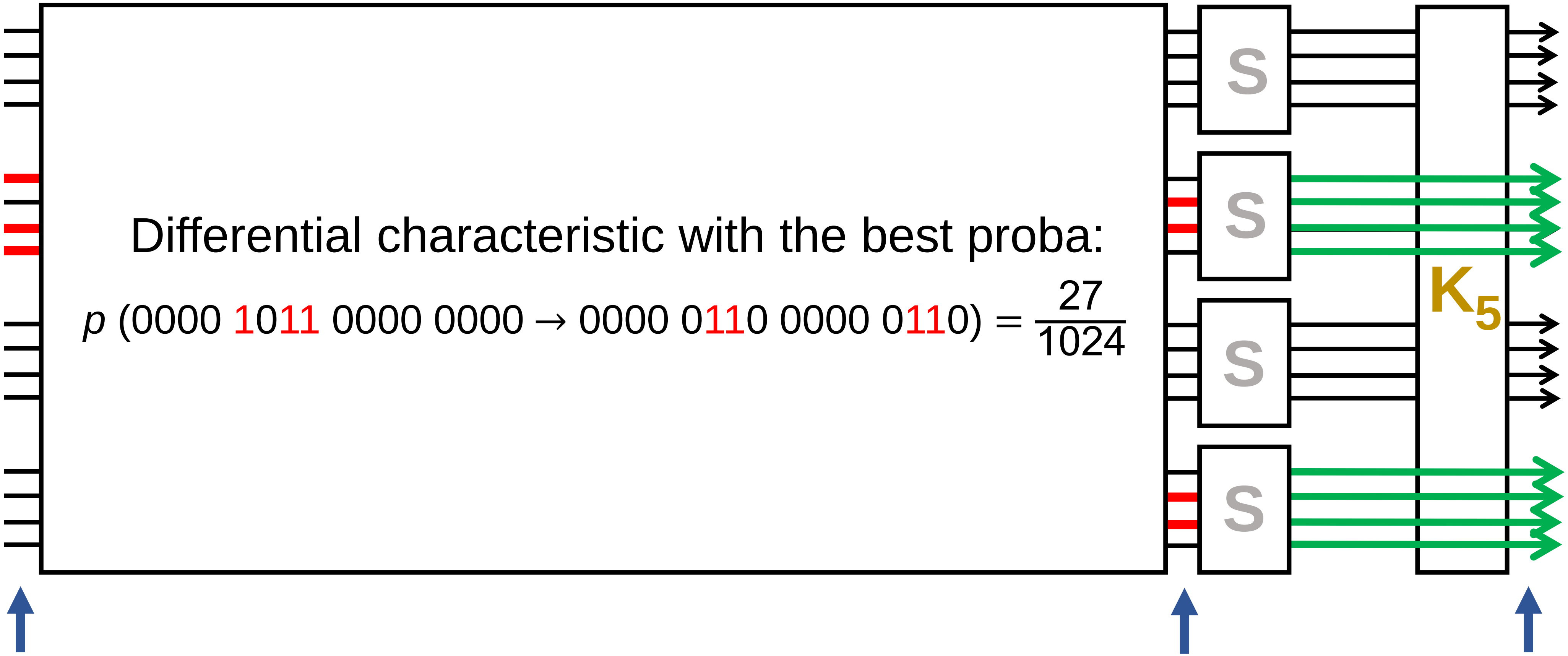


Probability to obtain with an input difference : **0000 1011 0000 0000**, la
the difference before the last round: **0000 0110 0000 0110**

$$p\,(1011 \Rightarrow 0010)\ \frac{8}{16} \times p\,(0100 \Rightarrow 0110)\ \frac{6}{16} \times p\,(0100 \Rightarrow 0101)\ \frac{6}{16} \times p\,(0100 \Rightarrow 0101)\ \frac{6}{16} = \frac{27}{1024}$$

Differential Trail Search

Last round



Differential characteristic with the best proba:

$$p\,(0000\ 1011\ 0000\ 0000 \rightarrow 0000\ 0110\ 0000\ 0110) = \frac{27}{1024}$$

(x , x')

chosen such that Δx = 0000 1011

($\tilde{y}$, $\tilde{y}$')

Partial deciphering of (z, z') according all the possible subkeys K_5

(z , z')

obtained after ciphering

We can attack bits 5 to 8 and 13 to 16 of K_5

We retain the subkey with the highest number of occurrences of couples ($\tilde{y}$, $\tilde{y}$') coherents with the best differential characteristic

What are we doing?

Know and improve existing attacks

Create new attacks

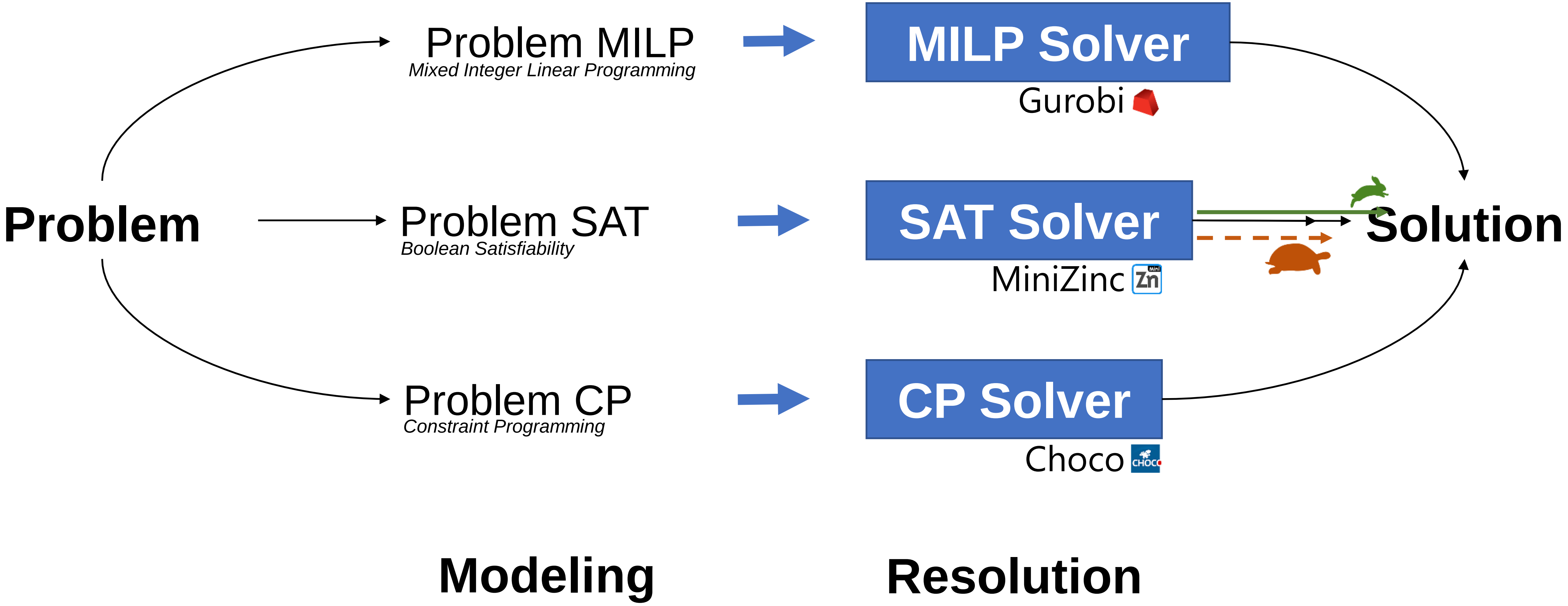
Why?

To be convinced about the security of current schemes

To elaborate new secure schemes

Modeling

Cryptanalysis Problem



Problem

Problem MILP

Mixed Integer Linear Programming

Problem SAT

Boolean Satisfiability

Problem CP

Constraint Programming

MILP Solver

Gurobi

SAT Solver

MiniZinc

CP Solver

Choco

Solution

Modeling

Resolution

How to model?

Here are my slides and there are less, less…

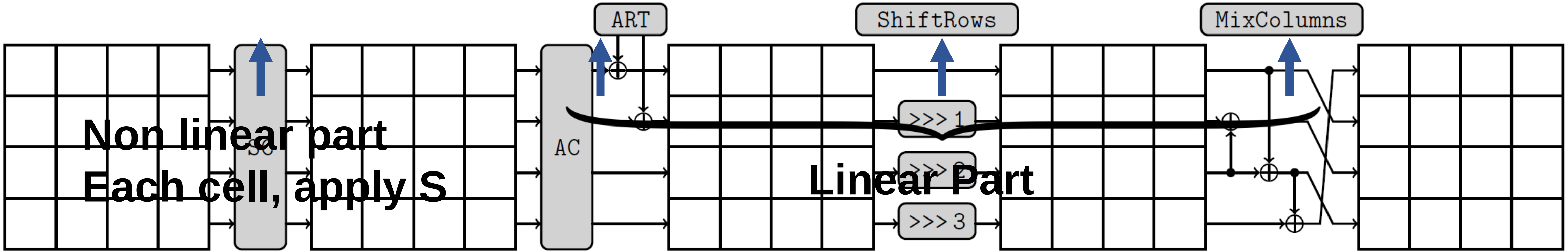
What scheme?

SC: Sboxes
AC/ART: Add Constants/Add Round Tweakey
Round Tweakey is like a Subkey

The SKINNY Family of Block Ciphers and its Low-Latency Variant MANTIS
Beierle, Jean, Kölbl, Leander, Moradi, Peyrin, Sasaki, Sasdrich & Sim
CRYPTO 2016

SKINNY

2 versions: SKINNY-64 and SKINNY-128
Key size variable
32 to 56 rounds



Non linear part
Each cell, apply S

Linear Part

How to model?

Round function

How to model?

- Two steps
  - Step 1, abstract cell differences δx with Boolean variables Δx in {0,1}
  - Find the path with the minimal weight
    - Active S-box means ΔSx = 1!
    - because less active S-box = better proba!
  - Then go to Step 2!

  - Step 2
    - Input the solutions of Step 1
    - Then try to instantiate cell differences δx to maximize the overall probability *p*

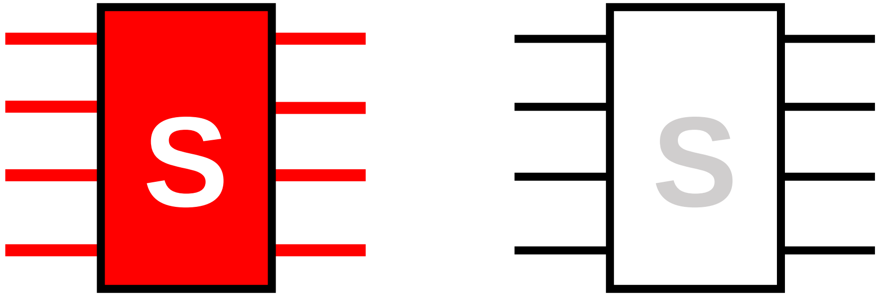
- How to do that?

Step 1

Step 1 (remember BOOLEAN): SC

- SC: SubCells: A 4-bit or an 8-bit S-box is applied to each cell of the state.
  - At cell level, use the DDT: δx => δy with a certain probability

- For Step 1 really simple model
  - At Boolean Level: S-box is bijective !
  - Thus if Δx=1, then Δy=1 => active S-box
  - if Δx=0, then Δy=0 => inactive S-box
  - Thus Good news! No effect!



Δx= Δy=1

Δx= Δy=0

Step 1: AC and ART

- AddConstants: Round constants are XORed to the state
- AddRoundTweakey: The first and second rows of all tweakey arrays are extracted and XORed

- No differences are inserted through AC and ART (if yes, more tricky…)

- So, do nothing to model ;o)

Step 1: ShiftRows

- ShiftRows. The rows of the cipher state cell array are rotated to the right (not to the left as in the AES!)
  - By 1 for the first row
  - By 2 for the second
  - By 3 for the third

- So, at cell level: $\delta y[i+j \bmod 4,j]=\delta x[i,j]$
- So, at boolean level: $\Delta y[i+j \bmod 4,j]= \Delta x[i,j]$

Step 1: MixColumns

- MixColumns. Each column of the cipher internal state array is multiplied by the 4x4 binary matrix

$$\mathbf{M} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

- Thus,

$$\delta y[0,j]=\delta x[0,j] \oplus \delta x[2,j] \oplus \delta x[3,j]$$

$$\delta y[1,j]= \delta x[1,j]$$

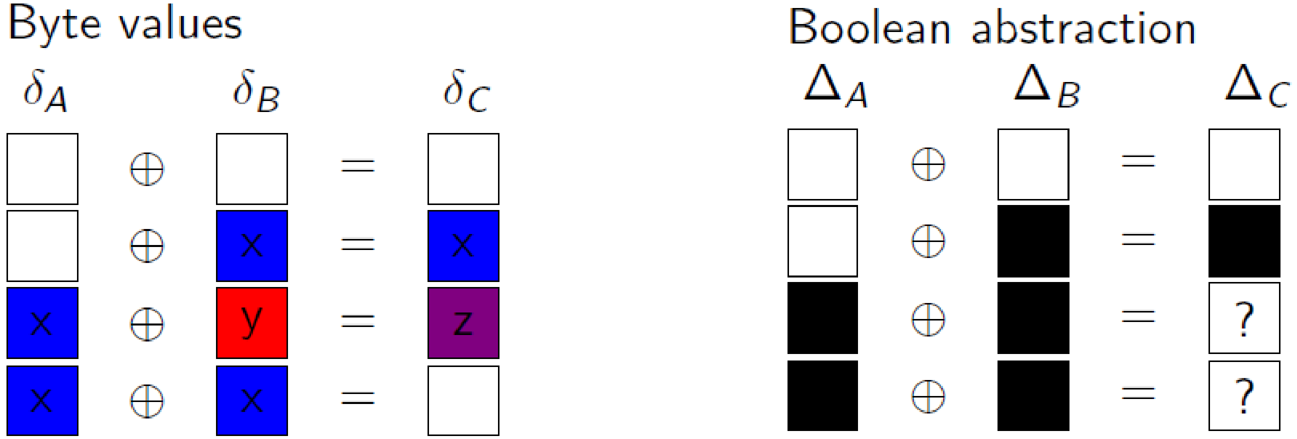
$$\delta y[2,j]=\delta x[1,j] \oplus \delta x[2,j]$$

$$\delta y[3,j]=\delta x[0,j] \oplus \delta x[2,j]$$

- Same for Boolean variables
- BUT $\oplus$ is not an available operation in the model, so…

Step 1: BUT the XOR?

(white $= 0$, colored $\neq 0$)

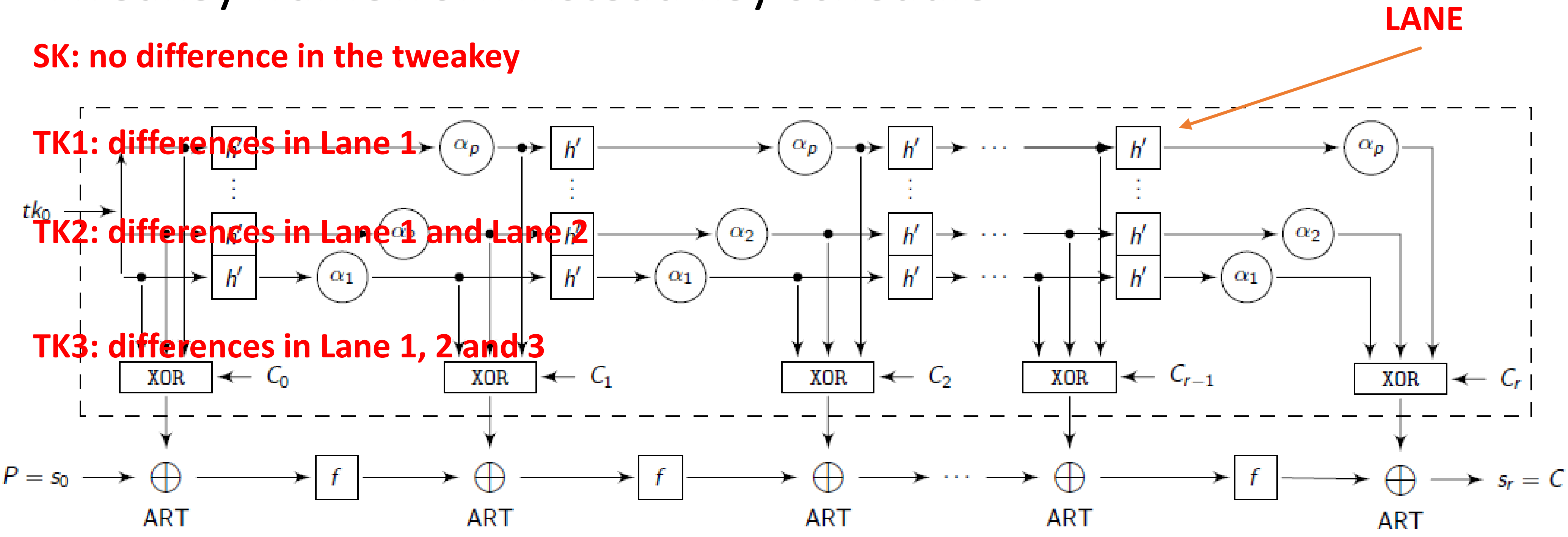


Δ_A	Δ_B	Δ_C
0	0	0
0	1	1
1	0	1
1	1	?

$$\Delta_A + \Delta_B + \Delta_C \neq 1$$

Step 2: Attacker models SK, TK1, TK2, TK3

- Tweakey framework instead key schedule



LANE

SK: no difference in the tweakey

TK1: differences in Lane 1

TK2: differences in Lane 1 and Lane 2

TK3: differences in Lane 1, 2 and 3

Step 1: what we have

- 4 models we tested: 1 MILP, 1 MiniZinc, 1 CP, 1 Ad-Hoc (C++)

- Step 1: 2 substeps
  - First, Minimize
  - Second, Enumerate
  - ..\..\..\..\BOULOT\ASIACRYPT_NEUF\tools\MiniZinc-Step1\SK\SK-Step1.mzn

- Lessons learnt:
  - MinZinc and CP are too slow
  - When you deviate from the optimal, MILP becomes too slow too
  - Only the Ad-Hoc model is able to provide us what we want
  - In TK1 (when differences are authorized also in the key), SKINNY-128 with 14 rounds:
    - 3 solutions for optimal value v= 45
    - 897 solutions for v = v+ 5 = 50
    - 137 019 solutions for v = v+ 10 = 55
    - 7 241 601 solutions for v = 59

Step 2

Where we are now

- With Step 1, we have the differential trails of minimal weights with Boolean variables
- Now, let us try to instantiate those trails to maximize the overall probability *p*
- Some trails could not be instantiated: they are called non-consistent BUT some are instantiable, we are looking for those trails
- So, take as input all the Step 1 solutions

Step 2: model each SKINNY transformation

- With δx variables with integer domains

- SC: SubCells. An S-box

- If, there is an active S-box, model the DDT:
  - (δx, δy, $-10.\log_2(p(\delta x \rightarrow \delta y))$) under a table constraint
  - To discard negative value and keep only integer value

  - Objective function becomes: Minimize sum($-10.\log_2(p(\delta x \rightarrow \delta y))$)

Step 2: model each SKINNY transformation

- AC and ART: no effect in differential cryptanalysis
- ShiftRows: Direct implementation, just shift to the right
- MixColumns: Direct implementation, just XOR through table constraint
- The XOR is implemented through a table constraint

Step 2: all in 1! Only CP!

$$\text{Minimize } Obj_{Step2} = \sum_{r=1}^{n}\sum_{i=1}^{4}\sum_{j=1}^{4} P_{r,i,j} \text{ subject to } 20 \times n \leq \sum_{r=1}^{n}\sum_{i=1}^{4}\sum_{j=1}^{4} P_{r,i,j} \leq \min(70 \times n, O^*)$$

$$\delta X_{r,i,j} \in 0..255,\ \ \delta SB_{r,i,j} \in 0..255,\ \ P_{r,i,j} \in \{0, 20, .., 70\},$$

$$\begin{cases} \delta X_{r,i,j} = 0 \wedge \delta SB_{r,i,j} = 0 \wedge P_{r,i,j} = 0 & \text{if } \Delta X_{r,i,j} = 0 \\ \delta X_{r,i,j} \geq 1 \wedge \delta SB_{r,i,j} \geq 1 \wedge P_{r,i,j} \geq 20 & \text{otherwise} \end{cases}$$

Sbox $\textsc{Table}(\langle \delta X_{r,i,j}, \delta SB_{r,i,j}, P_{r,i,j} \rangle, \langle \text{SBox} \rangle) \quad \text{if } \Delta X_{r,i,j} \neq 0$

MixColumns First Row $\delta SB_{r,0,j} = \delta X_{r+1,1,j}$

MixColumns Second Row

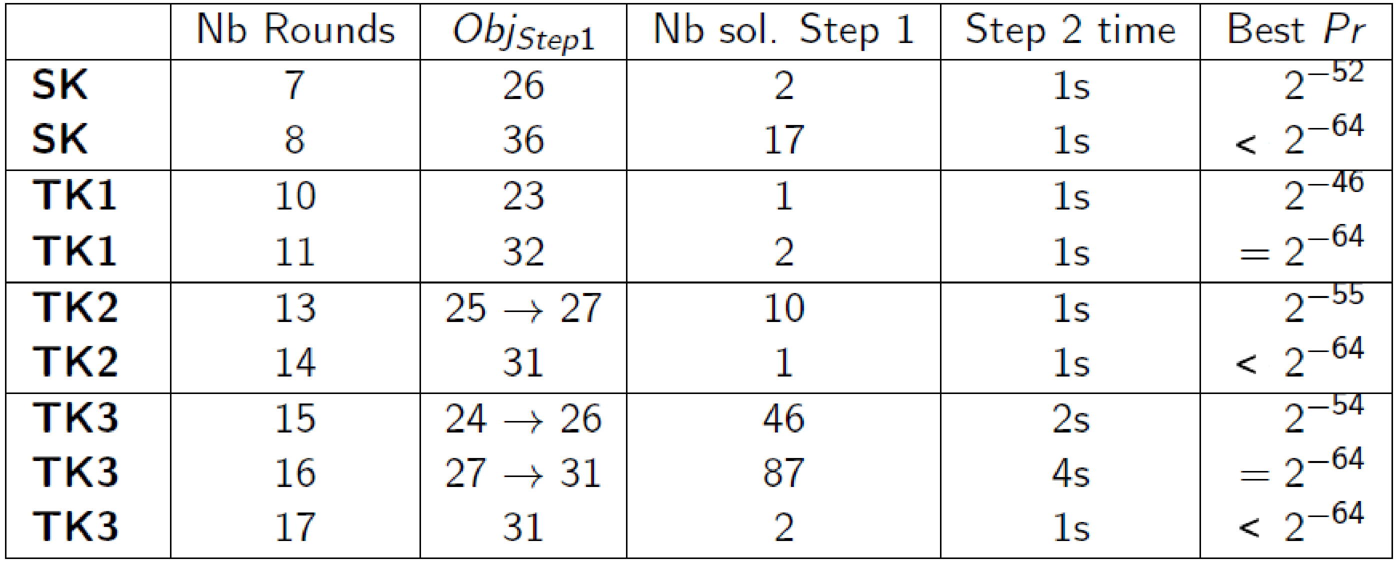
$$\begin{cases} \delta SB_{r,2,(2+j)\%4} = \delta X_{r+1,2,j} & \text{if } \Delta SB_{r,1,(3+j)\%4} = 0 \\ \delta SB_{r,1,(3+j)\%4} = \delta X_{r+1,2,j} & \text{if } \Delta SB_{r,2,(2+j)\%4} = 0 \\ \delta SB_{r,1,(3+j)\%4} = \delta SB_{r,2,(2+j)\%4} & \text{if } \Delta X_{r+1,2,j} = 0 \\ \textsc{Table}(\langle \delta SB_{r,1,(3+j)\%4}, \delta SB_{r,2,(2+j)\%4}, \delta X_{r+1,2,j} \rangle, \langle \text{XOR} \rangle) & \text{otherwise} \end{cases}$$

$\langle \text{XOR} \rangle$ encodes $\oplus$ relation and $\langle \text{SBox} \rangle$ the S-box constraint.

Results

SKINNY-64: few seconds!

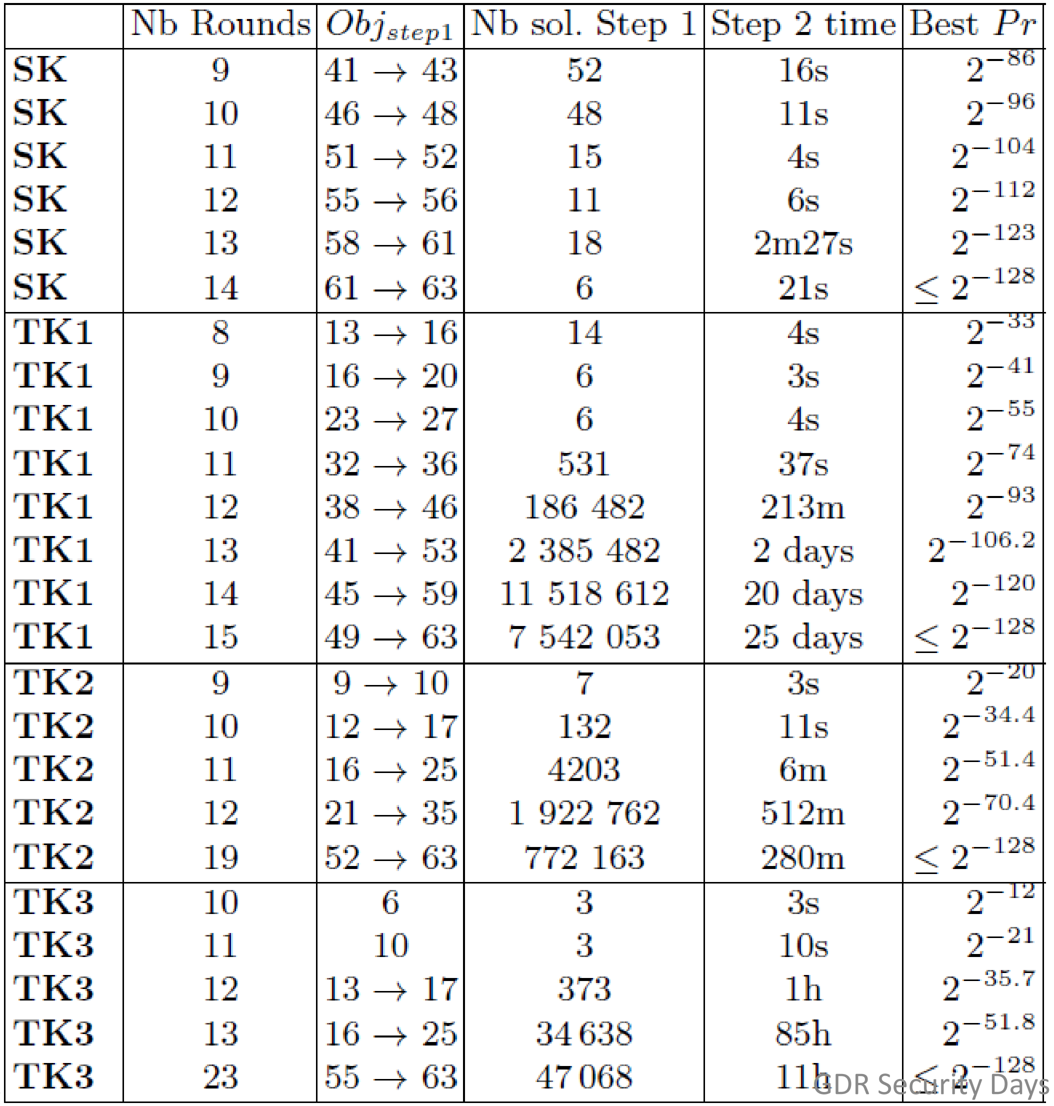
Limits: full code book = 2^{64} thus Pr < 2^{-64}



	Nb Rounds	Obj_{Step1}	Nb sol. Step 1	Step 2 time	Best Pr
SK	7	26	2	1s	2^{-52}
SK	8	36	17	1s	$< 2^{-64}$
TK1	10	23	1	1s	2^{-46}
TK1	11	32	2	1s	$= 2^{-64}$
TK2	13	$25 \rightarrow 27$	10	1s	2^{-55}
TK2	14	31	1	1s	$< 2^{-64}$
TK3	15	$24 \rightarrow 26$	46	2s	2^{-54}
TK3	16	$27 \rightarrow 31$	87	4s	$= 2^{-64}$
TK3	17	31	2	1s	$< 2^{-64}$

SKINNY-128: push the limits!

Limits: full code book = 2^{128} thus Pr < 2^{-128}



	Nb Rounds	Obj_{step1}	Nb sol. Step 1	Step 2 time	Best Pr
SK	9	$41 \to 43$	52	16s	2^{-86}
SK	10	$46 \to 48$	48	11s	2^{-96}
SK	11	$51 \to 52$	15	4s	2^{-104}
SK	12	$55 \to 56$	11	6s	2^{-112}
SK	13	$58 \to 61$	18	2m27s	2^{-123}
SK	14	$61 \to 63$	6	21s	$\leq 2^{-128}$
TK1	8	$13 \to 16$	14	4s	2^{-33}
TK1	9	$16 \to 20$	6	3s	2^{-41}
TK1	10	$23 \to 27$	6	4s	2^{-55}
TK1	11	$32 \to 36$	531	37s	2^{-74}
TK1	12	$38 \to 46$	186 482	213m	2^{-93}
TK1	13	$41 \to 53$	2 385 482	2 days	$2^{-106.2}$
TK1	14	$45 \to 59$	11 518 612	20 days	2^{-120}
TK1	15	$49 \to 63$	7 542 053	25 days	$\leq 2^{-128}$
TK2	9	$9 \to 10$	7	3s	2^{-20}
TK2	10	$12 \to 17$	132	11s	$2^{-34.4}$
TK2	11	$16 \to 25$	4203	6m	$2^{-51.4}$
TK2	12	$21 \to 35$	1 922 762	512m	$2^{-70.4}$
TK2	19	$52 \to 63$	772 163	280m	$\leq 2^{-128}$
TK3	10	6	3	3s	2^{-12}
TK3	11	10	3	10s	2^{-21}
TK3	12	$13 \to 17$	373	1h	$2^{-35.7}$
TK3	13	$16 \to 25$	34 638	85h	$2^{-51.8}$
TK3	23	$55 \to 63$	47 068	11h	$\leq 2^{-128}$

SK 14 rounds, Few minutes (vs 15 days before)!

But 25 days for TK1 and TK2 the holy Grail even with 128 threads and a different model...

The best TK2 solution has 15 rounds and a probability of $2^{-124.2}$ BUT maybe not optimal…

TK3 only results with 1 active byte in each lane

Conclusion

All those results were accepted to ACNS 2021
Or partly available: https://hal.archives-ouvertes.fr/hal-03040548

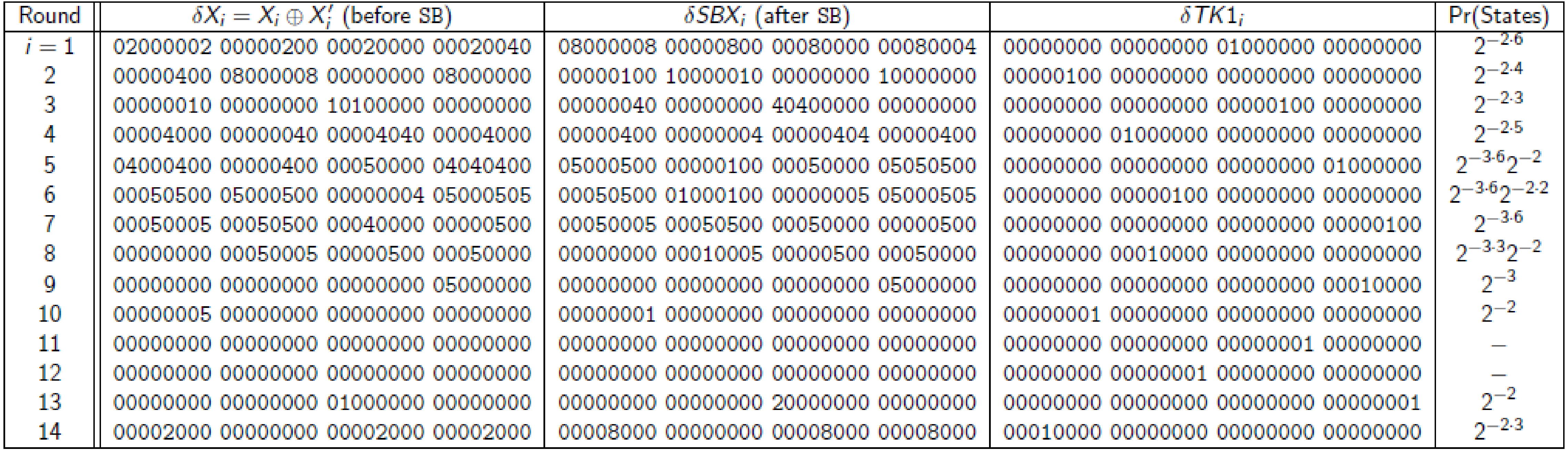
Part of the ANR Decrypt project

- Results on AES and Rijndael [AI 20, Africacrypt 22]
- Results on Boomerang attacks (SKINNY, WARP, Rijndael…) [FSE 21, FSE 22, submitted]
- Results on Division property on TRIVIUM [SAC 21]
- Dedicated tool: TAGADA [CP 21]
- Dedicated constraint: AbstractXOR [CP 20]

And because I love that

- The best TK1 differential characteristic on 14 rounds with a probability of 2^{-120}

Thank You for your attention!



Round	$\delta X_i = X_i \oplus X_i'$ (before SB)	δSBX_i (after SB)	$\delta TK1_i$	Pr(States)
$i = 1$	02000002 00000200 00020000 00020040	08000008 00000800 00080000 00080004	00000000 00000000 01000000 00000000	$2^{-2\cdot 6}$
2	00000400 08000008 00000000 08000000	00000100 10000010 00000000 10000000	00000100 00000000 00000000 00000000	$2^{-2\cdot 4}$
3	00000010 00000000 10100000 00000000	00000040 00000000 40400000 00000000	00000000 00000000 00000100 00000000	$2^{-2\cdot 3}$
4	00004000 00000040 00004040 00004000	00000400 00000004 00000404 00000400	00000000 01000000 00000000 00000000	$2^{-2\cdot 5}$
5	04000400 00000400 00050000 04040400	05000500 00000100 00050000 05050500	00000000 00000000 00000000 01000000	$2^{-3\cdot 6}2^{-2}$
6	00050500 05000500 00000004 05000505	00050500 01000100 00000005 05000505	00000000 00000100 00000000 00000000	$2^{-3\cdot 6}2^{-2\cdot 2}$
7	00050005 00050500 00040000 00000500	00050005 00050500 00050000 00000500	00000000 00000000 00000000 00000100	$2^{-3\cdot 6}$
8	00000000 00050005 00000500 00050000	00000000 00010005 00000500 00050000	00000000 00010000 00000000 00000000	$2^{-3\cdot 3}2^{-2}$
9	00000000 00000000 00000000 05000000	00000000 00000000 00000000 05000000	00000000 00000000 00000000 00010000	2^{-3}
10	00000005 00000000 00000000 00000000	00000001 00000000 00000000 00000000	00000001 00000000 00000000 00000000	2^{-2}
11	00000000 00000000 00000000 00000000	00000000 00000000 00000000 00000000	00000000 00000000 00000001 00000000	–
12	00000000 00000000 00000000 00000000	00000000 00000000 00000000 00000000	00000000 00000001 00000000 00000000	–
13	00000000 00000000 01000000 00000000	00000000 00000000 20000000 00000000	00000000 00000000 00000000 00000001	2^{-2}
14	00002000 00000000 00002000 00002000	00008000 00000000 00008000 00008000	00010000 00000000 00000000 00000000	$2^{-2\cdot 3}$

Bibliography

Cryptography: Theory and Practice
Stinson
CRC Press, 1995

Modern Cryptanalysis : Techniques for Advanced Code Breaking
Swenson
Wiley, 2008

The SKINNY Family of Block Ciphers and its Low-Latency Variant MANTIS
Beierle, Jean, Kölbl, Leander, Moradi, Peyrin, Sasaki, Sasdrich & Sim
CRYPTO 2016

MILP Modeling for (Large) S-boxes to Optimize Probability of Differential Characteristics
Abdelkhalek, Sasaki, Todo, Tolba & Youssef
ToSC 2017