Cryptanalysis of Lightweight Block Ciphers

María Naya-Plasencia
INRIA, France

Šibenik 2014

Outline

- Introduction
- *Impossible Differential* Attacks
- *Meet-in-the-middle* and improvements
- *Multiple Differential* Attacks
- Dedicated attacks (examples)

Outline

- Introduction
- *Impossible Differential* Attacks
- *Meet-in-the-middle* and improvements
- *Multiple Differential* Attacks

Cryptanalysis of Lightweight Block Ciphers

Lightweight Block Ciphers

- Lightweight Block Ciphers designed for constrained environments, like RFID tags, sensor networks.

- Real need $\Rightarrow$ an enormous amount of proposals in the last years:

PRESENT, LED, KATAN/KTANTAN, KLEIN, PRINCE, PRINTcipher, LBLOCK, TWINE, XTEA, mCrypton, Iceberg, HIGHT, Piccolo, SIMON, SPECK, SEA, DESL...

Lightweight Block Ciphers

- Cryptanalysis of lightweight block ciphers: a fundamental task, responsibility of the community.
- Importance of cryptanalysis (especially on new proposals): the more a block cipher is analyzed, the more confidence we can have in it...
- ...or know which algorithms are not secure to use.

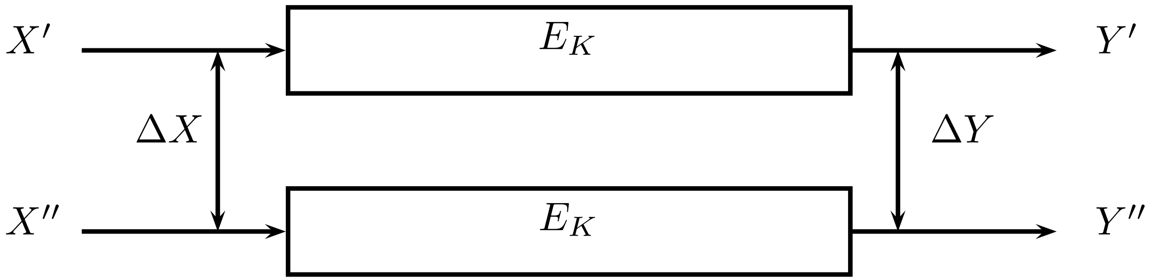
Lightweight Block Ciphers

- Lightweight: more 'risky' design, lower security margin, simpler components.
- Often innovative constructions: dedicated attacks
- Types of attacks: single-key/related-key, distinguisher/key-recovery, weak-keys, reduced versions.

Impossible Differential Attacks

Classical Differential Attacks [BS'90]

Given an input difference between two plaintexts, some output differences occur more often than others.



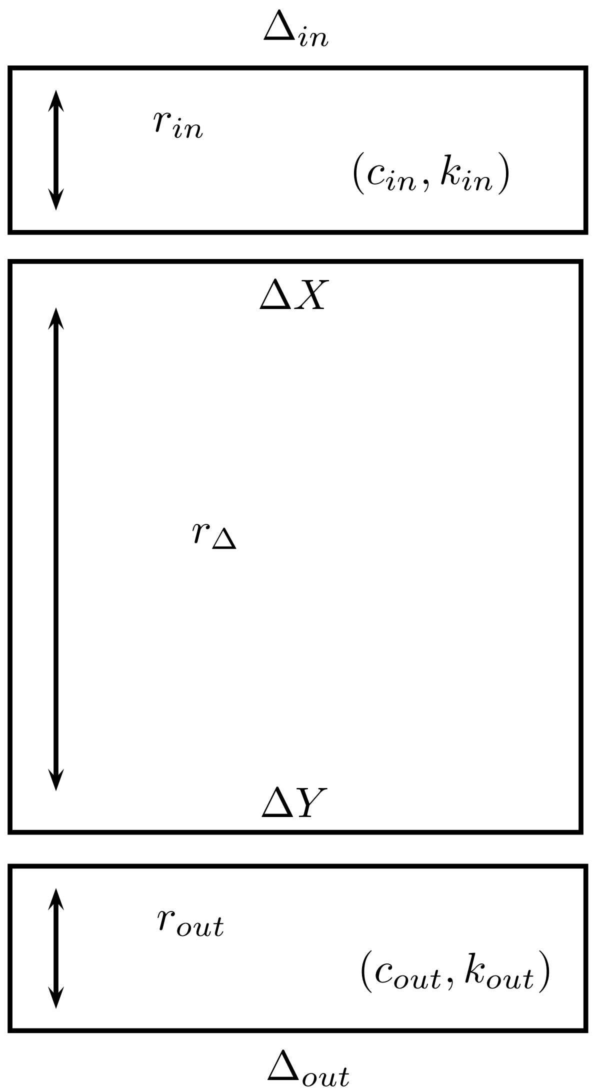
Impossible Differential Attacks [K,BBS'98]

- Impossible differential attacks use a differential with probability 0.

- We can find the impossible differential using the Miss-in-the-middle [BBS'99] technique.

- Extend the impossible differential backward and forward $\Rightarrow$ Active Sboxes transitions give information on the involved key bits.

Impossible Differential Attack



Discarding Wrong Keys

- Given a pair of inputs with Δ_{in} that generates Δ_{out},
- all the (partial) keys that produce ΔX from Δ_{in} and ΔY from Δ_{out} are not the correct one.

For the Attacks to Work

We need

$$C_{data} < 2^s$$

and

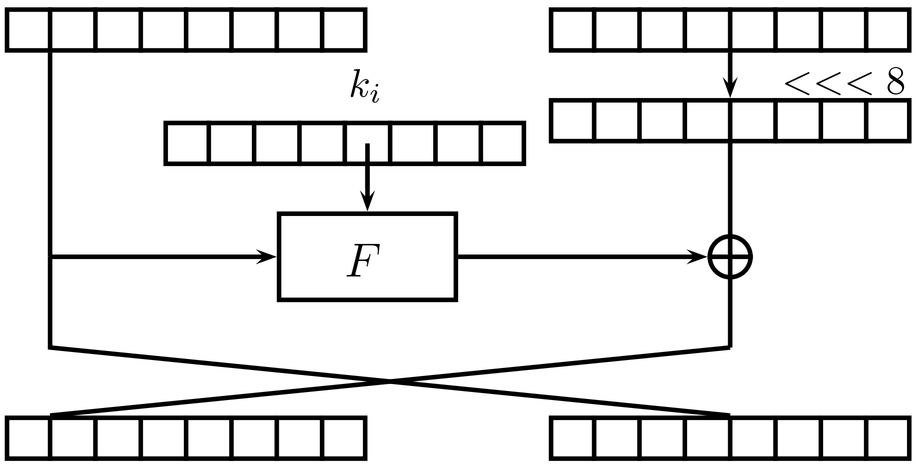
$$C_{data} + 2^{|k_{in} \cup k_{out}|} C_N + 2^{|K| - |k_{in} \cup k_{out}|} P 2^{|k_{in} \cup k_{out}|} < 2^{|K|}$$

where C_{data} is the data needed for obtaining N pairs $(\Delta_{in}, \Delta_{out})$, C_N is the average cost of testing the pairs per candidate key (early abort technique [LKKD08]) and P is the probability of not discarding a trial key.

Example: LBlock

Designed by Wu and Zhang, (ACNS 2011).

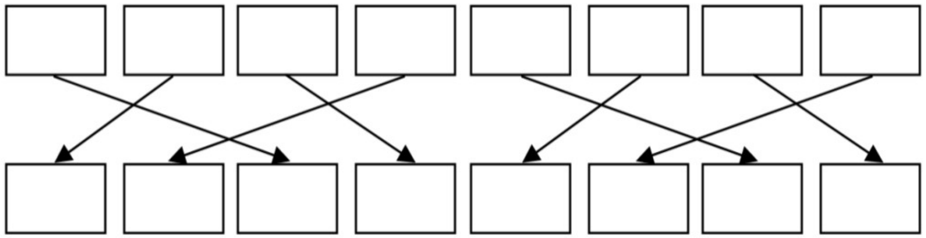
- 80-bit key and 64-bit state.
- 32 rounds.



Example: LBlock

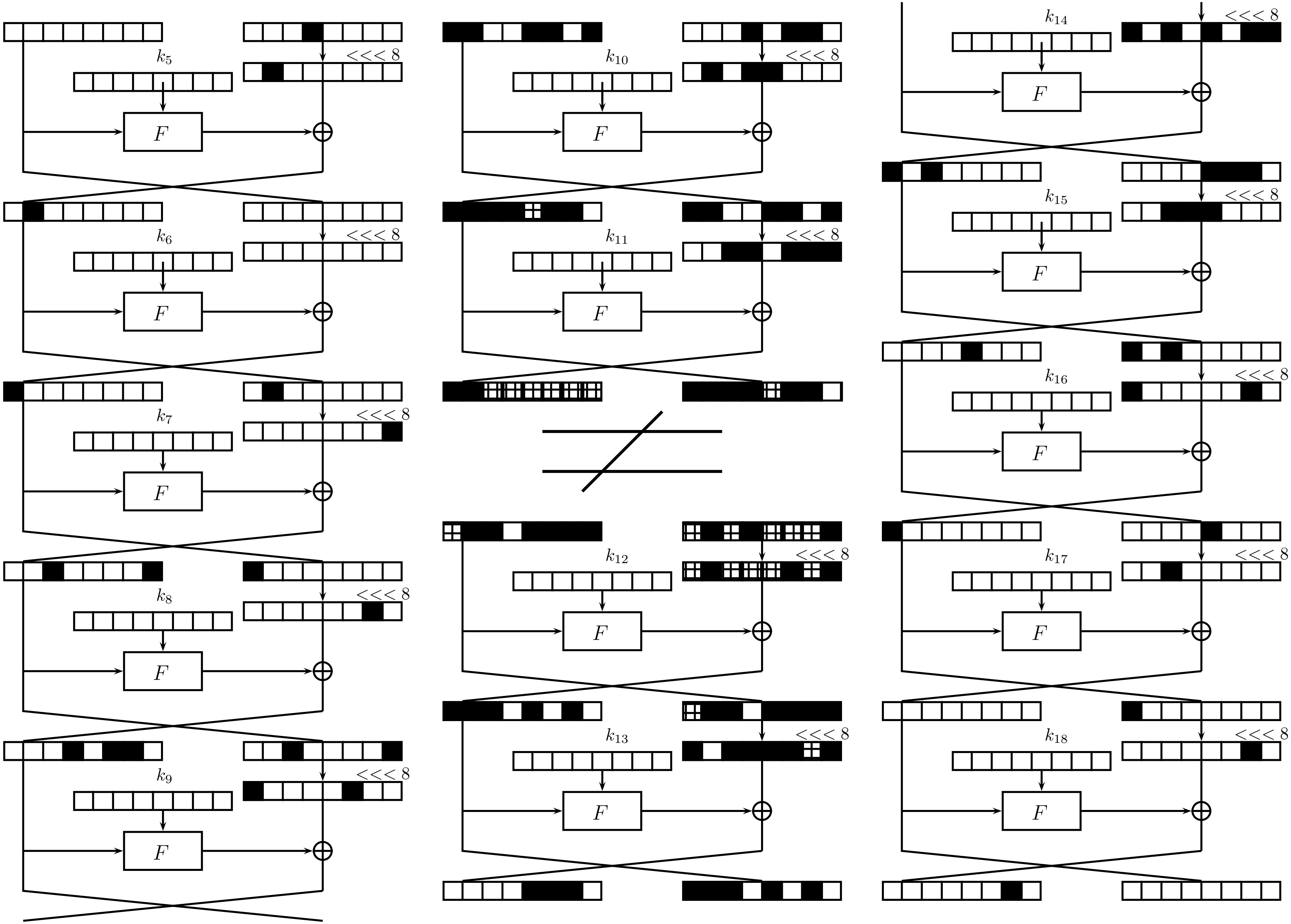
Inside the function F:

- add the subkey to the input.
- 8 different Sboxes 4×4.
- a nibble permutation P:

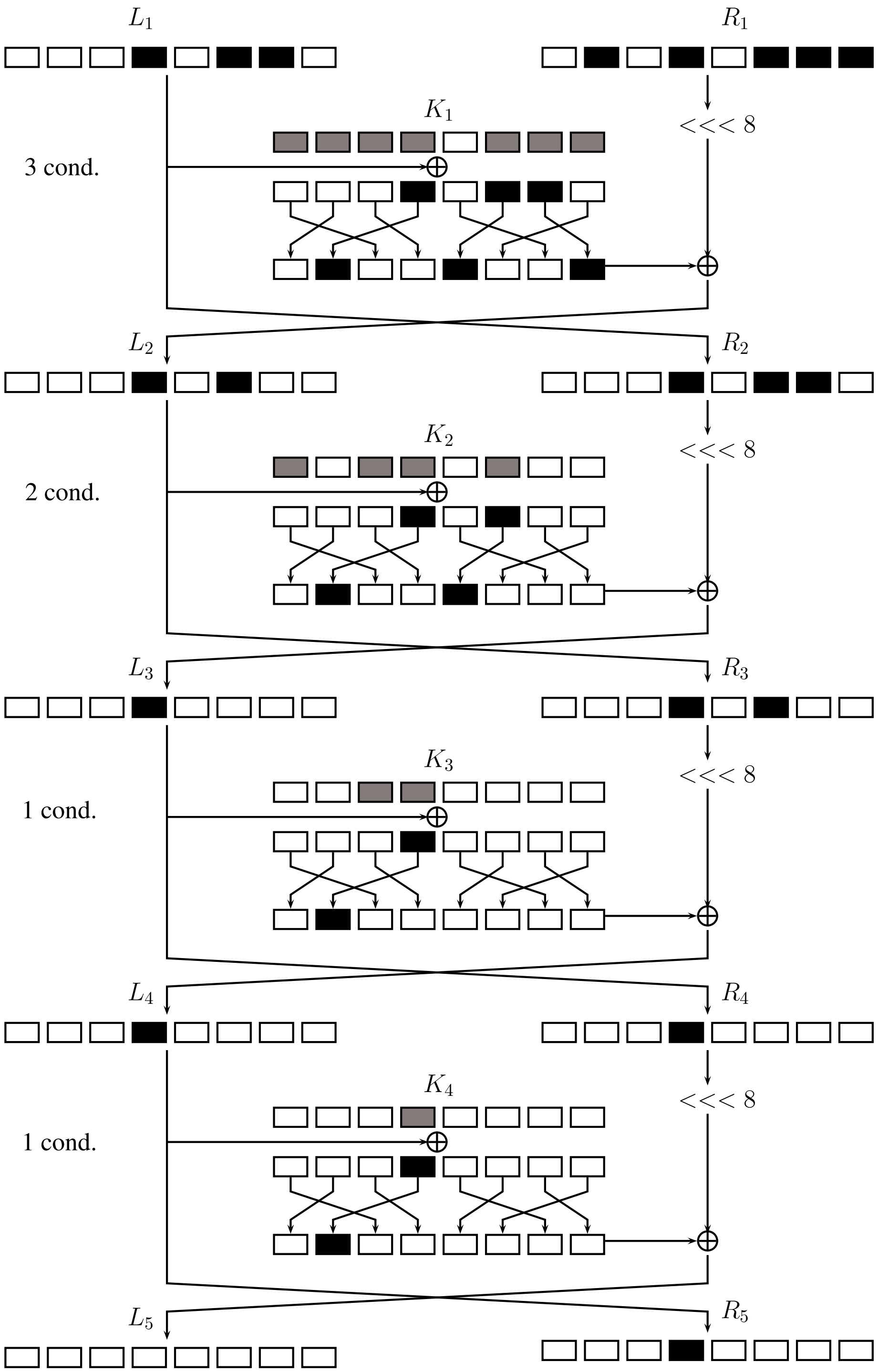


Best attack so far: Imp. Diff. on 23 rounds [CFMS'14,BMNPS'14].

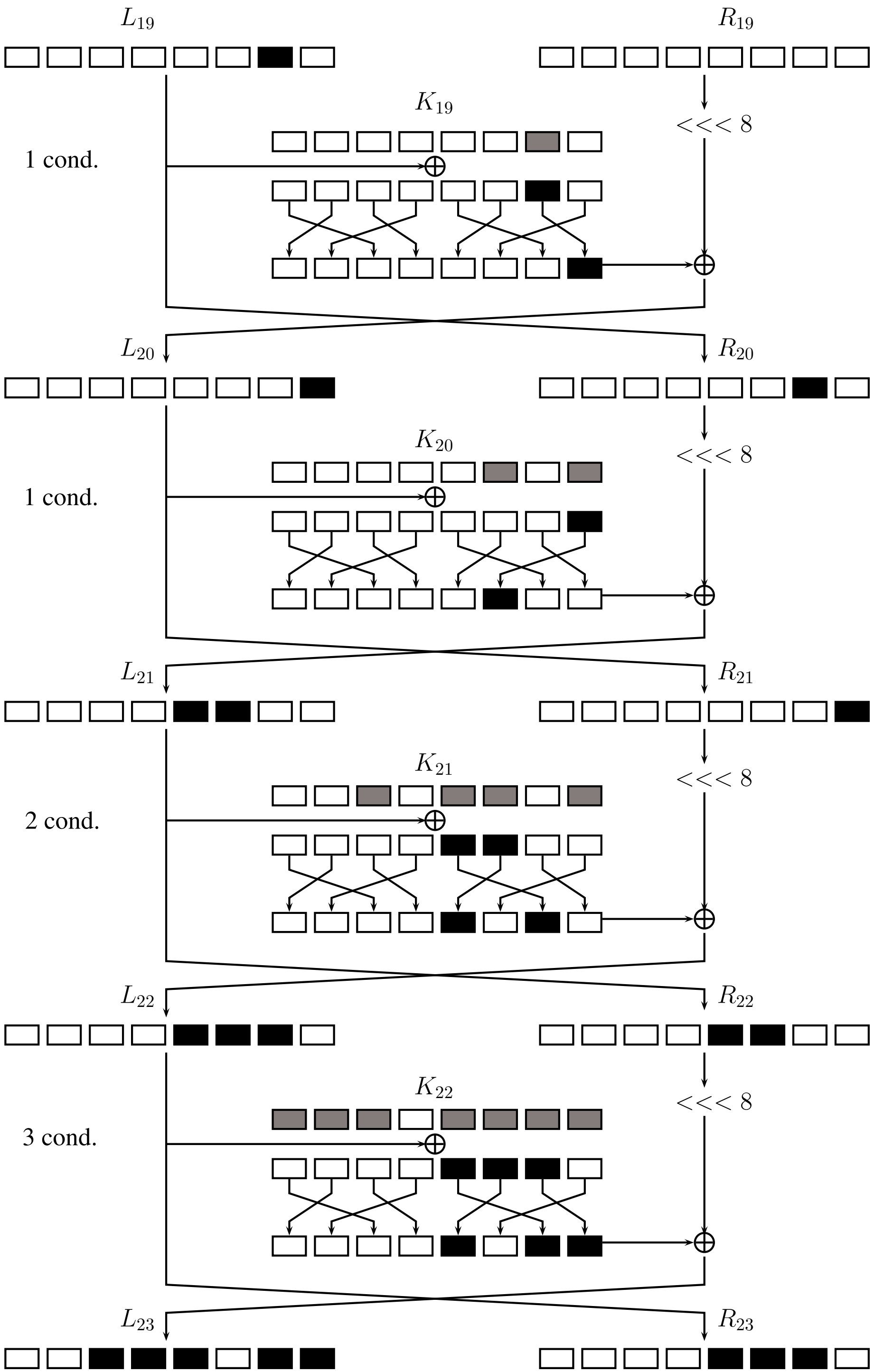
Impossible differential: 14 rounds



First Rounds



Last Rounds



L_{19}
R_{19}
K_{19}
$<<< 8$
1 cond.
L_{20}
R_{20}
K_{20}
$<<< 8$
1 cond.
L_{21}
R_{21}
K_{21}
$<<< 8$
2 cond.
L_{22}
R_{22}
K_{22}
$<<< 8$
3 cond.
L_{23}
R_{23}

Impossible Differential on LBlock

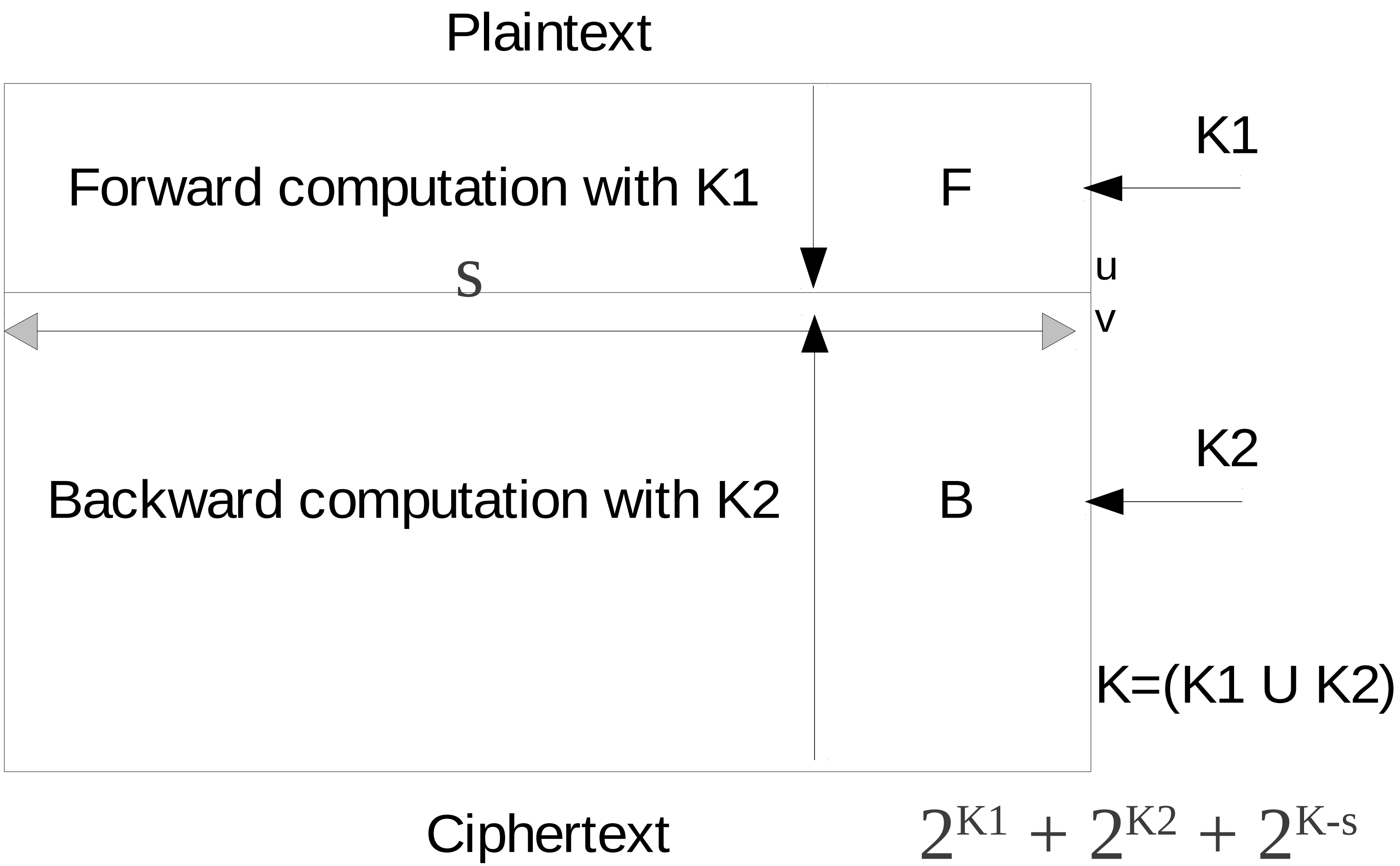
- For 21 rounds a complexity of $2^{69.5}$ in time with 2^{63} data, for 22: $2^{71.53}$ time and 2^{60} data, for 23: $2^{75.36}$ time and 2^{59} data.
- Feistel constructions in general are good targets

Meet-in-the-Middle Attacks

Meet-in-the-Middle Attacks

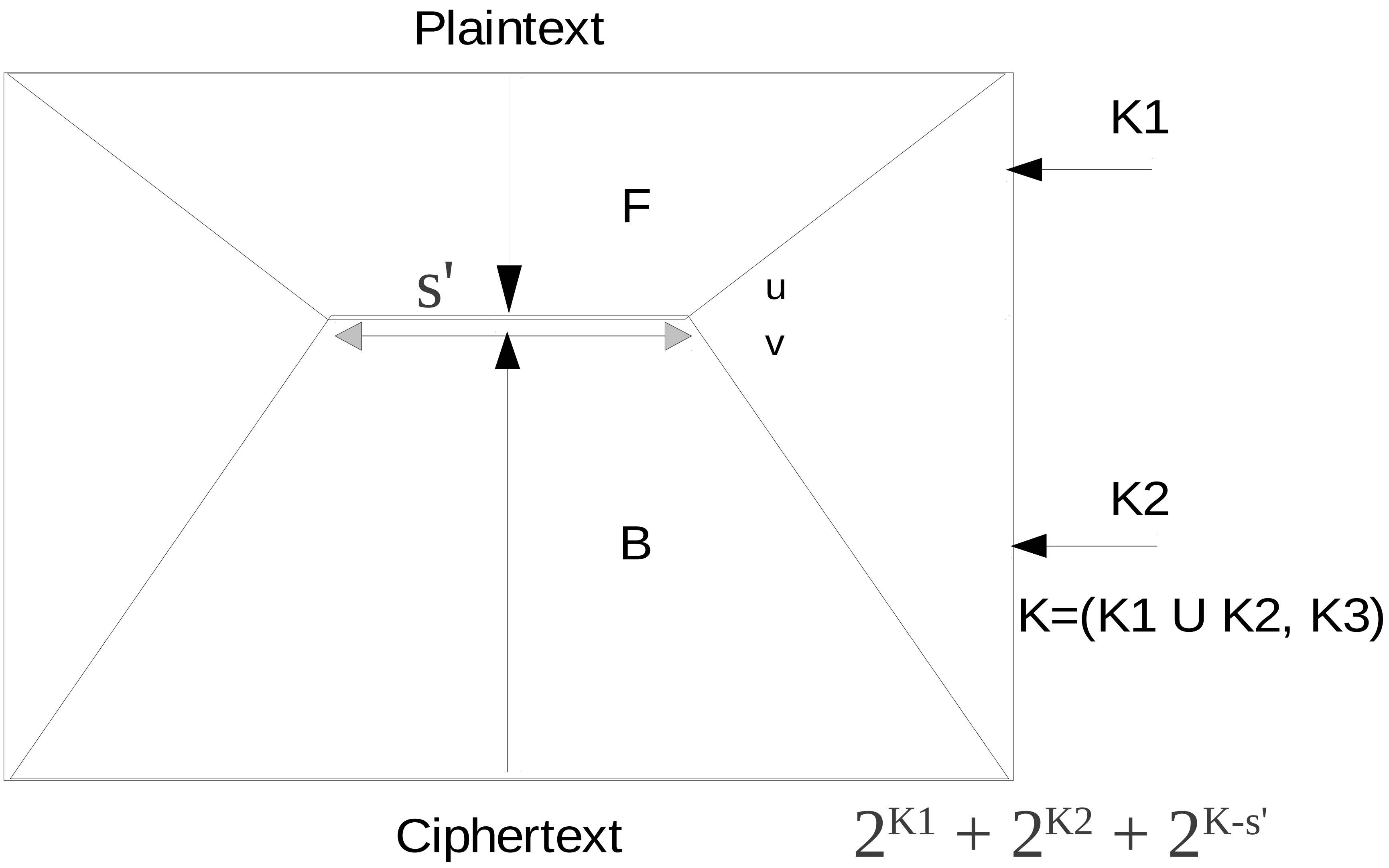
- Introduced by Diffie and Hellman in 1977.
- Largely applied tool.
- Few data needed.
- Many improvements: partial matching, bicliques, sieve-in-the-middle...

Meet-in-the-Middle Attacks



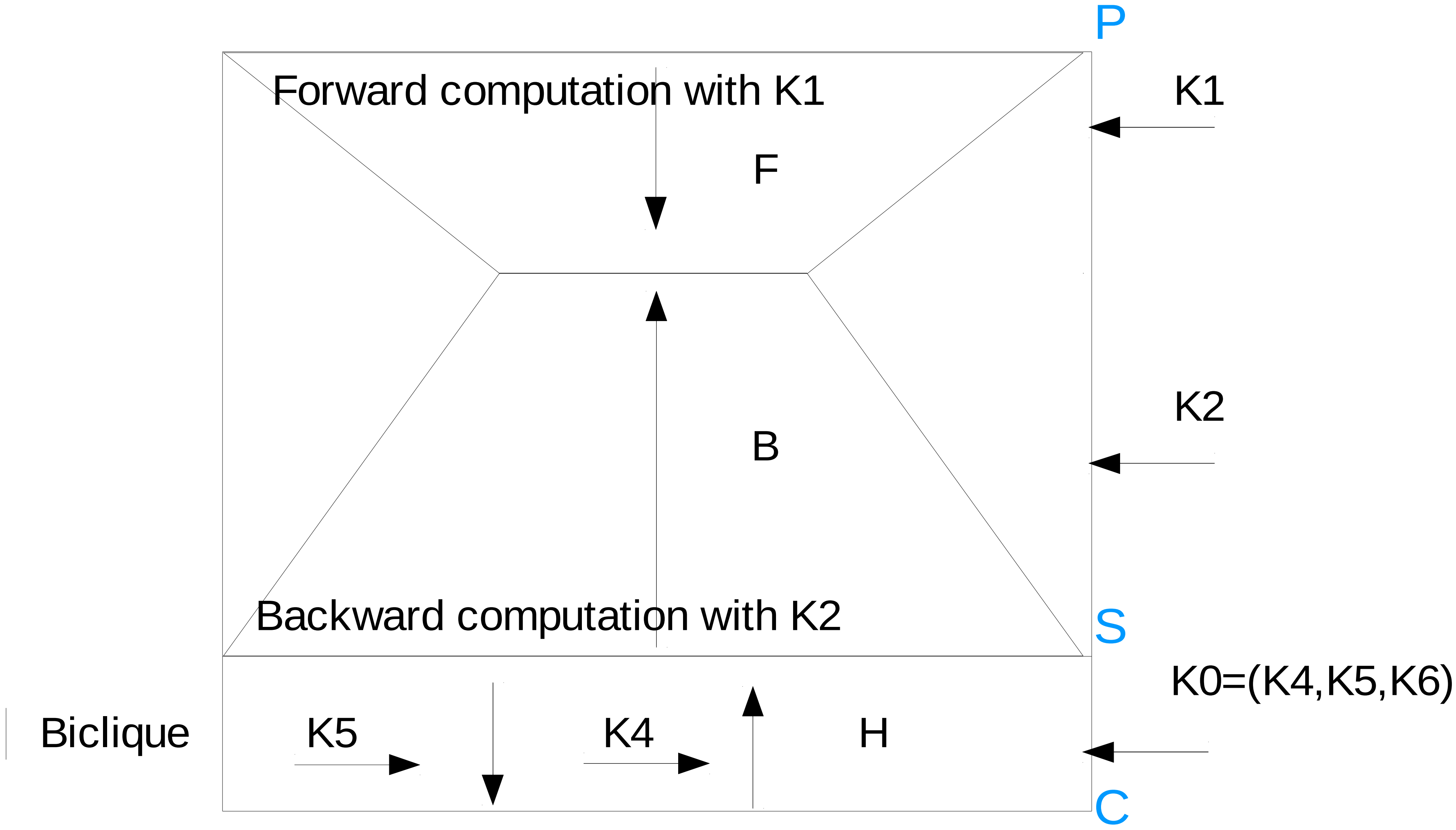
$$2^{K1} + 2^{K2} + 2^{K-s}$$

With Partial Matching [AS'08]



$2^{K1} + 2^{K2} + 2^{K-s'}$

With Bicliques [KRS'11]



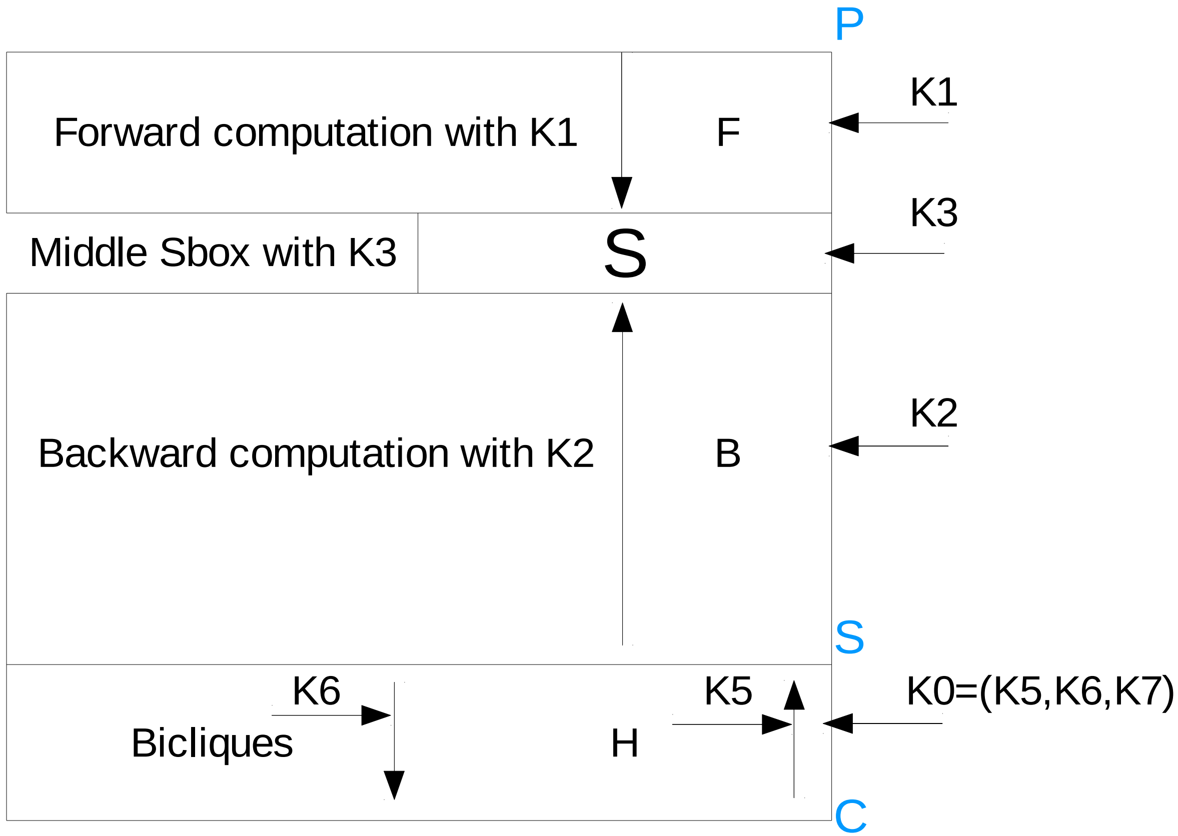
Bicliques

- Improvement of MITM attacks, but also...
- It can always be applied to reduce the total number of computations (at least the precomputed part) $\Rightarrow$ acceleration of exhaustive search [BKR'11] [1]
- Many other accelerated exhaustive search on LW block ciphers: PRESENT, LED, KLEIN, HIGHT, Piccolo, TWINE, LBlock ... (less than 2 bits of gain).
- Is everything broken? No.

[1] Most important application: best key-recovery on AES-128 in $2^{126.1}$ instead of the naive 2^{128}.

Sieve-in-the-Middle [CNPV'13]

- We compute some inputs and some outputs to an Sbox $S \Rightarrow$ sieving with transitions instead of collisions.



What is S?

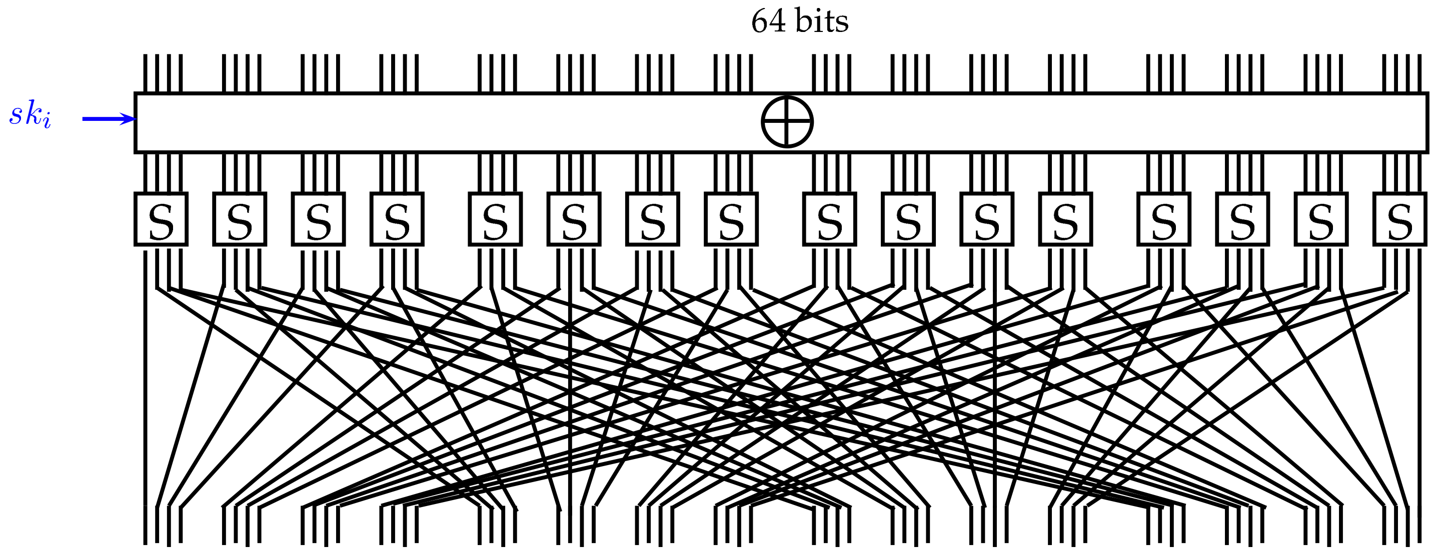
- It can basically be anything.

- We just need to be able to precompute and store the possible transitions (in the case of a classical Sbox, just the Sbox itself), or sometimes on-the-fly.

- Next we get a list of inputs forward and a list of outputs backward: and merge both with the middle conditions (for ex.: N-P 2011).

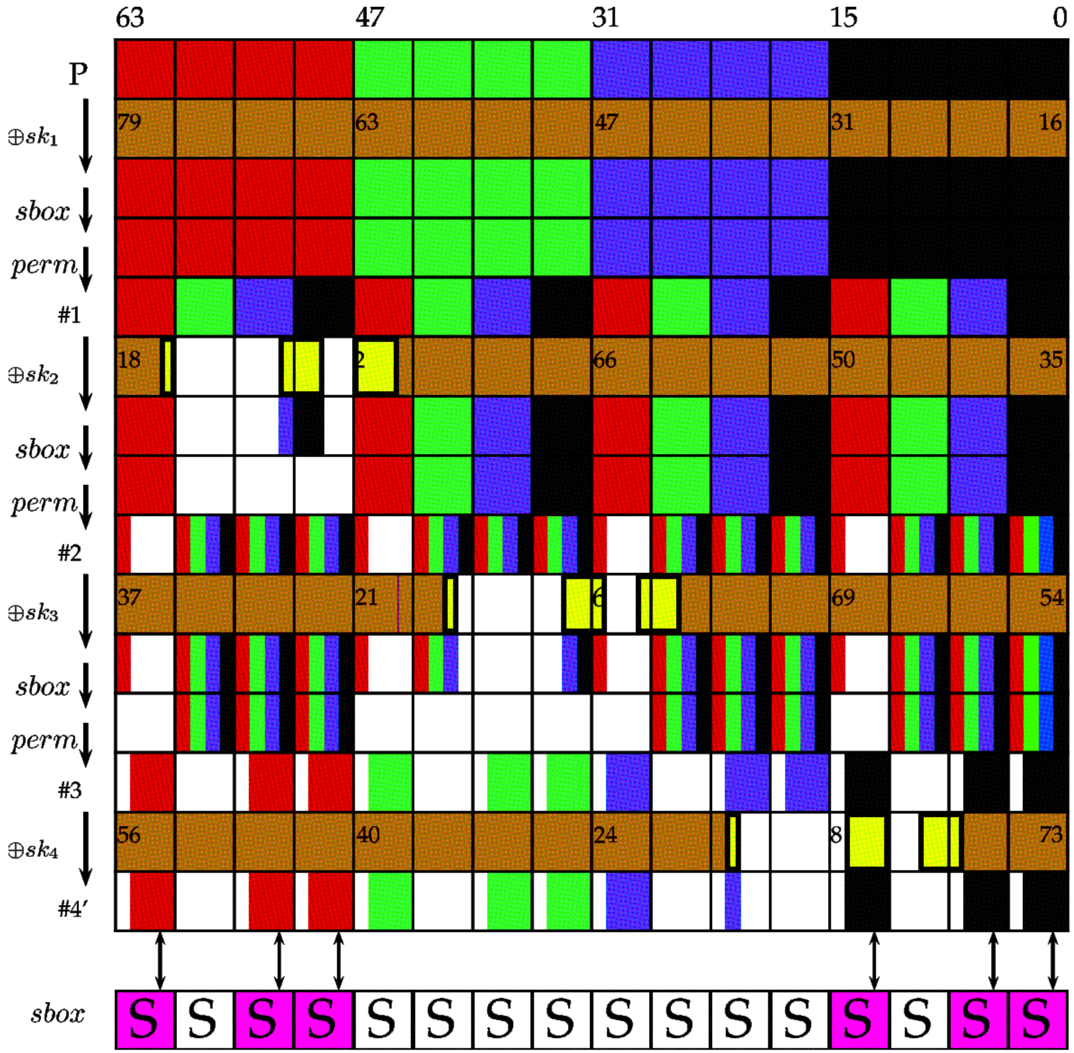
PRESENT [BKLPPRSV 2007]

Block $n = 64$ bits, key 80 or 128 bits.

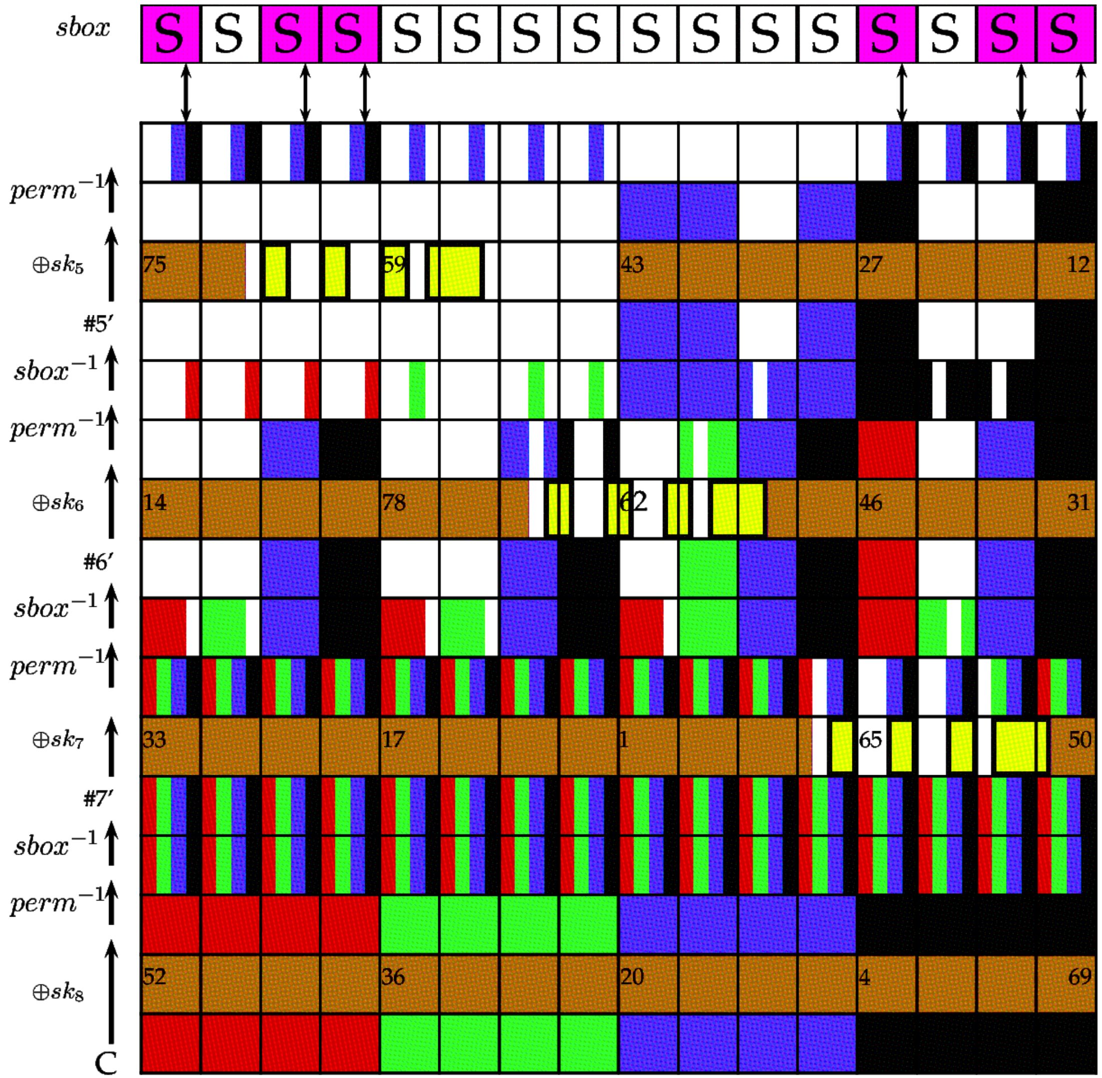


31 rounds $+$ 1 key addition.

Forward Computation



Backward Computation



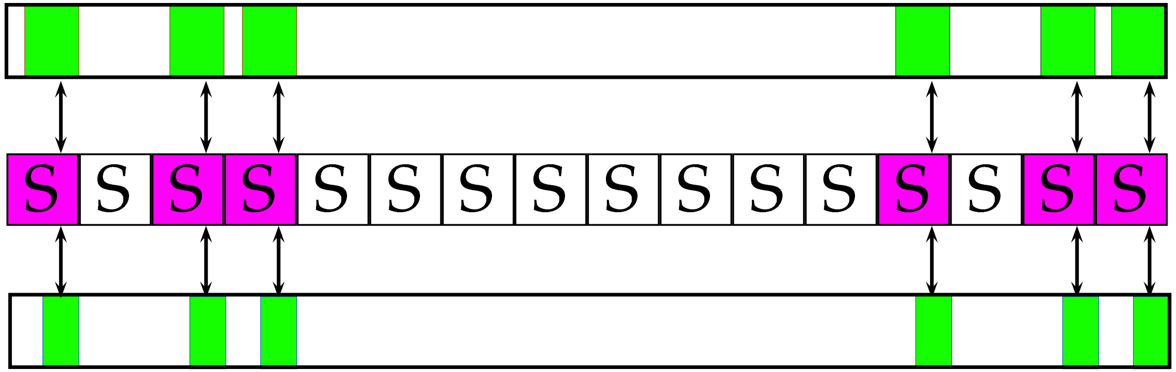
Sieving through the Sboxes: 1 Sbox

$x_3x_2x_1x_0$	$S(x)_3S(x)_2S(x)_1S(x)_0$
0000	1100
0001	0101
0010	0110
0011	1011
0100	1001
0101	0000
0110	1010
0111	1101
1000	0011
1001	1110
1010	1111
1011	1000
1100	0100
1101	0111
1110	0001
1111	0010

$x_2x_1x_0 \to_S y_1y_0$
000→00
000→11
001→01
001→10
010→10
010→11
011→00
011→11
100→00
100→01
101→00
101→11
110→01
110→10
111→01
111→10

16 values of x_2, x_1, x_0, y_1, y_0, out of 32, correspond to a valid transition.

Sieving through the Sboxes

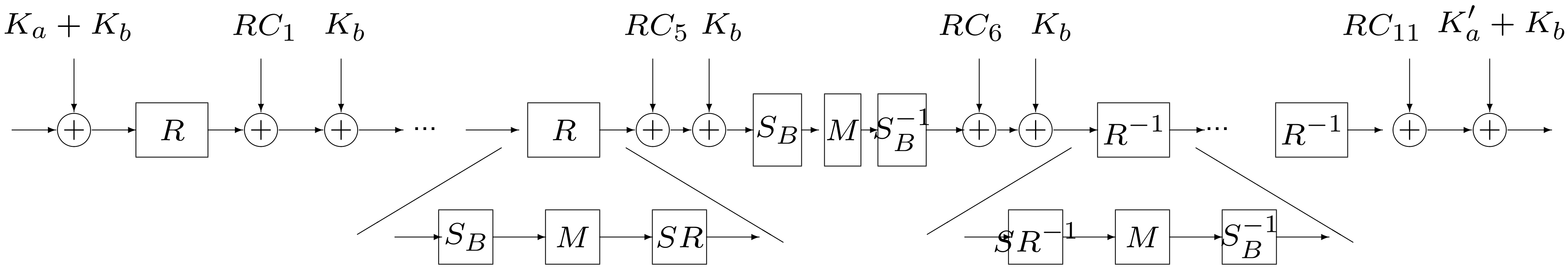


- Probability for 1 Sbox $p = 16/32 = 1/2$
- Probability for the 6 Sboxes: $\frac{1}{2^6}$
- We only try $2^{80-6} = 2^{74}$ potential key candidates.
- 7 rounds.

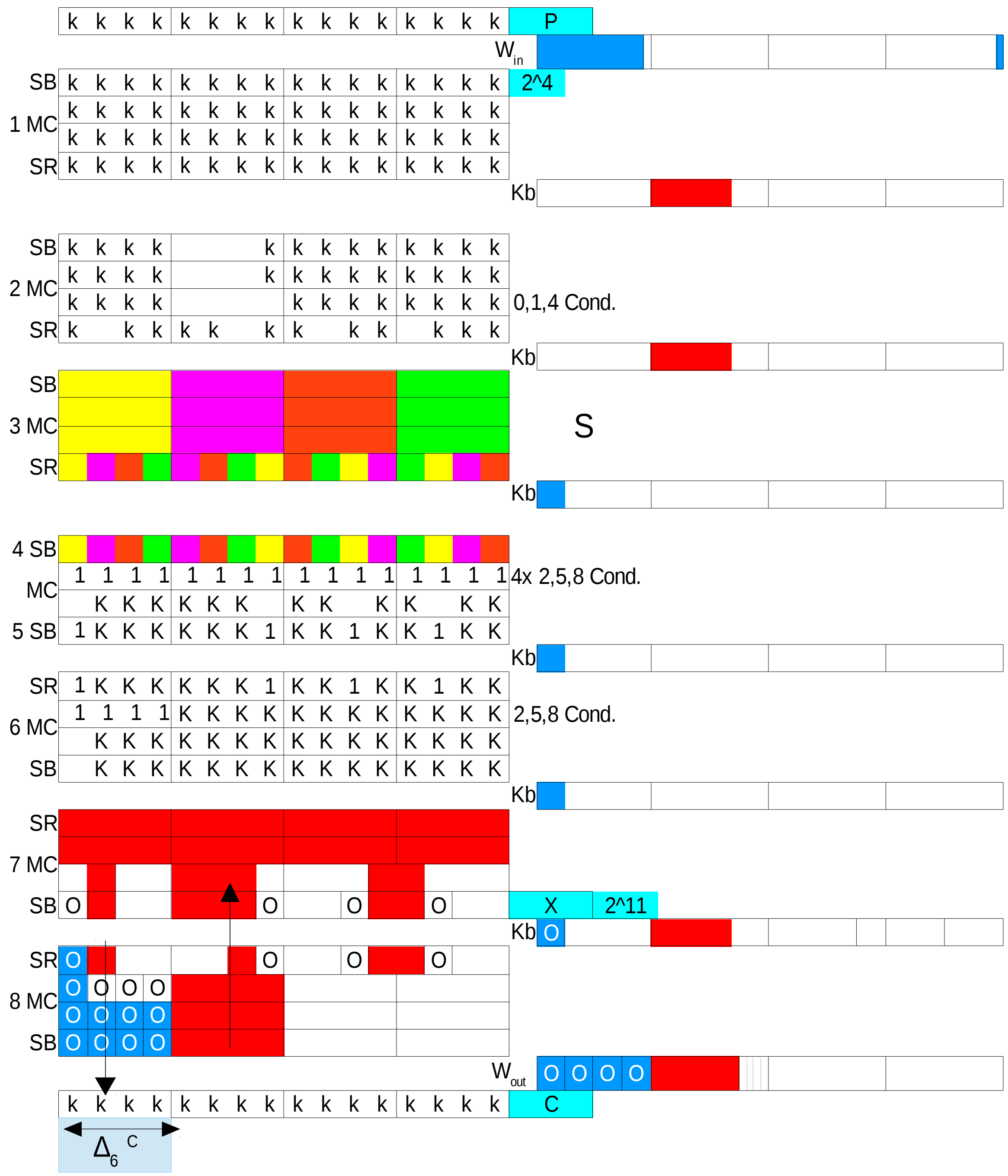
PRINCE [Borghoff et al. 2012]

Block cipher 64 bits. $|K_a| = |K_b| = 64$ (128 keybits).

- Non-linear layer of 16 4x4 Sboxes (S).
- Linear layers: permutation of nibbles (P) and "mixcolumns" on groups of 4 nibbles(M).



8 rounds attack



Complexity

- Improved bicliques when the key is bigger than the internal state: just 1 pair (P, C) of data.

- Complexity:

$$2^{97}(2^{20} + 2^{20+11-4})c_H + 2^{117}c_F + 2^{113}c_B + 2^{97+12} + 2^{128-36}c_E$$

$$< 2^{122}c_E$$

Multiple Differential Cryptanalysis

Multiple Differential Cryptanalysis

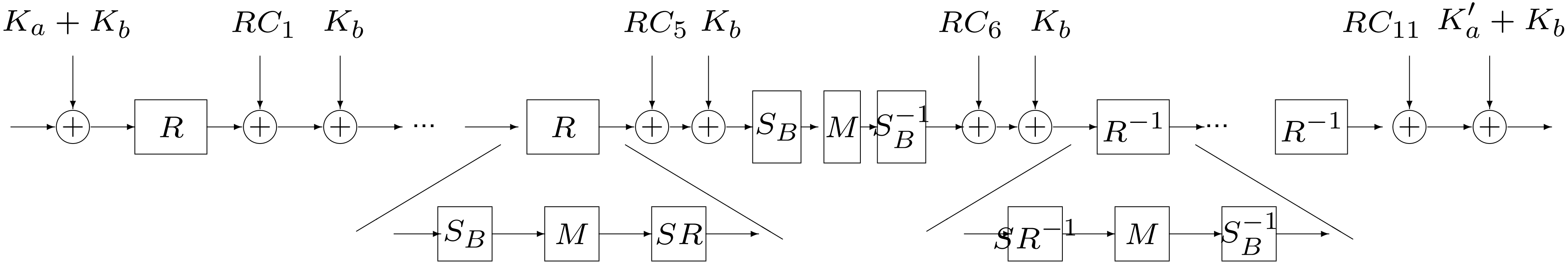
- Applied to Crypton[GM00], similar to multiple linear cryptanalysis[BDQ04].
- Formalized in [BG11]:

"...multiple differential cryptanalysis is the general case where the set of considered differentials has no particular structure, i.e., several input differences are considered together and the corresponding output differences can be different from an input difference to another."

- Applied to PUFFIN(full round), ICEBERG, PRINCE(best attacks)...

PRINCE [Borghoff et al. 2012]

Block cipher 64 bits. $|K_a| = |K_b| = 64$ (128 keybits).



	Column 0				Column 1				Column 2				Column 3			
Row 0	63	62	61	60	47	46	45	44	31	30	29	28	15	14	13	12
Row 1	59	58	57	56	43	42	41	40	27	26	25	24	11	10	9	8
Row 2	55	54	53	52	39	38	37	36	23	22	21	20	7	6	5	4
Row 3	51	50	49	48	35	34	33	32	19	18	17	16	3	2	1	0

Bits numbering

C 0	C 1	C 2	C 3
(0,0)	(0,1)	(0,2)	(0,3)
(1,0)	(1,1)	(1,2)	(1,3)
(2,0)	(2,1)	(2,2)	(2,3)
(3,0)	(3,1)	(3,2)	(3,3)

Nibbles numbering

Square Iterative Differentials

X	Y	X	Y					Y	X	Y	X				
X	Y	X	Y					Y	X	Y	X				

MC

X		X							X		X				
	Y		Y					Y		Y					
X		X							X		X				
	Y		Y					Y		Y					

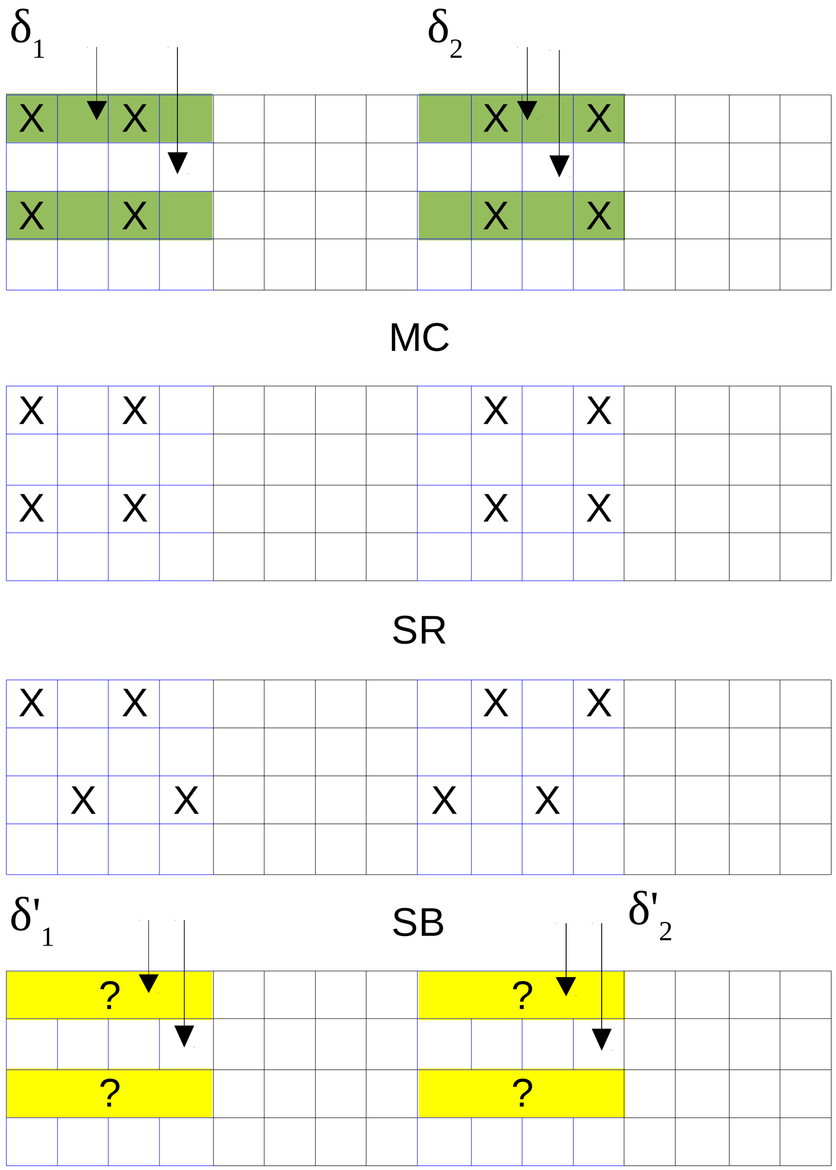
SR

X		X							X		X				
				Y		Y							Y		Y
	X		X					X		X					
					Y		Y					Y		Y	

SB

<table>
<tr><td colspan="4">?</td><td></td><td></td><td></td><td></td><td colspan="4">?</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td colspan="4">?</td><td></td><td></td><td></td><td></td><td colspan="4">?</td></tr>
<tr><td colspan="4">?</td><td></td><td></td><td></td><td></td><td colspan="4">?</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td colspan="4">?</td><td></td><td></td><td></td><td></td><td colspan="4">?</td></tr>
</table>

Square Iterative Differentials



$(\delta_1, \delta_2) \in (\Delta_1 \times \Delta_2) \cup (\Delta_2 \times \Delta_1)$

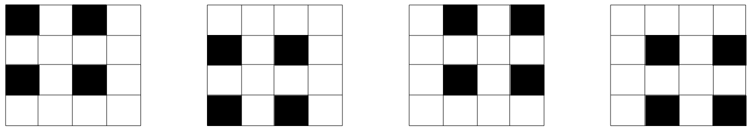
with $\Delta_1=\{1,4,5\}$ and $\Delta_2=\{2,8,10\}$

There are 4x2x9 differences that are mapped through MC and SR to a square pattern

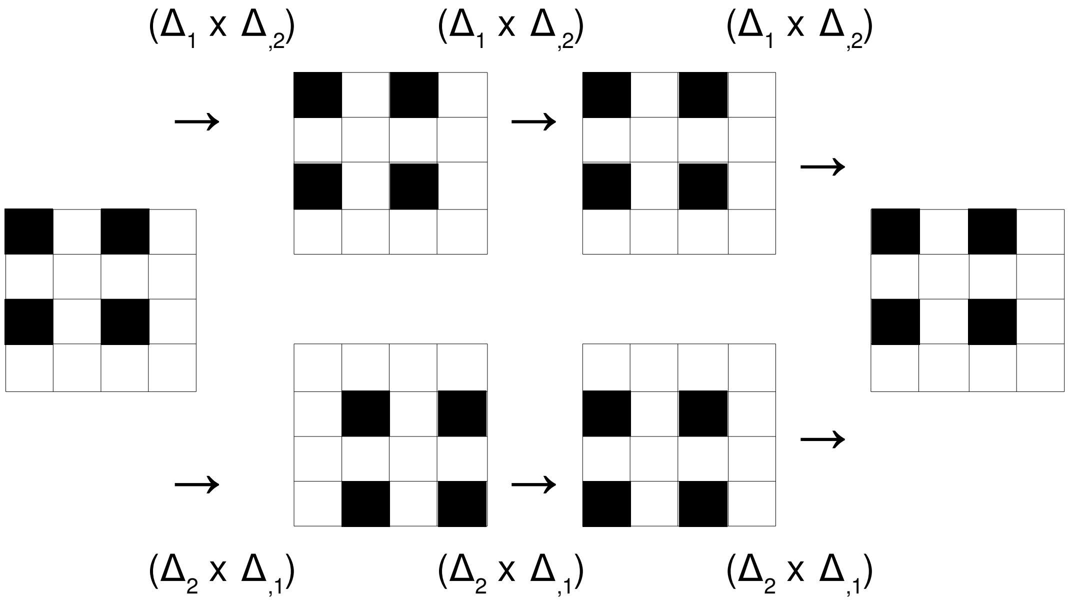
We need
$\delta_1 \rightarrow \delta_1'$, $\delta_1 \rightarrow \delta_2'$,
$\delta_2 \rightarrow \delta_1'$, $\delta_2 \rightarrow \delta_2'$
to be possible transitions

Multiple Differential on PRINCE[CFGNR'14]

We consider multiple differentials and multiple characteristics, all following square patterns as in



Example:



Multiple Differential on PRINCE

For 6 rounds:

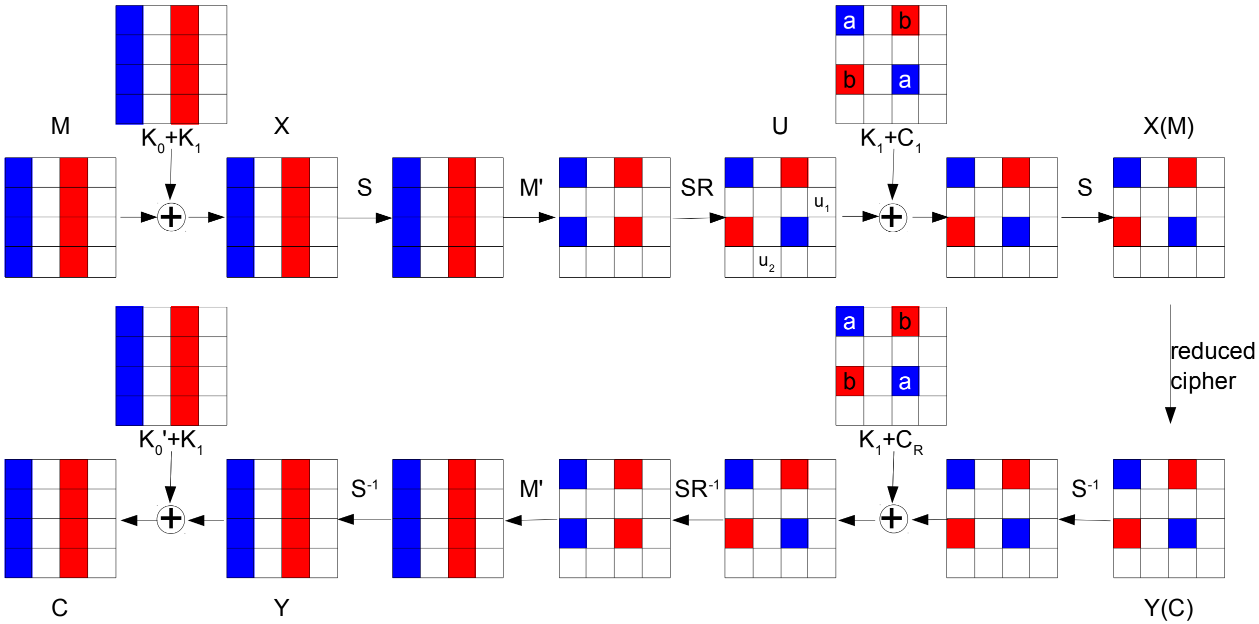
$$(M \to SR \to S)^2 \to M \to SR \to S_{sbox} \to SR^{-1} \to M \to (S^{-1} \to SR^{-1} \to M)^2$$

$\Delta_{in} = (\delta_1, \delta_2)$ and $\Delta_{out} = (\delta'_1, \delta'_2)$.

For any square pattern in the input and in the output, the probability of $\Delta_{in} \to \Delta_{out}$ when $(\Delta_{in}, \Delta_{out}) \in \{(1,2),(2,1)\} \times \{(1,2),(2,1)\}$ is $P_b = 2^{-56.47}$.

Recovering the key

We can add $2+2$ rounds:



- 66 key bits involved.
- N_s structures $\Rightarrow N_s 2^{32+31-32}$ pairs.
- Wrong guess: $N_s 2^{-33}|\Delta_{in}||\Delta_{out}|$ pairs.
- Good guess: $N_s 2^{31}|\Delta_{in}||\Delta_{out}|P_b$ pairs.

Multiple Differential on PRINCE

Best known attack on PRINCE: 10 rounds out of 12.

Complexity
$D \times T = 2^{118.6}$ compared to 2^{126} for the generic attack.

Good example for transition between classical attacks and dedicated ones.

Conclusion

To Sum Up[2]

- Classical attacks, but also new dedicated ones exploiting the originality of the designs.

- Importance of reduced-round analysis to update security margin, and/or as first steps of further analysis.

- A lot of ciphers to analyze/ a lot of work to do!

[2] Thank you to Valentin Suder for his help with the figures