Dedicated 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
- Dedicated attacks (examples):
  - Importance of dedicated attacks: PRINTcipher
  - Importance of reduced-round attacks: KLEIN-64

Importance of Dedicated Cryptanalysis

Lightweight Dedicated Analysis

- Lightweight: more 'risky' design, lower security margin, simpler components.
- Often innovative constructions: dedicated attacks

Lightweight Dedicated Analysis

- Normally, designers should have already analyzed the cipher with respect to known attacks...
- ...though not always!, or not always that straightforward.
- Dedicated attacks: New!

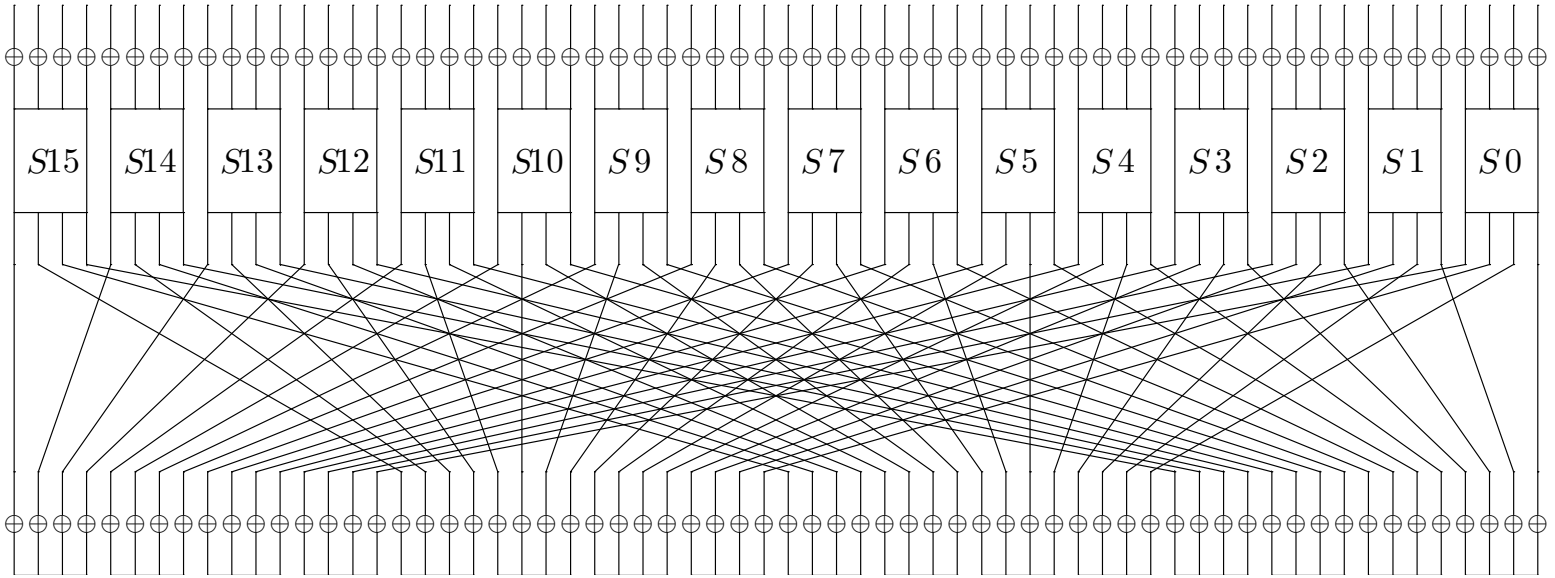
PRESENT and PRINTcipher

PRESENT [BKLPPRSV'07]

- One of the most popular ciphers, proposed in 2007, and now ISO/IEC standard is PRESENT.
- Very large number of analysis published (over 20).
- Best attacks so far: multiple linear attacks (26r/31r).

PRESENT

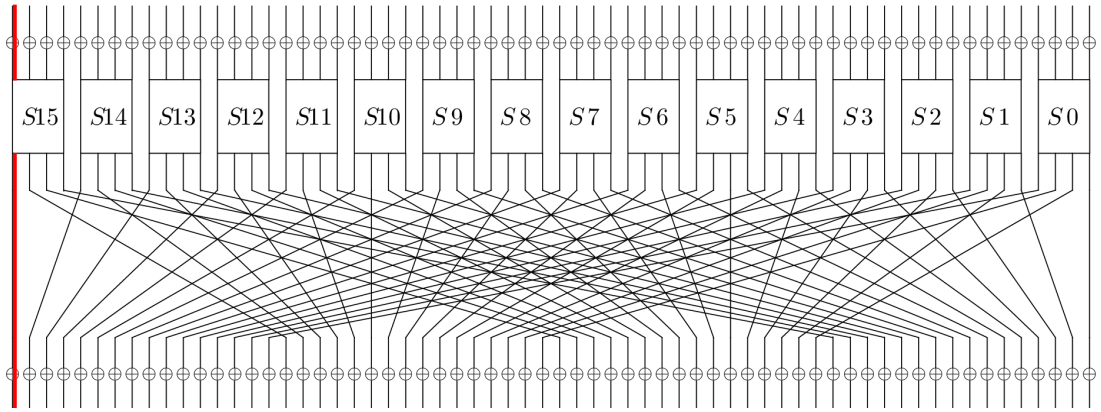
Block $n = 64$ bits, key 80 or 128 bits.



31 rounds + 1 key addition.

PRESENT

Linear cyptanalysis: because of the Sbox, a linear approximation 1 to 1 with bias 2^{-3} per round[Ohk.'09].

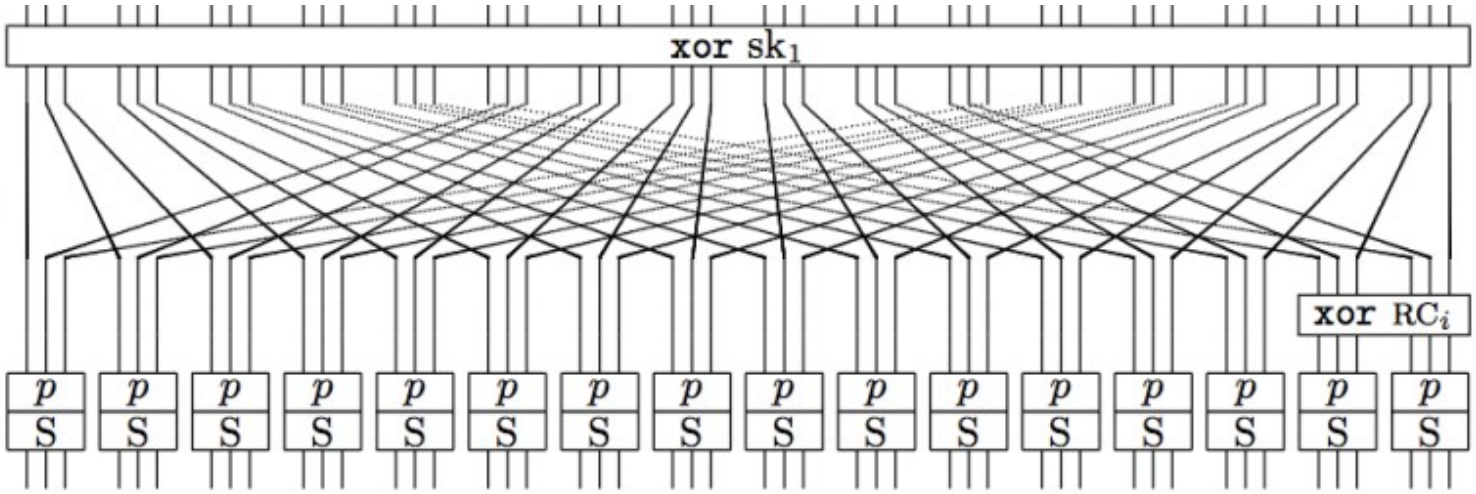


- Multiple linear attacks: consider several possible approxs simultaneously $\Rightarrow$ up to 26 rounds out of 31 [Cho'10].

PRINTcipher

- Many PRESENT-like ciphers proposed: Maya, Puffin, PRINTcipher
- Usually, weaker than the original.
- PRINTcipher[KLPR'10]: first cryptanalysis: invariant subspace attack[LAAZ'11].

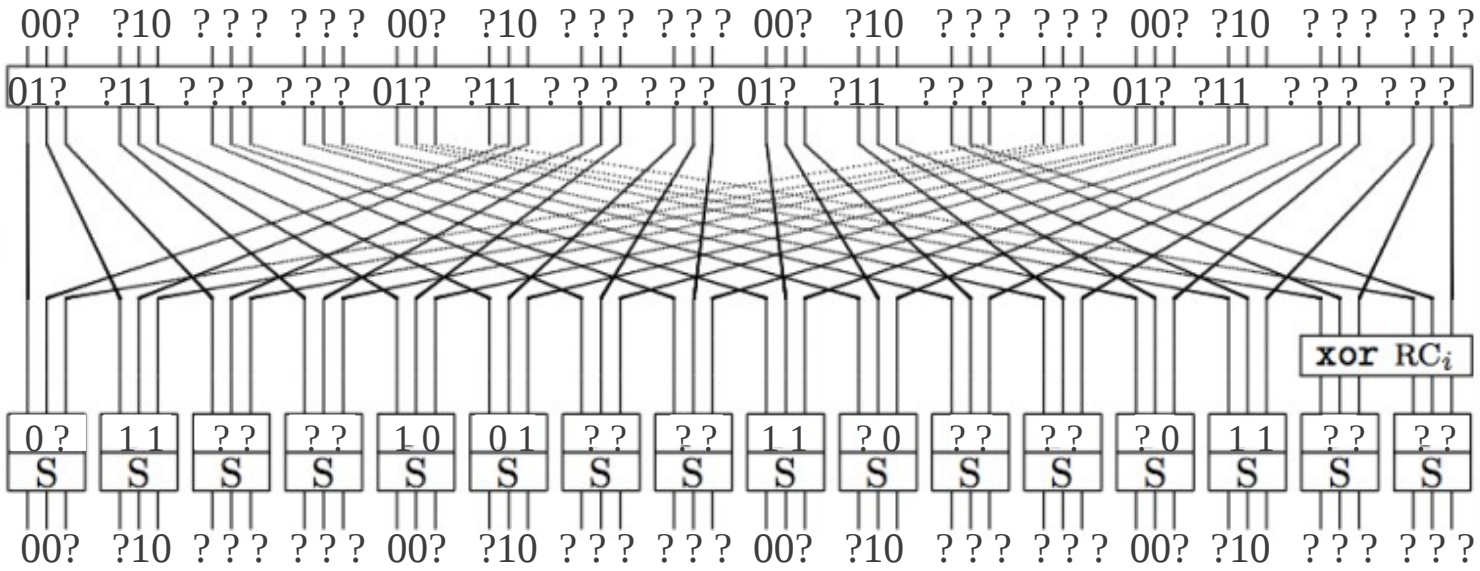
PRINTcipher



48rounds.

The Invariant Subspace Attack [LAAZ'11]

With probability 1:

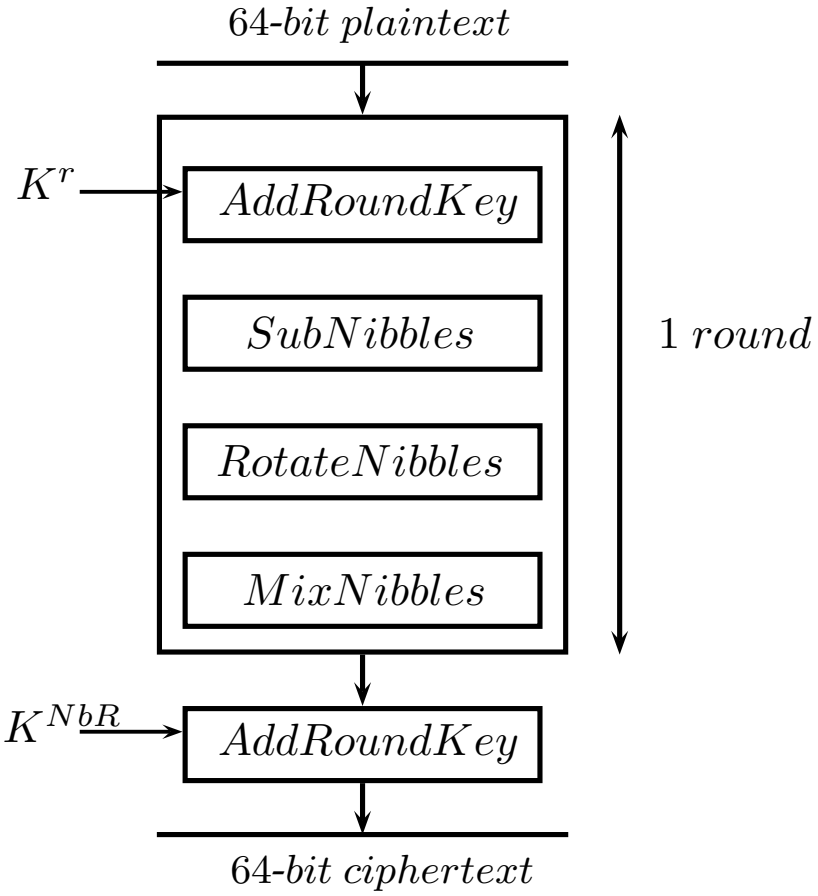


- Not a key recovery, but a very bad property for 2^{51} weak keys...

KLEIN-64: from reduced-round to full-version

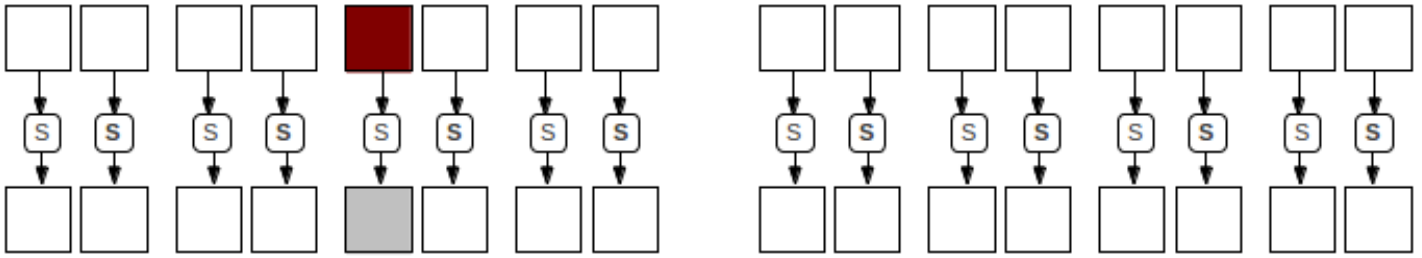
KLEIN [GNL'11]

- KLEIN-64 with 12 rounds.



KLEIN

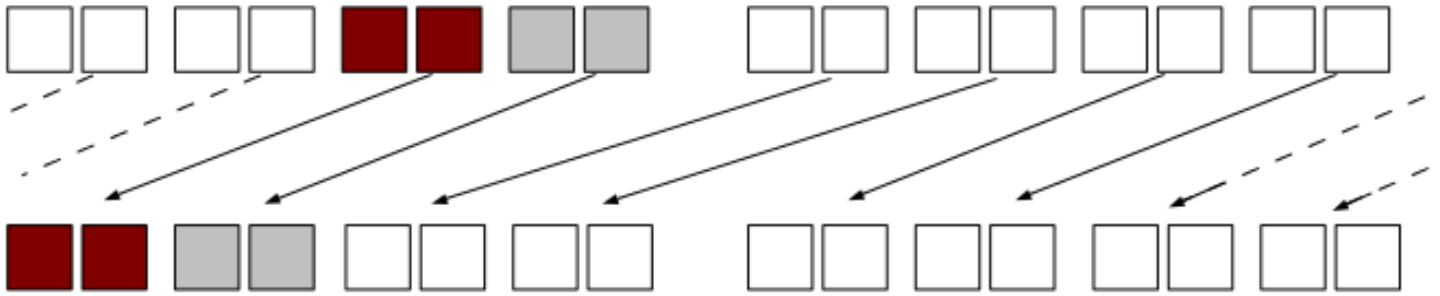
SubNibbles



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

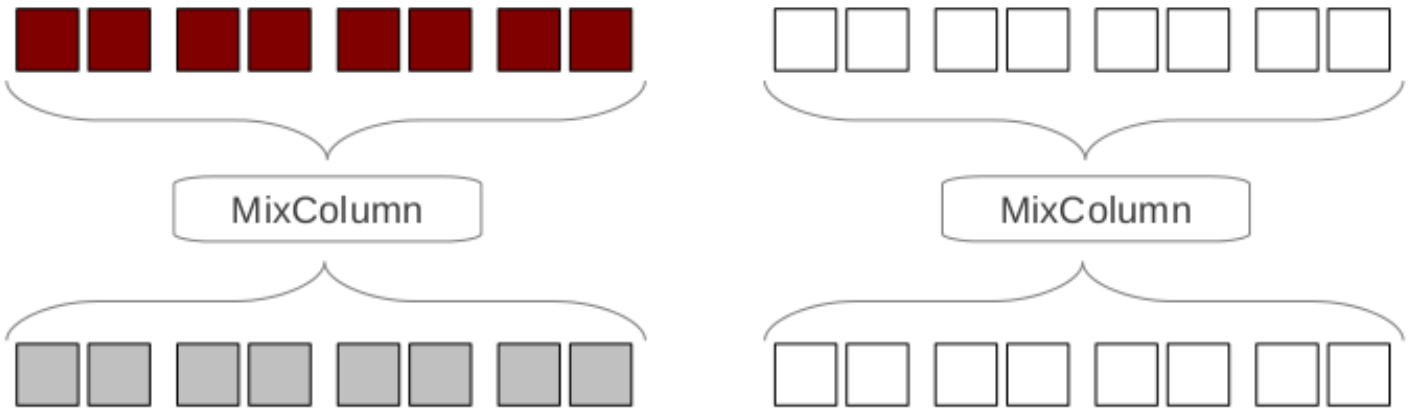
KLEIN

RotateNibbles



KLEIN

MixNibbles



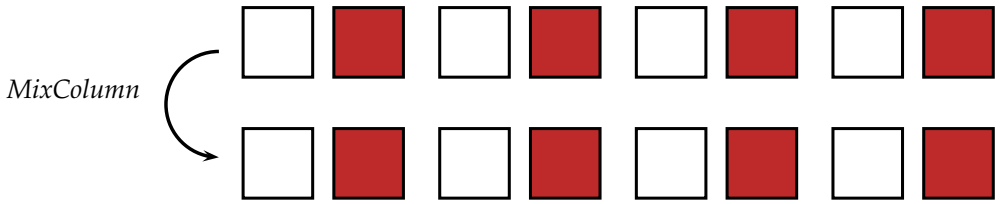
Previous Cryptanalysis

Version	Source	Rounds	Data	Time	Memory	Attack
KLEIN-64	[Yu, Wu, Li, Zhang, *Inscrypt11*]	7	$2^{34.3}$	$2^{45.5}$	2^{32}	integral
	[Yu, Wu, Li, Zhang, *Inscrypt11*]	8	2^{32}	$2^{46.8}$	2^{16}	truncated
	[Aumasson, Naya-Plasencia, Saarinen, *Indocrypt11*]	8	2^{35}	2^{35}	-	differential
	[Nikolic, Wang, Wu, *ePrint iacr 2013*]	10	1	2^{62}	2^{60}	mitm
	[Ahmadian, Salmasizadeh, Reza Aref *ePrint iacr 2013*]	12	2^{39}	$2^{62.84}$	$2^{4.5}$	biclique

Main Ideas From Previous Analysis

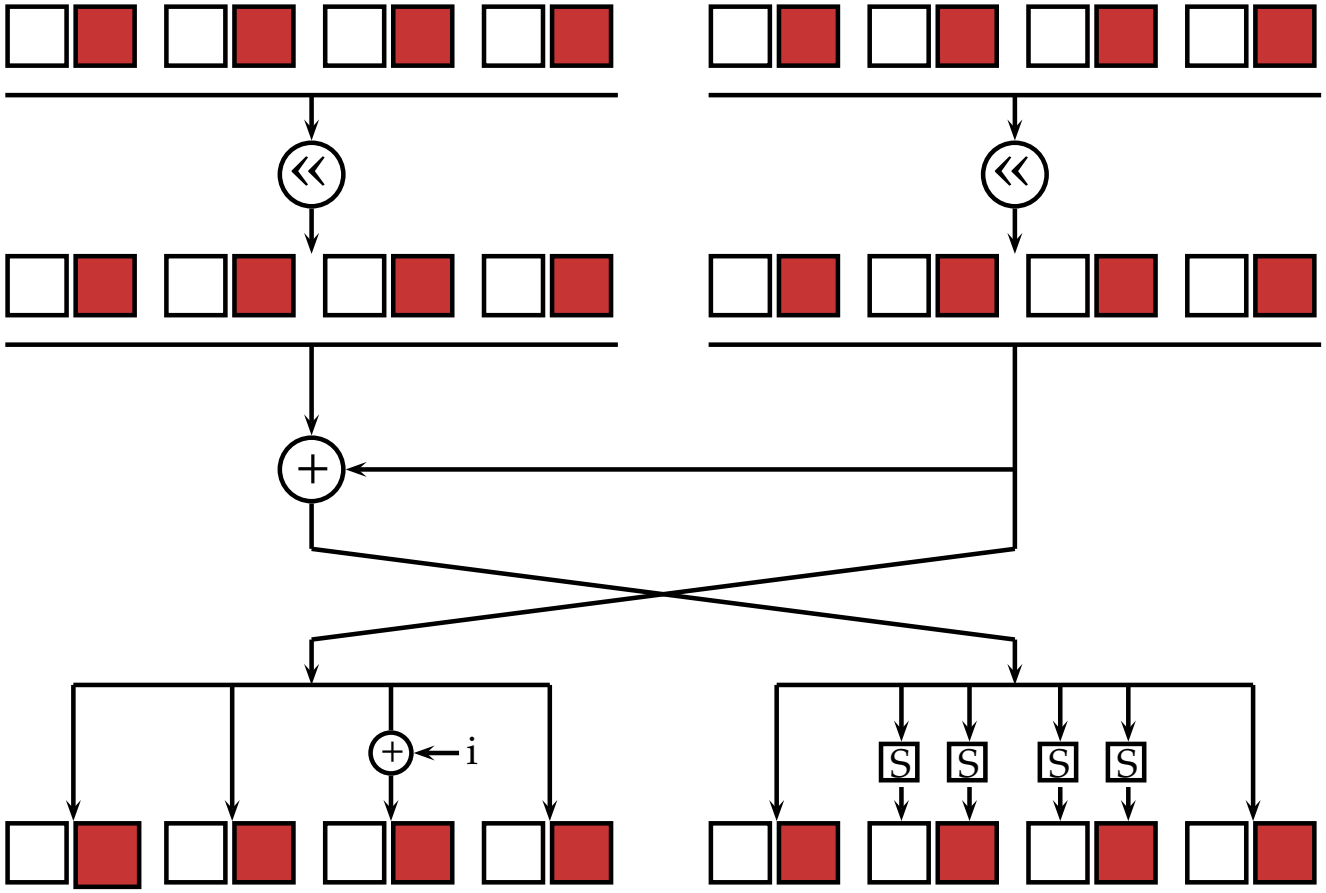
- All layers except `MixNibbles` do not mix higher nibbles with lower nibbles.

- `MixColumn`: inactive higher nibbles input $\Rightarrow$ same output pattern if the MSB of the 4 LN differences are equal (2^{-3}).



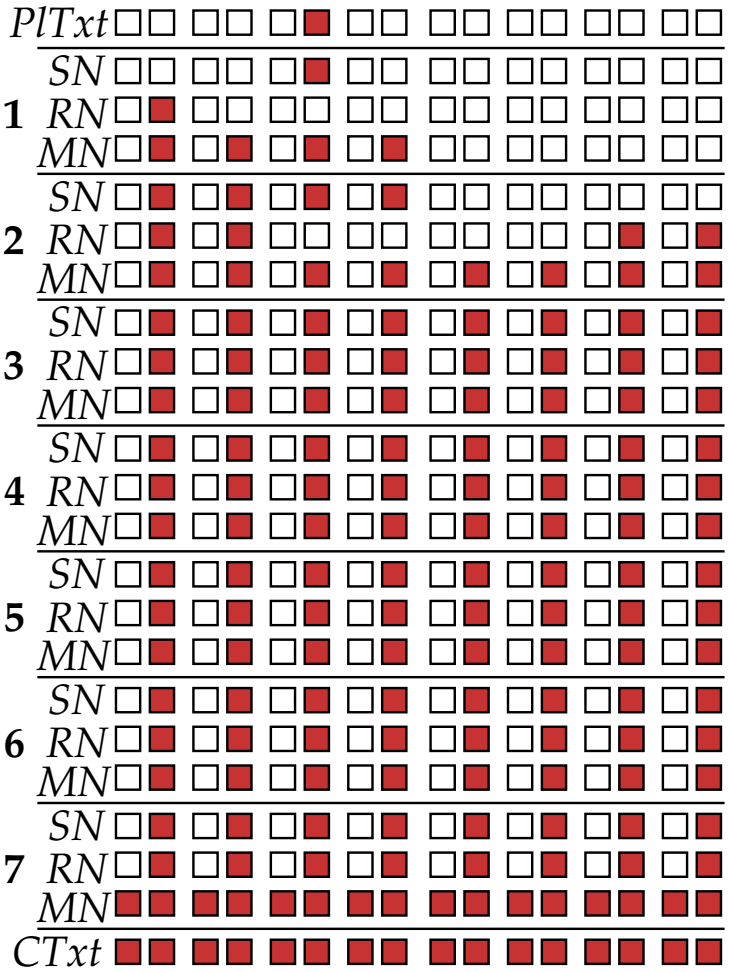
Main Ideas From Previous Analysis

- `KeySchedule` algorithm: lower nibbles and higher nibbles are not mixed.



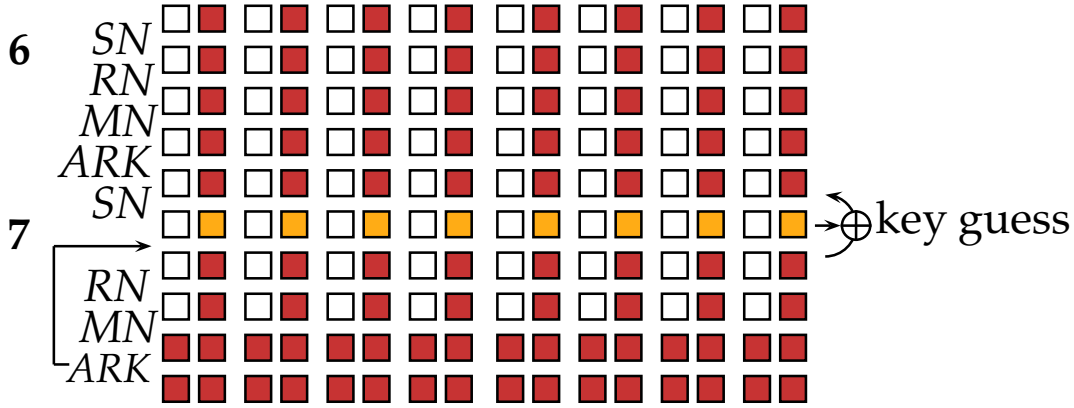
7-round attack

- Truncated differential path of probability $2^{-28.08} < 2^{-32}$, 64-bit key recovered with 2^{33} operations.



7-round attack

1. Generate data
2. Keep the pairs with $MN^{-1}(CTxt)$ that have higher nibbles inactive
3. Guess the lower nibbles of the key
4. Test it by checking the difference obtained when inverting MN of round 6



7-round attack

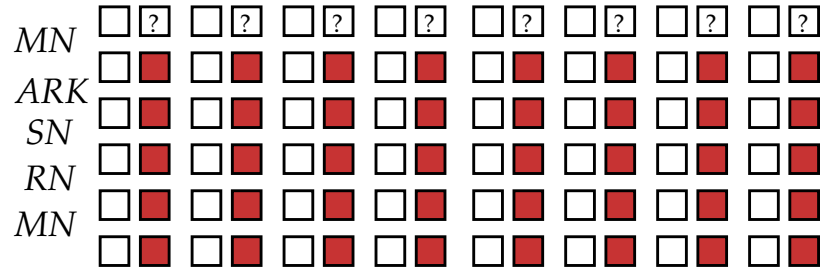
- Last round condition for a random pair $2^{-32} < 2^{-28.08}$.
  $\Rightarrow$ a pair with HN inactive difference in last round is a conforming one.

- Each conforming pair gives a 6-bit filter.

- Repeating the procedure, we can recover the correct value for the LN of the key.

New Atack [LNP'14]

- Use more MixNibble steps to discard more keys.



$\Rightarrow$ We want the difference output at the previous MN

- invert an entire LN round in values and diff.
- need only lower (key) nibbles to invert RN, SN and ARK.
- how to invert MN?

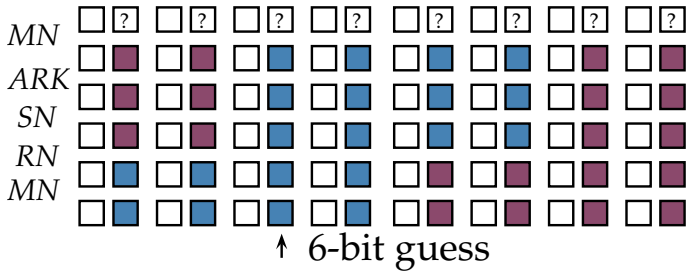
Inverting one $MixColumn^{-1}(a, b, c, d)$

- Let $a = (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7)$ be the binary decomposition of a byte.
- Given the input lower nibbles, we require 3 information bits from the higher nibbles:

$$\begin{cases} a_1 + a_2 + b_2 + c_0 + c_1 + c_2 + d_0 + d_2 \\ a_1 + b_0 + b_1 + c_1 + d_0 + d_1 \\ a_0 + a_1 + a_2 + b_0 + b_2 + c_1 + c_2 + d_2 \end{cases}$$

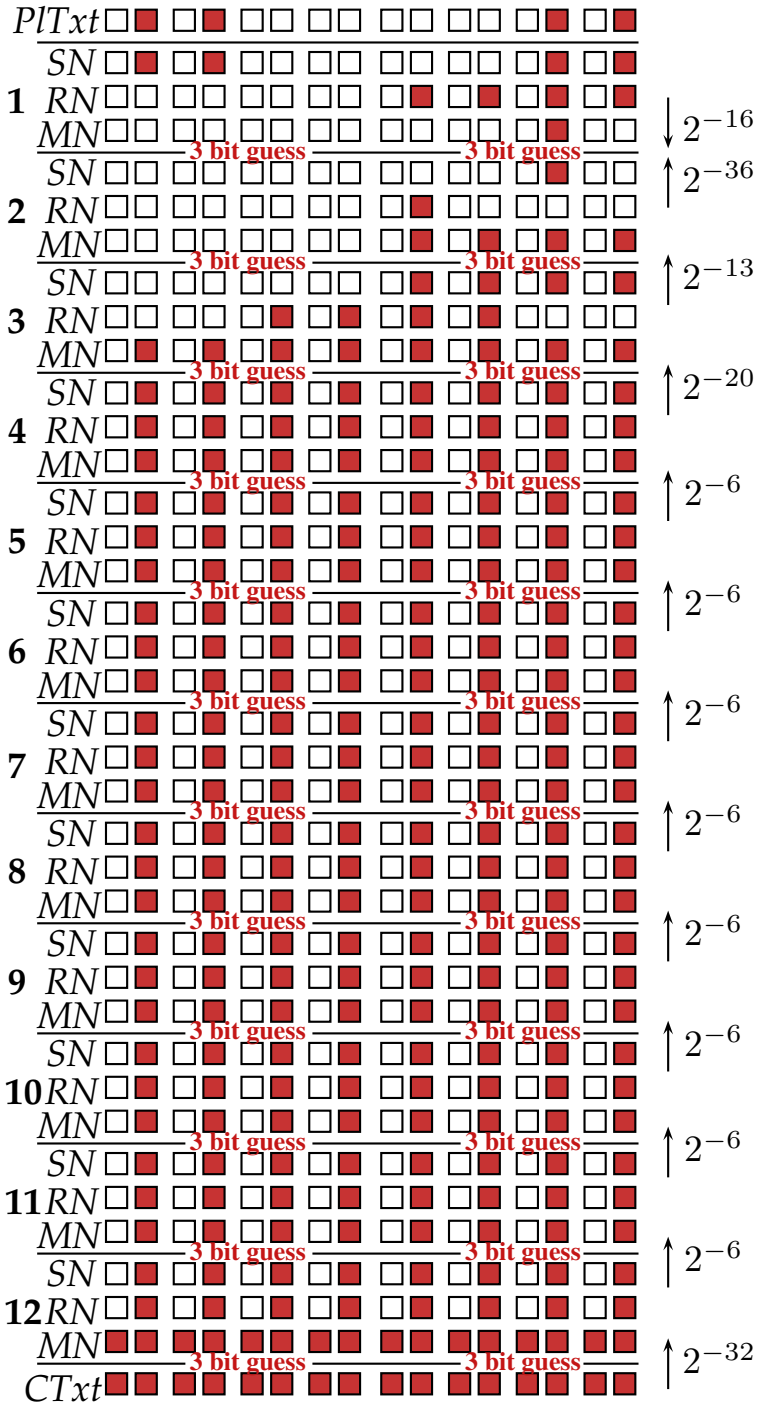
$\Rightarrow$ a 6-bit guess per round

Inverting one round



- Compute the LN state and check the difference shape by inverting MN (a certain probability).
- $\Rightarrow 2^6$ computations.
- In the iterative part (probability 2^{-6}), just one guess remains.

12 rounds of KLEIN-64



Attack on KLEIN-64

- Generate enough data (path probability $2^{-69.5}$). Keep pairs with higher nibbles inactive before the last MN.

- For each iterative rounds:
  - LN key guess and first round to discard some.
  - Invert round by round with a 6-bit guess and check if the difference obtained before MN is as wanted: 1 guess over 2^6 remains.

First rounds to discard candidates

- At the end of the attack, 2^8 candidates remain.
- Higher nibbles search discards the bad ones.
- Other differential paths are possible, offering different trade-offs data/time/memory.

Some Improvements

- Use structures to limit data complexity.
- Invert MN with a 2^4 complexity (instead of 2^6).
- Use MixColumn independence to reduce the cost of the lower nibbles key guess in the first round.
- Higher nibbles search can be speeded up using the information from the 6-bit guesses.

Attack Complexities on KLEIN-64

Case	Data	Time	Memory
1	$2^{54.5}$	2^{57}	2^{16}
2	$2^{56.5}$	2^{62}	2^{4}
3	2^{35}	$2^{63.8}$	2^{32}
4	2^{46}	2^{62}	2^{16}

KLEIN results

- First attack on full KLEIN-64.
- Verified experimentally on reduced-round versions (first practical attack on 9 rounds).
- Permits reaching 13 rounds over 16 of KLEIN-80 and 14 rounds over 20 of KLEIN-96.

Conclusion

To Sum Up[1]

- Classical attacks, but also new dedicated ones exploiting the originality of the designs.
- Importance of reduced-round analysis to re-think security margin, or as first steps of further analysis.
- A lot of ciphers to analyze/ a lot of work to do!

[1]Thank you to Valentin Suder, Virginie Lallemand and Christina Boura for their help with the figures