Cryptanalysis of full KLEIN-64

Virginie Lallemand and María Naya-Plasencia
INRIA Paris-Rocquencourt, France

The lightweight blockcipher KLEIN

- Proposed by Gong, Nikova and Law at RFIDSec 2011.
- 64-bit state, 64/80/96-bit keys and 12/16/20 rounds.

- **AddRoundKey**: XORs a round key to the 64-bit state.
- **SubNibbles**: applies the 4-bit Sbox to each nibble.
- **RotateNibbles**: left-rotates the state of 16 bits.
- **MixNibbles**: applies two MixColumn's in parallel.

Previous Cryptanalysis

- Inscrypt 2011: Yu et al, 7 rounds (64), 8 rounds(80)
- Indocrypt 2011: Aumasson et al, 8 rounds(64).
- eprint 2013: Ahmadian et al, bicliques, 12 rounds(64) (accelerated exhaustive search of the key: $2^{62.84}$t,2^{39}d).

Our new results

- Key recovery on full KLEIN-64

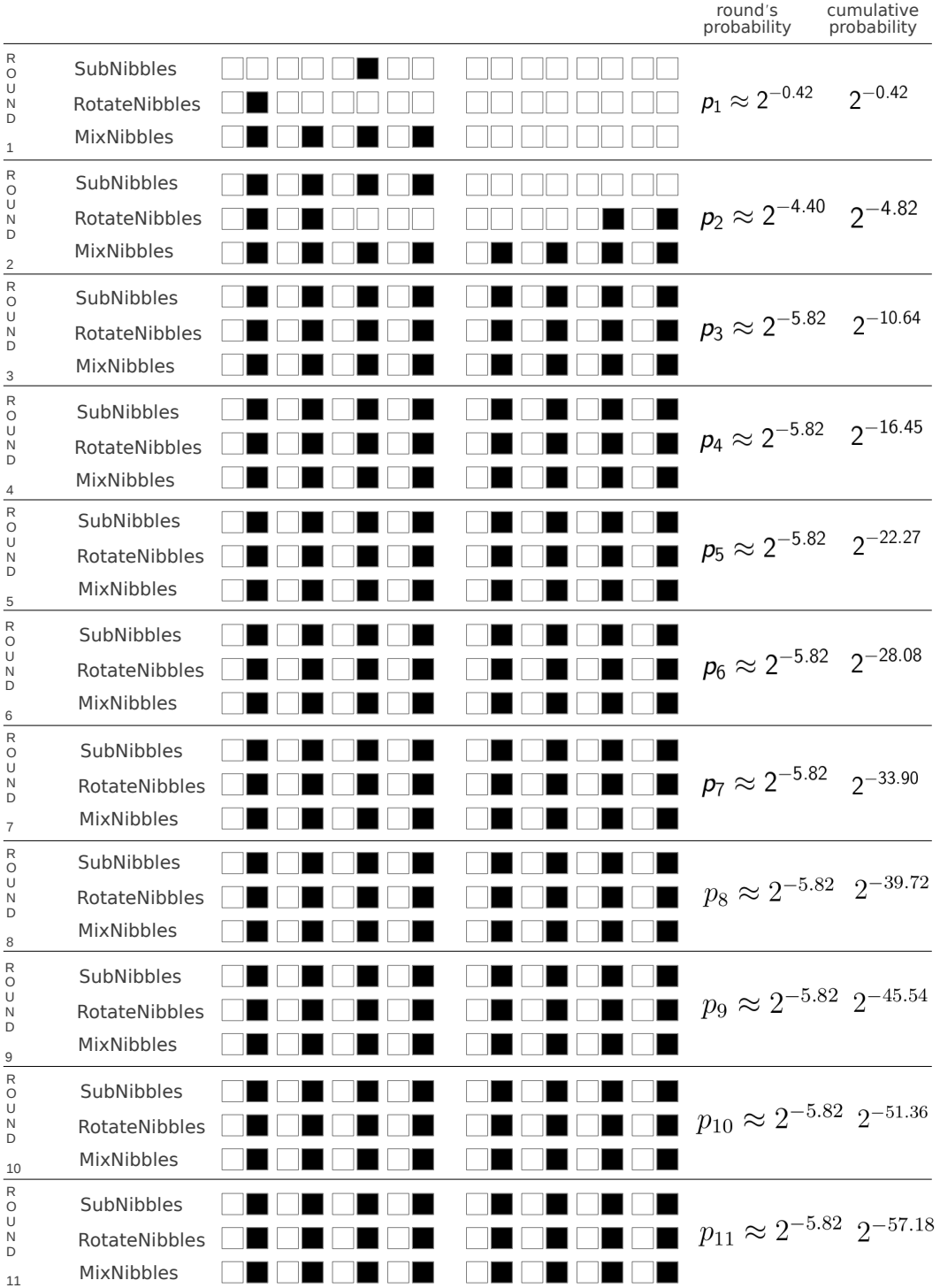
- For the 80 and 96 bit versions, improved number of rounds.

How do our attacks work?

- Same differential path than Indocrypt11.
- We do not use neutral bits anymore.

- Main idea: we guess the lower nibbles of the key, the remining guessed information bits per step are compensated with the conditions of the differential path.
- At the first round, collide at values and differences: enough conditions for filtering out most of the wrong low nibble keybits guessed.

$2^{57.18}$ data and $2^{60.76}$ in time.


round's probability
cumulative probability
ROUND 1
SubNibbles
RotateNibbles
MixNibbles
$p_1 \approx 2^{-0.42}$
$2^{-0.42}$
ROUND 2
$p_2 \approx 2^{-4.40}$
$2^{-4.82}$
ROUND 3
$p_3 \approx 2^{-5.82}$
$2^{-10.64}$
ROUND 4
$p_4 \approx 2^{-5.82}$
$2^{-16.45}$
ROUND 5
$p_5 \approx 2^{-5.82}$
$2^{-22.27}$
ROUND 6
$p_6 \approx 2^{-5.82}$
$2^{-28.08}$
ROUND 7
$p_7 \approx 2^{-5.82}$
$2^{-33.90}$
ROUND 8
$p_8 \approx 2^{-5.82}$
$2^{-39.72}$
ROUND 9
$p_9 \approx 2^{-5.82}$
$2^{-45.54}$
ROUND 10
$p_{10} \approx 2^{-5.82}$
$2^{-51.36}$
ROUND 11
$p_{11} \approx 2^{-5.82}$
$2^{-57.18}$

How do our attacks work?

We can improve the results by relaxing the differential path at the beginning.
With structures (and negligible memory), we obtain around:

- KLEIN-64: full 12 rounds (+4 rounds).

2^{33} data and 2^{58} time.

- KLEIN-80: 14 rounds (+6 rounds).

2^{44} data and 2^{77} time.

- KLEIN-96: 15 rounds (+15 rounds).

2^{50} data and 2^{91} time.