New Results on Modified Versions of KETJE JR

María Naya-Plasencia
Inria, France
(joint work with Thomas Fuhr and Yann Rotella)

Dagstuhl Seminar - Symmetric Cryptography - 11 Jan 2018

Ketje Jr [BDPVV16]

Family of AE algorithms: MonkeyDuplex + Keccak-f (*).

Ketje Jr: 5x5x8=200 bits, $r = 16$, claim= $\min(96, k)$.

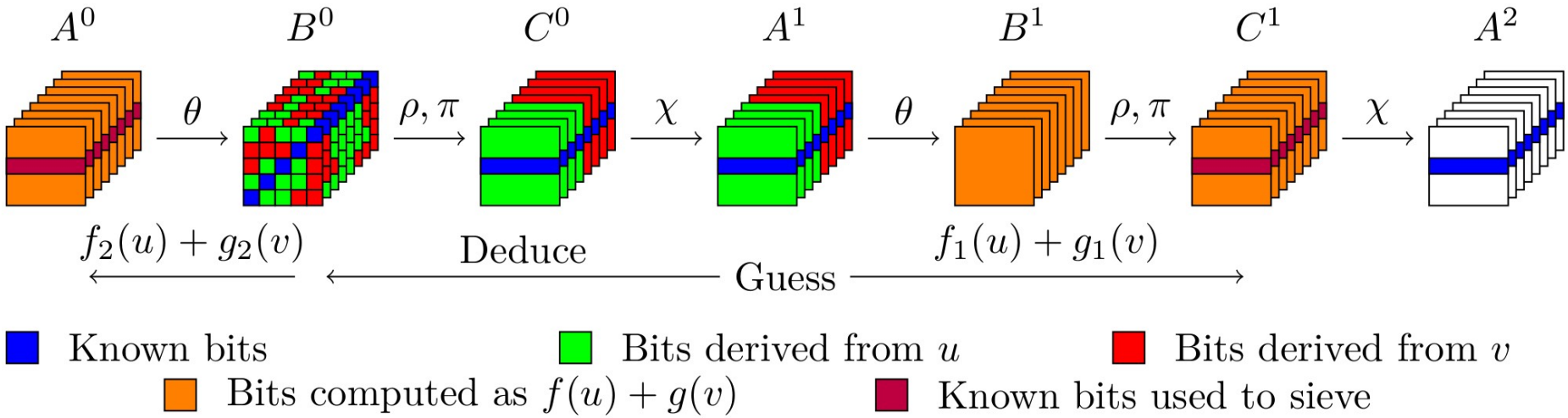
1) Initialization: K and N in internal state + 12 rounds (most analysis).
2) P_i processing: the state $S_i = S_i^r || S_i^C$ outputs $C_i = P_i \oplus S_i^r$ and updates as $S_{i+1} = \text{Keccak-f}(C_i || S_i^C)$.
3) Tag extraction after 6 rounds.

Results

- With 2 rounds:
  State recovery on the original KETJE JR and on tweaked KETJE JR both with increased rate of 40 bits and complexity of 2^{80} and 2^{90}.

- With 3 rounds:
  State recovery on the original KETJE JR with increased rate of 40 bits ($2^{71.5}$) and 32 bits (2^{92}).

Basic attack $(r = 40)$



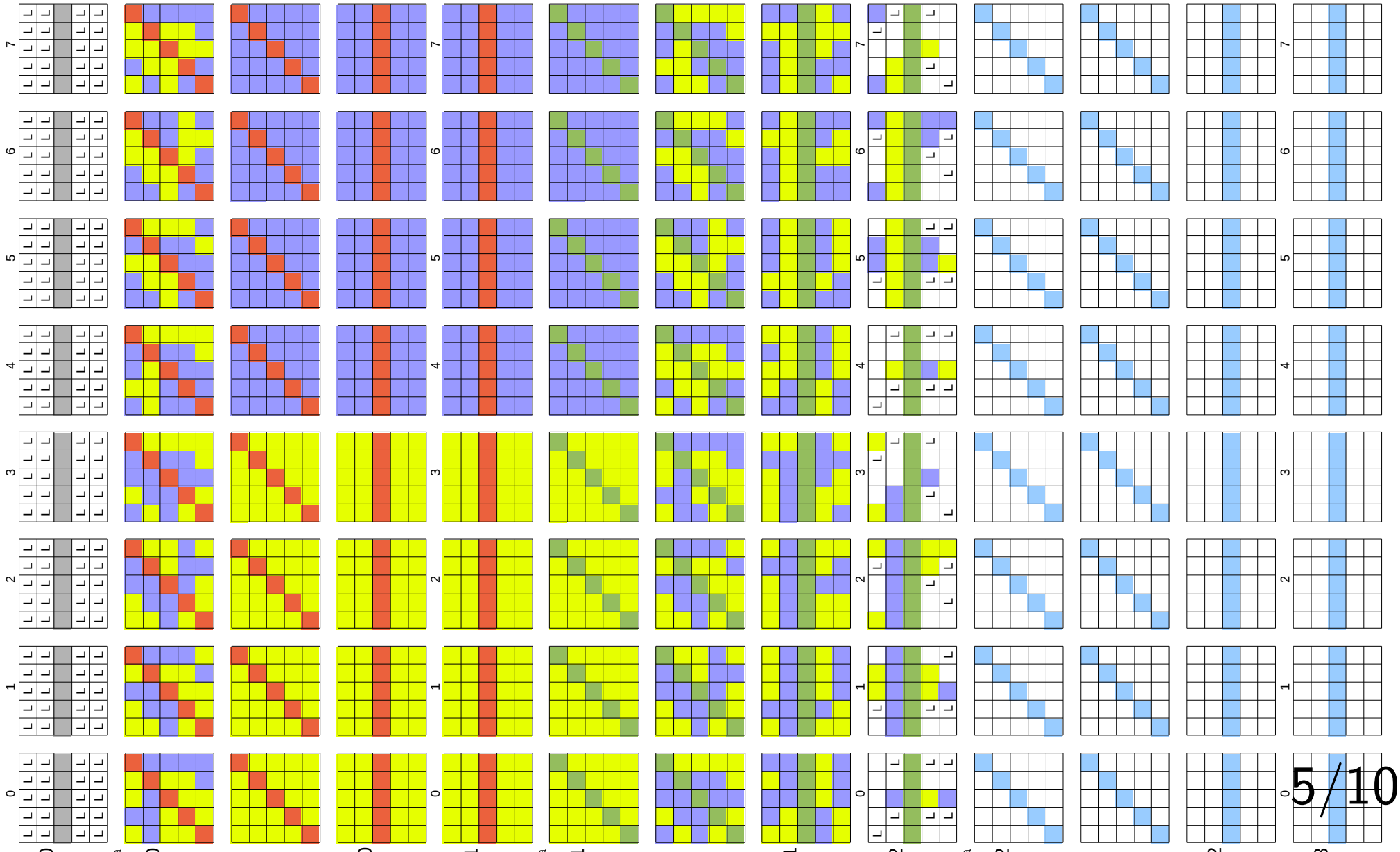
Basic attack $(r = 40)$

With 3 outputs:
time complexity cannot be better than $2^{200-3*r}$.

For $r = 40$: attack on 2^{80}, but no hope for smaller rates.

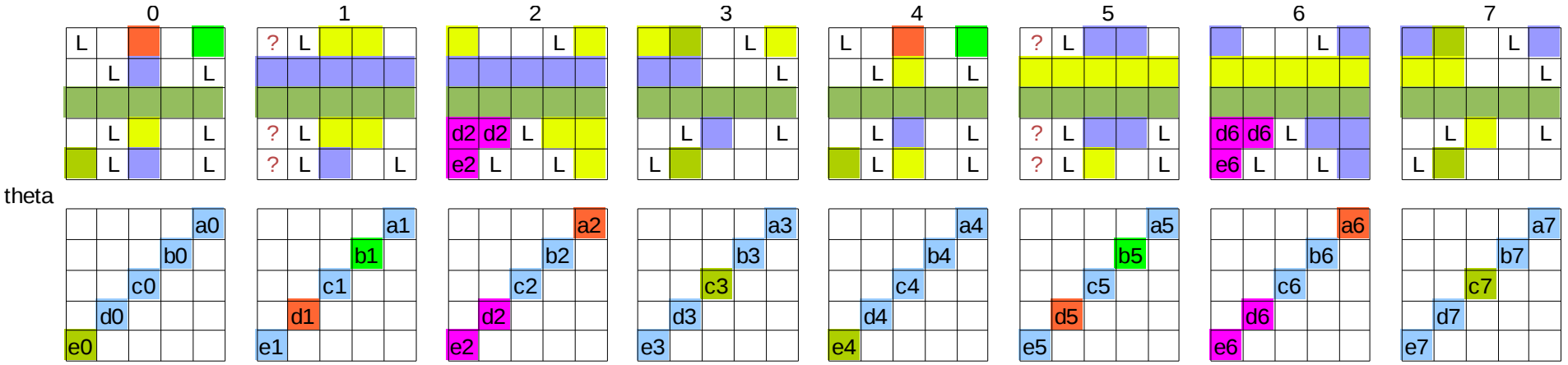
One more round!

Best Time Complexity Attack ($r = 40$)



The last round

If we have a look at exploitable relations...



Equations

$$b_1 = x_{040}y_{140} + \ell^x_{b_1}(A^f_+) + \ell^y_{b_1}(A^b_+) \quad (1)$$

$$c_7 = y_{247}x_{347} + y_{207}x_{307} + \ell^x_{c_7}(A^f_+) + \ell^y_{c_7}(A^b_+) \quad (2)$$

$$e_0 = x_{100}y_{200} + x_{040}y_{140} + y_{247}x_{347} + y_{207}x_{307} + \ell^x_{e_0}(A^f_+) + \ell^y_{e_0}(A^b_+) \quad (3)$$

$$b_5 = y_{044}x_{144} + \ell^x_{b_5}(A^f_+) + \ell^y_{b_5}(A^b_+) \quad (4)$$

$$c_3 = x_{243}y_{343} + x_{203}y_{303} + \ell^x_{c_3}(A^f_+) + \ell^y_{c_3}(A^b_+) \quad (5)$$

$$e_4 = y_{104}x_{204} + y_{044}x_{144} + x_{243}y_{343} + x_{203}y_{303} + \ell^x_{e_4}(A^f_+) + \ell^y_{e_4}(A^b_+) \quad (6)$$

$$a_2 + d_1 = x_{340}y_{440} + \ell^x_{a_2+d_1}(A^f_+) + \ell^y_{a_2+d_1}(A^b_+) \quad (7)$$

$$a_6 + d_5 = y_{344}x_{444} + \ell^x_{a_6+d_5}(A^f_+) + \ell^y_{a_6+d_5}(A^b_+) \quad (8)$$

$$e_2 = x_{102}y_{202} + \ell^x_{e_2}(A^f_+) + \ell^y_{e_2}(A^b_+) \quad (9)$$

$$e_6 = y_{106}x_{206} + \ell^x_{e_6}(A^f_+) + \ell^y_{e_6}(A^b_+) \quad (10)$$

$$e_2 + d_2 = y_{212}(x_{312} + x_{112}) + \ell^x_{e_2+d_2}(A^f_+) + \ell^y_{e_2+d_2}(A^b_+) \quad (11)$$

$$e_6 + d_6 = x_{216}(y_{316} + y_{116}) + \ell^x_{e_6+d_6}(A^f_+) + \ell^y_{e_6+d_6}(A^b_+) \quad (12)$$

Finding solutions

Two lists of size $2^{100-20*2+5} = 2^{65}$ (yellow and violet bits).

- First output: 40 bit linear filter (grey).
  Plus $5+5$ linear filter from the guessed parity and...
- ...10 quadratic equations involving 10 variables linearly and 11 quadraticaly (per list):
  Variables involved in the 50 linear equations define 2^{50} possible pairs of sublists of size 2^{15} to merge with respect to the quadratic ones (parallel matching):

Time complexity of $2^{50} \times 2^{21.5} = 2^{71.5}$

(More) Recent Improvements: $r = 32$

Works on a version with $r = 32$ (using some improvements):

- Guess 8 after the second χ and 7 bits from each half (previous equations become linear): size of the lists $2^{100-16*2+5-7-4} = 2^{62}$.
- Invert the last χ: We consider 2^{12} outputs, until one verifies the conditions where the unknown bit of the output does not affect the previous wanted equation.
- Time complexity:

$$2^{12} + 2^{14+8} \times 2^{62+1} + 2^{14+8} \times 2^{62+62-12-42} = 2^{92}$$

Conclusion and Future Work

- New direction analyzing message processing.

- It needs higher rates to work so not a threat.
  To reduce the rate:

  one more round?

- New ideas needed:
  4 lists to merge considering 4 rounds?

Two Short Announcements

1. Open PhD and Post-doc positions

In the context of the QUASYModo ERC project:
Symmetric cryptography for the post-quantum world.

Cryptanalysis and/or design (2 PhD, 2 post-docs).

Contact me if interested !

2. FSE 2018 (and 2019)

5-7 March in Brugges (general chair Elena Andreeva).

We hope to see you there!

Next co-chair: Yu Sasaki (+ Florian, - me)

FSE 2019: in Paris (general chair Jérémy Jean)