Radboud University

# Linear Cryptanalysis of MORUS

Tomer Ashur, Maria Eichlseder, Martin M. Lauridsen, Gaëtan Leurent, Brice Minaud, Yann Rotella, Yu Sasaki, **Benoît Viguier**

DS Lunch Talk, June 22, 2018

# Overview

- MORUS & MiniMORUS
- Linear Cryptanalysis of MiniMORUS
- Extension to MORUS and Consequences

# MORUS & MiniMORUS

# What is MORUS?

- Authenticated encryption algorithm (Encrypt-and-MAC)
- Designed by Wu and Huang

**Table:** Security goals of MORUS.

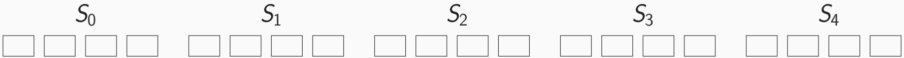
| | Confidentiality (bits) | Integrity (bits) |
|---|---|---|
| MORUS-640-128 | 128 | 128 |
| MORUS-1280-128 | 128 | 128 |
| MORUS-1280-256 | 256 | 128 |

Impose rekeying every $2^{64}$ encrypted blocks.

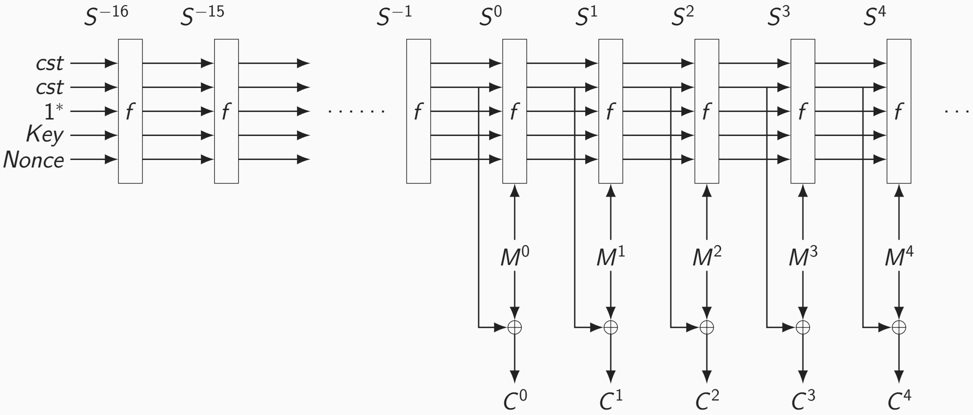
# What is MORUS?

MORUS state:

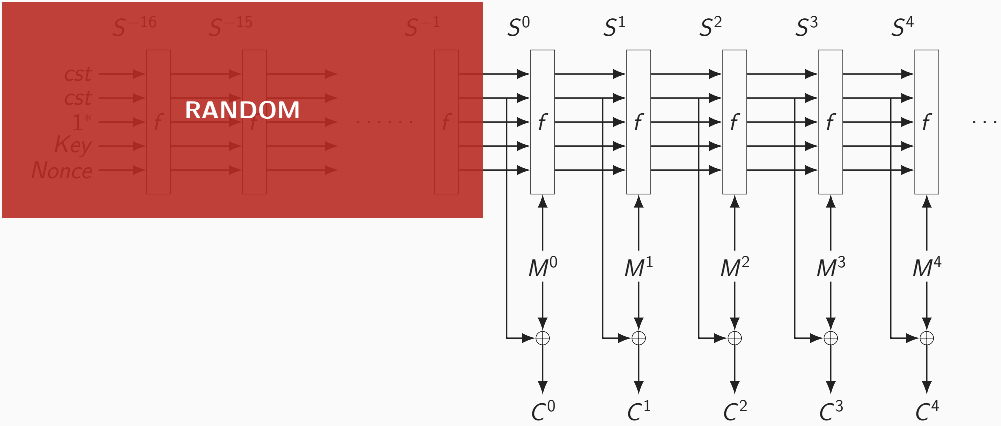
- 5 registers of 4 words.
- MORUS-640, 32-bit words ⟹ 128-bit registers ⟹ SSE instructions.
- MORUS-1280, 64-bit words ⟹ 256-bit registers ⟹ AVX2 instructions.



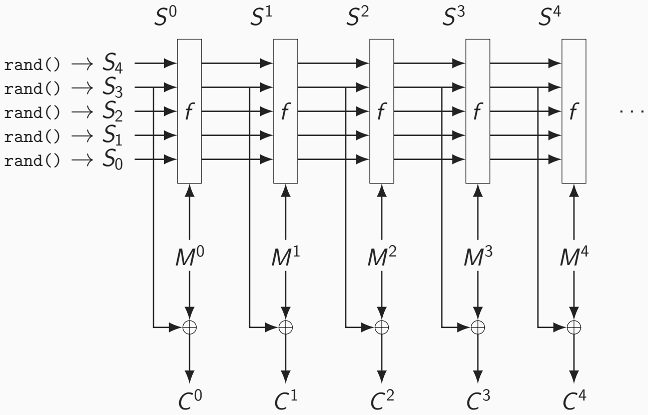
# What is MORUS?



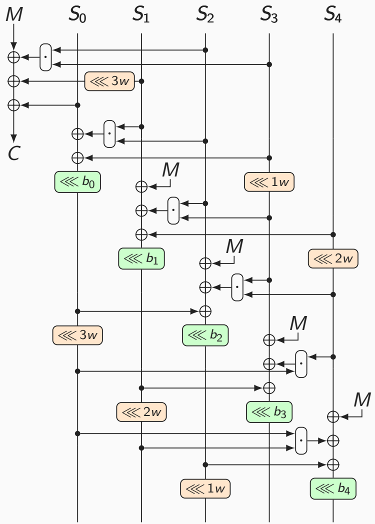
# What is MORUS?



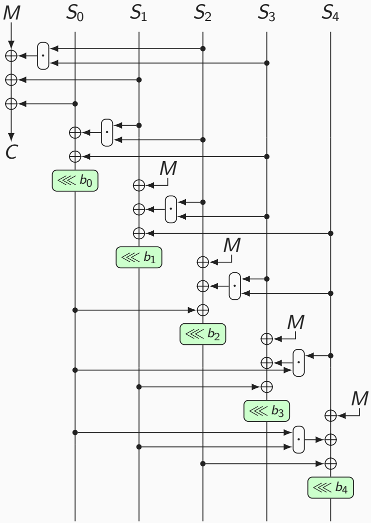
# What is MORUS?



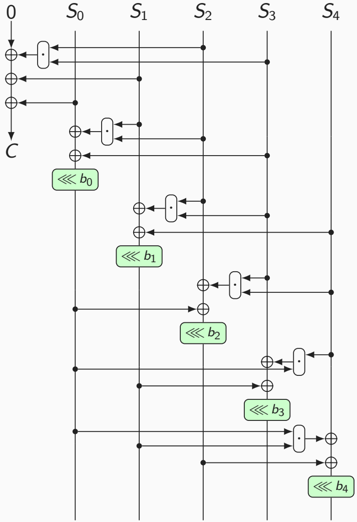
# What is MORUS?



# MiniMORUS!



# MiniMORUS with chosen plaintext!



# Linear Cryptanalysis of MiniMORUS

# Weight and Bias

$$\texttt{x = u} \oplus \texttt{y} \oplus \texttt{(z} \wedge \texttt{t)}$$

Can be linear approximated with

$$\texttt{E: x = u} \oplus \texttt{y}$$

This linear approximation holds with a bias $\varepsilon$:

$$\Pr(E) = \frac{1}{2} + \varepsilon$$

The *correlation* and *weight* of an approximation is:

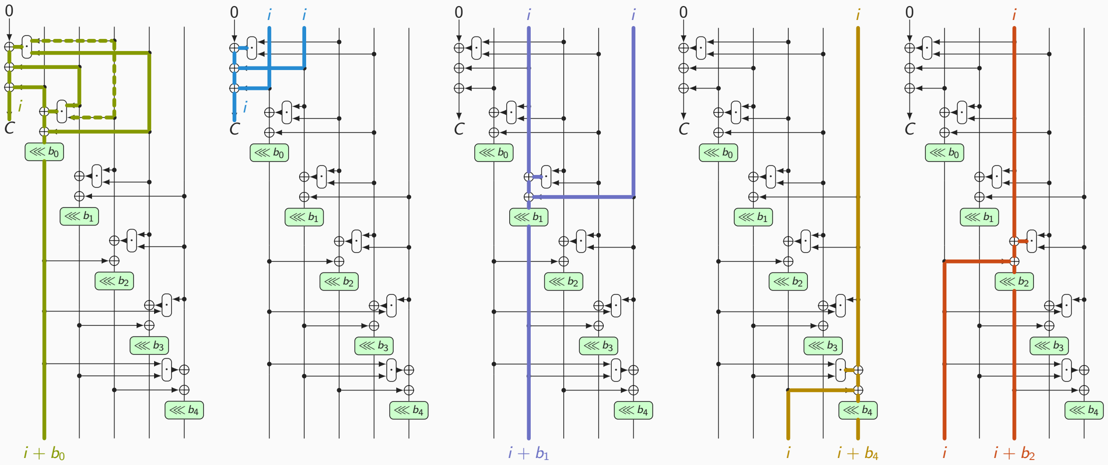
$$\mathrm{cor}(E) := 2\Pr(E) - 1 = 2\varepsilon$$

$$\mathrm{weight}(E) := -\log_2 |\mathrm{cor}(E)|$$

**Pilling Up Lemma (Matsui M., 1993)**

The correlation (resp. weight) of an XOR of independent variables is equal to the product (resp. sum) of their individual correlations (resp. weights)

# MiniMORUS: trails $\alpha, \beta, \gamma, \delta, \varepsilon$



weight($\alpha_i^t$) = 1 (not 2)

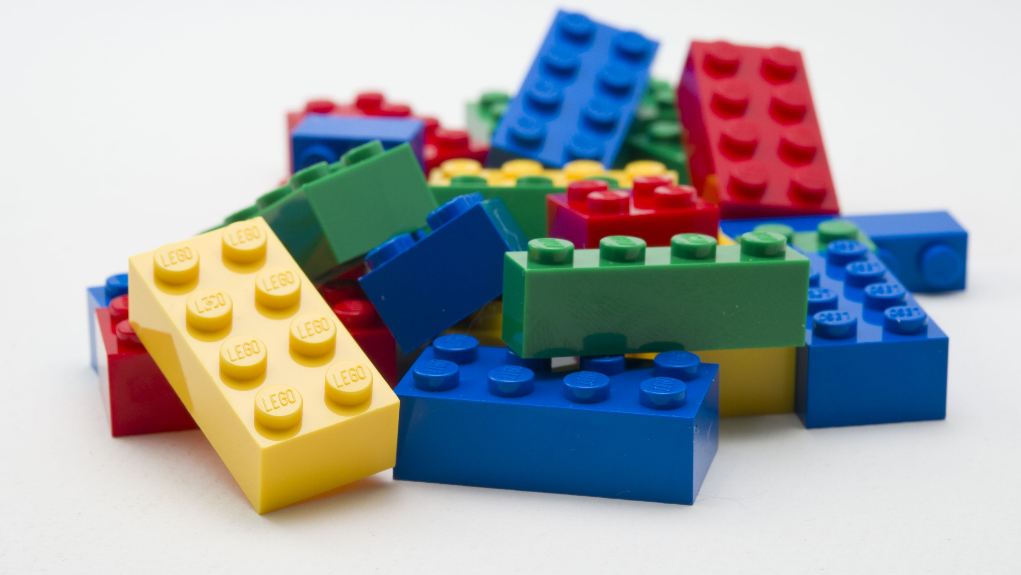
weight($\beta_i^t$) = 1

weight($\gamma_i^t$) = 1

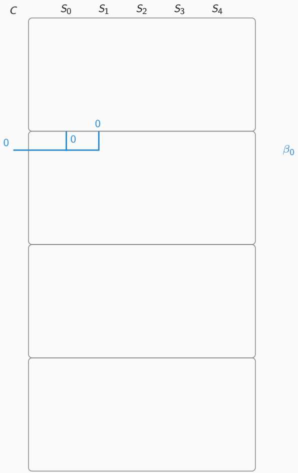
weight($\delta_i^t$) = 1

weight($\varepsilon_i^t$) = 1

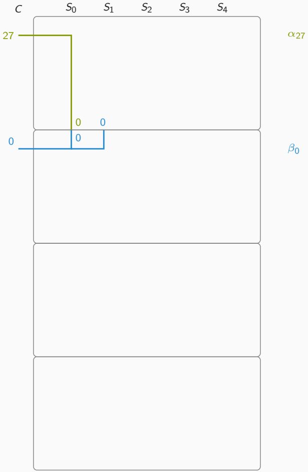
# Building Trails



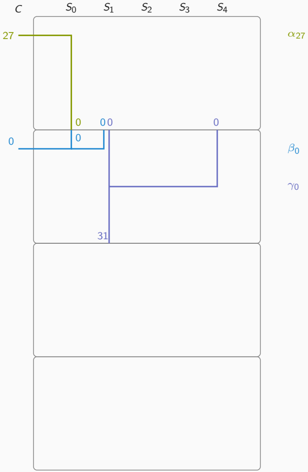
# MiniMORUS-640 : Building trails with $\chi_1$ and $\chi_2$



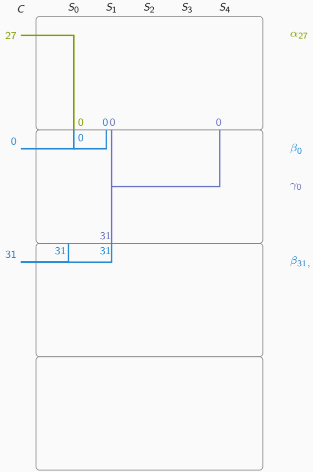
# MiniMORUS-640 : Building trails with $\chi_1$ and $\chi_2$



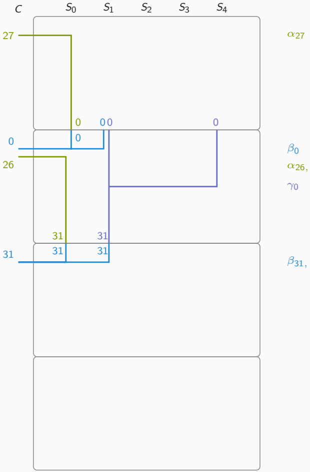
# MiniMORUS-640 : Building trails with $\chi_1$ and $\chi_2$



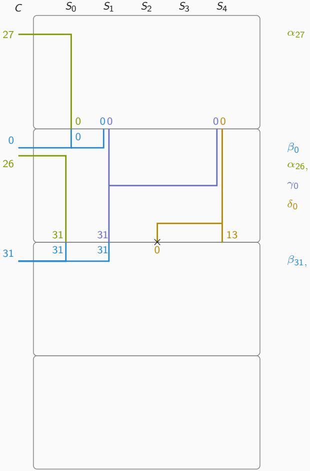
# MiniMORUS-640 : Building trails with $\chi_1$ and $\chi_2$



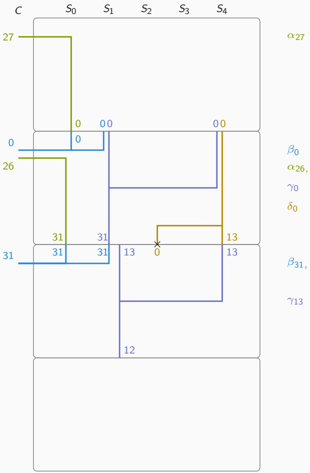
# MiniMORUS-640 : Building trails with $\chi_1$ and $\chi_2$



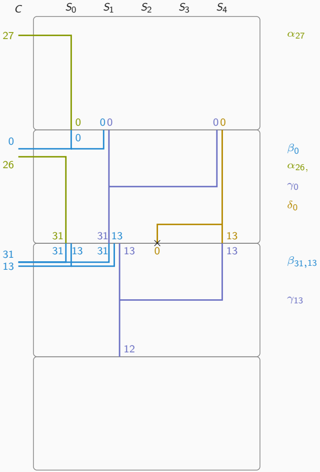
# MiniMORUS-640 : Building trails with $\chi_1$ and $\chi_2$



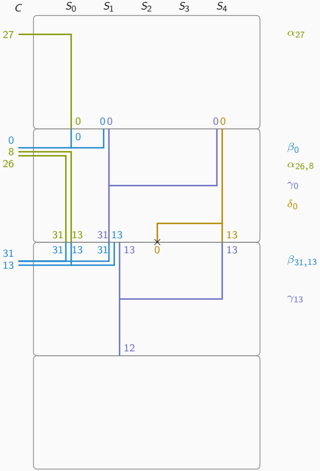
# MiniMORUS-640 : Building trails with $\chi_1$ and $\chi_2$



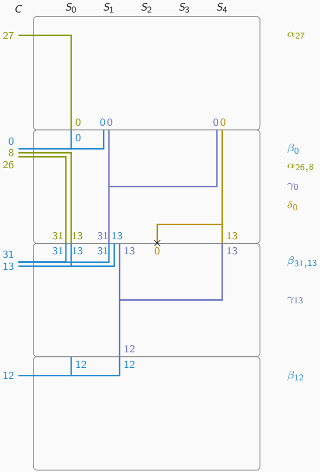
# MiniMORUS-640 : Building trails with $\chi_1$ and $\chi_2$



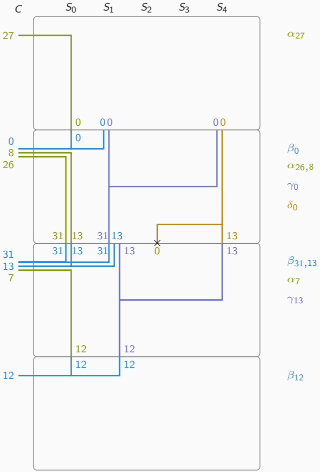
# MiniMORUS-640 : Building trails with $\chi_1$ and $\chi_2$



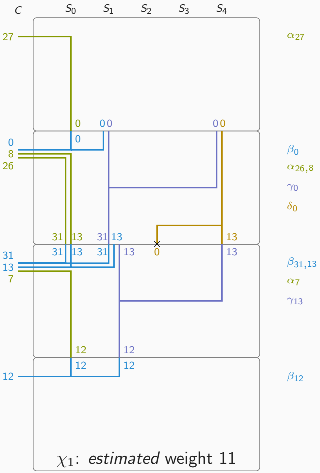
# MiniMORUS-640 : Building trails with $\chi_1$ and $\chi_2$



# MiniMORUS-640 : Building trails with $\chi_1$ and $\chi_2$



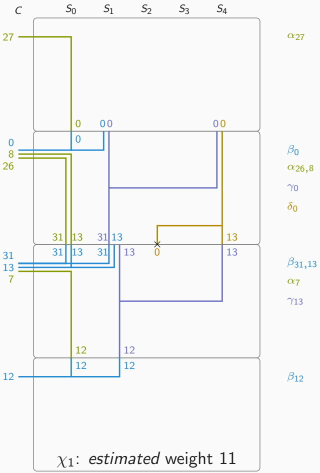
# MiniMORUS-640 : Building trails with $\chi_1$ and $\chi_2$



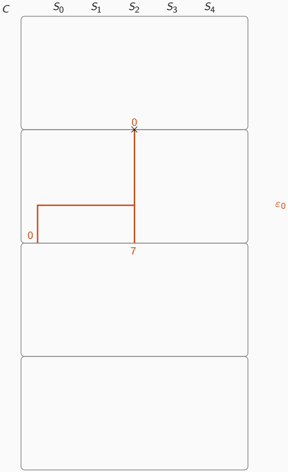
$\chi_1$: *estimated* weight 11

$$C^0_{27} \oplus C^1_0 \oplus C^1_8 \oplus C^1_{26} \oplus C^2_7 \oplus C^2_{13} \oplus C^2_{31} \oplus C^3_{12} \to S^2_{2,0}$$

# MiniMORUS-640 : Building trails with $\chi_1$ and $\chi_2$

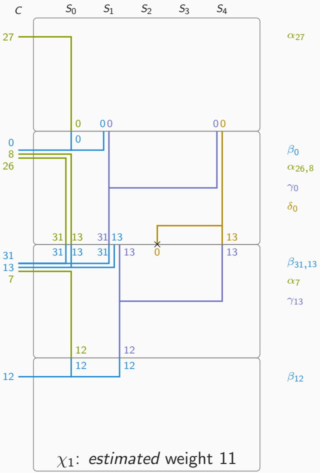


$\chi_1$: *estimated* weight 11

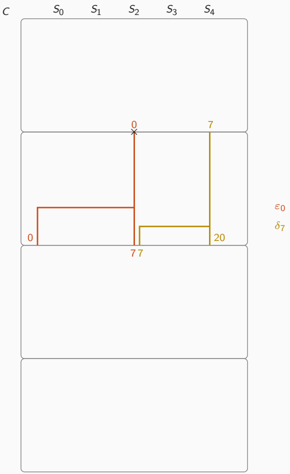


$$C^0_{27} \oplus C^1_0 \oplus C^1_8 \oplus C^1_{26} \oplus C^2_7 \oplus C^2_{13} \oplus C^2_{31} \oplus C^3_{12} \to S^2_{2,0}$$

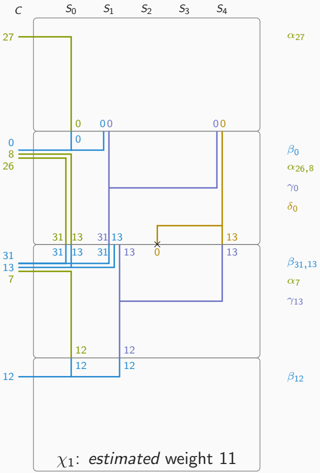
# MiniMORUS-640 : Building trails with $\chi_1$ and $\chi_2$



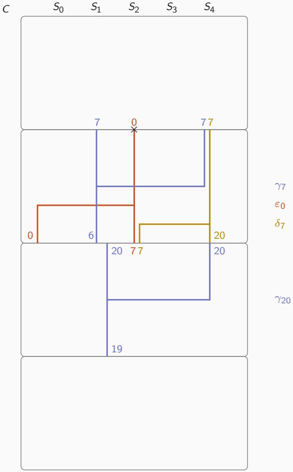
$$C^0_{27} \oplus C^1_0 \oplus C^1_8 \oplus C^1_{26} \oplus C^2_7 \oplus C^2_{13} \oplus C^2_{31} \oplus C^3_{12} \to S^2_{2,0}$$



# MiniMORUS-640 : Building trails with $\chi_1$ and $\chi_2$

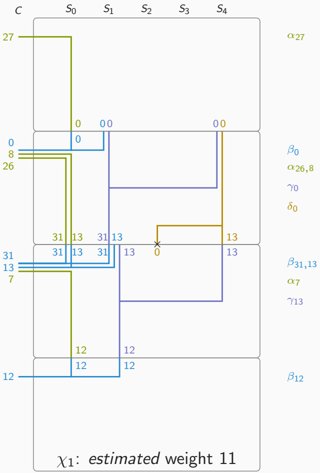


$\chi_1$: *estimated* weight 11

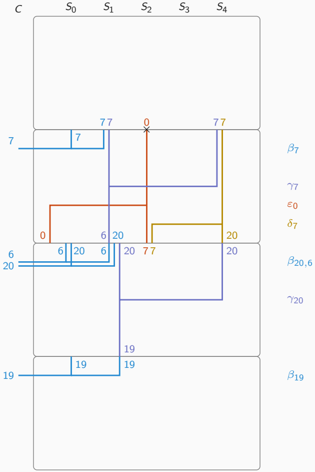


$$C^0_{27} \oplus C^1_0 \oplus C^1_8 \oplus C^1_{26} \oplus C^2_7 \oplus C^2_{13} \oplus C^2_{31} \oplus C^3_{12} \to S^2_{2,0}$$

# MiniMORUS-640 : Building trails with $\chi_1$ and $\chi_2$

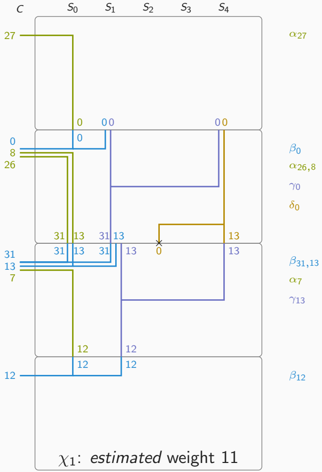


$\chi_1$: *estimated* weight 11



$$C^0_{27} \oplus C^1_0 \oplus C^1_8 \oplus C^1_{26} \oplus C^2_7 \oplus C^2_{13} \oplus C^2_{31} \oplus C^3_{12} \to S^2_{2,0}$$

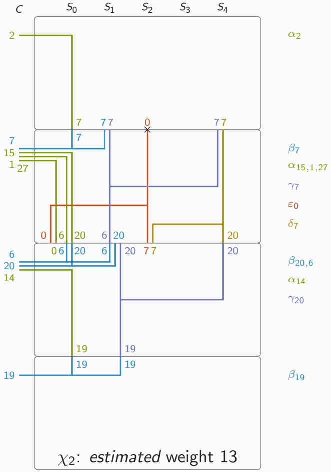
# MiniMORUS-640 : Building trails with $\chi_1$ and $\chi_2$



$\chi_1$: *estimated* weight 11

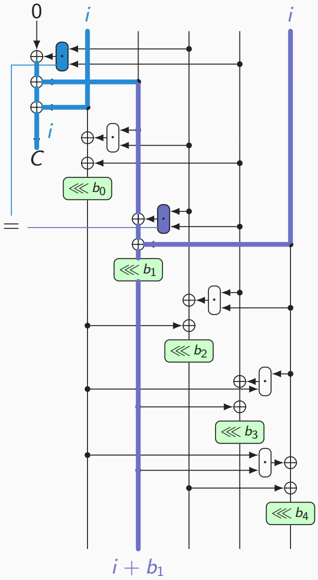
$$C^0_{27} \oplus C^1_0 \oplus C^1_8 \oplus C^1_{26} \oplus C^2_7 \oplus C^2_{13} \oplus C^2_{31} \oplus C^3_{12} \rightarrow S^2_{2,0}$$

$$C^1_2 \oplus C^2_1 \oplus C^2_7 \oplus C^2_{15} \oplus C^2_{27} \oplus C^3_6 \oplus C^3_{14} \oplus C^3_{20} \oplus C^4_{19} \rightarrow S^2_{2,0}$$



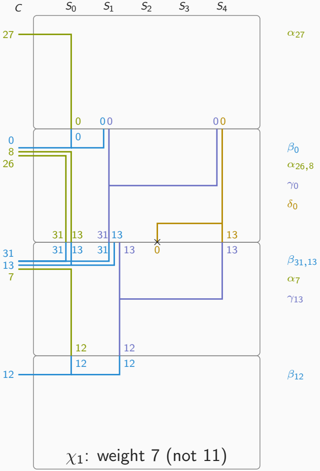
$\chi_2$: *estimated* weight 13

# MiniMORUS: Weight of $\beta_i^t \oplus \gamma_i^t$



Weight of $\beta_i^t \oplus \gamma_i^t$ is 0 (not 2).

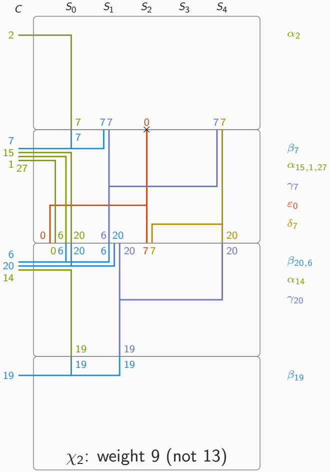
# MiniMORUS-640 : Weight corrected



$\chi_1$: weight 7 (not 11)

$$C^0_{27} \oplus C^1_0 \oplus C^1_8 \oplus C^1_{26} \oplus C^2_7 \oplus C^2_{13} \oplus C^2_{31} \oplus C^3_{12} \to S^2_{2,0}$$

$$C^1_2 \oplus C^2_1 \oplus C^2_7 \oplus C^2_{15} \oplus C^2_{27} \oplus C^3_6 \oplus C^3_{14} \oplus C^3_{20} \oplus C^4_{19} \to S^2_{2,0}$$



$\chi_2$: weight 9 (not 13)

# MiniMORUS: Full Trail

- MiniMORUS-640

$$\chi_1 \oplus \chi_2 = C^0_{27} \oplus C^1_0 \oplus C^1_2 \oplus C^1_8 \oplus C^1_{26} \oplus C^2_1 \oplus C^2_{13} \oplus C^2_{15} \oplus C^2_{27} \oplus C^2_{31} \oplus C^3_6 \oplus C^3_{12} \oplus C^3_{14} \oplus C^3_{20} \oplus C^4_{19} \to 0$$

- MiniMORUS-1280

$$C^0_{51} \oplus C^1_0 \oplus C^1_{25} \oplus C^1_{33} \oplus C^1_{55} \oplus C^2_4 \oplus C^2_7 \oplus C^2_{29} \oplus C^2_{37} \oplus C^2_{38} \oplus C^2_{46} \oplus C^2_{51} \oplus C^3_{11} \oplus C^3_{20} \oplus C^3_{42} \oplus C^3_{50} \oplus C^4_{24} \to 0$$

In both case, the weight of the trail is $7 + 9 = 16$.

# MiniMORUS: Experimental verification

| | | Weight | | |
|---|---|---|---|---|
| Approximations for MiniMORUS-640 | | Exp. | Bool. | Meas. |
| $\chi_1$ | $S_0^{2,2} = C_{27}^0 \oplus C_{0,8,26}^1 \oplus C_{7,13,31}^2 \oplus C_{12}^3$ | 7 | 7 | 7 |
| $\chi_2$ | $S_0^{2,2} = C_2^1 \oplus C_{1,7,15,27}^2 \oplus C_{6,14,20}^3 \oplus C_{19}^4$ | 9 | 9 | 9 |
| $\chi$ | $0 = C_{27}^0 \oplus C_{0,2,26,8}^1 \oplus C_{1,13,15,27,31}^2 \oplus C_{6,12,14,20}^3 \oplus C_{19}^4$ | 16 | 16 | 15.5 |
| Approximations for MiniMORUS-1280 | | | | |
| $\chi_1$ | $S_0^{2,2} = C_{51}^0 \oplus C_{0,33,55}^1 \oplus C_{4,37,46}^2 \oplus C_{50}^3$ | 7 | 7 | 7 |
| $\chi_2$ | $S_0^{2,2} = C_{25}^1 \oplus C_{7,29,38,51}^2 \oplus C_{11,20,42}^3 \oplus C_{24}^4$ | 9 | 9 | 9 |
| $\chi$ | $0 = C_{51}^0 \oplus C_{0,25,33,55}^1 \oplus C_{4,7,29,37,38,46,51}^2 \oplus C_{11,20,42,50}^3 \oplus C_{24}^4$ | 16 | 16 | 15.9 |

The programs we used to verify the bias experimentally are available at:
`https://github.com/ildyria/MorusBias`

# Extension to MORUS and Consequences

# From MiniMORUS to MORUS

- Trail extension:
  $S_{i,j}$ in MiniMORUS is translated into $S_{i,j} \oplus S_{i,j+w} \oplus S_{i,j+2w} \oplus S_{i,j+3w}$ in MORUS
  e.g. $S_{2,0}$ in MiniMORUS-1280 $\iff$ $S_{2,0} \oplus S_{2,64} \oplus S_{2,128} \oplus S_{2,192}$ in MORUS-1280.

- Weight implication:
  word "*equality*" occurs with probability $\frac{1}{2^4}$ $\implies$ weight $\times 4$

- $\beta_i + \gamma_i$ has weight 0 in MiniMORUS but weight 4 in MORUS

## Weight of the trails

$$\text{MORUS-640: Weight}(\chi) = 73$$

$$\text{MORUS-1280: Weight}(\chi) = 76$$

# Impact for MORUS

- **Keystream correlation**
  - The bias is *absolute*: does not depends on Key or Nonce!
  - Similar to RC4, BEAST attack. . .
  - Known plaintext $\implies$ Distinguisher.
  - Multiple fixed plaintext $\implies$ plaintext recovery.

# Impact for MORUS

- **Keystream correlation**
  - The bias is *absolute*: does not depends on Key or Nonce!
  - Similar to RC4, BEAST attack. . .
  - Known plaintext $\Longrightarrow$ Distinguisher.
  - Multiple fixed plaintext $\Longrightarrow$ plaintext recovery.
- **Data complexity**
  - Immune to rekeying every $2^{64}$ encrypted block.
  - Require $2^{146}$ blocks for MORUS-640
  - Require $2^{152}$ blocks for MORUS-1280 **(violate 256-bit confidentiality claim)**
  - trail is immune to bit-shift:

    - save $2^{5}$ data for MORUS-640.

    - save $2^{6}$ data for MORUS-1280.
  - Not practical. :(

https://eprint.iacr.org/2018/464.pdf