Radboud University

Linear Cryptanalysis of MORUS

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

Asiacrypt, December 4, 2018

Paper collision

Yanbin Li and Meiqin Wang. "Cryptanalysis of MORUS".
Designs, Codes and Cryptography, pages 1—24,
First Online: 09 June 2018

Our paper was submitted to ePrint on 17 May 2018.

MILP-aided search for reduced MORUS.

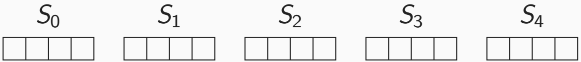
- Integral distinguishers for 6.5 steps of MORUS-640.
- Differential distinguishers for 4.5 steps of MORUS-1280.

Overview

- MORUS design
- Analysis of MiniMORUS
- Application to MORUS

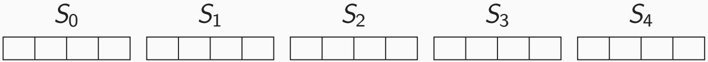
MORUS design

- Family of authenticated ciphers by Wu and Huang
  - MORUS-640 with 128-bit key



$5 \times 4 \times$ 32-bit words

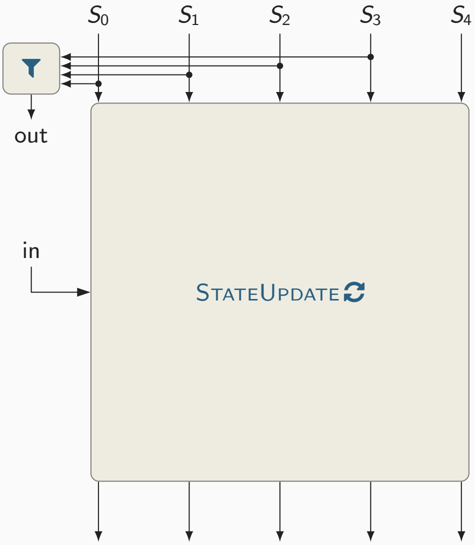
  - MORUS-1280-128 with 128-bit key
  - MORUS-1280-256 with 256-bit key



$5 \times 4 \times$ 64-bit words

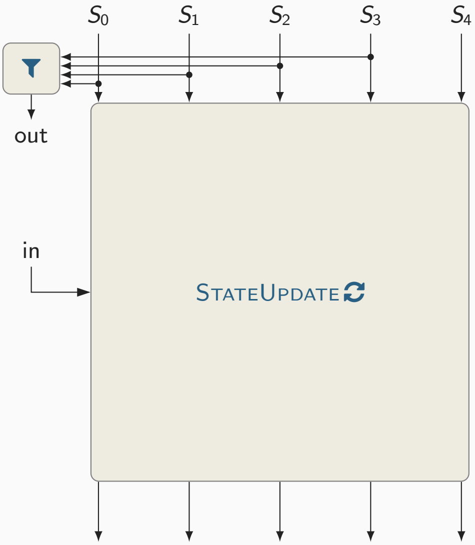
- Security claim for confidentiality = key size; re-key every 2^{64} blocks
- CAESAR finalist for Use-Case 2 (High Performance)

MORUS Authenticated Cipher (simplified)



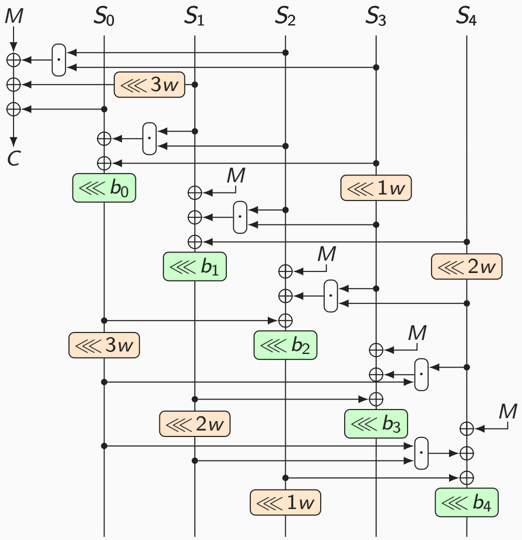
1. Initialization:
   a. $S_0 = N, \quad S_1 = K$
   b. $16 \times \textsc{StateUpdate}(0)$
   c. $S_1 = S_1 \oplus K$
2. Encryption: For each msg block M_i:
   a. $C_i = M_i \oplus ▼(S_0, \ldots, S_3)$
   b. $\textsc{StateUpdate}(M_i)$
3. Finalization:
   a. $S_4 = S_4 \oplus S_0$
   b. $10 \times \textsc{StateUpdate}(\text{len}(M))$
   c. $T = ▼(S_0, \ldots, S_3)$

MORUS Authenticated Cipher (simplified)

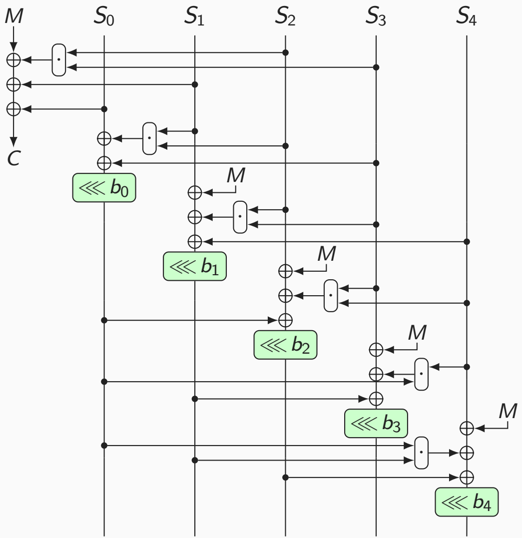


1. Initialization:
   - a. $S_0 = N, \quad S_1 = K$
   - b. $16 \times$ STATEUPDATE(0)
   - c. $S_1 = S_1 \oplus K$
2. Encryption: For each msg block M_i:
   - a. $C_i = M_i \oplus$ ▼$(S_0, \ldots, S_3)$
   - b. STATEUPDATE(M_i)
3. Finalization:
   - a. $S_4 = S_4 \oplus S_0$
   - b. $10 \times$ STATEUPDATE$(\mathrm{len}(M))$
   - c. $T =$ ▼$(S_0, \ldots, S_3)$

MORUS StateUpdate Function



- Nonlinearity:
  "Toffoli" gate $z = z \oplus (x \odot y)$
- Diffusion:
  Xors $z = z \oplus x$
  Rotation within words $\lll r$
  Rotate words $\lll rw$



- MORUS state

S_0 S_1 S_2 S_3 S_4

- MiniMORUS state

S_0 S_1 S_2 S_3 S_4

- We will later use $\square = \square + \square + \square + \square$
- Rotational invariance

Analysis of MiniMORUS

Weight and Bias

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

Can be linear approximated with

$$\texttt{E: x = u} \oplus \texttt{y} \qquad \text{and} \qquad \Pr(E) = \tfrac{3}{4}$$

The *bias* ε is:

$$\Pr(E) = \frac{1}{2} + \varepsilon \qquad \Longrightarrow \qquad \varepsilon = \frac{1}{4}$$

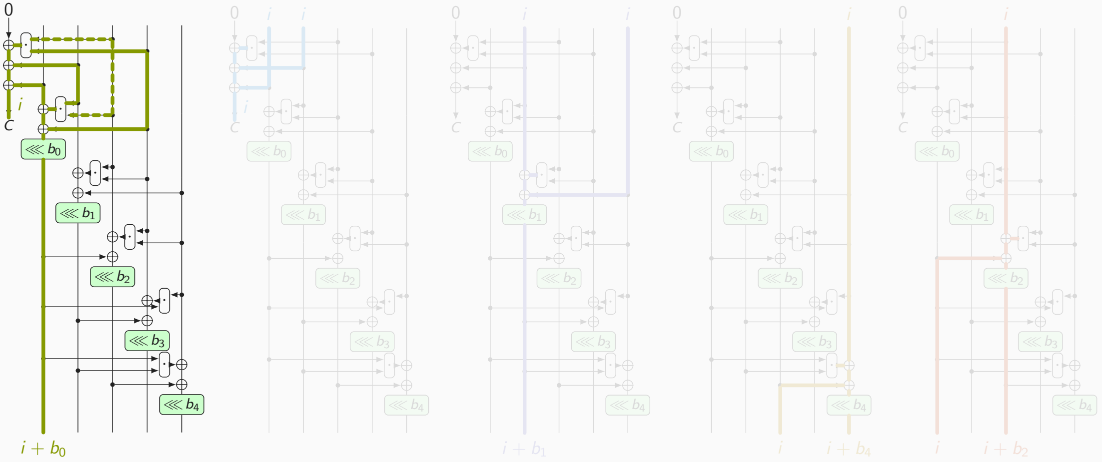
The *correlation* and *weight* of an approximation is:

$$\begin{aligned} \mathrm{cor}(E) &:= 2\varepsilon \\ \mathrm{weight}(E) &:= -\log_2 |\mathrm{cor}(E)| \qquad \Longrightarrow \qquad \mathrm{weight}(E) = 1 \end{aligned}$$

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: Approximation fragments $\alpha, \beta, \gamma, \delta, \varepsilon$



weight(α_i^t) $= 1$ (not 2)

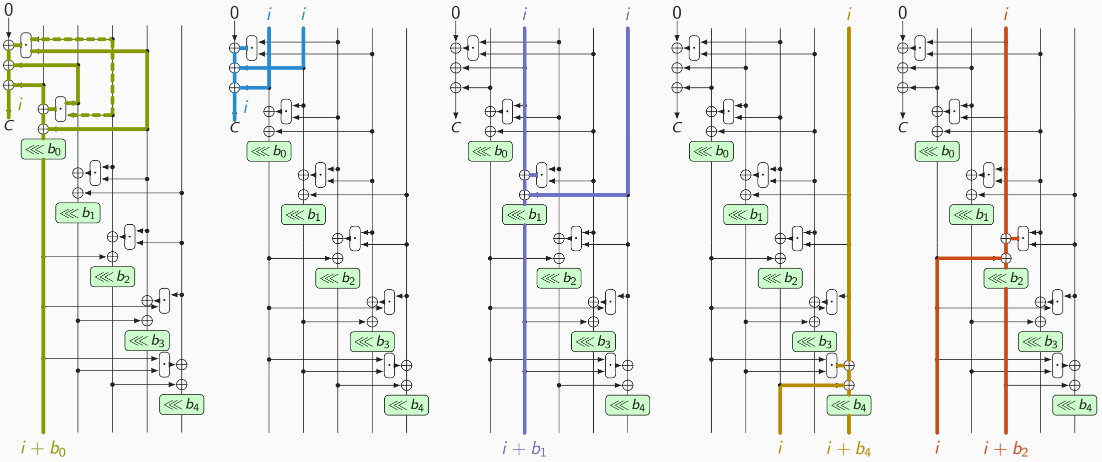
weight(β_i^t) $= 1$

weight(γ_i^t) $= 1$

weight(δ_i^t) $= 1$

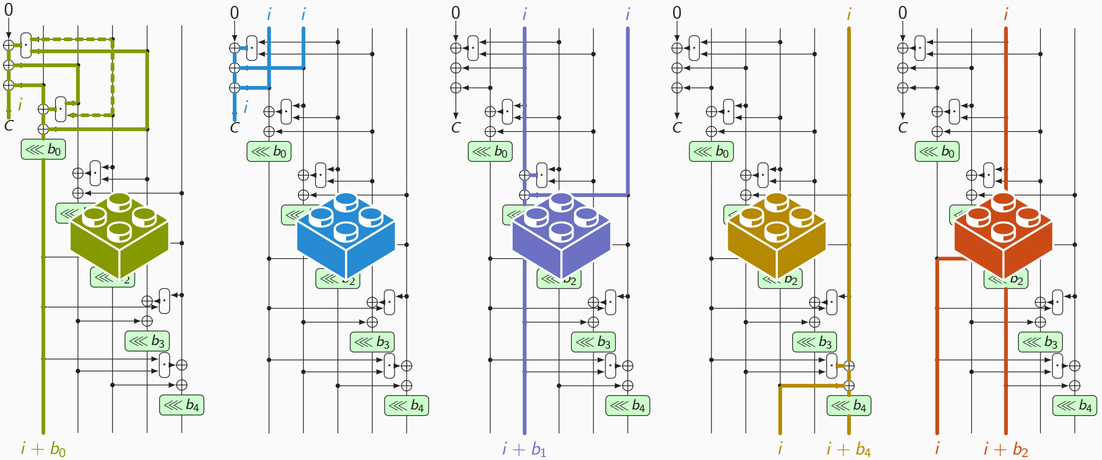
weight(ε_i^t) $= 1$

MiniMORUS: Approximation fragments $\alpha, \beta, \gamma, \delta, \varepsilon$



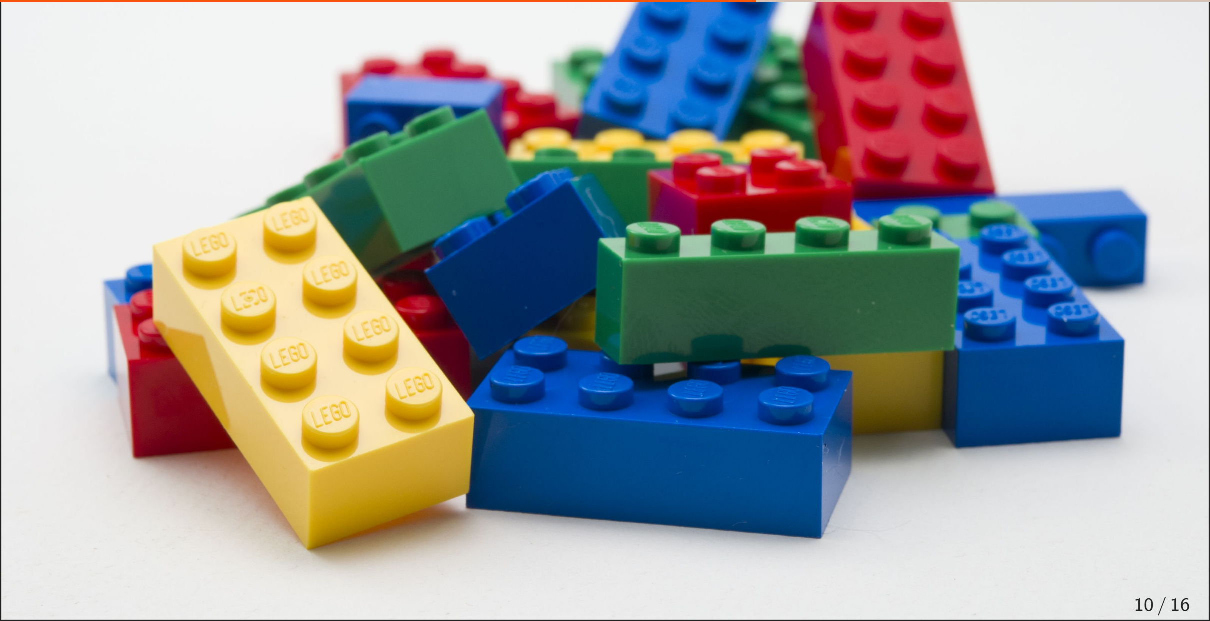
weight(α_i^t) = 1 (not 2) weight(β_i^t) = 1 weight(γ_i^t) = 1 weight(δ_i^t) = 1 weight(ε_i^t) = 1

MiniMORUS: Approximation fragments $\alpha, \beta, \gamma, \delta, \varepsilon$

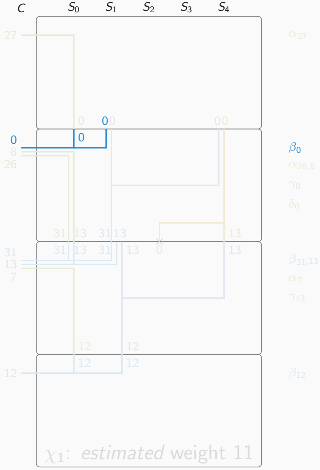


weight(α_i^t) = 1 (not 2) weight(β_i^t) = 1 weight(γ_i^t) = 1 weight(δ_i^t) = 1 weight(ε_i^t) = 1

Building Trails



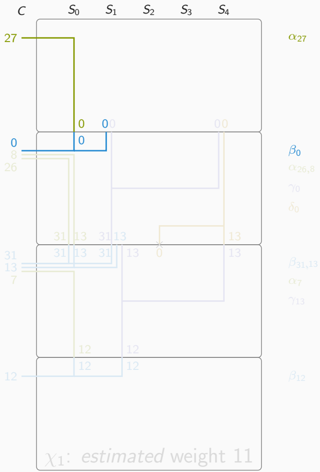
MINIMORUS-640: Building trails with χ_1 and χ_2



$$C_{27}^0 \oplus C_0^1 \oplus C_8^1 \oplus C_{26}^1 \oplus C_7^2 \oplus C_{13}^2 \oplus C_{31}^2 \oplus C_{12}^3 \to S_{2,0}^2$$

$$C_2^1 \oplus C_1^2 \oplus C_7^2 \oplus C_{15}^2 \oplus C_{27}^2 \oplus C_6^3 \oplus C_{14}^3 \oplus C_{20}^3 \oplus C_{19}^4 \to S_{2,0}^2$$

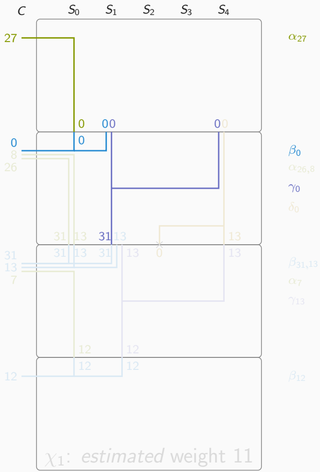
MiniMORUS-640: Building trails with χ_1 and χ_2



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

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

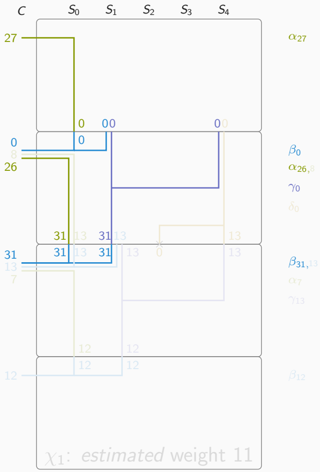
MiniMORUS-640: Building trails with χ_1 and χ_2



$$C_{27}^0 \oplus C_0^1 \oplus C_8^1 \oplus C_{26}^1 \oplus C_7^2 \oplus C_{13}^2 \oplus C_{31}^2 \oplus C_{12}^3 \to S_{2,0}^2$$

$$C_2^1 \oplus C_1^2 \oplus C_7^2 \oplus C_{15}^2 \oplus C_{27}^2 \oplus C_6^3 \oplus C_{14}^3 \oplus C_{20}^3 \oplus C_{19}^4 \to S_{2,0}^2$$

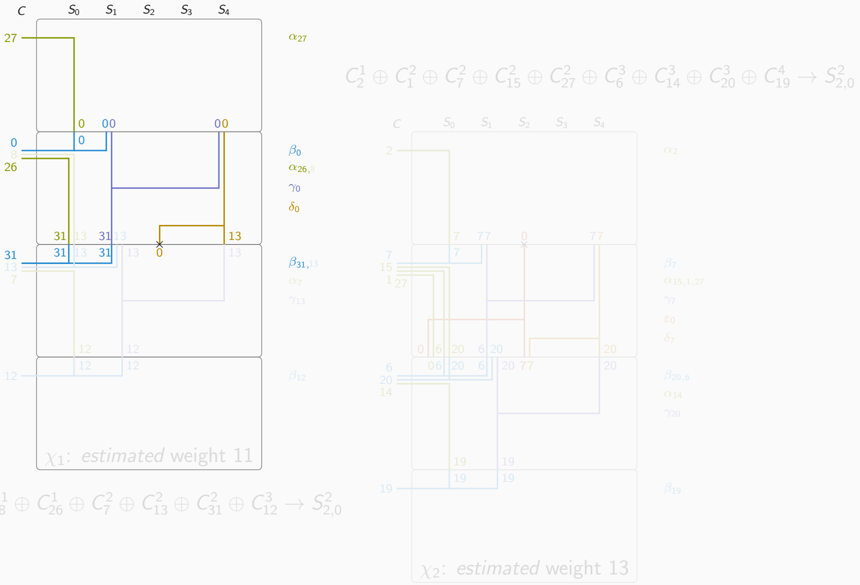
MINIMORUS-640: Building trails with χ_1 and χ_2



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

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

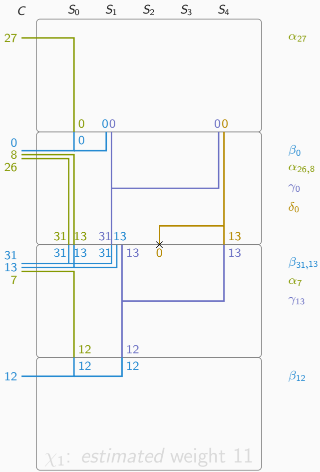
MINIMORUS-640: Building trails with χ_1 and χ_2



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

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

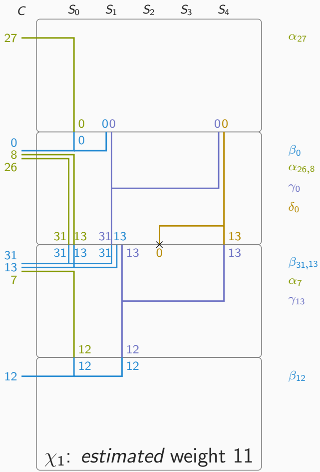
MiniMORUS-640: Building trails with χ_1 and χ_2



$$C_{27}^0 \oplus C_0^1 \oplus C_8^1 \oplus C_{26}^1 \oplus C_7^2 \oplus C_{13}^2 \oplus C_{31}^2 \oplus C_{12}^3 \to S_{2,0}^2$$

$$C_2^1 \oplus C_1^2 \oplus C_7^2 \oplus C_{15}^2 \oplus C_{27}^2 \oplus C_6^3 \oplus C_{14}^3 \oplus C_{20}^3 \oplus C_{19}^4 \to S_{2,0}^2$$

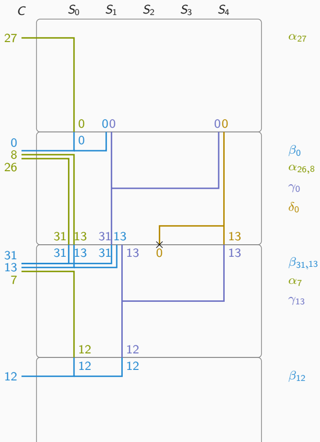
MiniMORUS-640: Building trails with χ_1 and χ_2



$$C_{27}^0 \oplus C_0^1 \oplus C_8^1 \oplus C_{26}^1 \oplus C_7^2 \oplus C_{13}^2 \oplus C_{31}^2 \oplus C_{12}^3 \to S_{2,0}^2$$

$$C_2^1 \oplus C_1^2 \oplus C_7^2 \oplus C_{15}^2 \oplus C_{27}^2 \oplus C_6^3 \oplus C_{14}^3 \oplus C_{20}^3 \oplus C_{19}^4 \to S_{2,0}^2$$

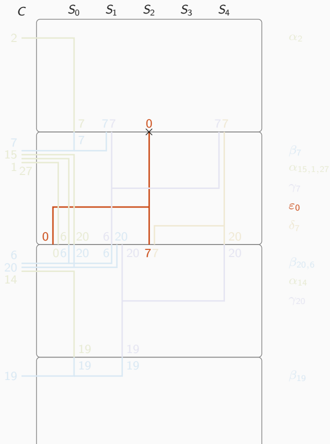
MiniMORUS-640: Building trails with χ_1 and χ_2



χ_1: *estimated* weight 11

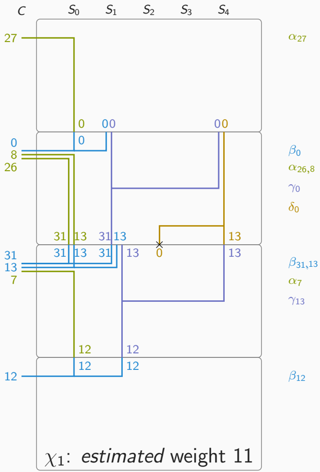
$$C^0_{27} \oplus C^1_0 \oplus C^1_8 \oplus C^1_{26} \oplus C^2_7 \oplus C^2_{13} \oplus C^2_{31} \oplus C^3_{12} \to S^2_{2,0}$$

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



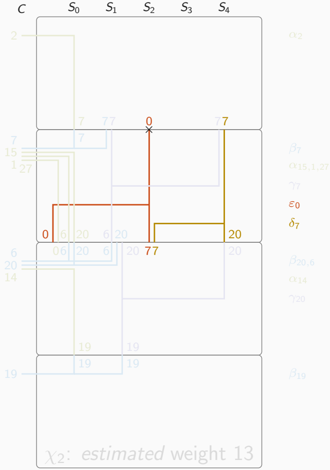
χ_2: *estimated* weight 13

MiniMORUS-640: Building trails with χ_1 and χ_2

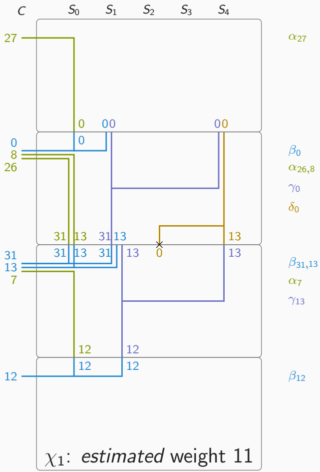


$$C^0_{27} \oplus C^1_0 \oplus C^1_8 \oplus C^1_{26} \oplus C^2_7 \oplus C^2_{13} \oplus C^2_{31} \oplus C^3_{12} \to S^2_{2,0}$$

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

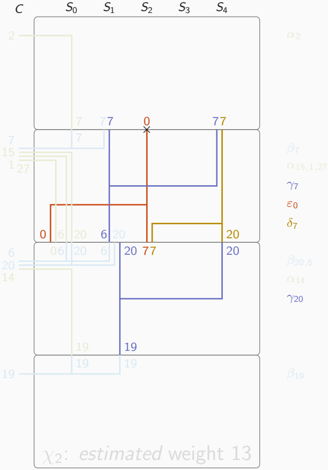


MiniMORUS-640: Building trails with χ_1 and χ_2

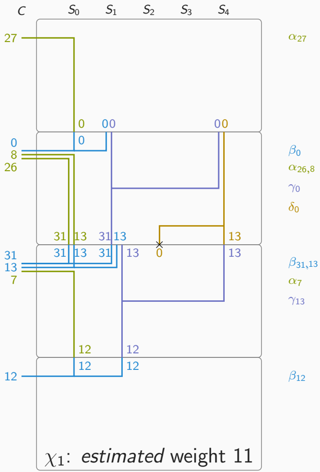


$$C_{27}^0 \oplus C_0^1 \oplus C_8^1 \oplus C_{26}^1 \oplus C_7^2 \oplus C_{13}^2 \oplus C_{31}^2 \oplus C_{12}^3 \to S_{2,0}^2$$

$$C_2^1 \oplus C_1^2 \oplus C_7^2 \oplus C_{15}^2 \oplus C_{27}^2 \oplus C_6^3 \oplus C_{14}^3 \oplus C_{20}^3 \oplus C_{19}^4 \to S_{2,0}^2$$

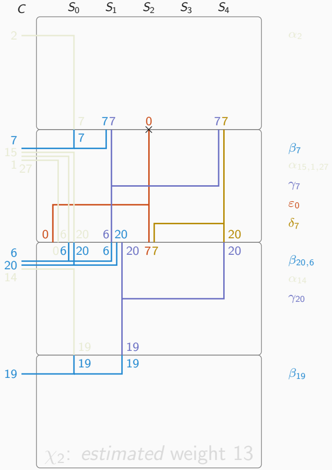


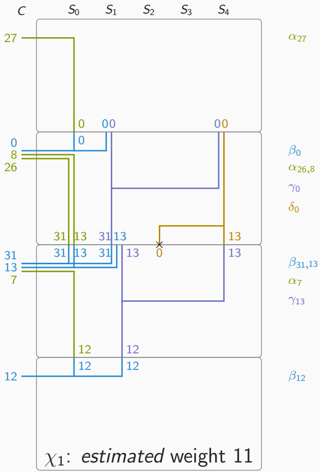
MiniMORUS-640: Building trails with χ_1 and χ_2



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

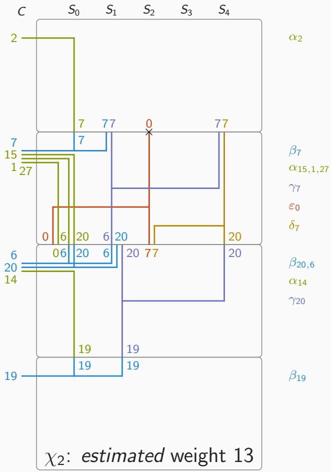
$$C^1_2 \oplus C^2_1 \oplus C^2_7 \oplus C^2_{15} \oplus C^2_{27} \oplus C^3_6 \oplus C^3_{14} \oplus C^3_{20} \oplus C^4_{19} \to S^2_{2,0}$$



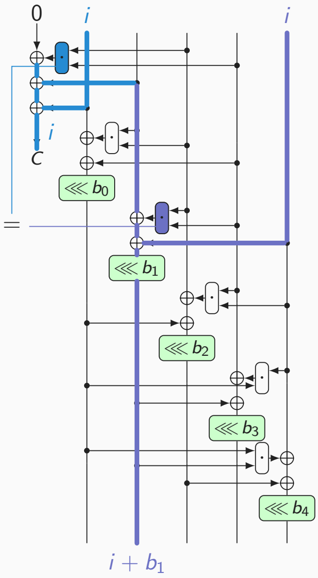


$$C^0_{27} \oplus C^1_0 \oplus C^1_8 \oplus C^1_{26} \oplus C^2_7 \oplus C^2_{13} \oplus C^2_{31} \oplus C^3_{12} \to S^2_{2,0}$$

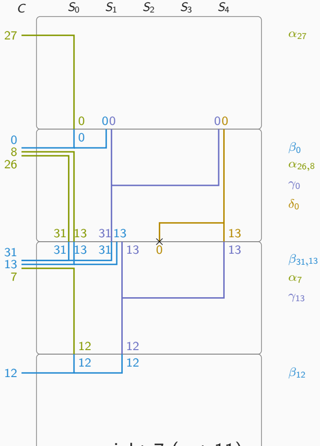
$$C^1_2 \oplus C^2_1 \oplus C^2_7 \oplus C^2_{15} \oplus C^2_{27} \oplus C^3_6 \oplus C^3_{14} \oplus C^3_{20} \oplus C^4_{19} \to S^2_{2,0}$$



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



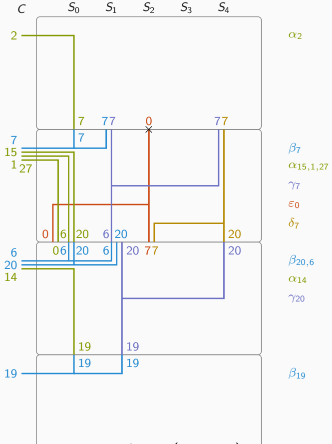
Weight of $\beta_i^t \oplus \gamma_i^t$ is 0 (not 2).



χ_1: weight 7 (not 11)

$$C_{27}^0 \oplus C_0^1 \oplus C_8^1 \oplus C_{26}^1 \oplus C_7^2 \oplus C_{13}^2 \oplus C_{31}^2 \oplus C_{12}^3 \to S_{2,0}^2$$

$$C_2^1 \oplus C_1^2 \oplus C_7^2 \oplus C_{15}^2 \oplus C_{27}^2 \oplus C_6^3 \oplus C_{14}^3 \oplus C_{20}^3 \oplus C_{19}^4 \to S_{2,0}^2$$



χ_2: weight 9 (not 13)

MiniMORUS: Final Approximation

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

- Total weight of χ: $7 + 9 = 16$.

- Experimentally verified
  - Analysis of the Algebraic Normal Form
  - Measurements on random inputs (slightly better than expected)

Application to MORUS

From MiniMORUS to MORUS

- $\square = \square + \square + \square + \square$
  $S_{i,j}$ in MiniMORUS $= S_{i,j} \oplus S_{i,j+w} \oplus S_{i,j+2w} \oplus S_{i,j+3w}$ in MORUS
- Weight $\times 4$, except $\beta_i + \gamma_i$ has weight 0 in MiniMORUS but 3 in MORUS

➔ MORUS-640: Weight $4 \times 16 + 3 \times 3 = 73 \rightarrow$ data complexity $\approx 2^{146}$ ☹

➔ MORUS-1280: Weight $4 \times 16 + 4 \times 3 = 76 \rightarrow$ data complexity $\approx 2^{152}$ 😐

- trail is immune to bit-shift: actual data complexity is about a factor of 2^5 to 2^6 lower

From MiniMORUS to MORUS

- $\square \,{=}\, \square + \square + \square + \square$
  $S_{i,j}$ in MiniMORUS $= S_{i,j} \oplus S_{i,j+w} \oplus S_{i,j+2w} \oplus S_{i,j+3w}$ in MORUS
- Weight $\times 4$, except $\beta_i + \gamma_i$ has weight 0 in MiniMORUS but 3 in MORUS

➔ MORUS-640: Weight $4 \times 16 + 3 \times 3 = 73$ $\rightarrow$ data complexity $\approx 2^{146}$ ☹

➔ MORUS-1280: Weight $4 \times 16 + 4 \times 3 = 76$ $\rightarrow$ data complexity $\approx 2^{152}$ ☺

- trail is immune to bit-shift: actual data complexity is about a factor of 2^5 to 2^6 lower

Impact for MORUS

- **Keystream correlation**
  - The bias is *independent* of Key or Nounce!
  - Known plaintext $\implies$ Distinguisher.
  - Multiple fixed plaintext $\implies$ plaintext recovery.
  - Similar to RC4, BEAST attack...
- **Data complexity**
  - Data limit 2^{64}... but correlation holds under rekeying.
  - Require 2^{141} blocks for MORUS-640
  - Require 2^{146} blocks for MORUS-1280 **(violate 256-bit confidentiality claim)**
  - Not practical ;-)

Impact for MORUS

- **Keystream correlation**
  - The bias is *independent* of Key or Nounce!
  - Known plaintext $\Longrightarrow$ Distinguisher.
  - Multiple fixed plaintext $\Longrightarrow$ plaintext recovery.
  - Similar to RC4, BEAST attack...
- **Data complexity**
  - Data limit 2^{64}... but correlation holds under rekeying.
  - Require 2^{141} blocks for MORUS-640
  - Require 2^{146} blocks for MORUS-1280 **(violate 256-bit confidentiality claim)**
  - Not practical ;-)

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