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>
<thead>
<tr>
<th></th>
<th>Confidentiality (bits)</th>
<th>Integrity (bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MORUS-640-128</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>MORUS-1280-128</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>MORUS-1280-256</td>
<td>256</td>
<td>128</td>
</tr>
</tbody>
</table>

Impose rekeying every $2^{64}$ encrypted blocks.
What is MORUS?

MORUS state:

- 5 registers of 4 words.
- MORUS-640, 32-bit words $\rightarrow$ 128-bit registers $\rightarrow$ SSE instructions.
- MORUS-1280, 64-bit words $\rightarrow$ 256-bit registers $\rightarrow$ AVX2 instructions.
What is MORUS?

\[
\begin{align*}
S^{-16} & \quad S^{-15} \\
cst & \quad f \\
\text{cst} & \quad f \\
1^* & \quad f \\
\text{Key} & \quad f \\
\text{Nonce} & \quad f \\
\end{align*}
\]

\[
\begin{align*}
S^{-1} & \quad S^0 & \quad S^1 & \quad S^2 & \quad S^3 & \quad S^4 \\
f & \quad f & \quad f & \quad f & \quad f & \quad \ldots \\
M^0 & \quad M^1 & \quad M^2 & \quad M^3 & \quad M^4 \\
C^0 & \quad C^1 & \quad C^2 & \quad C^3 & \quad C^4 \\
\end{align*}
\]
What is MORUS?

\[ S^{-16} \rightarrow f \rightarrow S^{-15} \rightarrow f \rightarrow \ldots \rightarrow f \rightarrow S^{-1} \]

\[ \text{cst} \rightarrow f \rightarrow 1^* \rightarrow f \rightarrow \text{Key} \rightarrow f \rightarrow \text{Nonce} \rightarrow f \rightarrow \ldots \]

\[ M^0 \rightarrow f \rightarrow M^1 \rightarrow f \rightarrow M^2 \rightarrow f \rightarrow M^3 \rightarrow f \rightarrow M^4 \rightarrow \ldots \]

\[ C^0 \rightarrow f \rightarrow C^1 \rightarrow f \rightarrow C^2 \rightarrow f \rightarrow C^3 \rightarrow f \rightarrow C^4 \rightarrow \ldots \]
What is MORUS?

\[ S^0 \rightarrow f \rightarrow S^1 \rightarrow f \rightarrow S^2 \rightarrow f \rightarrow S^3 \rightarrow f \rightarrow S^4 \rightarrow \ldots \]

rand() → \( S_4 \)
rand() → \( S_3 \)
rand() → \( S_2 \)
rand() → \( S_1 \)
rand() → \( S_0 \)

\[ M^0 \rightarrow C^0 \]
\[ M^1 \rightarrow C^1 \]
\[ M^2 \rightarrow C^2 \]
\[ M^3 \rightarrow C^3 \]
\[ M^4 \rightarrow C^4 \]
What is MORUS?

\[ M \preceq b_0 \preceq b_1 \preceq b_2 \preceq b_3 \preceq b_4 \preceq 3w \preceq 1w \preceq 2w \preceq 1w \preceq b_4 \]
MiniMORUS with chosen plaintext!

\[
\begin{align*}
M_0 & < b_0 \\
& < b_1 \\
& < b_2 \\
& < b_3 \\
& < b_4 
\end{align*}
\]
Linear Cryptanalysis of MiniMORUS
Weight and Bias

\[ x = u \oplus y \oplus (z \land t) \]

Can be linear approximated with

\[ E: x = u \oplus y \]

This linear approximation holds with a bias \( \varepsilon \):

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

The correlation and weight of an approximation is:

\[ \text{cor}(E) := 2 \Pr(E) - 1 = 2\varepsilon \]

\[ \text{weight}(E) := -\log_2 |\text{cor}(E)| \]

Piling 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 $\alpha, \beta, \gamma, \delta, \epsilon$

weight($\alpha_i^j$) = 1 (not 2)  
weight($\beta_i^j$) = 1  
weight($\gamma_i^j$) = 1  
weight($\delta_i^j$) = 1  
weight($\epsilon_i^j$) = 1
MiniMORUS-640: Building trails with $\chi_1$ and $\chi_2$
MiniMORUS-640: Building trails with $\chi_1$ and $\chi_2$

\[
\begin{array}{cccccc}
C & s_0 & s_1 & s_2 & s_3 & s_4 \\
27 & 0 & 0 \\
0 & 0 \\
\end{array}
\]

\[
C_0 \oplus C_1 \oplus C_2 \oplus C_3 \oplus C_4 \rightarrow S_2, 0
\]

\[
\begin{array}{cccccc}
C & s_0 & s_1 & s_2 & s_3 & s_4 \\
\alpha_{27} \\
\beta_0 \\
\end{array}
\]

$\chi_1$: estimated weight 11

$\chi_2$: estimated weight 13
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 $\chi_2$. 

\begin{align*}
C & \rightarrow S_{22}, 0 \\
& \alpha_{27} \\
& \beta_9 \\
& \alpha_{26,8} \\
& \gamma_0 \\
& \delta_0 \\
& \beta_{31,13} \\
& \gamma_{13}
\end{align*}
MiniMORUS-640: Building trails with $\chi_1$ and $\chi_2$
MiniMORUS-640: Building trails with $\chi_1$ and $\chi_2$. 

$C, S_0, S_1, S_2, S_3, S_4$ 

$\alpha_27, \beta_9, \gamma_0, \delta_0, \beta_{31,13}, \alpha_7, \gamma_{13}, \beta_{12}$
MiniMORUS-640: Building trails with $\chi_1$ and $\chi_2$

$\chi_1$: estimated weight 11

$C_{27}^0 \oplus C_0^1 \oplus C_8^1 \oplus C_{26}^1 \oplus C_7^2 \oplus C_{13}^2 \oplus C_{31}^2 \oplus C_{12}^2 \rightarrow S_{2,0}^2$
MiniMORUS-640: Building trails with $\chi_1$ and $\chi_2$

$\chi_1$: estimated weight 11

$C_{27}^0 \oplus C_0^1 \oplus C_6^1 \oplus C_{26}^1 \oplus C_7^2 \oplus C_{13}^3 \oplus C_{31}^4 \oplus C_{12}^5 \rightarrow S_{2,0}^4$
MiniMORUS-640: Building trails with $\chi_1$ and $\chi_2$

$\chi_1$: estimated weight 11

$C_{27}^0 \oplus C_0^1 \oplus C_8^1 \oplus C_{26}^1 \oplus C_7^2 \oplus C_{13}^2 \oplus C_{31}^2 \oplus C_{32}^0 \rightarrow S_{2,0}^2$
MiniMORUS-640: Building trails with $\chi_1$ and $\chi_2$

\[ C_0^0 \oplus C_1^0 \oplus C_6^1 \oplus C_{26}^1 \oplus C_{13}^2 \oplus C_{31}^2 \oplus C_{12}^3 \rightarrow S_{2,0}^2 \]
MiniMORUS-640: Building trails with $\chi_1$ and $\chi_2$

$\chi_1$: estimated weight 11

$C^0_{27} \oplus C^1_0 \oplus C^1_6 \oplus C^1_{26} \oplus C^2_7 \oplus C^2_{13} \oplus C^2_{31} \oplus C^2_{12} \rightarrow S^2_{2,0}$
MiniMORUS-640: Building trails with $\chi_1$ and $\chi_2$

$\chi_1$: estimated weight 11

$C_0^{27} \oplus C_1^0 \oplus C_6^1 \oplus C_{26}^1 \oplus C_7^2 \oplus C_{13}^2 \oplus C_{31}^3 \oplus C_{12}^4 \rightarrow S_{2,0}^2$

$\chi_2$: estimated weight 13

$C_2^1 \oplus C_1^2 \oplus C_7^2 \oplus C_{15}^2 \oplus C_{27}^3 \oplus C_6^3 \oplus C_{14}^3 \oplus C_{20}^3 \oplus C_{19}^4 \rightarrow S_{2,0}^2$
MiniMORUS: Weight of $\beta_i^t \oplus \gamma_i^t$

Weight of $\beta_i^t \oplus \gamma_i^t$ is 0 (not 2).
\[ C^0_{27} \oplus C^1_0 \oplus C^1_6 \oplus C^2_{26} \oplus C^2_7 \oplus C^3_{13} \oplus C^3_{31} \oplus C^3_{12} \rightarrow S^2_{2,0} \]

\[ C^1_2 \oplus C^2_1 \oplus C^2_7 \oplus C^3_{15} \oplus C^3_{27} \oplus C^3_6 \oplus C^3_{14} \oplus C^3_{20} \oplus C^4_{19} \rightarrow S^2_{2,0} \]
MiniMORUS: Full Trail

- MiniMORUS-640

\[ \chi_1 \oplus \chi_2 = C_{27}^0 \oplus C_0^1 \oplus C_2^1 \oplus C_8^1 \oplus C_{26}^1 \oplus C_1^2 \oplus C_{13}^1 \oplus C_{15}^2 \oplus C_{27}^2 \oplus C_{31}^2 \oplus C_6^3 \oplus C_{12}^3 \oplus C_{14}^3 \oplus C_{20}^3 \oplus C_{19}^4 \rightarrow 0 \]

- MiniMORUS-1280

\[ C_{51}^0 \oplus C_0^1 \oplus C_{25}^1 \oplus C_{33}^1 \oplus C_{55}^1 \oplus C_4^2 \oplus C_7^2 \oplus C_{29}^2 \oplus C_{37}^2 \oplus C_{38}^2 \oplus C_{46}^2 \oplus C_{51}^2 \oplus C_{11}^3 \oplus C_{20}^3 \oplus C_{42}^3 \oplus C_{50}^3 \oplus C_{24}^4 \rightarrow 0 \]

In both cases, the weight of the trail is \(7 + 9 = 16\).
## MiniMORUS: Experimental verification

### Approximations for MiniMORUS-640

<table>
<thead>
<tr>
<th>( \chi )</th>
<th>( S_{0,2}^2 )</th>
<th>Weight</th>
<th>Exp.</th>
<th>Bool.</th>
<th>Meas.</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \chi_1 )</td>
<td>( S_{0,2}^2 = C_0^0 \oplus C_{0,8,26}^1 \oplus C_{7,13,31}^2 \oplus C_{12}^3 )</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>( \chi_2 )</td>
<td>( S_{0,2}^2 = C_2^1 \oplus C_{1,7,15,27}^2 \oplus C_{19}^3 \oplus C_{14,20}^4 )</td>
<td>9</td>
<td>9</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>( \chi )</td>
<td>( 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 )</td>
<td>16</td>
<td>16</td>
<td>15.5</td>
<td></td>
</tr>
</tbody>
</table>

### Approximations for MiniMORUS-1280

<table>
<thead>
<tr>
<th>( \chi )</th>
<th>( S_{0,2}^2 )</th>
<th>Weight</th>
<th>Exp.</th>
<th>Bool.</th>
<th>Meas.</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \chi_1 )</td>
<td>( S_{0,2}^2 = C_{51}^0 \oplus C_{0,33,55}^1 \oplus C_{4,37,46}^2 \oplus C_{50}^3 )</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>( \chi_2 )</td>
<td>( S_{0,2}^2 = C_{25}^1 \oplus C_{7,29,38,51}^2 \oplus C_{11,20,42}^3 \oplus C_{24}^4 )</td>
<td>9</td>
<td>9</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>( \chi )</td>
<td>( 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 )</td>
<td>16</td>
<td>16</td>
<td>15.9</td>
<td></td>
</tr>
</tbody>
</table>

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

\[ \text{e.g. } S_{2,0} \text{ in MiniMORUS-1280 } \iff S_{2,0} \oplus S_{2,64} \oplus S_{2,128} \oplus S_{2,192} \text{ in MORUS-1280.} \]

▶ Weight implication:
word “equality” occurs with probability $\frac{1}{2^4} \implies \text{weight } \times 4$

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

Weight of the trails

<table>
<thead>
<tr>
<th>Trail</th>
<th>Weight of $\chi$</th>
</tr>
</thead>
<tbody>
<tr>
<td>MORUS-640</td>
<td>$\text{Weight}(\chi) = 73$</td>
</tr>
<tr>
<td>MORUS-1280</td>
<td>$\text{Weight}(\chi) = 76$</td>
</tr>
</tbody>
</table>
Impact for MORUS

Keystream correlation

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

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