Exact MEDP/MELP for «heavy» 2R-SPN

Vitaly Kiryukhin, Anton Naumenko

JSC «InfoTeCS»

Fast Software Encryption – March 27, 2019
«Heavy» 2-round SPN

- $m$-bit bijective Sbox, $m \geq 8$
- Block size $n \cdot m \geq 64$ bits
- Branch number $B_d = n + 1$

Typical example: Khazad and Kuznyechik
2-round trail and differential

$\Delta x$

$\Delta_1$

$L$

$\Delta_2$

$\Delta y$
2-round trail and differential

\[ \Omega = \Delta x \xrightarrow{S} \Delta_1 \xrightarrow{L} \Delta_2 \xrightarrow{S} \Delta y - \text{2-round differential trail} \]

\[ EDCP(\Omega) = \prod_{i=1}^{n} DP(\Delta x[i] \rightarrow \Delta_1[i]) \cdot \prod_{i=1}^{n} DP(\Delta_2[i] \rightarrow \Delta y[i]) \]

\[ DIFF(\Delta x, \Delta y) = \{ \Omega : \Omega = \Delta x \rightarrow \ldots \rightarrow \Delta y \} \]

\[ EDP(\Delta x, \Delta y) = \sum_{\Omega \in DIFF(\Delta x, \Delta y)} EDCP(\Omega) \]

\[ MEDP = \max_{DIFF(\Delta x, \Delta y)} \sum_{\Omega \in DIFF(\Delta x, \Delta y)} EDCP(\Omega) \]
How to compute the exact MEDP?

- compute exact MEDP of minimum-weight \((B_d = n + 1)\) differentials
- compute the upper bound on non-minimum-weight differentials
- If the first is greater than the second then we have exact MEDP of 2R-SPN
Upper bound on non-minimum-weight differentials

We design dynamic programming algorithm for bounding non-minimum-weight differentials in 2R-SPN.

The algorithm uses only:
– difference distribution table of the Sbox
– $B_d$ – the value of the branch number
Example: 2R-Khazad

<table>
<thead>
<tr>
<th>FSE2003 Bound</th>
<th>Exact 2R-MEDP</th>
<th>Bound on non-min-weight differential</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^{-43.36}$</td>
<td>$2^{-45} + 2^{-60}$</td>
<td>$2^{-45.02}$</td>
</tr>
</tbody>
</table>

Example of one of the best 2R-differentials

<table>
<thead>
<tr>
<th>$\Delta x$</th>
<th>$f0001208000f0000$</th>
<th>$\log_2 EDCP(\Omega_i)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\Omega_1$</td>
<td>$f0001248000f0000$</td>
<td>$b54800004800fbeb$ -45</td>
</tr>
<tr>
<td>$\Omega_2$</td>
<td>$0a00c80700230000$</td>
<td>$13070000070053a6$ -60</td>
</tr>
<tr>
<td>$\Delta y$</td>
<td>$bf08000008001891$</td>
<td></td>
</tr>
</tbody>
</table>
Thank you for attention!

Questions?