MILP-aided cryptanalysis of symmetric ciphers

Zahra Ahmadian

Department of Electrical Engineering
Shahid Beheshti University

ISCwsISC 2020, Tehran, Iran @ January 21, 2020
Outline

• What is MILP?

• Application of MILP in cryptanalysis of symmetric primitives,

• How to model the problem of searching optimum truncated differential characteristic,

• Application to Midorri, SKINNY and CRAFT block ciphers,

• Future work.
What is MILP?

• Mixed Integer Linear Programing (MILP) is a well known class of optimization problems:

\[
\begin{align*}
\text{minimize} & \quad c^T x \\
\text{subject to} & \quad Ax \leq b \\
\text{and} & \quad x \geq 0
\end{align*}
\]
• MILP problem is inherently an **NP-complete** problem, however there are either commercial or open source **solvers**, able to solve some MILP instances which are not too complicated.

• A recent trend in symmetric cryptanalysis is using this tool for **automatic** finding **(sub-)optimal** (differential, linear, integral, cube, etc.) **characteristics** for symmetric primitives.
Linear and Differential attacks family

• Automatic finding the optimum bit-wise differential (linear) characteristic
  – With the objective of minimizing the number of active sbox
  – With the objective of maximizing the characteristic probability (correlation)
  – Efficient and distinct methods have been developed for $4 \times 4$ Sboxes and $8 \times 8$ Sboxes

• Automatic finding impossible differential and zero correlation characteristics

• What about truncated differential?
  – just as a facilitator to find the optimal bit-wise differential characteristic
  – as a tool for finding the impossible differential characteristic
Truncated differential attack by MILP

- **No systematic method to prove** an upper bound for its probability.

- **No MILP model** for automatic search of the optimal truncated differential characteristic.
  - The only automatic search algorithm is an exhaustive-type one, dating back two decades [MSA99].

- **We propose an MILP model which efficiently finds** the highest probability truncated differential characteristic.
Summery of our results

- Bit-wise differential characteristic v.s. truncated differential characteristic

### Midorri64

<table>
<thead>
<tr>
<th># rounds</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit-wise characteristic</td>
<td>$2^{-32}$</td>
<td>$2^{-46}$</td>
<td>$2^{-60}$</td>
<td>[BBI14]</td>
</tr>
<tr>
<td>Truncated characteristic</td>
<td>$2^{-44}$</td>
<td>-</td>
<td>-</td>
<td>[DS16]</td>
</tr>
<tr>
<td>Truncated characteristic</td>
<td>$2^{-12}$</td>
<td>$2^{-24}$</td>
<td>$2^{-52}$</td>
<td>This work</td>
</tr>
</tbody>
</table>

### SKINNY 64/X

<table>
<thead>
<tr>
<th># rounds</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit-wise characteristic</td>
<td>$2^{-32}$</td>
<td>$2^{-52}$</td>
<td>$2^{-72}$</td>
<td>$2^{-82}$</td>
<td>$2^{-92}$</td>
<td>[BJK16]</td>
</tr>
<tr>
<td>Truncated characteristic</td>
<td>$2^{-4}$</td>
<td>$2^{-4}$</td>
<td>$2^{-8}$</td>
<td>$2^{-20}$</td>
<td>$2^{-40}$</td>
<td>This work</td>
</tr>
</tbody>
</table>

### CRAFT

<table>
<thead>
<tr>
<th># rounds</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit-wise characteristic</td>
<td>$2^{-52}$</td>
<td>$2^{-64}$</td>
<td>$2^{-72}$</td>
<td>$2^{-80}$</td>
<td>$2^{-88}$</td>
<td>[BLM19]</td>
</tr>
<tr>
<td>Bit-wise differential</td>
<td>-</td>
<td>$2^{-54.67}$</td>
<td>$2^{-62.61}$</td>
<td>-</td>
<td>-</td>
<td>[BLM19]</td>
</tr>
<tr>
<td>Truncated characteristic</td>
<td>$2^{-4}$</td>
<td>$2^{-20}$</td>
<td>$2^{-24}$</td>
<td>$2^{-32}$</td>
<td>$2^{-36}$</td>
<td>This work</td>
</tr>
</tbody>
</table>

Target Ciphers

• Middori
Target Ciphers

- Middori
  - AddRoundKey
Target Ciphers

- Middori
  - AddRoundKey
  - SubCell
Target Ciphers

- Middori
  - AddRoundKey
  - SubCell
  - ShuffleCell
Target Ciphers

- Middori
  - AddRoundKey
  - SubCell
  - ShuffleCell
  - MixColumn

\[ M = \begin{pmatrix}
0 & 1 & 1 & 1 \\
1 & 0 & 1 & 1 \\
1 & 1 & 0 & 1 \\
1 & 1 & 1 & 0
\end{pmatrix} \]
Target Ciphers

- SKINNY
Target Ciphers

- **SKINNY**
  - SubCell
Target Ciphers

- SKINNY
  - SubCell
  - AddConstant
  - AddRoundTweakey
Target Ciphers

• SKINNY
  – SubCell
  – AddConstant
  – AddRoundTweakey
  – ShiftRows
Target Ciphers

• SKINNY
  – SubCell
  – AddConstant
  – AddRoundTweakey
  – ShiftRows
  – MixColumn

\[ M = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix} \]
Target Ciphers

- **CRAFT**

MILP-aided cryptanalysis of symmetric ciphers
Target Ciphers

- **CRAFT**
  - MixCoulmn

\[ M = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \]
Target Ciphers

- CRAFT
  - MixColumn
  - AddConstant
  - AddTweakey

\[ M = \begin{pmatrix}
1 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
\end{pmatrix} \]
Target Ciphers

- **CRAFT**
  - MixColumn
  - AddConstant
  - AddTweakey
  - PermuteNibbles

\[ M = \begin{pmatrix}
1 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
\end{pmatrix} \]
Target Ciphers

- CRAFT
  - MixColumn
  - AddConstant
  - AddTweakey
  - PermuteNibbles
  - SubBox

\[ M = \begin{pmatrix}
1 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
\end{pmatrix} \]
How to model truncated differential?

- Variables of MILP model:
  - word-wise, where the word size is the S-box size in the cipher 😊
  - binary-values, indicating that the associated word is active (1) or inactive (0).

- Different layers in differential attack:
  - Add constants/round keys/tweakeys layer → **effectless**
  - S-box layer → **bypassed 😊**
  - ShuffleCell, ShiftRows and PermuteNibbles → **variable change**

- So, only the **MixColumn layer** plays the key role in both the propagation pattern and the probability of the truncated characteristic.
MILP model for MixColumn

- **Cipher state**: a $k \times k$ matrix of $m$-bit words.
- **MixColumn matrix**: a $k \times k$ matrix $M$ over $GF(2^m)$
- For a single MixColumn, the input and output differences are $x = (x_0, x_1, ..., x_{k-1})^T$ and $y = (y_0, y_1, ..., y_{k-1})^T$
MILP model for MixColumn

- **Definition.** The *Branching property table* of $M$ is a table of size $2^k \times 2^k$ in which the $(x, y)^{th}$ entry is $-\log_2 P(x \rightarrow y)$.

- The possible values, with a good approximation fall into the set:

$$\{0, 1, 2^{-m}, 2^{-2m}, \ldots, 2^{-(k-1)m}\}$$
The Branching property table of CRAFT

<table>
<thead>
<tr>
<th>in/out</th>
<th>0x0</th>
<th>0x1</th>
<th>0x2</th>
<th>0x3</th>
<th>0x4</th>
<th>0x5</th>
<th>0x6</th>
<th>0x7</th>
<th>0x8</th>
<th>0x9</th>
<th>0xa</th>
<th>0xb</th>
<th>0xc</th>
<th>0xd</th>
<th>0xe</th>
<th>0xf</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0x1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0x2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0x3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0x4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0x5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0x6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0x7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0x8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0x9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0xa</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0xbb</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0xc</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0xd</td>
<td>0</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0xe</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0xf</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

\[ M = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \]
The Branching property table of CRAFT

<table>
<thead>
<tr>
<th>in/out</th>
<th>0x0</th>
<th>0x1</th>
<th>0x2</th>
<th>0x3</th>
<th>0x4</th>
<th>0x5</th>
<th>0x6</th>
<th>0x7</th>
<th>0x8</th>
<th>0x9</th>
<th>0xa</th>
<th>0xb</th>
<th>0xc</th>
<th>0xd</th>
<th>0xe</th>
<th>0xf</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0x1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0x2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0x3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0x4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0x5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0x6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0x7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0x8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0x9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0xa</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0xb</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0xc</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0xd</td>
<td>0</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0xe</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0xf</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

\[
\begin{bmatrix}
1 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{bmatrix}
\begin{bmatrix}
0 \\
x_1 \\
x_2 \\
x_3
\end{bmatrix}
= 
\begin{bmatrix}
x_2 + x_3 \\
x_1 + x_3 \\
x_2 \\
x_3
\end{bmatrix}
= 
\begin{bmatrix}
y_0 \\
0 \\
y_2 \\
y_3
\end{bmatrix}
\]

\[
M = 
\begin{pmatrix}
1 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{pmatrix}
\]

\[
P((0,1,1,1) \rightarrow (1,0,1,1)) = P(x_1 = x_3) = 2^{-4}
\]
The method is very similar to the Sun et al.’s method for modeling 4-bit S-boxes [SHW14]:

1. Extract the possible differences of BPT along with their probabilities encoded.

\[(x_0, \ldots, x_{k-1}, y_0, \ldots, y_{k-1}, p_0, \ldots, p_{t-1})\]

\[
\begin{align*}
2^0 & \rightarrow (0,0) \\
2^{-4} & \rightarrow (1,0) \\
2^{-8} & \rightarrow (0,1)
\end{align*}
\]
2. Then, using SAGE computer algebra:
   
   – **Input:** All feasible points
   
   – **Output:** The convex hull of the input points (= the set of linear constraints in MILP model)

3. Refine the constraints to find a small subset of them, presenting the convex hull, using the *greedy* algorithm by Sun et al. [SHW14].
• The objective function is:

\[ d = \sum_{\text{All MixCols}} \sum_{i=0}^{t-1} p_i 2^i \]

• Where the truncated differential characteristic probability simply is:

\[ P_T = 2^{-m.d} \]
Efficient characteristic

- Must be able to distinguish the cipher from a Pseudo Random Permutation (PRP).

- Therefore,

\[ P^E(\Delta_{in} \rightarrow \Delta_{out}) > P^{PRP}(\Delta_{in} \rightarrow \Delta_{out}) = \frac{|\Delta_{out}|}{2^n} \]

where \( n \) is the block size of the cipher in bits, here \( n = 2^k m \).
Efficient characteristic

• For precise enumeration of $|\Delta_{out}|$, count the number of active words in the last S-box layer:

$$|\Delta_{out}| = 2^m \cdot \text{Hw}(\Delta_{out}^S)$$

• For example, for 6-round Middori:

$$|\Delta_{out}| = 2^m \cdot \text{Hw}(\Delta_{out}^S) = 2^{4\times2} = 2^8$$
Efficient characteristic

- The **distinguishability constraint** in the MILP model:

\[ P_{E'} > P_{PRP} \]

\[ 2^{-m.d'} > 2^{m.k^2-m.Hw(Δ^S_{out})} \]

\[ d' < k^2 - Hw(Δ^S_{out}) \]

- Where \( P_{E'} = 2^{-m.d'} \) is the probability of the characteristic up to the last S-box Layer and

\[ d' = \sum_{\text{MixCols up to last Sbox}} \sum_{i=0}^{t-1} p_i 2^i \]

- To avoid a fully active output state characteristic: \( Hw(Δ_{out}) < k^2 \)
Application to Middori, SKINNY and CRAFT

- 4, 5 and 6-round truncated differential characteristic for Midori64
• 8, 9, 10-round truncated differential characteristics for SKINNY64/X.
Application to Middori, SKINNY and CRAFT

• 10, 11 and 12 round truncated differential characteristics for CRAFT
Application to Middori, SKINNY and CRAFT

- 10, 11 and 12 round truncated differential characteristics for CRAFT
Application to Middori, SKINNY and CRAFT

- 10, 11 and 12 round truncated differential characteristics for CRAFT
Future work

• Modeling with precise values of the probabilities of BPT.

• Experiments shows that the truncated differential probability is much higher than the truncated characteristic probability.
  – How to find the optimum truncated differential?

• This model, (and all the other MILP models) optimizes the probability of the truncated distinguisher. The highest probability distinguisher does not necessarily construct the optimum key recovery attack.
  – How to extend the MILP model, in such a way to optimize the complexity of the key recovery attack?
References


