Dedicated Cryptanalysis of Lightweight Block Ciphers

María Naya-Plasencia
INRIA, France

Šibenik 2014
Outline

- Introduction
- Impossible Differential Attacks
- Meet-in-the-middle and improvements
- Multiple Differential Attacks
- Dedicated attacks (examples)
Introduction

Dedicated attacks (examples):

- Importance of dedicated attacks: PRINTcipher
- Importance of reduced-round attacks: KLEIN-64
Importance of Dedicated Cryptanalysis
Lightweight Dedicated Analysis

- Lightweight: more 'risky' design, lower security margin, simpler components.

- Often innovative constructions: dedicated attacks
Normally, designers should have already analyzed the cipher with respect to known attacks...

...though not always!, or not always that straight-forward.

Dedicated attacks: New!
PRESENT and PRINTcipher
One of the most popular ciphers, proposed in 2007, and now ISO/IEC standard is PRESENT.

Very large number of analysis published (over 20).

Best attacks so far: multiple linear attacks (26r/31r).
Block $n = 64$ bits, key 80 or 128 bits.

31 rounds + 1 key addition.
Linear cryptanalysis: because of the Sbox, a linear approximation 1 to 1 with bias $2^{-3}$ per round [Ohk.'09].

- Multiple linear attacks: consider several possible approxs simultaneously $\Rightarrow$ up to 26 rounds out of 31 [Cho’10].
Many PRESENT-like ciphers proposed: Maya, Puffin, PRINTcipher

Usually, weaker than the original.

PRINTcipher[KLPR’10]: first cryptanalysis: invariant subspace attack[LAAZ’11].
PRINTcipher

48 rounds.
With probability 1:

Not a key recovery, but a very bad property for $2^{51}$ weak keys...
KLEIN-64: from reduced-round to full-version
KLEIN-64 with 12 rounds.

- **AddRoundKey**
- **SubNibbles**
- **RotateNibbles**
- **MixNibbles**

64-bit plaintext

1 round

64-bit ciphertext

KLEIN [GNL’11]
SubNibbles

\[
\begin{array}{cccccccccccccccc}
\times & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & a & b & c & d & e & f \\
S[x] & 7 & 4 & a & 9 & 1 & f & b & 0 & c & 3 & 2 & 6 & 8 & e & d & 5 \\
\end{array}
\]
RotateNibbles
MixNibbles
### Previous Cryptanalysis

<table>
<thead>
<tr>
<th>Version</th>
<th>Source</th>
<th>Rounds</th>
<th>Data</th>
<th>Time</th>
<th>Memory</th>
<th>Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>KLEIN-64</td>
<td>[Yu, Wu, Li, Zhang, <em>Inscrypt11</em>]</td>
<td>7</td>
<td>$2^{34.3}$</td>
<td>$2^{45.5}$</td>
<td>$2^{32}$</td>
<td>integral</td>
</tr>
<tr>
<td></td>
<td>[Yu, Wu, Li, Zhang, <em>Inscrypt11</em>]</td>
<td>8</td>
<td>$2^{32}$</td>
<td>$2^{40.8}$</td>
<td>$2^{16}$</td>
<td>truncated</td>
</tr>
<tr>
<td></td>
<td>[Aumasson, Naya-Plasencia, Saarinen, <em>Indocrypt11</em>]</td>
<td>8</td>
<td>$2^{35}$</td>
<td>$2^{35}$</td>
<td>-</td>
<td>differential</td>
</tr>
<tr>
<td></td>
<td>[Nikolic, Wang, Wu, <em>ePrint iacr 2013</em>]</td>
<td>10</td>
<td>1</td>
<td>$2^{62}$</td>
<td>$2^{60}$</td>
<td>mitm</td>
</tr>
<tr>
<td></td>
<td>[Ahmadian, Salmasizadeh, Reza Aref, <em>ePrint iacr 2013</em>]</td>
<td>12</td>
<td>$2^{39}$</td>
<td>$2^{62.84}$</td>
<td>$2^{4.5}$</td>
<td>biclique</td>
</tr>
</tbody>
</table>
Main Ideas From Previous Analysis

► All layers except MixNibbles do not mix higher nibbles with lower nibbles.

► MixColumn: inactive higher nibbles input $\Rightarrow$ same output pattern if the MSB of the 4 LN differences are equal ($2^{-3}$).
Main Ideas From Previous Analysis

- **KeySchedule algorithm**: lower nibbles and higher nibbles are not mixed.
7-round attack

- Truncated differential path of probability $2^{-28.08} < 2^{-32}$,
- 64-bit key recovered with $2^{33}$ operations.

```
PlTxt | SN | RN | MN | SN | RN | MN | SN | RN | MN | SN | RN | MN | SN | RN | MN | SN | RN | MN | SN | RN | MN | SN | RN | MN |
-----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
1    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
2    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
3    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
4    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
5    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
6    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
7    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
CTxt |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
```
7-round attack

1. Generate data
2. Keep the pairs with $MN^{-1}(CTxt)$ that have higher nibbles inactive
3. Guess the lower nibbles of the key
4. Test it by checking the difference obtained when inverting MN of round 6
7-round attack

- Last round condition for a random pair $2^{-32} < 2^{-28.08}$. 
  $\Rightarrow$ a pair with HN inactive difference in last round is a conforming one.

- Each conforming pair gives a 6-bit filter.

- Repeating the procedure, we can recover the correct value for the LN of the key.
New Attack [LNP’14]

- Use more MixNibble steps to discard more keys.

We want the difference output at the previous MN

- invert an entire LN round in values and diff.
- need only lower (key) nibbles to invert RN, SN and ARK.
- how to invert MN?
Inverting one $MixColumn^{-1}(a, b, c, d)$

- Let $a = (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7)$ be the binary decomposition of a byte.
- Given the input lower nibbles, we require 3 information bits from the higher nibbles:

$$\begin{cases}
  a_1 + a_2 + b_2 + c_0 + c_1 + c_2 + d_0 + d_2 \\
  a_1 + b_0 + b_1 + c_1 + d_0 + d_1 \\
  a_0 + a_1 + a_2 + b_0 + b_2 + c_1 + c_2 + d_2
\end{cases}$$

$\Rightarrow$ a 6-bit guess per round
Inverting one round

Compute the LN state and check the difference shape by inverting MN (a certain probability).

\[ \Rightarrow 2^6 \text{ computations.} \]

In the iterative part (probability \(2^{-6}\)), just one guess remains.
12 rounds of KLEIN-64

<table>
<thead>
<tr>
<th>layer</th>
<th>input</th>
<th>output</th>
<th>probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>PlTxt</td>
<td>SN</td>
<td>2^{-16}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RN</td>
<td>2^{-36}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MN</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>SN</td>
<td>2^{-13}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RN</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>MN</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>SN</td>
<td>2^{-20}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RN</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>MN</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>SN</td>
<td>2^{-6}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RN</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>MN</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>SN</td>
<td>2^{-6}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RN</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>MN</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>SN</td>
<td>2^{-6}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RN</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>MN</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>SN</td>
<td>2^{-6}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RN</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>MN</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td>SN</td>
<td>2^{-6}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RN</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>MN</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td>SN</td>
<td>2^{-6}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RN</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>MN</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td>SN</td>
<td>2^{-6}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RN</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>MN</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td>SN</td>
<td>2^{-6}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RN</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>MN</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td>SN</td>
<td>2^{-32}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RN</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>MN</td>
<td></td>
</tr>
</tbody>
</table>

CTxt
Generate enough data (path probability $2^{-69.5}$). Keep pairs with higher nibbles inactive before the last MN.

For each iterative rounds:
- LN key guess and first round to discard some.
- Invert round by round with a 6-bit guess and check if the difference obtained before MN is as wanted: 1 guess over $2^6$ remains.
First rounds to discard candidates

- At the end of the attack, $2^8$ candidates remain.

- Higher nibbles search discards the bad ones.

- Other differential paths are possible, offering different trade-offs data/time/memory.
Some Improvements

- Use structures to limit data complexity.

- Invert MN with a $2^4$ complexity (instead of $2^6$).

- Use MixColumn independence to reduce the cost of the lower nibbles key guess in the first round.

- Higher nibbles search can be speeded up using the information from the 6-bit guesses.
### Attack Complexities on KLEIN-64

<table>
<thead>
<tr>
<th>Case</th>
<th>Data</th>
<th>Time</th>
<th>Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$2^{54.5}$</td>
<td>$2^{57}$</td>
<td>$2^{16}$</td>
</tr>
<tr>
<td>2</td>
<td>$2^{56.5}$</td>
<td>$2^{62}$</td>
<td>$2^{4}$</td>
</tr>
<tr>
<td>3</td>
<td>$2^{35}$</td>
<td>$2^{63.8}$</td>
<td>$2^{32}$</td>
</tr>
<tr>
<td>4</td>
<td>$2^{46}$</td>
<td>$2^{62}$</td>
<td>$2^{16}$</td>
</tr>
</tbody>
</table>
KLEIN results

- First attack on full KLEIN-64.

- Verified experimentally on reduced-round versions (first practical attack on 9 rounds).

- Permits reaching 13 rounds over 16 of KLEIN-80 and 14 rounds over 20 of KLEIN-96.
Conclusion
To Sum Up

▶ Classical attacks, but also new dedicated ones exploiting the originality of the designs.

▶ Importance of reduced-round analysis to re-think security margin, or as first steps of further analysis.

▶ A lot of ciphers to analyze/ a lot of work to do!

---

1Thank you to Valentin Suder, Virginie Lallemand and Christina Boura for their help with the figures