More Accurate Differential Properties of LED64 and Midori64

Ling Sun\textsuperscript{1,2}, Wei Wang\textsuperscript{1}, Meiqin Wang\textsuperscript{1}

1. Shandong University, Jinan, China
2. Nanyang Technological University, Singapore

FSE 2019, Paris, France © March 25, 2019
Outline

Background & Contribution

Preliminaries

Automatic Search of Differentials

Differential Analysis of the LED64 Block Cipher

Differentials of Midori64 Considering Key-Schedule

Conclusion
Background & Contribution

Differential Cryptanalysis

- Most fundamental techniques Biham and Shamir @ CRYPTO 1990
- More accurate distribution of the fixed-key differential probability

Automatic Search

- Automatic tools for the search of differential trails or differentials

Essential Problems

- Fixed-key probability of a differential trail
- Fixed-key probability of a differential when multiple trails are available
- Weak-key ratio of the differential distinguisher

Contribution

- Automatic method based on SAT for the search of differentials
- Automatically search for right pairs of the STEP functions of LED64
  - Improved differential attacks
- Models for the estimation of the weak-key space of a differential
  - Applying to the analysis of Midori64
Outline

Background & Contribution

Preliminaries

Automatic Search of Differentials

Differential Analysis of the LED64 Block Cipher

Differentials of Midori64 Considering Key-Schedule

Conclusion
Preliminaries

Differential Cryptanalysis

- An $r$-round differential characteristic/trail $C = (C_0, C_1, \ldots, C_r)$.
- The differential probability (DP) of a differential $(\alpha, \beta)$ is
  \[ \text{DP}_f(\alpha, \beta) = \frac{\{x \in \mathbb{F}_2^n \mid f(x) \oplus f(x \oplus \alpha) = \beta\}}{2^n}. \]
  For a keyed function $f(\cdot, k)$: $\text{DP}_f[k](\alpha, \beta)$ & $\text{DP}_f[k](C)$
- Expected differential probability (EDP):
  \[ \text{EDP}_f(\alpha, \beta) = \text{mean}_{k \in K} \left( \text{DP}_f[k](\alpha, \beta) \right). \]
- The weight of a differential or a trail:
  \[ -\log_2 (\text{EDP}_f(\alpha, \beta)). \]
A Markov cipher is an iterative cipher for which the average differential probability over one round is independent of the input of the round function.

With the assumption of independent round keys, we have

\[
EDP_f(C) = \prod_{i=1}^{r} EDP_{f_i}(C_{i-1}, C_i),
\]

\[
EDP_f(\alpha, \beta) = \sum_{C_0=\alpha, C_r=\beta} EDP_f(C).
\]

Since Markov cipher is an ideal primitive, the EDP may deviate from the real differential probability.

Hypothesis of Stochastic Equivalence

For all differentials \((\alpha, \beta)\), it holds that for most values of the key \(k\),

\[
DP_f[k](\alpha, \beta) = EDP_f(\alpha, \beta).
\]
Theorem 1 (Daemen and Rijmen @ 2007)

In a key-alternating cipher $f(\cdot, k)$, the fixed-key cardinality $N_f[k](\alpha, \beta)$ of a differential $(\alpha, \beta)$ is a stochastic variable with the following distribution:

$$\Pr(N_f[k](\alpha, \beta) = i) \approx \text{Poisson}(i; 2^{n-1}\text{EDP}(\alpha, \beta)),$$

where the distribution function measures the probability over all possible values of the key and all possible choices of the key schedule.

- Since the key-alternating cipher is an abstract of the real cipher, the distribution might not fit the real one, entirely.
- We call the keys fulfilling $N[k](\alpha, \beta) \geq 2^{n-1}\text{EDP}(\alpha, \beta)$ the weak-keys.
- The set of weak-keys is denoted as $W_K(\alpha, \beta)$. 
Outline

Background & Contribution

Preliminaries

Automatic Search of Differentials

Differential Analysis of the LED64 Block Cipher

Differentials of Midori64 Considering Key-Schedule

Conclusion
Automatic Search of Differentials

Main Idea

SAT Problem

- The boolean satisfiability problem (SAT) considers the satisfiability of a given Boolean formula.
- Cryptominisat
  - Compatible with the XOR operation
  - The usage of searching for multiple solutions

![Diagram showing the flow of data from P-layer, S-layer, and Objective Function to the SAT Solver, then to CNF, Trail, and finally to Differential.](image)
The number of solutions handled by the solver is determined by the individual SAT problem.

According to our experience, $2^{32}$ is an upper-bound.

The crucial problem is how to use these trails to conduct differential cryptanalysis more accurately.
Outline

Background & Contribution

Preliminaries

Automatic Search of Differentials

Differential Analysis of the LED64 Block Cipher

Differentials of Midori64 Considering Key-Schedule

Conclusion
Differential Analysis of the LED64 Block Cipher

Main Idea

- Computing the probability of a differential
- Equivalent
- Searching for the right pairs of a differential

Planar mapping
- Constraints on the values of the right pairs
- SAT solver
- Right pairs for the differential

Trail 0
- Planar mapping
- Trails 0 to m-1
- Planar mapping
- Constraints on the values of the right pairs
- Right pairs for Trail 0

Trail 1
- Planar mapping
- Constraints on the values of the right pairs
- Right pairs for Trail 1

\ldots

Trail m-1
- Planar mapping
- Constraints on the values of the right pairs
- Right pairs for Trail 1
Planar Differentials and Maps

- For the differential \((\alpha, \beta)\) of the function \(f\),
  \[
  F_f(\alpha, \beta) = \{x \mid f(x) \oplus f(x \oplus \alpha) = \beta\},
  \]
  \[
  G_f(\alpha, \beta) = \{y \mid y = f(x), x \in F_f(\alpha, \beta)\}.
  \]
- \((\alpha, \beta)\) is called a **planar differential** if \(F_f(\alpha, \beta)\) and \(G_f(\alpha, \beta)\) are affine subspaces.
- A mapping is **planar** if all differentials over it are planar.
- The S-layer composed of the parallel applications of S-boxes is planar when all the S-boxes have differential uniformity of 4.

\[
\begin{align*}
\Delta x^i & \quad \Delta y^i & \quad k^i & \quad \Delta x^{i+1} & \quad \Delta y^{i+1} & \quad k^{i+1} & \quad \Delta x^{i+2} \\
x^i & \quad S & \quad y^i & \quad P & \quad x^{i+1} & \quad S & \quad y^{i+1} & \quad P & \quad x^{i+2}
\end{align*}
\]

\[x^i \in F_S(\Delta x^i, \Delta y^i) \text{ if and only if } \text{Mat}^i_F \cdot x^i = \text{Vec}^i_F,\]
\[y^i \in G_S(\Delta x^i, \Delta y^i) \text{ if and only if } \text{Mat}^i_G \cdot y^i = \text{Vec}^i_G.\]
Differential Analysis of the LED64 Block Cipher

Constraints for the Right Pairs

\[
\begin{bmatrix}
\text{Mat}_G^i \\
\text{Mat}_{F+1}^i \cdot P
\end{bmatrix}
\cdot
\begin{bmatrix}
\Delta x^i \\
\Delta y^i
\end{bmatrix}
\begin{bmatrix}
\text{Vec}_G^i \\
\text{Vec}_{F+1}^i \oplus \text{Mat}_{F+1}^i \cdot c^{i+1}
\end{bmatrix}
\]

\[
y^i = \text{SC}(x^i).
\]

\[
x^{i+1} = \text{MC} \circ \text{SR}(y^i) \oplus c^{i+1}.
\]

Framework for the Search of Right Pairs

- To obtain the right pairs of a given differential
  - Searching for many characteristics within the differential
  - Generating \( \text{Mat}_G, \text{Mat}_F, \text{Vec}_G \) and \( \text{Vec}_F \) corresponding to the differential trail
  - Applying SAT solver to get the right pairs for every trail
Differential Analysis of the LED64 Block Cipher

Improved Differential Attacks

### 3-STEP Related-key Attack for LED64 (Mendel et al. @ ASIACRYPT 2012)

![Diagram](image1)

\[
\Delta \oplus \Delta^* \rightarrow F_i \rightarrow \Delta^* \rightarrow \Delta \rightarrow ? \quad \text{Probability 1}
\]

\[
\Delta \rightarrow \Delta^* \rightarrow \Delta \rightarrow \Delta C \rightarrow 2^{59.00} \rightarrow 2^{56.50}
\]

### 4-STEP Related-key Attack for LED64 (Mendel et al. @ ASIACRYPT 2012)

![Diagram](image2)

\[
\Delta \rightarrow \Delta \rightarrow F_{i+1} \rightarrow \Delta \rightarrow ? \rightarrow \Delta \rightarrow \Delta C \rightarrow 2^{62.71} \rightarrow 2^{60.82}
\]

### 5-STEP Related-key Attack for LED64 (Nikolić et al. @ FSE 2013)

![Diagram](image3)

\[
\Delta \rightarrow \Delta \rightarrow F_{i+1} \rightarrow \Delta \rightarrow \Delta^* \rightarrow \Delta \rightarrow \Delta_{\text{Meet-in-the-middle}} \rightarrow \Delta \rightarrow \Delta C \rightarrow 2^{60.20} \rightarrow 2^{57.70}
\]
Outline

Background & Contribution

Preliminaries

Automatic Search of Differentials

Differential Analysis of the LED64 Block Cipher

Differentials of Midori64 Considering Key-Schedule

Conclusion
Differentials of Midori64 Considering Key-Schedule

Outline

Minimising the weak-key ratio

Detecting the maximum number of compatible characteristics

Designer View

Attacker View

\( \mathcal{K} \)

\( \mathcal{K} \)

Trail 0

Trail 1

Trail \( m - 1 \)

V\(^{(0)}\)\( _K \)

V\(^{(1)}\)\( _K \)

V\(^{(m-1)}\)\( _K \)
Weak-key Space of a Differential

\[
\begin{align*}
\Delta x^i & \\
x^i & \xrightarrow{S} y^i & P & \xrightarrow{\Delta x^{i+1}} x^{i+1} & \xrightarrow{S} y^{i+1} & P & \xrightarrow{\Delta x^{i+2}} x^{i+2} \\
\end{align*}
\]

\[y^i \in G_S(\Delta x^i, \Delta y^i) \text{ if and only if } \text{Mat}_G \cdot y^i = \text{Vec}_G.\]

\[
\text{Mat}_F^{i+1} \cdot x^{i+1} = \text{Mat}_F^{i+1} \cdot \left( P \cdot y^i \oplus k^i \right) = \text{Mat}_F^{i+1} \cdot P \cdot y^i \oplus \text{Mat}_F^{i+1} \cdot k^i = \text{Vec}_F^{i+1}. \\
\Rightarrow \begin{bmatrix} \text{Mat}_U^i \\ 0 \end{bmatrix} \cdot \begin{bmatrix} y^i \\ k^i \end{bmatrix} = \begin{bmatrix} \text{Vec}_U^i \\ \text{Vec}_K^i \end{bmatrix}.
\]

**Necessary Condition**

- The \(i\)-th subkey \(k^i\) falls into the affine space \(\{x \mid \text{Mat}_K^i \cdot x = \text{Vec}_K^i\}\).
- For an \(r\)-round differential consisting of \(m\) characteristics, if a particular key leads all \(m\) characteristics to become impossible trails, the differential under this fixed-key turns into an **impossible differential**.
- For the differential \((\alpha, \beta)\), we denote the set of these keys as \(l_K(\alpha, \beta)\), which satisfies \(W_K(\alpha, \beta) \subseteq \mathcal{K} - l_K(\alpha, \beta)\).
Upper-Bound for Weak-key Ratio of Differential

Estimating the Cardinality of the Weak-key Space

- \( W_K(\alpha, \beta) \subseteq \bigcup_{j=0}^{m-1} V_K^{(j)} \).

- \( \Pr\{K \mid K \in \bigcup_{j=0}^{m-1} V_K^{(j)}\} \): a natural upper-bound for the weak-key ratio.

- By De Morgan’s laws, we know
  \[
  \mathcal{K} - \bigcup_{j=0}^{m-1} V_K^{(j)} = \bigcap_{j=0}^{m-1} \left( \mathcal{K} - V_K^{(j)} \right). 
  \]

- Main idea: converting the restrictions on the set into clauses in CNF.
Upper-Bound for Weak-key Ratio of Differential
4-round Differentials with Weak-key Ratio Lower than 50%

The First Example

0x0022022202200202 → 0x2220000022022022.

- $\Pr \left\{ K \mid K \in \mathcal{K} - \bigcup_{j=0}^{m-1} V_K^{(j)} \right\} \approx 78.64\%$.
- The weak-key ratio for this differential is less than 21.36\%.
- The experimental results illustrate that the probability for a fixed-key with no right pair is about 78.66\%.

The Second Example

0x70000000000a0000a → 0x5ffa05ff5faf00aa.

- $\Pr \left\{ K \mid K \in \mathcal{K} - \bigcup_{j=0}^{m-1} V_K^{(j)} \right\} \approx 96.06\%$.
- For 96.06\% of the keys, the differential is an impossible one.
- The experimental results illustrate that the probability for a fixed-key with no right pair is about 96.09\%.
Maximum Number of Compatible Characteristics

Max-PoSSo Problem

- \( \mathcal{F} = \{ f_0(x), f_1(x), \ldots, f_{m-1}(x) \} \), where \( f_i(x) \)'s are polynomial functions over \( \mathbb{F}_2^n \), \( x \in \mathbb{F}_2^n \).

- The Max-PoSSo problem is to find any \( x \in \mathbb{F}_2^n \) that satisfies the maximum number of polynomials in \( \mathcal{F} \).

- If \( f_j(K) \) denotes \( f_j(K) = M^{(j)} \cdot K \oplus V^{(j)} \), we know \( K \in V^{(j)}_K \) if and only if \( f_j(K) = 0 \).

- Determining the maximum number of compatible characteristics

- Finding \( K \) under which the number of functions following \( f_j(K) = 0 \) is maximised

- We use an automatic method based on SAT to settle this problem.
Maximum Number of Compatible Characteristics

Application

<table>
<thead>
<tr>
<th>#{Trails}</th>
<th>212</th>
<th>211</th>
<th>208</th>
<th>128</th>
</tr>
</thead>
<tbody>
<tr>
<td>#{Groups}</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>Rank</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>16</td>
</tr>
<tr>
<td>EDP&lt;sub&gt;P&lt;/sub&gt;</td>
<td>$2^{-16}$</td>
<td>$2^{-16}$</td>
<td>$2^{-16}$</td>
<td>$2^{-18}$</td>
</tr>
</tbody>
</table>

- The EDP on the eight subspaces is improved to $2^{-16}$ (EDP = $2^{-23.79}$).
- For a randomly drawn key, the possibility that the EDP of the differential under this key is no less than $2^{-16}$ is at least $2^{-15} \times 8 = 2^{-12}$.
- To verify the validity of this probability, we do some tests for the randomly selected keys. The probability is about $2^{-12.18}$.
Outline

Background & Contribution

Preliminaries

Automatic Search of Differentials

Differential Analysis of the LED64 Block Cipher

Differentials of Midori64 Considering Key-Schedule

Conclusion
Conclusion

- Automatic method based on SAT for the search of differentials
- Automatically search for right pairs of the STEP functions of LED64
  - Improved differential attacks
- Models for the estimation of the weak-key space of a differential
  - Applying to the analysis of Midori64

Discussion

- All automatic methods can be generalised to analyse other ciphers.
- For some lightweight block ciphers with a simple key schedule, we need to pay more attention to the analysis of the differential.
- How to utilise automatic tools to provide more precise evaluation for the linear hull effect considering the key schedule is an open problem.
Thank you for your attention!