More Accurate Differential Properties of LED64 and Midori64

Ling Sun[1,2], Wei Wang[1], Meiqin Wang[1]

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

FSE 2019, Paris, France @ March 25, 2019

山东大学
SHANDONG UNIVERSITY

Outline

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

- An r-round **differential characteristic/trail** $C = (C_0, C_1, \ldots, C_r)$.
- The **differential probability** (DP) of a differential (α, β) is

$$\mathrm{DP}_f(\alpha, \beta) = \frac{\{x \in \mathbb{F}_2^n \mid f(x) \oplus f(x \oplus \alpha) = \beta\}}{2^n}.$$

  - For a keyed function $f(\cdot, k)$: $\mathrm{DP}_f[k](\alpha, \beta)$ & $\mathrm{DP}_f[k](C)$
- **Expected differential probability** (EDP):

$$\mathrm{EDP}_f(\alpha, \beta) = \operatorname*{mean}_{k \in \mathcal{K}} \left(\mathrm{DP}_f[k](\alpha, \beta)\right).$$

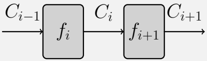
- The **weight** of a differential or a trail:

$$-\log_2 \left(\mathrm{EDP}_f(\alpha, \beta)\right).$$

Preliminaries

Markov Cipher Theory (Lai et al. @ EUROCRYPT 1991)

- 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

$$\begin{aligned} \mathsf{EDP}_f(C) &= \prod_{i=1}^{r} \mathsf{EDP}_{f_i}(C_{i-1}, C_i), \\ \mathsf{EDP}_f(\alpha, \beta) &= \sum_{C_0=\alpha, C_r=\beta} \mathsf{EDP}_f(C). \end{aligned}$$

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

Hypothesis of Stochastic Equivalence

For all differentials (α, β), it holds that for most values of the key k,

$$\mathsf{DP}_f[k](\alpha, \beta) = \mathsf{EDP}_f(\alpha, \beta).$$

Preliminaries

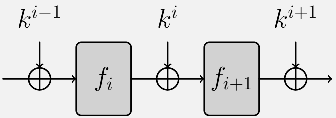
Distribution of the Fixed-key Probability

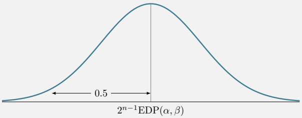
Theorem 1 (Daemen and Rijmen @ 2007)

In a **key-alternating** cipher $f(\cdot, k)$, the fixed-key cardinality $N_f[k](\alpha, \beta)$ of a differential (α, β) 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 $N[k](\alpha, \beta) \geqslant 2^{n-1}\text{EDP}(\alpha, \beta)$ the **weak-keys**.
- The set of weak-keys is denoted as $W_K(\alpha, \beta)$.

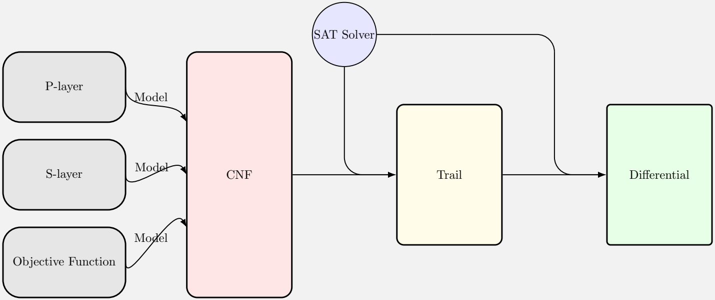
Outline

Automatic Search of Differentials

Main Idea

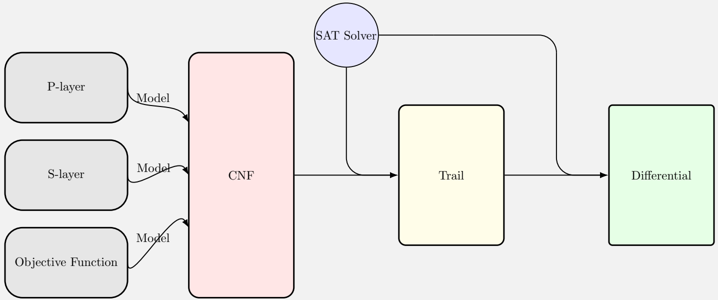
SAT Problem

- 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



Automatic Search of Differentials

Main Idea

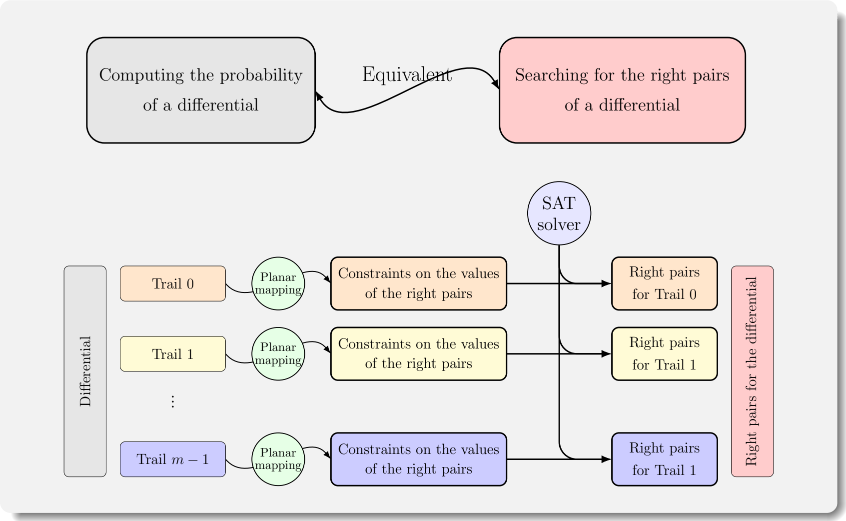


- The number of solutions handled by the solver is determined by the individual SAT problem.
- According to our experience, 2^{32} is an upper-bound.
- The **crucial** problem is how to use these trails to conduct differential cryptanalysis more accurately.

Outline

Differential Analysis of the LED64 Block Cipher

Main Idea



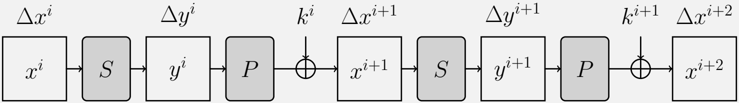
Differential Analysis of the LED64 Block Cipher

Planar Differentials and Maps

- For the differential (α, β) of the function f,

$$\begin{aligned} F_f(\alpha,\beta) &= \{x \mid f(x) \oplus f(x \oplus \alpha) = \beta\}, \\ G_f(\alpha,\beta) &= \{y \mid y = f(x), x \in F_f(\alpha,\beta)\}. \end{aligned}$$

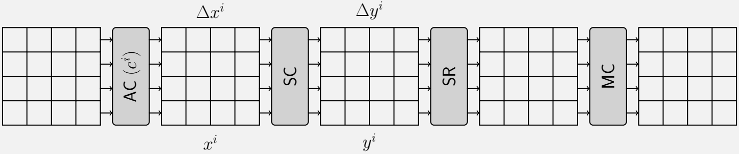
- (α, β) is called a **planar differential** if $F_f(\alpha, \beta)$ and $G_f(\alpha, \beta)$ are affine subspaces.
- A mapping is **planar** if all differentials over it are planar.
- The S-layer composed of the parallel applications of S-boxes is planar when all the S-boxes have differential uniformity of 4.



$$\begin{aligned} x^i \in F_S(\Delta x^i, \Delta y^i) &\text{ if and only if } \mathrm{Mat}_F^i \cdot x^i = \mathrm{Vec}_F^i, \\ y^i \in G_S(\Delta x^i, \Delta y^i) &\text{ if and only if } \mathrm{Mat}_G^i \cdot y^i = \mathrm{Vec}_G^i. \end{aligned}$$

Differential Analysis of the LED64 Block Cipher

Constraints for the Right Pairs



$$\left[\begin{array}{c}\mathrm{Mat}^i_G \\ \hdashline \mathrm{Mat}^{i+1}_F \cdot P\end{array}\right] \cdot \left[\ y^i\ \right] = \left[\begin{array}{c}\mathrm{Vec}^i_G \\ \hdashline \mathrm{Vec}^{i+1}_F \oplus \mathrm{Mat}^{i+1}_F \cdot c^{i+1}\end{array}\right].$$

$$\begin{aligned} y^i &= \mathrm{SC}(x^i). \\ x^{i+1} &= \mathrm{MC} \circ \mathrm{SR}(y^i) \oplus c^{i+1}. \end{aligned}$$

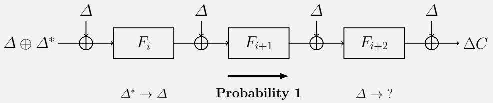
Framework for the Search of Right Pairs

- To obtain the right pairs of a given differential
  - Searching for **many characteristics** within the differential
  - Generating Mat_G, Mat_F, Vec_G and 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

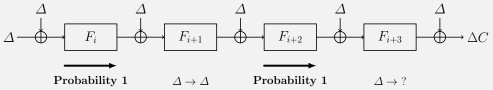
Improved Differential Attacks

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



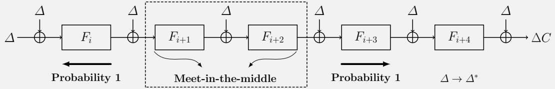
$2^{59.00} \searrow 2^{56.50}$

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



$2^{62.71} \searrow 2^{60.82}$

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



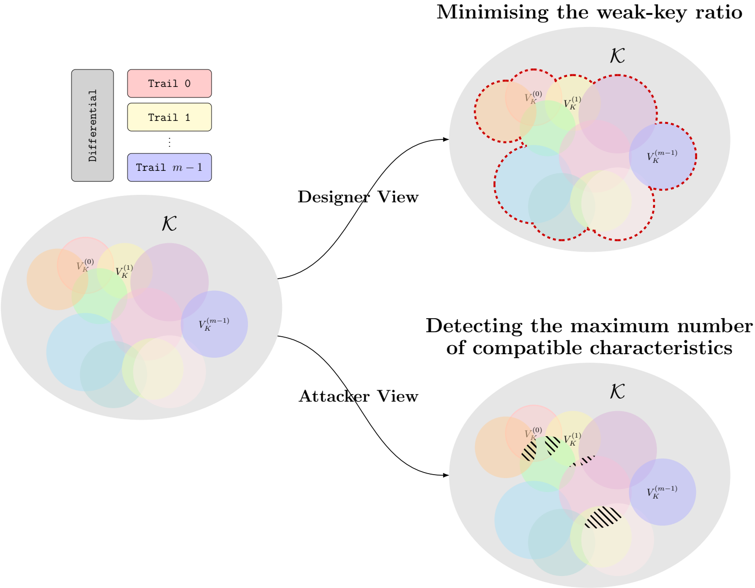
$2^{60.20} \searrow 2^{57.70}$

山东大学 SHANDONG UNIVERSITY

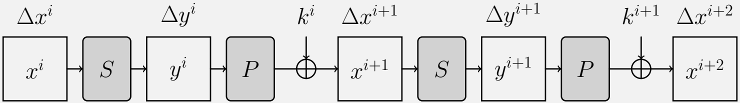
Outline

SHANDONG UNIVERSITY 山东大学

Outline


Minimising the weak-key ratio
Differential
Trail 0
Trail 1
Trail $m-1$
$\mathcal{K}$
$V_K^{(0)}$
$V_K^{(1)}$
$V_K^{(m-1)}$
Designer View
Attacker View
Detecting the maximum number of compatible characteristics

Weak-key Space of a Differential



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

$$\mathrm{Mat}_F^{i+1} \cdot x^{i+1} = \mathrm{Mat}_F^{i+1} \cdot \left(P \cdot y^i \oplus k^i\right) = \mathrm{Mat}_F^{i+1} \cdot P \cdot y^i \oplus \mathrm{Mat}_F^{i+1} \cdot k^i = \mathrm{Vec}_F^{i+1}.$$

$$\Rightarrow \begin{bmatrix} \multicolumn{2}{c}{\mathrm{Mat}_U^i} \\ \hline 0 & \mathrm{Mat}_K^i \end{bmatrix} \cdot \begin{bmatrix} y^i \\ \hline k^i \end{bmatrix} = \begin{bmatrix} \mathrm{Vec}_U^i \\ \hline \mathrm{Vec}_K^i \end{bmatrix}.$$

Necessary Condition

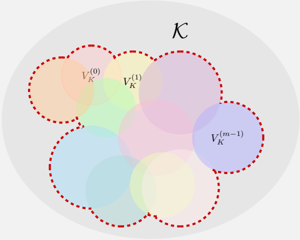
- The i-th subkey k^i falls into the affine space $\{x \mid \mathrm{Mat}_K^i \cdot x = \mathrm{Vec}_K^i\}$.

- 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 (α, β), we denote the set of these keys as $I_K(\alpha, \beta)$, which satisfies $W_K(\alpha, \beta) \subseteq \mathcal{K} - I_K(\alpha, \beta)$.

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

$$\texttt{0x0022022202200202} \rightarrow \texttt{0x2220000022022022}.$$

- $\Pr\left\{K \middle| K \in \mathcal{K} - \bigcup_{j=0}^{m-1} V_K^{(j)}\right\} \approx 78.64\%.$
- 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

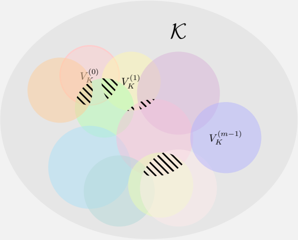
$$\texttt{0x7000000000a0000a} \rightarrow \texttt{0x5ffa05ff5faf00aa}.$$

- $\Pr\left\{K \middle| K \in \mathcal{K} - \bigcup_{j=0}^{m-1} V_K^{(j)}\right\} \approx 96.06\%.$
- 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

- $\mathcal{F} = \{f_0(\boldsymbol{x}), f_1(\boldsymbol{x}), \ldots, f_{m-1}(\boldsymbol{x})\}$, where $f_i(\boldsymbol{x})$'s are polynomial functions over $\mathbb{F}_2^n$, $\boldsymbol{x} \in \mathbb{F}_2^n$.
- The **Max-PoSSo** problem is to find any $\boldsymbol{x} \in \mathbb{F}_2^n$ 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

$$K \in V_K^{(j)} \text{ if and only if } f_j(K) = 0.$$

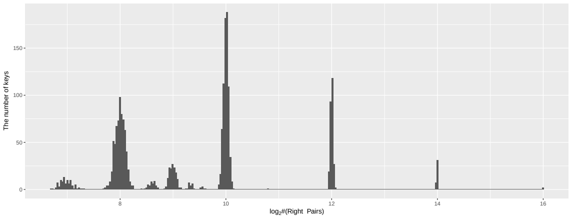
- Determining the maximum number of compatible characteristics
- Finding K under which the number of functions following $f_j(K) = 0$ is maximised
- We use an automatic method based on SAT to settle this problem.

Maximum Number of Compatible Characteristics

Application

#{Trails}	212	211	208	128
#{Groups}	3	4	1	8
Rank	15	15	15	16
EDP_P	2^{-16}	2^{-16}	2^{-16}	2^{-18}

- 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

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!