Provable Security Evaluation of Structures against Impossible Differential Cryptanalysis

Jian Guo
joint with Ruilin Li, Meicheng Liu, Vincent Rijmen, and Bing Sun

NANYANG TECHNOLOGICAL UNIVERSITY

Dagsthul, 15 Jan 2016

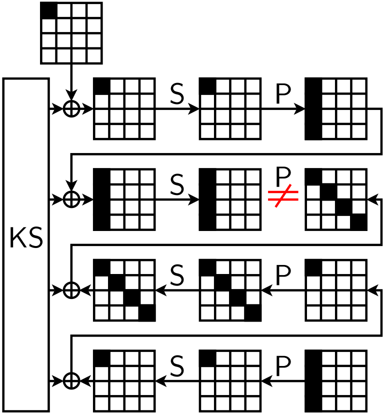
Outline

Motivation

We know how to upper bound the probability of differential / linear characteristics, e.g., 25 active sboxes with prob. $\leq 2^{-6*25} = 2^{-150}$ in **4** consecutive AES rounds,

but less on impossible differential. How to bound the maximum number of round of ID of a given SPN cipher ?

4R AES ID



The structure

SP Network:

$$AK \circ S \circ P \circ \underbrace{AK \circ S \circ P}_{\text{1 round}} \circ \cdots \circ AK \circ S \circ P \circ AK \circ S \circ P$$

The structure

SP Network:

$$AK \circ S \circ P \circ \underbrace{AK \circ S \circ P}_{\text{1 round}} \circ \cdots \circ AK \circ S \circ P \circ AK \circ {\color{red}S} \circ {\color{gray}P}$$

Assume each Sbox can take all permutations S' of the same size,

The structure

SP Network:

$$AK \circ S \circ P \circ \underbrace{AK \circ S \circ P}_{1 \text{ round}} \circ \cdots \circ AK \circ S \circ P \circ AK \circ S \circ P$$

Assume each Sbox can take all permutations S' of the same size,

The Structure:

$$S' \circ P \circ \underbrace{S' \circ P}_{1 \text{ round}} \circ \cdots \circ S' \circ P \circ S'$$

Some Properties I

Since S' can take any permutation, if the differential $\alpha \xrightarrow{S'} \beta$ is possible, then the differential $\alpha' \xrightarrow{S'} \beta'$ is also possible for all (α', β') sharing the same truncated characteristic with (α, β). Hence such property preserves for $S' \circ P$, and for $(S' \circ P)^r \circ S'$ for any $r \geq 0$.

Some Properties II

If the differentials $\alpha_1 \xrightarrow{S' \circ P \circ S'} \beta_1$ and $\alpha_2 \xrightarrow{S' \circ P \circ S'} \beta_2$ are possible, then $\alpha_1 | \alpha_2 \xrightarrow{S' \circ P \circ S'} \beta_1 | \beta_2$ is also possible. Hence such property preserves for any $(S' \circ P)^r \circ S'$ for any $r \geq 0$.

Some Properties II

If the differentials $\alpha_1 \xrightarrow{S' \circ P \circ S'} \beta_1$ and $\alpha_2 \xrightarrow{S' \circ P \circ S'} \beta_2$ are possible, then $\alpha_1 | \alpha_2 \xrightarrow{S' \circ P \circ S'} \beta_1 | \beta_2$ is also possible. Hence such property preserves for any $(S' \circ P)^r \circ S'$ for any $r \geq 0$.

The Contrapositive:

If $\alpha \xrightarrow{(S' \circ P)^r \circ S'} \beta$ is impossible, then $\alpha' \xrightarrow{(S' \circ P)^r \circ S'} \beta'$ is impossible for some α' and β' with single active nibble.

Some Properties II

If the differentials $\alpha_1 \xrightarrow{S' \circ P \circ S'} \beta_1$ and $\alpha_2 \xrightarrow{S' \circ P \circ S'} \beta_2$ are possible, then $\alpha_1 | \alpha_2 \xrightarrow{S' \circ P \circ S'} \beta_1 | \beta_2$ is also possible. Hence such property preserves for any $(S' \circ P)^r \circ S'$ for any $r \geq 0$.

The Contrapositive:

If $\alpha \xrightarrow{(S' \circ P)^r \circ S'} \beta$ is impossible, then $\alpha' \xrightarrow{(S' \circ P)^r \circ S'} \beta'$ is impossible for some α' and β' with single active nibble.

Useful Induction:

Then, the search of impossible differential of $r + 1$ rounds is reduced to checking all m^2 (v.s. previous 2^{2m}) such (α', β') pairs (m denotes the number of nibbles of the state).

How to determine the maximum round of ID

Represent the state as a vector, and P as a matrix, denote the truncated characteristic matrix as P^*, determine minimum r_1 such that $(P^*)^{r_1}$ is all one matrix, similarly minimum r_2 such that $(P^*)^{-r_2}$ is all one matrix, then the max round of ID is $r_1 + r_2$.

Determine the maximum round of ID - example of AES

The AES MixColumn Matrix

$$\begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix} \xrightarrow{\text{truncated characteristic}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

Determine the maximum round of ID - example of AES

$$P^* = \begin{pmatrix}
1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1\\
1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1\\
1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1\\
1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1\\
0&0&0&1&1&0&0&0&0&1&0&0&0&0&1&0\\
0&0&0&1&1&0&0&0&0&1&0&0&0&0&1&0\\
0&0&0&1&1&0&0&0&0&1&0&0&0&0&1&0\\
0&0&0&1&1&0&0&0&0&1&0&0&0&0&1&0\\
0&0&1&0&0&0&0&1&1&0&0&0&0&1&0&0\\
0&0&1&0&0&0&0&1&1&0&0&0&0&1&0&0\\
0&0&1&0&0&0&0&1&1&0&0&0&0&1&0&0\\
0&0&1&0&0&0&0&1&1&0&0&0&0&1&0&0\\
0&1&0&0&0&0&1&0&0&0&0&1&1&0&0&0\\
0&1&0&0&0&0&1&0&0&0&0&1&1&0&0&0\\
0&1&0&0&0&0&1&0&0&0&0&1&1&0&0&0\\
0&1&0&0&0&0&1&0&0&0&0&1&1&0&0&0
\end{pmatrix}$$

and $(P^*)^2 = 1$, hence $r_1 = 2$ and similarly $r_2 = 2$, maximum round is $r_1 + r_2 = 4$.

Results

- Proved, without considering the details of Sboxes, ID of AES is bounded by 4 rounds, and 8 rounds for Camellia w/o FL. In other words, the only way to find longer ID is to consider the Sbox properties.
- Gave simple way to determine such bounds.
- Due to the duality of ID cryptanalysis and zero-correlation cryptanalysis, similar results apply to ZC as well.

EoT

Thank you!

Questions?