Cryptanalysis of PRESENT-like ciphers with secret S-boxes

Julia Borghoff Lars Knudsen Gregor Leander Søren S. Thomsen

DTU, Denmark

FSE 2011

Cryptanalysis of Maya

Julia Borghoff Lars Knudsen Gregor Leander Søren S. Thomsen

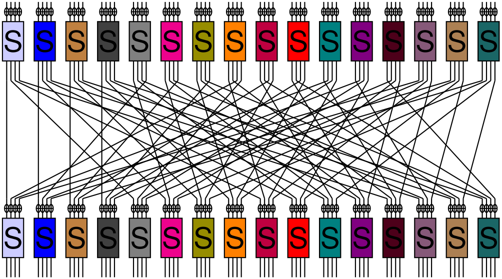
DTU, Denmark

FSE 2011

Outline

Outline

Maya



- 64 bit block size
- key-dependent 4-bit Sbox
- fixed bit permutation
- round keys
- 16 rounds

A more efficient variant of PRESENT.

Outline

Our Contribution

Main Result

In this talk we explain how to break Maya with a complexity of $\approx 2^{37}$.

Technique: Differential attack with a twist.

Idea

Use good differentials without knowing them.

Differential Attack on Maya

- We cannot specify characteristics
- Thus: no characteristic to be followed

$$\begin{matrix}(x||r)\\(y||r)\end{matrix} \longrightarrow \boxed{E_{K_1}} \xrightarrow{\Delta?} \boxed{E_{K_2}} \xrightarrow{\Delta?} \boxed{E_{K_3}} \quad \cdots \quad \boxed{E_{K_r}} \longrightarrow \Delta\gamma$$

Differential Attack on Maya

- We cannot specify characteristics
- Thus: no characteristic to be followed

$$\begin{matrix}(x||r)\\(y||r)\end{matrix} \rightarrow \boxed{E_{K_1}} \xrightarrow{\Delta ?} \boxed{E_{K_2}} \xrightarrow{\Delta ?} \boxed{E_{K_3}} \cdots \boxed{E_{K_r}} \rightarrow \Delta\gamma$$

Use relative information:

$$\begin{matrix}(x||r)\\(y||r)\end{matrix} \rightarrow \boxed{E_{K_1}} \xrightarrow{\Delta\alpha} \boxed{E_{K_2}} \xrightarrow{\Delta ?} \boxed{E_{K_3}} \cdots \boxed{E_{K_r}} \rightarrow \Delta\gamma$$

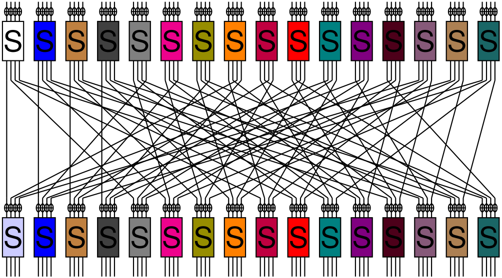
$$\begin{matrix}(x'||r)\\(y'||r)\end{matrix} \rightarrow \boxed{E_{K_1}} \xrightarrow{\Delta\alpha'} \boxed{E_{K_2}} \xrightarrow{\Delta ?} \boxed{E_{K_3}} \cdots \boxed{E_{K_r}} \rightarrow \Delta\gamma'$$

Informally: Compare distribution of $\Delta\gamma$ and $\Delta\gamma'$: Learn something about $\Delta\alpha$ and/or $\Delta\alpha'$.

Left Most Sbox

Remark

We focus on the leftmost Sbox in the first round. Other Sboxes similar.



- try to recover the white Sbox
- using differentials
- with a twist

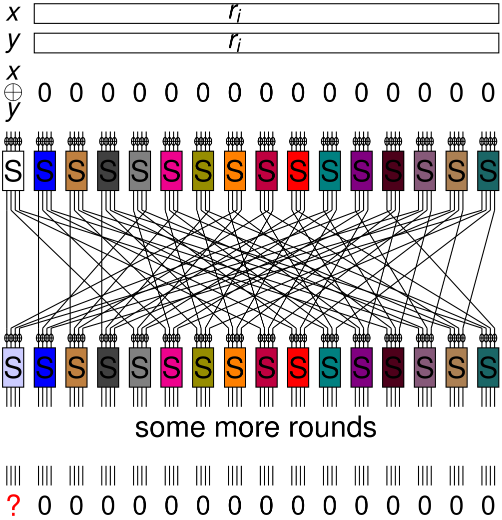
The basic idea to recover the Sboxes

- Fix two inputs $x \neq y \in \mathbb{F}_2^4$ to the leftmost Sbox S.
- Estimate the probability of

$$(x \oplus y)||0^{60} \rightarrow ?||0^{60}$$

using counters for each pair (x, y).

The basic idea in a picture



- Fix x, y
- Encrypt pair $(x|r_i, y|r_i)$, $0 \leq i < N$.
- Count how often only first Sbox active in the output

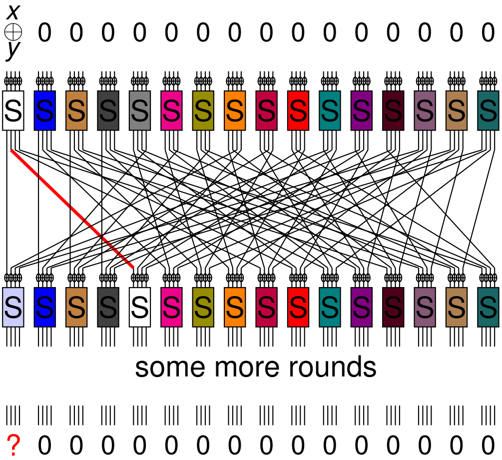
First Assumption

Assumption

The smaller the hamming weight of $S(x) \oplus S(y)$ is, the higher the counter.

The highest counters correspond to one bit differences $S(x) \oplus S(y)$. This will tell us something about the Sbox.

First Assumption in a Picture

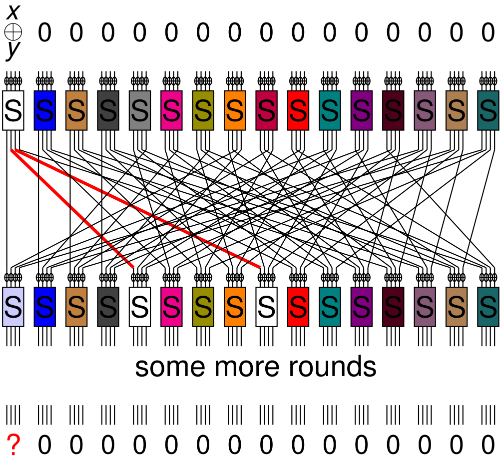


- x, y with one bit output difference

  $$\mathrm{wt}(S(x)+S(y)) = 1$$

- One active Sboxes in the second round

First Assumption in a Picture



- x, y with two bit output difference

  $$\mathrm{wt}(S(x)+S(y)) = 2$$

- Two active Sboxes in the second round

A bit more precise

- Encrypt structures $\star || r_i$, $\star$ runs through all 4 bit values and $r_i \in \mathbb{F}_2^{60}$ is random and fixed. $0 \leq i < Ns$.
- For each pair $\{x, y\}$ with $x \neq y \in \mathbb{F}_2^4$ we have a counter

$$C(\{x, y\}) = \sharp\{r_i \,|Enc(x||r_i) \oplus Enc(y||r_i) =?||0^{64}\}$$

Assumption

The highest counters $C(\{x, y\})$ correspond to x, y such that $\mathrm{wt}(S(x) \oplus S(y)) = 1$.

For the rest: Examples only!

Example

$$C(\{x,y\}) = \sharp\{r_i \mid Enc(x||r_i) \oplus Enc(y||r_i) =?||0^{64}\}$$

(sorted and only the 24 highest values out of 120)

$C(x,y)$	273	265	264	263	261	261	253	243
$\{x,y\}$	(b,9)	(7,2)	(d,a)	(6,5)	(3,1)	(f,8)	(e,4)	(c,0)
$C(x,y)$	163	157	139	136	119	114	102	95
$\{x,y\}$	(a,6)	(8,4)	(2,0)	(9,1)	(f,e)	(d,5)	(c,7)	(b,3)
$C(x,y)$	11	8	8	7	6	6	5	5
$\{x,y\}$	(8,0)	(8,3)	(f,4)	(e,7)	(4,2)	(5,2)	(6,1)	(a,9)

Do the highest counters $C(\{x,y\})$ correspond to x, y such that $\mathrm{wt}(S(x) \oplus S(y)) = 1$?

Example for the counters

$C(x,y)$	273	265	264	263	261	261	253	243
$\{x,y\}$	(b,9)	(7,2)	(d,a)	(6,5)	(3,1)	(f,8)	(e,4)	(c,0)
$\mathrm{wt}(S(x) \oplus S(y))$	1	1	1	1	1	1	1	1
$C(x,y)$	163	157	139	136	119	114	102	95
$\{x,y\}$	(a,6)	(8,4)	(2,0)	(9,1)	(f,e)	(d,5)	(c,7)	(b,3)
$\mathrm{wt}(S(x) \oplus S(y))$	1	1	1	1	1	1	1	1
$C(x,y)$	11	8	8	7	6	6	5	5
$\{x,y\}$	(8,0)	(8,3)	(f,4)	(e,7)	(4,2)	(5,2)	(6,1)	(a,9)
$\mathrm{wt}(S(x) \oplus S(y))$	2	2	1	3	2	1	2	2

The assumption is fulfilled! But there is more...

Probabilities of Differentials

Assumption

The probability of a (truncated) differential depends on the (second round) input difference.

Implication for the counters $C(\{x, y\})$: High counters should correspond to the same output difference.

Example for the counters

$C(x,y)$	273	265	264	263	261	261	253	243
$\{x,y\}$	(b,9)	(7,2)	(d,a)	(6,5)	(3,1)	(f,8)	(e,4)	(c,0)
$\mathrm{wt}(S(x) \oplus S(y))$	1	1	1	1	1	1	1	1
$S(x) \oplus S(y)$	4	4	4	4	4	4	4	4
$C(x,y)$	163	157	139	136	119	114	102	95
$\{x,y\}$	(a,6)	(8,4)	(2,0)	(9,1)	(f,e)	(d,5)	(c,7)	(b,3)
$\mathrm{wt}(S(x) \oplus S(y))$	1	1	1	1	1	1	1	1
$S(x) \oplus S(y)$	2	2	2	2	2	2	2	2
$C(x,y)$	11	8	8	7	6	6	5	5
$\{x,y\}$	(8,0)	(8,3)	(f,4)	(e,7)	(4,2)	(5,2)	(6,1)	(a,9)
$\mathrm{wt}(S(x) \oplus S(y))$	2	2	1	3	2	1	2	2
$S(x) \oplus S(y)$	5	6	8	7	5	8	5	5

Example for the counters

$C(x,y)$	273	265	264	263	261	261	253	243
$\{x,y\}$	(b,9)	(7,2)	(d,a)	(6,5)	(3,1)	(f,8)	(e,4)	(c,0)
$\mathrm{wt}(S(x) \oplus S(y))$	1	1	1	1	1	1	1	1
$S(x) \oplus S(y)$	4	4	4	4	4	4	4	4

- The highest 8 counters correspond to 8 pairs with the same output difference.
- There are exactly 8 such pairs, so we learn them all.
- We do not know the exact difference.
- But we assume it is of hamming weight one.

Recovering the Sbox

Remark

That is a lot(?) of information about the Sbox!

We learn up to 4 sets

$$D_e = \{\{x, y\} \mid S(x) \oplus S(y) = e\}$$

- Still too many possibilities!
- Learning all 4 sets is difficult.

Attack the Inverse

We learn up to 4 sets

$$D_e = \{\{x, y\} \mid S(x) \oplus S(y) = e\}$$

Even better

We can do the attack upside down!

We learn up to 4 sets

$$E_f = \{\{x, y\} \mid S^{-1}(x) \oplus S^{-1}(y) = f\}$$

Experimental Fact

Given two sets D_e and one set E_f: Often only one possible Sbox.

Some Improvements

Improvements over the basic idea:

- Relaxed truncated differentials
- Detect errors, i.e. discard wrong sets

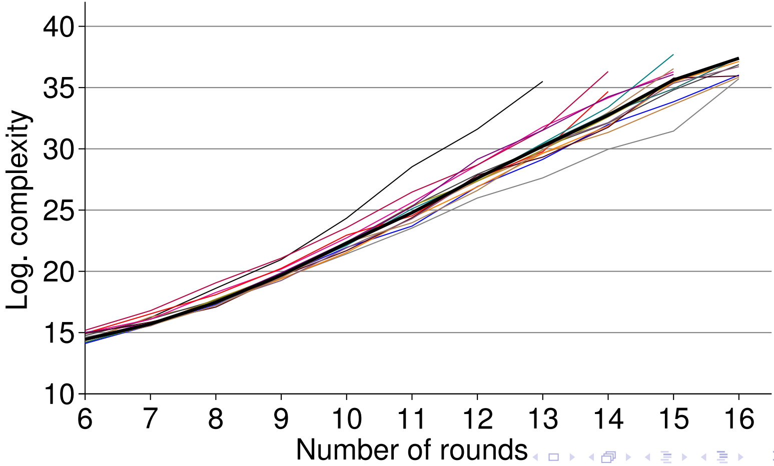
Details in the paper

Crucial

Those make the difference between a practical and a theoretical attack.

Outline

Experimental Complexity of the Attack



Conclusions

- Practical attack on Maya
- Applies to a broader class
- Up to 28 rounds: not secure
- Technique: Twist on truncated differentials
- Mathematical model of the complexity in the paper

The End

Thanks a lot!