Optimal Differential Trails in SIMON-like Ciphers

Zhengbin Liu, Yongqiang Li, Mingsheng Wang

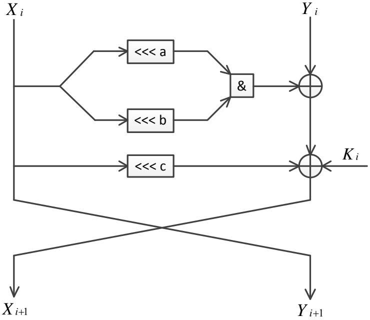
State Key Laboratory of Information Security,
Institute of Information Engineering, CAS;
University of Chinese Academy of Science

FSE 2017, Tokyo, Japan
March 8, 2017

Outline

Outline

SIMON-like Ciphers



- SIMON-like round function:

  $$F(x) = ((x \lll a) \wedge (x \lll b)) \oplus (x \lll c)$$

- For SIMON:

  $$(a, b, c) = (1, 8, 2)$$

- For SIMECK:

  $$(a, b, c) = (0, 5, 1)$$

The Differential Trails for SIMON

The threshold search algorithm (Biryukov et al., FSE'14)

Improved differential trails for SIMON32, SIMON48 and SIMON64.

The SAT/SMT solvers (Kölbl et al., CRYPTO'15)

The optimal differential trails for SIMON32, SIMON48 and SIMON64.

Pen and paper arguments (Beierle, SCN'16)

An upper bound on the probability of differential trails.

Motivations and Contributions

Motivations

The optimal differential trails for SIMON96 and SIMON128 aren't found.

Our Contribution

- An efficient search algorithm for the optimal differential trails in SIMON-like ciphers.
- Our search algorithm can find the optimal differential trails for SIMON96 and SIMON128.

Outline

Differential Probability of SIMON-like Round Function

Theorem (Kölbl et al., CRYPTO'15)

Let $F(x) = ((x \lll a) \wedge (x \lll b)) \oplus (x \lll c)$, n *is even,* $a > b$ *and* $\gcd(n, a-b) = 1$. *Then with* $varibits = (\alpha \lll a) \vee (\alpha \lll b)$ *and*

$$doublebits = (\alpha \lll b) \wedge \overline{(\alpha \lll a)} \wedge (\alpha \lll (2a-b))$$

and $\gamma = \beta \oplus (\alpha \lll c)$, *it holds*

$$P(\alpha \mapsto \beta) = \begin{cases} 2^{-n+1} & if \alpha = 2^n - 1, wt(\gamma) \equiv 0 \mod 2 \\ 2^{-wt(varibits \oplus doublebits)} & if \alpha \neq 2^n - 1, \gamma \wedge \overline{varibits} = 0_n, \\ & (\gamma \oplus (\gamma \lll (a-b))) \wedge doublebits \\ & = 0_n \\ 0 & else. \end{cases}$$

Upper Bound on the Differential Probability

Theorem (Beierle, SCN'16)

Let $F(x) = ((x \lll a) \wedge (x \lll b)) \oplus (x \lll c)$, $n \geq 6$ *is even,* $a > b$ *and* $\gcd(n, a-b) = 1$. *Let* α *be an input difference, then it holds that*

(1) *If* $wt(\alpha) = 1$, *then* $P_\alpha \leq 2^{-2}$;

(2) *If* $wt(\alpha) = 2$, *then* $P_\alpha \leq 2^{-3}$;

(3) *If* $wt(\alpha) \neq n$, *then* $P_\alpha \leq 2^{-wt(\alpha)}$;

(4) *If* $wt(\alpha) = n$, *then* $P_\alpha \leq 2^{-n+1}$.

Upper Bound on the Differential Probability

Theorem (Our Bound)

Let $F(x) = ((x \lll a) \wedge (x \lll b)) \oplus (x \lll c)$, n *is even,* $a > b$ *and* $\gcd(n, a-b) = 1$. *Let* α *be an input difference, then it holds that*

(1) *If* $1 \leq wt(\alpha) < n/2$, *then* $P_\alpha \leq 2^{-wt(\alpha)-1}$;

(2) *If* $n/2 \leq wt(\alpha) < n$, *then* $P_\alpha \leq 2^{-wt(\alpha)}$;

(3) *If* $wt(\alpha) = n$, *then* $P_\alpha \leq 2^{-n+1}$.

With this bound, we can traverse plaintext differences from low to high Hamming weight.

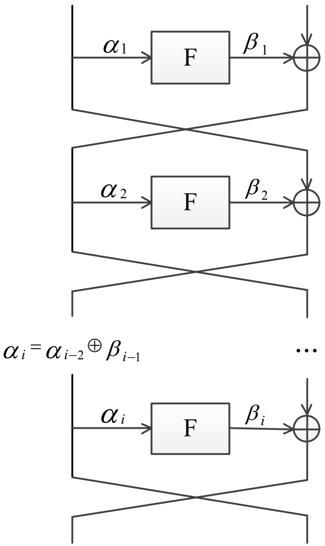
Comparison of the three bounds

Table: The impact of the three bounds on SIMON128

Round	Probability (log_2p)	Kölbl's bound	Beierle's bound	our bound
1	−0	$0.00s$	$0.00s$	$0.00s$
2	−2	$0.00s$	$0.00s$	$0.00s$
3	−4	$0.02s$	$0.01s$	$0.00s$
4	−6	$0.11s$	$0.12s$	$0.02s$
5	−8	$0.14s$	$0.13s$	$0.02s$
6	−12	$15.69s$	$14.89s$	$2.51s$
7	−14	$13.79s$	$13.06s$	$2.36s$
8	−18	$16.30s$	$13.81s$	$3.41s$
9	−20	$14.49s$	$12.05s$	$2.33s$
10	−26	$0.47h$	$0.44h$	$0.08h$
11	−30	$22.66h$	$22.67h$	$6.52h$
12	−36	$53.12h$	$52.88h$	$12.20h$
13	−38	$0.33h$	$0.33h$	$0.06h$
14	−44	$4.74h$	$4.70h$	$3.42h$

Outline

Matsui's Algorithm



Round-1:

For all α_1:

$p_1 = \max_\beta p(\alpha_1 \mapsto \beta)$

If $p_1 B_{n-1} \geq \overline{B}_n$ then

Call Round-2

Round-2:

For all α_2 and β_2:

$p_2 = p(\alpha_2 \mapsto \beta_2)$

If $p_1 p_2 B_{n-2} \geq \overline{B}_n$ then

Call Round-3

Round-i:

$\alpha_i = \alpha_{i-2} \oplus \beta_{i-1}$:

$p_i = p(\alpha_i \mapsto \beta_i)$

If $p_1 p_2 \cdots p_i B_{n-i} \geq \overline{B}_n$ then

Call Round-$(i+1)$

Matsui's Algorithm for SIMON-like ciphers

Matsui's Algorithm

- Returns optimal results if $\overline{B}_n \leq B_n$.
- Applicable to S-box based ciphers.

Main Idea

- Adapt Matsui's algorithm to SIMON-like ciphers.
- Compute the probability according to K$\ddot{o}$lbl et al..
- Use lookup tables to obtain the output differences.

The Search Strategy

Traverse plaintext differences from low to high Hamming weight

- According to the upper bound, the maximum probability decreases with the Hamming weight of input difference increasing.
- IF find some difference with $P_{max}B_{n-1} < \overline{B_n}$, break the branch and needn't traverse differences with higher Hamming weight.

The Search Strategy

Compute the probability and then find output differences

- According to K$\ddot{o}$lbl et al., the differential probability $P(\alpha \mapsto \beta)$ is the same for all possible output differences β.
- Compute the probability firstly, and if it satisfies the search condition, then find the output differences and search the next round.

The Search Strategy

The difference distribution table

- For n-bit AND operation ($n = mt$), build the difference distribution table of t-bit AND operation.

$$
\begin{array}{rccccc}
 & S_m & & S_1 & S_0 \\
 & x_{n-1} \cdots x_{n-t} & \cdots & x_{2t-1} \cdots x_t & x_{t-1} \ldots x_0 \\
\& & y_{n-1} \cdots y_{n-t} & \cdots & y_{2t-1} \cdots y_t & y_{t-1} \cdots y_0 \\
\hline
 & z_{n-1} \cdots z_{n-t} & \cdots & z_{2t-1} \cdots z_t & z_{t-1} \cdots z_0
\end{array}
$$

The Search Strategy

Find output differences with lookup tables

- For an n-bit input difference α, compute $\alpha \lll a$ and $\alpha \lll b$.
- Look up the tables to obtain corresponding output differences.
- Check whether the input and output differences satisfy the condition in K$\ddot{o}$lbl's Theorem.

Outline

Optimal Differential Trails for SIMON and SIMECK[1]

Table: The optimal differential trails for SIMON.

Block Size	Round	Probability ($log_2 p$)	time	Reference
32	12	−34	–	Kölbl et al., CRYPTO'15
	12	−34	40s	this paper
48	16	−50	–	Kölbl et al., CRYPTO'15
	16	−50	5h	this paper
64	16	−54	–	Kölbl et al., CRYPTO'15
	19	−64	6d	this paper
96	–	–	–	–
	28	−96	35d	this paper
128	–	–	–	–
	37	−128	66d	this paper

[1] All experiments are performed on a PC with a single core.

Optimal Differential Trails for SIMON and SIMECK

Table: The optimal differential trails for SIMECK.

Block Size	Round	Probability ($log_2 p$)	time	Reference
32	13	-32	–	Kölbl et al., ePrint
	13	-32	2s	this paper
48	19	-48	–	Kölbl et al., ePrint
	19	-48	4m	this paper
64	25	-64	–	Kölbl et al., ePrint
	25	-64	2m	this paper

The Differentials for SIMON and SIMECK

Table: The differentials for SIMON.

Block Size	Round	Probability ($log_2 p$)	Reference
32	14	−30.81	Kölbl et al., CRYPTO'15
	14	−30.76	this paper
48	17	−46.32	Kölbl et al., CRYPTO'15
	17	−46.38	this paper
64	22	−61.32	Kölbl et al., CRYPTO'15
	23	−61.93	this paper
96	30	−92.2	Abed et al., FSE'14
	31	−95.34	this paper
128	41	−124.6	Abed et al., FSE'14
	41	−123.74	this paper

The Differentials for SIMON and SIMECK

Table: The differentials for SIMECK.

Block Size	Round	Probability ($log_2 p$)	Reference
32	13	-27.28	Kölbl et al., ePrint
	14	-31.64	this paper
48	21	-45.65	Kölbl et al., ePrint
	21	-45.28	this paper
64	26	-60.02	Kölbl et al., ePrint
	27	-61.49	this paper

Outline

Conclusion

- A more accurate upper bound on the differential probability of SIMON-like round function.
- An efficient automatic search algorithm for optimal differential trails in SIMON-like ciphers.
- The provably optimal differential trails for all versions of SIMON and SIMECK.
- The best differentials for SIMON and SIMECK so far.

Thanks for your attention!