山东大学密码技术与信息安全教育部重点实验室
Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University

Improved Linear Hull Attack on Round-Reduced SIMON with Dynamic Key-guessing Techniques

Huaifeng Chen [1], Xiaoyun Wang[1,2]

[1] Shandong University; [2] Tsinghua University

March 22, 2016

Outline

SIMON and Its Cryptanalysis Results

Simon

- Proposed by NSA in 2013 (10 versions)
- Feistel structure (And ($\&$), Rotation($\lll$), Xor($\oplus$))
- Optimal performance in hardware applications

Existing cryptanalysis on Simon

- Differential attacks [Alkhzaimi et al.13, Abed et al.14, Biryukov et al.14, Wang et al.14]
- Linear (Hull) attacks [Abed et al.13, Alizadeh et al.14, Abdelraheem et al.14, Shi et al.14, Sun et al.14]
- Impossible Differential attacks [Alizadeh et al.14, Boura 14, Chen et al.15, Wang et al.$^+$14]
- Zero-correlation attacks [Wang et al.$^+$14]
- Integral attacks [Wang et al.$^+$14]

Motivation and Contributions

Cryptanalysis on Simon

- Search better distinguishers
  - all kinds of automatic search for differential and linear distinguishers
  - connection between differential and linear characteristic
- Improve the attack procedure
  - differential attack with dynamic key-guessing technique by Wang *et al.*
  - linear attack with dynamic key-guessing technique?

Contributions

- Propose the dynamic key-guessing technique for linear attack
  - Guess, Split and Combine
- Improve the linear hull attack on all versions of Simon
  - 23-round Simon32/64, . . . , 53-round Simon128/256
- Implement the 21-round attack on Simon32/64

Outline

General Framework of Matsui's Algorithm 2

$$P \underbrace{\xleftarrow{r_1}}_{K_P} X \boxed{\alpha \xleftarrow{\quad r \quad} \beta} Y \underbrace{\xrightarrow{r_2}}_{K_C} C$$

- Suppose

$$y = \alpha \cdot X \oplus \beta \cdot Y = F(P, C, K_P, K_C)$$

Then

$$c(K_P, K_C) = \sum_{P,C} (-1)^{F(P,C,K_P,K_C)} \qquad (T = N * |K_P| * |K_C|)$$

- Further, let $x = compress(P, C)$ is l_1-bit, $k = compress(K_P, K_C)$ is l_2-bit and $y = f(x, k)$, the first step of linear cryptanalysis is to compute

$$B^k(y) = \sum_{x} (-1)^{f(x,k)} V[x] \qquad (T = 2^{l_1+l_2})$$

General Framework of Matsui's Algorithm 2 - Linear Compression

- If $y = f(x, k)$ is linear with some bits of x and k, for example

$$y = x_0 \oplus k_0 \oplus f_1(x', k'), x = x'||x_0, k = k'||k_0,$$

then x can be compressed further $V'[x'] = V[x'||0] - V[x'||1]$,

$$B^k(y) = (-1)^{k_0} \sum_x (-1)^{f_1(x',k')} V'[x'] \quad (T = 2^{l_1+l_2-2})$$

- k_0 can be omitted (defined as the *related bit*)
- Multiple linear bits ($\sum_{0 \le i \le t} k_i$ is the related bit)

$$\begin{aligned} y &= (x_0 \oplus k_0) \oplus \cdots \oplus (x_t \oplus k_t) \oplus f_t(x'', k'') \\ &= (\sum_{0 \le i \le t} x_i) \oplus (\sum_{0 \le i \le t} k_i) \oplus f_t(x'', k'') \end{aligned}$$

Dynamic Key-guessing in Linear Attacks

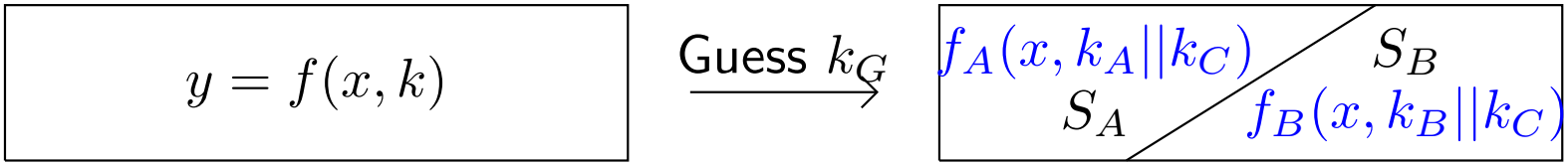

Figure: When k_G is known, the set of x can be splitted to two sets. f is independent of k_B in set S_A and independent of k_A in set S_B.

- For a boolean funciton $y = f(x, k)$ and a counter vector V, computing $B^k(y) = \sum_x (-1)^{f(x,k)} V[x]$ with a straight-forward method needs $2^{l_1+l_2}$ calculations.
- If for different keys, the expression of $y = f(x, k)$ is different, the key can be guessed dynamically.
  - Let $k = k_G||k_A||k_B||k_C$ and the length is $l_2^G, l_2^A, l_2^B, l_2^C$ respectively
  - When k_G is known, according to the value of x anf k_G, the x can be splitted into two sets: S_A and S_B
  - For $x \in S_A$, $y = f_A(x, k_A||k_C)$
  - For $x \in S_B$, $y = f_B(x, k_B||k_C)$

Dynamic Key-guessing in Linear Attacks

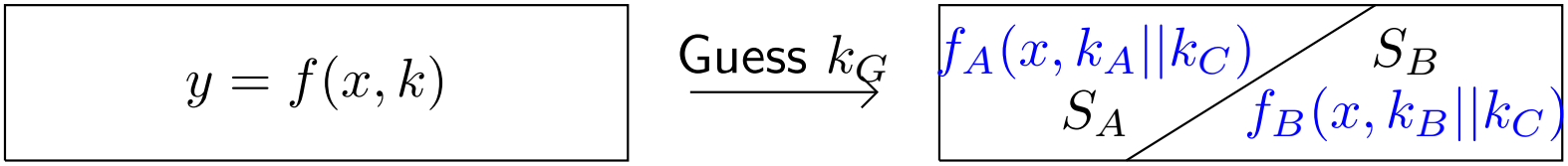

Figure: When k_G is known, the set of x can be splitted to two sets. f is independent of k_B in set S_A and independent of k_A in set S_B.

The attack procedure and time complexity

- Guess k_G
  - Split the x into two sets S_A, S_B according to the value of x and k_G
  - Compute $B^{k_A||k_C}(y) = \sum_{x \in S_A} (-1)^{f_A(x, k_A||k_C)}$ $(T_A = N_A 2^{l_2^A + l_2^C})$
  - Compute $B^{k_B||k_C}(y) = \sum_{x \in S_B} (-1)^{f_B(x, k_B||k_C)}$ $(T_B = N_B 2^{l_2^B + l_2^C})$
  - Combine $B^k(y) = B^{k_A||k_C}(y) + B^{k_B||k_C}(y)$ $(T_C = 2^{l_2^A + l_2^B + l_2^C})$
- The total time is $2^{l_2^G}(T_A + T_B + T_C)$, which is

$$N_A 2^{l_2^G + l_2^A + l_2^C} + N_B 2^{l_2^G + l_2^B + l_2^C} + 2^{l_2} \quad < \quad 2^{l_1 + l_2}$$

Dynamic Key-guessing in Linear Attacks

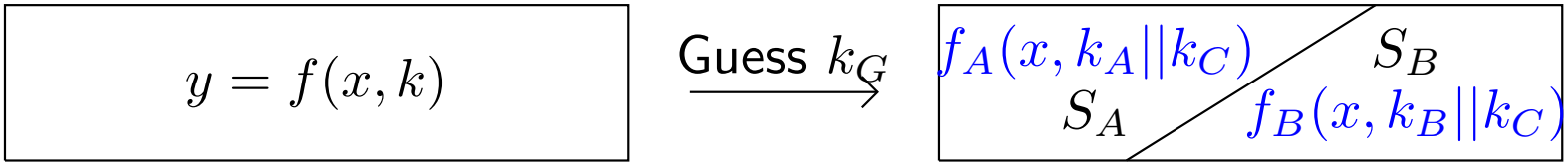

Figure: When k_G is known, the set of x can be splitted to two sets. f is independent of k_B in set S_A and independent of k_A in set S_B.

Example:$y = f(x, k) = (x_0 \oplus k_0)\&(x_1 \oplus k_1)$, compute the bias of y where $V[x]$ denotes the numer of x

- GUESS k_0 and SPLIT the x into two sets
  - For the x with $x_0 = k_0$, initialize a counter T_0 and set $T_0 = V[0||x_0] + V[1||x_0]$ (1 addition)
  - For the x with $x_0 = k_0 \oplus 1$, initialize a counter T_1 and set $T_1 = V[0||x_0] - V[1||x_0]$ (1 addition)
  - COMBINE $B^k(y) = T_0 + (-1)^{k_1} T_1$ (2 additions)
- TIME: $(2^2 \times 2^2 = 2^4) \rightarrow (2 \times (1 + 1 + 2) = 2^3)$

Outline

Brief Description of Simon

block size $(2n)$	key size (mn)	rounds
32 $(n = 16)$	64 $(m = 4)$	32
48 $(n = 24)$	72 $(m = 3)$	36
	96 $(m = 4)$	36
64 $(n = 32)$	96 $(m = 3)$	42
	128 $(m = 4)$	44
96 $(n = 48)$	96 $(m = 2)$	52
	144 $(m = 3)$	54
128 $(n = 64)$	128 $(m = 2)$	68
	192 $(m = 3)$	69
	256 $(m = 4)$	72

Table: The SIMON Family Block Ciphers

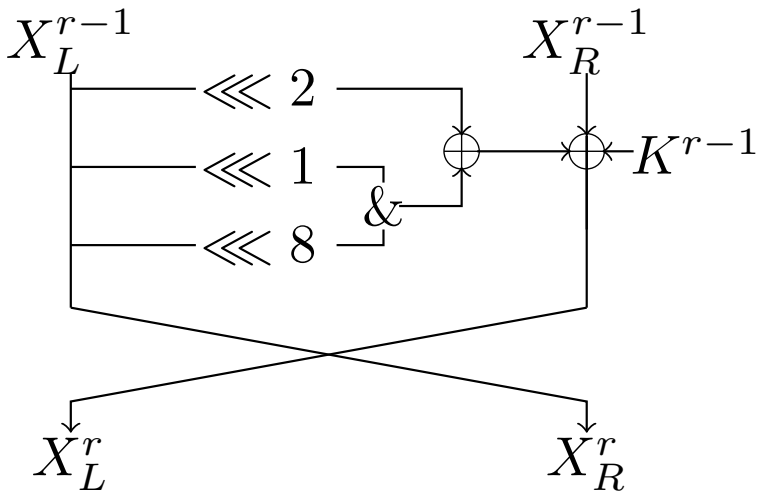

Figure: Round Function of SIMON

$$X_{L,i}^r = X_{i-2}^{r-1} \oplus (X_{i-1}^{r-1} \& X_{i-8}^{r-1}) \oplus X_{R,i}^{r-1} \oplus K_i^{r-1}$$
$$X_{R,i}^r = X_{L,i}^{r-1}$$

Linear Hulls of Simon

BS	Input Active Bits	Output Active Bits	ALH	#R	Ref.
32	$X^i_{L,6}$	$X^{i+13}_{R,14}$	$2^{-31.69}$	13	[1]
	$\boldsymbol{X^i_{L,5}}$	$\boldsymbol{X^{i+13}_{R,13}}$	$\boldsymbol{2^{-30.19}}$	**13**	**[2]**
	$X^i_{L,0}$	$X^{i+14}_{L,8}, X^{i+14}_{R,6}$	$2^{-32.56}$	14	[1]
48	$X^i_{L,7,11,19}, X^i_{R,9,17}$	$X^{i+15}_{L,5}, X^{i+15}_{R,3,7,11,19}$	$2^{-44.11}$	15	[1]
	$X^i_{L,6,14,18,22}, X^i_{R,16}$	$X^{i+15}_{L,4,20}, X^{i+15}_{R,6,18,20,22}$	$2^{-42.28}$	15	[2]
	$\boldsymbol{X^i_{L,1,5,21}, X^i_{R,23}}$	$\boldsymbol{X^{i+16}_{L,1,5}, X^{i+16}_{R,23}}$	$\boldsymbol{2^{-44.92}}$	**16**	**[3]**
64	$\boldsymbol{X^i_{L,20,24}, X^i_{R,22}}$	$\boldsymbol{X^{i+21}_{L,22}, X^{i+21}_{R,20,24}}$	$\boldsymbol{2^{-62.53}}$	**21**	**[1]**
	$X^i_{L,6}$	$X^{i+21}_{L,0}, X^{i+21}_{R,2,6,30}$	$2^{-60.72}$	21	[2]
	$X^i_{L,3,27,31}, X^i_{R,29}$	$X^{i+22}_{L,3}, X^{i+22}_{R,1,2}$	$2^{-63.83}$	22	[2]
96	$\boldsymbol{X^i_{L,2,34,38,42}, X^i_{R,36}}$	$\boldsymbol{X^{i+30}_{L,2,42,46}, X^{i+30}_{R,0,40}}$	$\boldsymbol{2^{-94.2}}$	**30**	**[1]**
128	$\boldsymbol{X^i_{L,2,58,62}, X^i_{R,60}}$	$\boldsymbol{X^{i+41}_{L,60}, X^{i+41}_{R,0,2,58,62}}$	$\boldsymbol{2^{-126.6}}$	**41**	**[1]**

* BS means the block size of SIMON; #R means the number of rounds for the linear hull

[1] Mohamed Ahmed Abdelraheem *et al.* IACR Cryptology ePrint Archive 2014/681, 2014

[2] Danping Shi *et al.*IACR Cryptology ePrint Archive 2014/973, 2014

[3] Siwei Sun *et al.* IACR Cryptology ePrint Archive 2014/747, 2014

Experimental Bias for the 13-round Linear Hull of Simon32

Property 1 (Rotational Property)

If the potential of the linear hull $(\alpha_L, \alpha_R) \xrightarrow{r-round} (\beta_L, \beta_R)$ *for Simon*$2n$ *is* $\bar{\epsilon}^2$*, then for any* $i, 0 \leq i \leq n$*, the potential of*

$$(\alpha_L \lll i, \alpha_R \lll i) \xrightarrow{r-round} (\beta_L \lll i, \beta_R \lll i)$$

for Simon$2n$ *is also* $\bar{\epsilon}^2$*.*

For Simon32:

$X^i_{L,5} \rightarrow X^{i+13}_{R,13} \quad \bar{\epsilon}^2 = 2^{-30.19}$

$X^i_{L,6} \rightarrow X^{i+13}_{R,14} \quad \bar{\epsilon}^2 = 2^{-31.69}$

Choose 600 random keys and compute the empirical bias

$\epsilon^2 = \lvert p - 1/2 \rvert^2$	Number/600
$\epsilon^2 \geq 2^{-27.19}$	0.012
$2^{27.19} > \epsilon^2 \geq 2^{-28.19}$	0.035
$2^{28.19} > \epsilon^2 \geq 2^{-29.19}$	0.097
$2^{29.19} > \epsilon^2 \geq 2^{-30.19}$	0.12
$2^{30.19} > \epsilon^2 \geq 2^{-31.19}$	0.173
$\epsilon^2 < 2^{-31.19}$	0.563

Boolean representation of $X^i_{L,5}$ and $X^{i+13}_{R,13}$

- One round backward for $X^i_{L,5}$

$$X^i_{L,5} = \underbrace{(X^{i-1}_{L,4} \& X^{i-1}_{L,13}) \oplus X^{i-1}_{L,3} \oplus X^{i-1}_{R,5}}_{x_0} \oplus \underbrace{K^{i-1}_5}_{k_0} = x_0 \oplus k_0.$$

- Four rounds backward for $X^i_{L,5}$: $X^i_{L,5} = f(x,k)$ where

$$\begin{aligned} f(x,k) =& x_0 \oplus k_0 \oplus ((x_1 \oplus k_1)\&(x_2 \oplus k_2)) \oplus ((x_3 \oplus k_3)\&(x_4 \oplus k_4)) \oplus \\ & [(x_5 \oplus k_5 \oplus ((x_6 \oplus k_6)\&(x_7 \oplus k_7)))\&(x_8 \oplus k_8 \oplus ((x_9 \oplus k_9)\&(x_7 \oplus k_7)))] \oplus \\ & \{(x_{10} \oplus k_{10} \oplus ((x_6 \oplus k_6)\&(x_7 \oplus k_7)) \oplus \\ & [(x_{11} \oplus k_{11} \oplus ((x_{12} \oplus k_{12})\&(x_{13} \oplus k_{13})))\&(x_{14} \oplus k_{14} \oplus ((x_3 \oplus k_3)\&(x_{13} \oplus k_{13})))])\& \\ & (x_{15} \oplus k_{15} \oplus ((x_7 \oplus k_7)\&(x_9 \oplus k_9)) \oplus \\ & [(x_{14} \oplus k_{14} \oplus ((x_{13} \oplus k_{13})\&(x_3 \oplus k_3)))\&(x_{16} \oplus k_{16} \oplus ((x_3 \oplus k_3)\&(x_4 \oplus k_4)))])\}, \end{aligned}$$

  $x_0, \ldots, x_{16}$ can be computed from X^{i-4}, $k_0, \ldots, k_{16}$ are the xor-sums of some bits of $K^{i-4}, \ldots, K^{i-1}$ (See the following table)

- Four rounds forward for $X^{i+13}_{R,13}$: similar to that above

Table: 4 rounds before $X^i_{L,5}$ for SIMON32

x_0	$X^{i-4}_{L,13} \oplus (X^{i-4}_{L,14} \& X^{i-4}_{L,7}) \oplus X^{i-4}_{R,15} \oplus X^{i-4}_{L,1} \oplus X^{i-4}_{L,5}$	k_0	$K^{i-4}_{15} \oplus K^{i-3}_{1} \oplus K^{i-3}_{5} \oplus K^{i-2}_{3} \oplus K^{i-1}_{5}$
x_1	$X^{i-4}_{L,14} \oplus (X^{i-4}_{L,15} \& X^{i-4}_{L,8}) \oplus X^{i-4}_{R,0}$	k_1	K^{i-4}_{0}
x_2	$X^{i-4}_{L,7} \oplus (X^{i-4}_{L,8} \& X^{i-4}_{L,1}) \oplus X^{i-4}_{R,9}$	k_2	K^{i-4}_{9}
x_3	$X^{i-4}_{L,2} \oplus (X^{i-4}_{L,3} \& X^{i-4}_{L,12}) \oplus X^{i-4}_{R,4}$	k_3	K^{i-4}_{4}
x_4	$X^{i-4}_{L,11} \oplus (X^{i-4}_{L,12} \& X^{i-4}_{L,5}) \oplus X^{i-4}_{R,13}$	k_4	K^{i-4}_{13}
x_5	$X^{i-4}_{L,14} \oplus (X^{i-4}_{L,15} \& X^{i-4}_{L,8}) \oplus X^{i-4}_{R,0} \oplus X^{i-4}_{L,2}$	k_5	$K^{i-4}_{0} \oplus K^{i-3}_{2}$
x_6	$X^{i-4}_{L,15} \oplus (X^{i-4}_{L,0} \& X^{i-4}_{L,9}) \oplus X^{i-4}_{R,1}$	k_6	K^{i-4}_{1}
x_7	$X^{i-4}_{L,8} \oplus (X^{i-4}_{L,9} \& X^{i-4}_{L,2}) \oplus X^{i-4}_{R,10}$	k_7	K^{i-4}_{10}
x_8	$X^{i-4}_{L,7} \oplus (X^{i-4}_{L,8} \& X^{i-4}_{L,1}) \oplus X^{i-4}_{R,9} \oplus X^{i-4}_{L,11}$	k_8	$K^{i-4}_{9} \oplus K^{i-3}_{11}$
x_9	$X^{i-4}_{L,1} \oplus (X^{i-4}_{L,2} \& X^{i-4}_{L,11}) \oplus X^{i-4}_{R,3}$	k_9	K^{i-4}_{3}
x_{10}	$X^{i-4}_{L,14} \oplus (X^{i-4}_{L,15} \& X^{i-4}_{L,8}) \oplus X^{i-4}_{R,0} \oplus (X^{i-4}_{L,3} \& X^{i-4}_{L,12}) \oplus X^{i-4}_{R,4}$	k_{10}	$K^{i-4}_{0} \oplus K^{i-3}_{2} \oplus K^{i-4}_{4} \oplus K^{i-2}_{4}$
x_{11}	$X^{i-4}_{L,15} \oplus (X^{i-4}_{L,0} \& X^{i-4}_{L,9}) \oplus X^{i-4}_{R,1} \oplus X^{i-4}_{L,3}$	k_{11}	$K^{i-4}_{1} \oplus K^{i-3}_{3}$
x_{12}	$X^{i-4}_{L,0} \oplus (X^{i-4}_{L,1} \& X^{i-4}_{L,10}) \oplus X^{i-4}_{R,2}$	k_{12}	K^{i-4}_{2}
x_{13}	$X^{i-4}_{L,9} \oplus (X^{i-4}_{L,10} \& X^{i-4}_{L,3}) \oplus X^{i-4}_{R,11}$	k_{13}	K^{i-4}_{11}
x_{14}	$X^{i-4}_{L,8} \oplus (X^{i-4}_{L,9} \& X^{i-4}_{L,2}) \oplus X^{i-4}_{R,10} \oplus X^{i-4}_{L,12}$	k_{14}	$K^{i-4}_{10} \oplus K^{i-3}_{12}$
x_{15}	$X^{i-4}_{L,7} \oplus (X^{i-4}_{L,8} \& X^{i-4}_{L,1}) \oplus X^{i-4}_{R,9} \oplus (X^{i-4}_{L,12} \& X^{i-4}_{L,5}) \oplus X^{i-4}_{R,13}$	k_{15}	$K^{i-4}_{9} \oplus K^{i-3}_{11} \oplus K^{i-4}_{13} \oplus K^{i-2}_{13}$
x_{16}	$X^{i-4}_{L,1} \oplus (X^{i-4}_{L,2} \& X^{i-4}_{L,11}) \oplus X^{i-4}_{R,3} \oplus X^{i-4}_{L,5}$	k_{16}	$K^{i-4}_{3} \oplus K^{i-3}_{5}$

Notice: $x_{10} = x_3 \oplus x_5, x_{15} = x_4 \oplus x_8$

Compute the correlation of f

- 15 independent bits for x since $x_{10} = x_3 \oplus x_5, x_{15} = x_4 \oplus x_8$
- 17 key bits of k
- Compress x_0 since $f(x,k)$ is linear with $x_0 \oplus k_0$, 14 independent bits of x remain; 16 bits of k remain
- Guess k_1, k_3, k_7. CASE $(x_1 \oplus k_1, x_3 \oplus k_3, x_7 \oplus k_7)$
  - $(0,0,0)$
    - $f = f_{00}$

$$f_{00} = ((x_5 \oplus k_5)\&(x_8 \oplus k_8)) \oplus \{(x_{10} \oplus k_{10} \oplus [(x_{11} \oplus k_{11} \oplus ((x_{12} \oplus k_{12})\&(x_{13} \oplus k_{13})))\&(x_{14} \oplus k_{14})])\&(x_{15} \oplus k_{15} \oplus [(x_{14} \oplus k_{14})\&(x_{16} \oplus k_{16})])\}$$

    - 8 independent bits of x remain $(x_{10} = x_3 \oplus x_5)$
    - 7 additions to compress the other bits of x
    - Getting new counters needs $T_s = 2^8 \times 7$ additions
  - $(0,0,1), \ldots, (1,1,1)$ similar to $(0,0,0)$

Compute the correlation of f_{00}

- Guess k_5, k_{14} and split the x into 4 sets

Table: Simplification for f_{00} after guessing k_5, k_{14}

Guess	Value	f_{00}	RB
k_5, k_{14}	0,0	$(x_{10} \oplus k_{10})\&(x_{15} \oplus k_{15})$	
	0,1	$(x_{10,11} \oplus k_{10,11} \oplus ((x_{12} \oplus k_{12})\&(x_{13} \oplus k_{13})))\&(x_{15,16} \oplus k_{15,16})$	
	1,0	$(x_{10} \oplus k_{10})\&(x_{15} \oplus k_{15})$	k_8
	1,1	$(x_{10,11} \oplus k_{10,11} \oplus ((x_{12} \oplus k_{12})\&(x_{13} \oplus k_{13})))\&(x_{15,16} \oplus k_{15,16})$	k_8

  - Case $(0,0), (1,0)$
    - Getting new counters: $2^6 - 2$ additions
    - Similar to the example, however there is dependence between x_5 and x_{10}, computing the bias needs no more than 2^2 additions
  - Case $(0,1), (1,1)$
    - Getting new counters: $2^6 - 2^4$ additions
    - Computing the bias needs about $2^{5.64}$ additions
- Total time $2^{11.19}$ additions

Attacks on Simon32/64

- Time of computing correlation of f is about

$$((\underbrace{2^8 \times 7}_{T_{split}} + \underbrace{2^{11.19}}_{T_{inner}}) \times 8 + \underbrace{2^{13} \times 7}_{T_{combine}}) \times 2^3 = 2^{19.46}$$

- Data $N = 2\bar{\epsilon}^{-2} = 2^{31.19}$, advantage $a = 8$
- 21-round (4+13+4) attack: $2^{35.84} Additions + 2^{56} Encryptions$
  - computing the bias: $\underbrace{2^{14} \times 2^{19.46}}_{head\ part} + \underbrace{2^{16} \times 2^{19.46}}_{tail\ part} = 2^{35.84} Additions$
  - exhaustive part: $2^{64-a} = 2^{56} Encryptions$
- 22-round (4+13+5) attack: $2^{48.84} Additions + 2^{56} Encryptions$
- 23-round (5+13+5) attack: $2^{61.84} Additions + 2^{56.3} Encryptions$

Implementation of the 21-round Attack on Simon32

Table: Expected success probability using $2^{31.19}$ data and advantage $a = 8$

$\epsilon^2 = \lvert p - 1/2 \rvert^2$	proportion	Pr_{succ} [SB02]
$\epsilon^2 \geq 2^{-27.19}$	0.012	$p_0 \approx 1.000$
$2^{27.19} > \epsilon^2 \geq 2^{-28.19}$	0.035	$1 > p_1 > 0.997$
$2^{28.19} > \epsilon^2 \geq 2^{-29.19}$	0.097	$0.997 > p_2 > 0.846$
$2^{29.19} > \epsilon^2 \geq 2^{-30.19}$	0.12	$0.846 > p_3 > 0.477$
$2^{30.19} > \epsilon^2 \geq 2^{-31.19}$	0.173	$0.477 > p_3 > 0.188$
$\epsilon^2 < 2^{-31.19}$	0.563	negligible
Expected success probability		$0.33 > Pr > 0.22$

- Experimental success probability: 0.277 (1000 experiments done)
- Data collection: 11 minutes (encrypt and compress $2^{31.19}$ data)
- Key recovery: 11 minutes (get $2^{32-a} = 2^{24}$ key candidates)
- About 5GB memory
- source code (http://eprint.iacr.org/2015/666.pdf.)

Summary of Linear Hull Attacks on SIMON

Cipher	Attacked rounds	Data	Time	Reference
SIMON32/64	21	$2^{30.56}$	$2^{55.56}$	Abdelraheem et al
	21	-	-	Shi et al
	23	$\mathbf{2^{31.19}}$	$\mathbf{2^{61.84}A + 2^{56.3}E}$	**Our result**
SIMON48/72	20	$2^{44.11}$	$2^{70.61}$	Abdelraheem et al
	24	$\mathbf{2^{47.92}}$	$\mathbf{2^{67.89}A + 2^{65.34}E}$	**Our result**
SIMON48/96	21	$2^{44.11}$	$2^{70.61}$	Abdelraheem et al
	21	-	-	Shi et al
	23	$2^{47.92}$	$2^{92.92}$	Sun et al
	25	$\mathbf{2^{47.92}}$	$\mathbf{2^{89.89}A + 2^{88.28}E}$	**Our result**
SIMON64/96	27	$2^{62.53}$	$2^{88.53}$	Abdelraheem et al
	30	$\mathbf{2^{63.53}}$	$\mathbf{2^{93.62}A + 2^{88.13}E}$	**Our result**
SIMON64/128	29	$2^{62.53}$	$2^{123.53}$	Abdelraheem et al
	29	-	-	Shi et al
	31	$\mathbf{2^{63.53}}$	$\mathbf{2^{119.62}A + 2^{120.00}E}$	**Our result**
SIMON96/96	**37**	$\mathbf{2^{95.2}}$	$\mathbf{2^{67.94}A + 2^{88}E}$	**Our result**
SIMON96/144	36	$2^{94.2}$	$2^{123.5}$	Abdelraheem et al
	38	$\mathbf{2^{95.2}}$	$\mathbf{2^{98.94}A + 2^{136.00}E}$	**Our result**
SIMON128/128	**49**	$\mathbf{2^{127.6}}$	$\mathbf{2^{87.77}A + 2^{120}E}$	**Our result**
SIMON128/192	48	$2^{126.6}$	$2^{187.6}$	Abdelraheem et al
	51	$\mathbf{2^{127.6}}$	$\mathbf{2^{155.77}A + 2^{184.00}E}$	**Our result**
SIMON128/256	50	$2^{126.6}$	$2^{242.6}$	Abdelraheem et al
	53	$\mathbf{2^{127.6}}$	$\mathbf{2^{239.77}A + 2^{248.01}E}$	**Our result**

* '-' means not given; A means addition; E means encryption;

Thanks for Your Attention