Algebraic Differential Fault Attacks on SIMON Lightweight Block Ciphers

Le Duc Phong

Canadian Institute for Cybersecurity
Uiniversity of New Brunswick

29th August 2019

Agenda

- SIMON lightweight block ciphers
  - Design of SIMON ciphers
  - Existing security analysis of SIMON ciphers
- ADFA on SIMON ciphers in the bit-flip model
  - Algebraic Differential Fault Analysis Attacks (ADFA)
  - ADFA based on Differential trail
  - ADFA based on simplified Gröbner basis
  - ADFA based on SAT solvers

SIMON Lightweight Block Ciphers

- NSA (National Security Agency), U.S. introduced two families of lightweight block ciphers in June 2013
  - SIMON has been optimized for performance in Hardware implementations and
  - SPECK has been optimized for Software implementations
- Standardized by ISO as part of the RFID air interface standard, namely, ISO/29167-21, in 2018

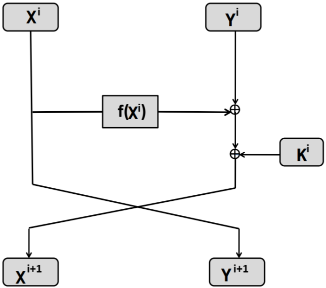
SIMON Lightweight Block Ciphers

Based on a typical Feistel design, each round consists of three simple bitwise operations: "AND", "XOR" and "rotation"

$$X^{i+1} = F(X^i) \oplus Y^i \oplus K^i$$
$$Y^{i+1} = X^i,$$

where

$$F(X^i) = (S^1(X^i) \& S^8(X^i)) \oplus S^2(X^i)$$



SIMON Lightweight Block Ciphers

Members of the SIMON family

Cipher	Block size $2n$	Key words m	Key size mn	Rounds T
SIMON-32/64	32	4	64	32
SIMON-48/72	48	3	72	36
SIMON-48/96	48	4	96	36
SIMON-64/96	64	3	96	42
SIMON-64/128	64	4	128	44
SIMON-96/96	96	2	96	52
SIMON-96/144	96	3	144	54
SIMON-128/128	128	2	128	68
SIMON-128/196	128	3	196	69
SIMON-128/256	128	4	256	72

A brief summary of attacks against SIMON Ciphers

There have been more than 70 security analysis papers on SIMON by 2018

- Statistics-based attacks: Differential and Linear cryptanalysis
  - require a large amount of data
- Algebraic attack
  - deterministic, i.e., it doesn't depend on any statistical property
  - requires just a couple of pair plainttexts/ciphertexts
  - complexity heavily depends on the complexity of algebraic solving techniques
- Implementation attacks
  - Side-channel analysis
  - Fault analysis

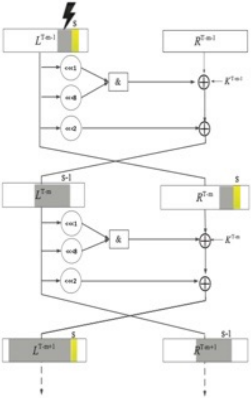
Algebraic Differential Fault Attacks on SIMON ciphers

Algebraic Differential Fault attacks

Inject a fault at intermediate input of an r^{th}-round cipher

In bit-flip fault model, (only) one bit will be flipped when a fault injected

- Let x_ℓ^r denote the value of the bit before it is flipped, so $\bar{x}_j^r = x_j^r + 1$, where $j = \ell$ and $\bar{x}_j^r = x_j^r$ for everywhere else.
- Let input difference $\delta_j^r = \bar{x}_j^r + x_j^r$, so $\delta_\ell^r = 1$, and $\delta_j^r = 0$ for $j \neq \ell$
- Each bit flipped will affect to 3 input bits in the next round



Algebraic Fault Attacks against SIMON ciphers

Lemma

Let $\delta_j^i = x_j^i + x_j'^i$ *for* $r \leq i \leq T$ *be the differential representation of two correct and faulty bits* x_j^i *and* $x_j'^i$*. We have,* $\delta_j^r = 0$ *for* $j \neq l$ *and equal to* 1 *if* $j = l$*, and:*

$$\delta_j^{i+1} = \delta_{j-1}^i x_{j-8}^i + \delta_{j-8}^i x_{j-1}^i + \delta_{j-1}^i \delta_{j-8}^i + \delta_{j-2}^i + \delta_j^{i-1} \qquad (1)$$

We have:

$$\begin{aligned} x_j^{i+1} &= x_{j-1}^i x_{j-8}^i + x_{j-2}^i + y_j^i + k_j^i, \text{ and} \\ \bar{x}_j^{i+1} &= \bar{x}_{j-1}^i \bar{x}_{j-8}^i + \bar{x}_{j-2}^i + \bar{y}_j^i + k_j^i \end{aligned}$$

Summing up the two equations:

$$\begin{aligned} \delta_j^{i+1} = & x_{j-1}^i x_{j-8}^i + \bar{x}_{j-1}^i \bar{x}_{j-8}^i + \delta_{j-2}^i + \delta_j^{i-1} \\ = & \delta_{j-1}^i x_{j-8}^i + \delta_{j-8}^i x_{j-1}^i + \delta_{j-1}^i \delta_{j-8}^i + \delta_{j-2}^i + \delta_j^{i-1}. \end{aligned}$$

Bit-flip attack at the second last round $(T-2)$

Aim: retrieve the last round key K^{T-1}

$$K^{T-1} = X^{T-2} \oplus F(Y^T) \oplus X^T \tag{2}$$

Bit	**15**	**14**	**13**	**12**	**11**	**10**	**9**	**8**
Δ^{T-3}	0	0	0	0	0	0	0	0
Δ^{T-2}	1	0	0	0	0	0	0	0
Δ^{T-1}	0	0	0	0	0	0	0	0
Δ^{T}	$*$	0	0	0	0	0	$x_6^{T-2} + x_8^{T-1}$	$*$

Bit	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
Δ^{T-3}	0	0	0	0	0	0	0	0
Δ^{T-2}	0	0	0	0	0	0	0	0
Δ^{T-1}	x_6^{T-2}	0	0	0	0	0	1	x_8^{T-2}
Δ^{T}	0	0	0	0	1	$x_8^{T-2} + x_{10}^{T-1}$	$*$	0

Conclusion: If the attacker controls the position of faults, she could retrieve the last round key with $n/2$ faults.

Bit-flip attack at the third last round $(T-3)$

Aim: retrieve the last two round keys K^{T-1} and K^{T-2}

Bit	15	14	13	12	11	10	9	8
Δ^{T-4}	0	0	0	0	0	0	0	0
Δ^{T-3}	1	0	0	0	0	0	0	0
Δ^{T-2}	0	0	0	0	0	0	0	0
Δ^{T-1}	$x_6^{T-3}x_{14}^{T-2}+1$	0	0	0	0	0	$x_6^{T-3}+x_8^{T-2}$	$x_6^{T-3}x_0^{T-2}+x_8^{T-3}x_7^{T-2}+x_6^{T-3}x_8^{T-3}$
Δ^{T}	0	0	0	0	$*$	$*$	$*$	0

Bit	7	6	5	4	3	2	1	0
Δ^{T-4}	0	0	0	0	0	0	0	0
Δ^{T-3}	0	0	0	0	0	0	0	0
Δ^{T-2}	x_6^{T-3}	0	0	0	0	0	1	x_8^{T-3}
Δ^{T-1}	0	0	0	0	1	$x_8^{T-3}+x_{10}^{T-2}$	$x_8^{T-3}x_9^{T-2}$	0
Δ^{T}	$*$	0	1	$*$	$*$	$*$	$*$	$*$

Attacker can retrieve 3.5 bits X^{T-2} and 2 bits X^{T-3} with 1 fault

<u>Conclusion</u>: If the attacker controls the position of faults, she could retrieve the last two round key with $n/2$ faults.

Recover the master key

- Ciphers with key words $m = 2$ require two round keys to recover the master key, so the attack at the third last round $T - 3$ could be used

- Likewise, ciphers with key words $m = 3$ and 4 require 3 (resp. 4) round keys to recover the master key

- To get more round keys, attacker will inject faults in an earlier round, e.g., at the round $T - 5$ to get 4 round keys

Differential Trail Table

Bit	15	14	13	12	11	10	9	8
Δ^{T-6}	0	0	0	0	0	0	0	0
Δ^{T-5}	1	0	0	0	0	0	0	0
Δ^{T-4}	0	0	0	0	0	0	0	0
Δ^{T-3}	$*$	0	0	0	0	0	$x_6^{T-5} + x_8^{T-4}$	$*$
Δ^{T-2}	0	0	0	0	$x_6^{T-5} + x_8^{T-4} + x_{10}^{T-3}$	$*$	$*$	0
Δ^{T-1}	$*$	0	$x_6^{T-5} + x_8^{T-4} + x_{10}^{T-3} + x_{12}^{T-2}$	$*$	$*$	$*$	$*$	$*$
Δ^{T}	Known values							

Bit	7	6	5	4	3	2	1	0
Δ^{T-6}	0	0	0	0	0	0	0	0
Δ^{T-5}	0	0	0	0	0	0	0	0
Δ^{T-4}	x_6^{T-5}	0	0	0	0	0	1	x_8^{T-5}
Δ^{T-3}	0	0	0	0	1	$x_8^{T-5} + x_{10}^{T-4}$	$*$	0
Δ^{T-2}	$*$	0	1	$x_8^{T-5} + x_{10}^{T-4} + x_{12}^{T-3}$	$*$	$*$	$*$	$*$
Δ^{T-1}	1	$x_8^{T-5} + x_{10}^{T-4} + x_{12}^{T-3} + x_{14}^{T-2}$	$*$	$*$	$*$	$*$	$*$	0
Δ^{T}	Known values							

Bit flip attack using simplified Gröbner basis

- Choose one pair of plaintext/ciphertext
- Perform t bit flips at round $r - 6$.
- This gives $t + 1$ different plaintext/ciphertext pairs.
- Form the equations together with the linear equations for the bit flips.
- Perform ElimLin until no more linear equation can be found.
- Extract out all the equations involving the key bits. Let S denote this set of equations.
- Let $S^* = S \cup \{k_i f : f \in S, k_i \text{ is a key variable } \}$. Perform Gaussian elimination and extract out all the equations with degree ≤ 2. Continue the process until all the key variables are found.

Our experimental results

We carried out the above attack on 3 versions of SIMON

Cipher	Round	Total no of key variables	No of faults	Average No of key variables found	Timing (s)
SIMON-32/64	$T-5$	512	4	508.38	2.6
SIMON-32/64	$T-5$	512	5	511.46	0.7
SIMON-32/64	$T-6$	512	3	511.8	35.3
SIMON-32/64	$T-6$	512	4	511.9	2
SIMON-48/72	$T-6$	864	4	864	26
SIMON-48/72	$T-6$	864	5	864	8.5
SIMON-48/96	$T-6$	864	4	864	5.3
SIMON-48/96	$T-6$	864	5	864	4.1
SIMON-64/128	$T-6$	1048	5	1046	34.3
SIMON-64/128	$T-7$	1048	5	1048	28.8

Bit-flip attacks using SAT solvers

- Randomly select a plaintext/ciphertext pair
- Fix a round $r_0 < T$.
- For each $i = 0$ to $t - 1$, flip bit i at round r_0 and obtain the corresponding faulty ciphertext. We therefore have 1 actual ciphertext and t faulty ciphertexts.
- Decrypt the faulty ciphertexts to find the corresponding plaintexts.
- Write down the equations for the $t + 1$ plaintext/ciphertext pairs together with the linear relations representing the bit flips.
- Solve the system using the SAT solver

Our experimental results

Table: Number of instances solved out of 50 in 10 minutes and corresponding executed timings.

Cipher	No of faults	No of key bits fixed	Instances solved	Timing (s)
SIMON-32/64	1	18	34	99.1
SIMON-32/64	1	20	42	69.4
SIMON-32/64	1	22	46	47.4
SIMON-48/72	1	22	36	41.2
SIMON-48/72	1	24	42	31.9
SIMON-48/72	1	26	45	37
SIMON-48/96	1	40	22	77.1
SIMON-48/96	1	42	30	103.7
SIMON-48/96	1	44	34	72.4

Thank you for listening!

Questions