Security of SIMON against Linear Cryptanalysis

Javad Alizadeh[1] Nasour Bagheri[1]
Praveen Gauravaram[2] Abhishek Kumar[3]
Somitra Kumar Sanadhya[3]

[1]Shahid Rajaee Teacher Training University, Iran,
[2]Tata Consultancy Services Limited, India,
[3]Indraprastha Institute of Information Technology, Delhi, India,

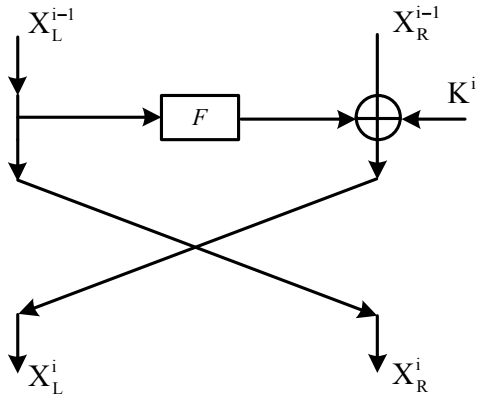
Asiacrypt 2013 Rump Session

December 3, 2013

Design Description

- SIMON is a family of 10 lightweight ciphers published by Beaulieu *et al.* from U.S.National Security Agency.
- SIMONN/k: classical Feistel structure, N bit blocks, k-bit key. The number of rounds vary for different variants.
- For example, SIMON32/64 has block size of 32 bits with a 64-bit key and has 32 rounds.
- Each round of SIMON includes a non-invertible function F. For $X \in \{0,1\}^n$, $F(x)$ is defined as :

$$F(X) = (X \lll 2) \oplus ((X \lll 1) \& (X \lll 8))$$



Linear Cryptanalysis of SIMON

- Some highly biased Linear characteristics for F:

$$\left.\begin{array}{ll} \text{Linear Approximation 1}: & Pr[(F(X))_i = (X)_{i-2}] = \frac{3}{4} \\ \text{Linear Approximation 2}: & Pr[(F(X))_i = (X)_{i-2} \oplus (X)_{i-1}] = \frac{3}{4} \\ \text{Linear Approximation 3}: & Pr[(F(X))_i = (X)_{i-2} \oplus (X)_{i-8}] = \frac{3}{4} \\ \text{Linear Approximation 4}: & Pr[(F(X))_i = (X)_{i-2} \oplus ((X)_{i-1} \oplus (X)_{i-8})] = \frac{1}{4} \end{array}\right\} \quad (1)$$

- Given Eq(1), one round linear expression for SIMON :

$$Pr[(P_R)_2 \oplus (K^1)_2 \oplus (X_L^1)_2 \oplus (P_L)_0 = 0] = \frac{3}{4} \quad (2)$$

- 3-round linear expression for SIMON :

$$Pr[(X_R^{i-1})_2 \oplus (K^i)_2 \oplus (X_L^{i-1})_0 \oplus (X_R^{i+2})_0 \oplus (K^{i+2})_2 \oplus (X_L^{i+2})_2 = 0] = \frac{5}{8} \quad (3)$$

- Our attack works for 12 rounds of SIMON32/64. Using Eq(1) any variant of SIMON can be linearized for any number of rounds, but the complexity of attack is bounded by the data complexity.
- For example, 13-round SIMON32/64 has bias 2^{-16}, hence data complexity exceeds 2^{32}, for a good success probability.

Conncetion between Linear and Differential Cryptanalysis of SIMON

- Some high probability differential characteristic for SIMON:

$$\left.\begin{aligned}
&\text{Differential Characteristic 1}: (\Delta X)_i \xrightarrow{\frac{1}{4}} (\Delta F(X))_{i+2} \\
&\text{Differential Characteristic 2}: (\Delta X)_i \xrightarrow{\frac{1}{4}} (\Delta F(X))_{i+2,i+1} \\
&\text{Differential Characteristic 3}: (\Delta X)_i \xrightarrow{\frac{1}{4}} (\Delta F(X))_{i+2,i+8} \\
&\text{Differential Characteristic 4}: (\Delta X)_i \xrightarrow{\frac{1}{4}} (\Delta F(X))_{i+2,i+1,i+8}
\end{aligned}\right\} \quad (4)$$

- For linear characteristics, we approximate bits from output of F-function with bits from its input.
- For differential characteristics, we propagate input bit differences of F to output bit differences.
- Given Eq(1) and Eq(4), for an r-round differential characteristic we can construct an equivalent r-round linear characteristic by employing the related approximations.
- This connection is used to improve the previous LC attacks on SIMON for all variants with block size more than 32 bits.

Our Results

Table: N = Block size, ϵ = Bias for the linear expression to hold, # approximation = number of times the biased linear characteristic is used to attack the cipher.

Variant of SIMON	32/64	48/96	64/128	96/144	128/256
Total numbers of rounds	32	36	44	54	72
# rounds with $\epsilon \geq 2^{-\frac{N}{2}+2}$	10	13	17	26	33
# rounds attacked	12	15	19	28	35
# approximation	13	19	28	44	59
Data Complexity	2^{31}	2^{43}	2^{61}	2^{93}	2^{123}

- Please refer http://eprint.iacr.org/2013/663.pdf for detailed analysis.

THANK YOU