A Brief Comparison of SIMON and SIMECK

Stefan Kölbl[1] Arnab Roy[1]

September 21, 2016

[1]DTU Compute, Technical University of Denmark, Denmark

The Simeck block cipher family

Simeck

SIMECK is a family of lightweight block ciphers [YZS+15]

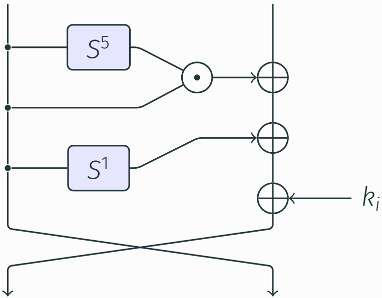
- Combines ideas from SIMON and SPECK.
- Uses different rotation constants.
- Key-schedule reuses the round function.
- Uses less (up to 3.5%) area than SIMON.

Parameters (gray only SIMON):

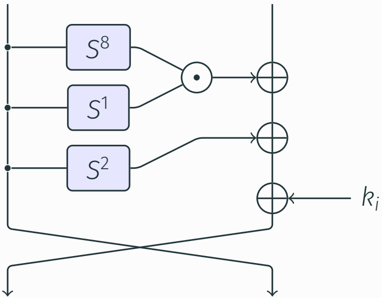
Block size	Key size
32	64
48	72, 96
64	96, 128
96	96, 144
128	128, 192, 256

Simeck

Construction of the round function



(a) Simeck



(b) Simon

Simeck

Design of SIMON and SIMECK

- No design rationales for SIMON and SPECK published.
- Impact of the design changes on the security is unclear.

Comparison of Simeck and Simon

Comparison of Simeck and Simon

After how many rounds do we get full *diffusion*?

- Rotation constants have a strong effect on this.
- Often influences efficiency of attacks.

Table 1: Number of rounds required for full diffusion.

Wordsize	32-bit	48-bit	64-bit
SIMON	7 Rounds	8 Rounds	9 Rounds
SIMECK	8 Rounds	9 Rounds	11 Rounds

Comparison of Simeck and Simon

Best attacks on SIMON are based on differential and linear cryptanalysis.

- Various papers on this topic [ALLW15, SHW+15, AAA+14, WWJZ14, BRV15, SHW+14, CW16].
- We study how the design changes of SIMECK affect the resistance against these type of attacks.

Comparison of Simeck and Simon

Differential cryptanalysis tries to find a correlation between pairs of plaintexts (p, p') and ciphertexts (c, c').

Definition

A *differential trail* Q is a sequence of differences

$$Q = (\alpha_0 \xrightarrow{f_0} \alpha_1 \xrightarrow{f_1} \cdots \alpha_{r-1} \xrightarrow{f_{r-1}} \alpha_r).$$

How to compute the probability that a random pair of plaintexts follows this trail?

- Always involves some assumptions.
- Use framework from [KLT15] to compute probabilities.

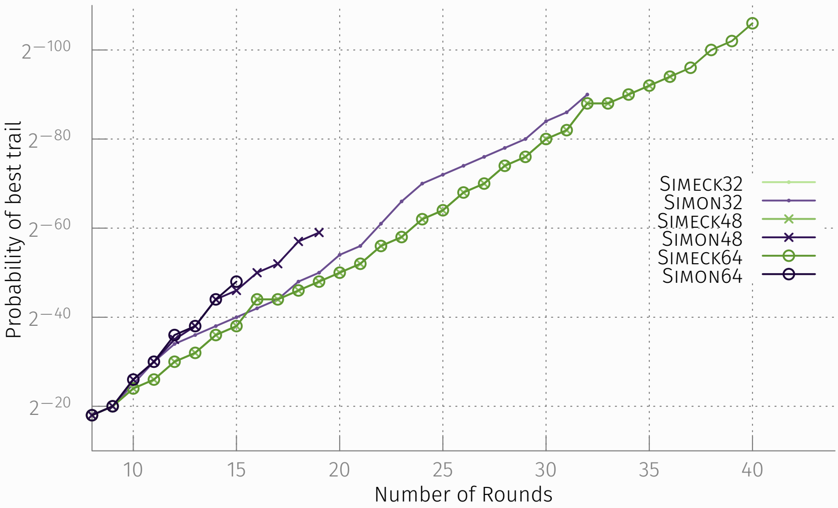
Comparison of Simeck and Simon

Interested in the differential trail with highest probability

$$p_{\max} = \max_{\alpha_0,\ldots,\alpha_r} \Pr(\alpha_0 \xrightarrow{f_0} \alpha_1 \xrightarrow{f_1} \cdots \alpha_{r-1} \xrightarrow{f_{r-1}} \alpha_r) \tag{1}$$

- Use approach based on SAT solvers to find bounds on $p_{\max}$.
- Publicly available tool `https://github.com/kste/cryptosmt`.

Comparison of Simeck and Simon



Comparison of Simeck and Simon

Cipher	Rounds	Upper Bounds	
		differential	linear
SIMON32/64	32	**32**	**32**
SIMECK32/64	32	**32**	**32**
SIMON48/96	36	**19**	**20**
SIMECK48/96	36	**36**	**36**
SIMON64/128	44	15 [KLT15]	**17**
SIMECK64/128	44	**40**	**41**

- For the large variants the bounds for SIMECK are worse.
- Takes significant less time finding bounds for SIMECK.
- Can cover more rounds for SIMECK.

Comparison of Simeck and Simon

In attack we only care about the probability of the *differential*.

Definition

The probability of a *differential* is the sum of all r round differential trails

$$\Pr(\alpha_0 \xrightarrow{f} \alpha_r) = \sum_{\alpha_1,\ldots,\alpha_{r-1}} (\alpha_0 \xrightarrow{f_0} \alpha_1 \xrightarrow{f_1} \cdots \alpha_{r-1} \xrightarrow{f_{r-1}} \alpha_r) \tag{2}$$

which have the same input and output difference.

Comparison of Simeck and Simon

Example for SIMECK64 using 26 rounds:

- The best single trail Q has $\Pr(Q) = 2^{-68}$.
- The differential $(0, 4400000) \xrightarrow{f^{26}} (8800000, 400000)$ has a probability of $\geq 2^{-60.02}$.
- We need to collect a large set of trails to get a good estimate for the probability.

Comparison of Simeck and Simon

We are interested in the number of pairs following the differential

- For SIMON32 and SIMECK32 we can run experiments for the full codebook.
- Use Poisson distribution to estimate the distribution for a random function.

Definition

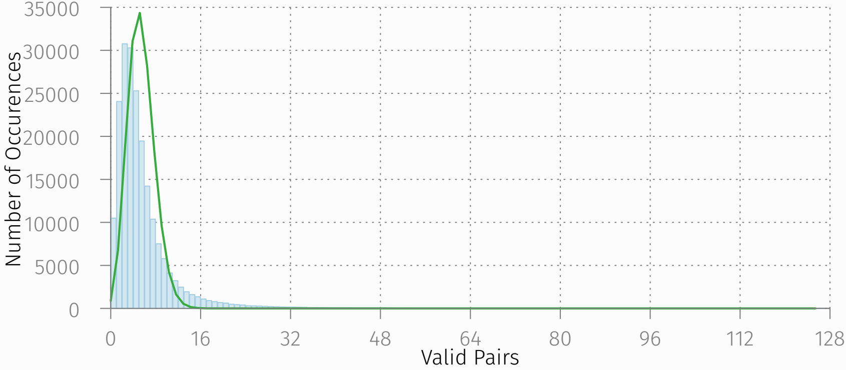
Let X be a Poisson distributed random variable representing the number of pairs (a, b) with values in $\mathbb{F}_2^n$ following a differential $Q = (\alpha \xrightarrow{f} \beta)$, that means $f(a) \oplus f(a \oplus \alpha) = \beta$, then

$$\Pr(X = l) = \frac{1}{2}(2^n p)^l \frac{e^{-(2^n p)}}{l!} \quad (3)$$

where p is the probability of the differential.

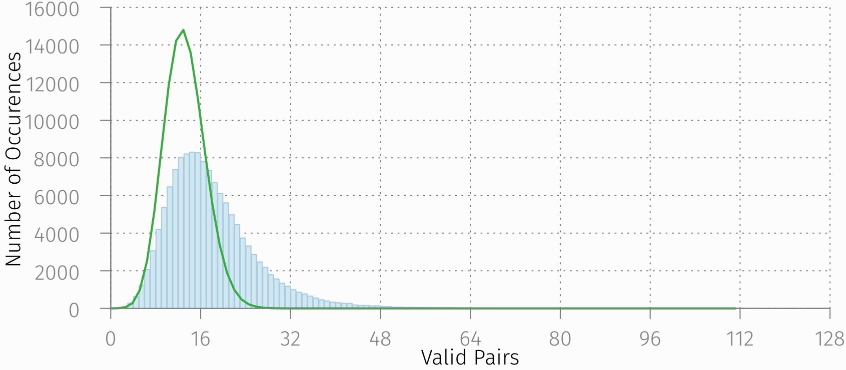
Comparison of Simeck and Simon

Distribution for 202225 randomly chosen keys for the differential $(0, 40) \xrightarrow{f^{13}} (4000, 0)$ for Simon32.



Comparison of Simeck and Simon

Distribution for 134570 randomly chosen keys for the differential $(8000, 4011) \xrightarrow{f^{13}} (4000, 0)$ for SIMECK32.



Comparison of Simeck and Simon

Approximation seems quite good but for some keys the number of valid pairs is significant higher.

Example: $K = (k_0, k_1, k_2, k_3) = (\texttt{8ec1}, \texttt{1cf8}, \texttt{e84a}, \texttt{cee2})$ we get 1082 pairs for the previous SIMON differential.

Key Recovery

Comparison of Simeck and Simon

Key recovery attacks based on differential distinguisher

- Use differential $\alpha \xrightarrow{f^r} \beta$ over r rounds.
- Extend in both directions using truncated differentials.

Round	ΔL	ΔR	$*$	$*$
−4	***0************	****************	15	16
−3	**000***0****1**	***0************	11	15
−2	0*0000*000***01*	**000***0****1**	6	11
−1	0100000000010001	0*0000*000***01*	0	6
0	1000000000000000	0100000000010001	0	0
		$(8000, 4011) \xrightarrow{f^{13}} (4000, 0)$		
13	0100000000000000	0000000000000000	0	0
14	1*000000000*000	0100000000000000	2	0
15	**00000*000**001	1*000000000*000	5	2
16	***000**00***01*	**00000*000**001	9	5
17	***00***0*******	***000**00***01*	13	9
18	***0************	***00***0*******	15	13
19	****************	***0************	16	15

Comparison of Simeck and Simon

Attacks can cover more rounds for Simeck

- Weaker diffusion allows better filtering and key guessing.
- Differential distinguisher can cover more rounds for the larger variants.

Comparison of Simeck and Simon

Example attack on 26-round SIMECK48

- Use four 20-round differentials with probability $\approx 2^{-44}$.
- Complexity: $T = 2^{62}, D = 2^{47}, M = 2^{47}$

Cipher	Rounds	Attack
SIMECK32/64	32	19
SIMECK48/96	36	26
SIMECK64/128	44	33

- Can be improved further by two rounds with dynamic key-guessing [QHS15].

Conclusion

Results

- Can show bounds for the best differential/linear trail for significant higher number of rounds.
- Statistical attacks can cover more rounds.

Open problems

- Find better approximation for distribution of valid pairs.
- Identify which (class of) keys give unusual high number of pairs.

Thank you for your attention!

References i

Javad Alizadeh, Hoda AlKhzaimi, Mohammad Reza Aref, Nasour Bagheri, Praveen Gauravaram, Abhishek Kumar, Martin M. Lauridsen, and Somitra Kumar Sanadhya, *Cryptanalysis of SIMON variants with connections*, Radio Frequency Identification: Security and Privacy Issues, RFIDSec 2014 (Nitesh Saxena and Ahmad-Reza Sadeghi, eds.), Lecture Notes in Computer Science, vol. 8651, Springer, 2014, pp. 90–107.

Farzaneh Abed, Eik List, Stefan Lucks, and Jakob Wenzel, *Differential cryptanalysis of round-reduced SIMON and SPECK*, Fast Software Encryption, FSE 2014 (Carlos Cid and Christian Rechberger, eds.), Lecture Notes in Computer Science, vol. 8540, Springer, 2015, pp. 525–545.

Alex Biryukov, Arnab Roy, and Vesselin Velichkov, *Differential analysis of block ciphers SIMON and SPECK*, Fast Software Encryption, FSE 2014 (Carlos Cid and Christian Rechberger, eds.), Lecture Notes in Computer Science, vol. 8540, Springer, 2015, pp. 546–570.

Huaifeng Chen and Xiaoyun Wang, *Improved linear hull attack on round-reduced simon with dynamic key-guessing techniques*, Fast Software Encryption - 23rd International Conference, FSE 2016, 2016, pp. 428–449.

Stefan Kölbl, Gregor Leander, and Tyge Tiessen, *Observations on the SIMON block cipher family*, Advances in Cryptology - CRYPTO 2015, 2015, pp. 161–185.

- Kexin Qiao, Lei Hu, and Siwei Sun, *Differential security evaluation of simeck with dynamic key-guessing techniques*, Cryptology ePrint Archive, Report 2015/902, 2015, `http://eprint.iacr.org/`.
- Siwei Sun, Lei Hu, Peng Wang, Kexin Qiao, Xiaoshuang Ma, and Ling Song, *Automatic security evaluation and (related-key) differential characteristic search: Application to SIMON, PRESENT, LBlock, DES(L) and other bit-oriented block ciphers*, Advances in Cryptology - ASIACRYPT 2014 (Palash Sarkar and Tetsu Iwata, eds.), Lecture Notes in Computer Science, vol. 8873, Springer, 2014, pp. 158–178.

- Siwei Sun, Lei Hu, Meiqin Wang, Peng Wang, Kexin Qiao, Xiaoshuang Ma, Danping Shi, Ling Song, and Kai Fu, *Constructing mixed-integer programming models whose feasible region is exactly the set of all valid differential characteristics of SIMON*, Cryptology ePrint Archive, Report 2015/122, 2015, `http://eprint.iacr.org/`.
- Ning Wang, Xiaoyun Wang, Keting Jia, and Jingyuan Zhao, *Differential attacks on reduced simon versions with dynamic key-guessing techniques*, Cryptology ePrint Archive, Report 2014/448, 2014, `http://eprint.iacr.org/`.
- Gangqiang Yang, Bo Zhu, Valentin Suder, Mark D. Aagaard, and Guang Gong, *The simeck family of lightweight block ciphers*, Cryptographic Hardware and Embedded Systems - CHES 2015, 2015, pp. 307–329.