Pen and Paper Arguments for SIMON and SIMON-like Designs

Christof Beierle

Horst Görtz Institute for IT Security
Ruhr-Universität Bochum, Germany

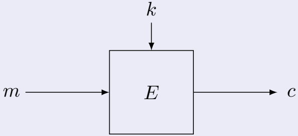
SCN 2016

Horst Görtz Institute
for IT-Security

Block Ciphers

Definition

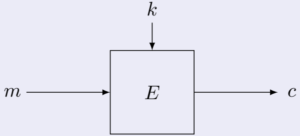
A block cipher is a function $E : \mathbb{F}_2^n \times \mathbb{F}_2^s \to \mathbb{F}_2^n$, such that $E(\cdot, k)$ is a permutation for every key $k \in \mathbb{F}_2^s$.



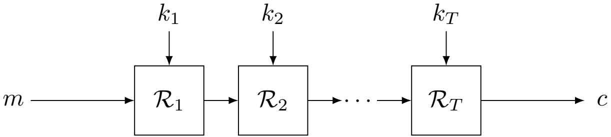
Block Ciphers

Definition

A block cipher is a function $E : \mathbb{F}_2^n \times \mathbb{F}_2^s \to \mathbb{F}_2^n$, such that $E(\cdot, k)$ is a permutation for every key $k \in \mathbb{F}_2^s$.



Typically, we use round-iterated constructions.



New Block Cipher Designs

- In the last years, many new primitives were proposed (e.g. CAESAR competition, lightweight designs)
- Lots of them use well-known constructions (e.g. AES-like ciphers)
- Some of them are more innovative (e.g. SIMON and SPECK)

New Block Cipher Designs

- In the last years, many new primitives were proposed (e.g. CAESAR competition, lightweight designs)
- Lots of them use well-known constructions (e.g. AES-like ciphers)
- Some of them are more innovative (e.g. SIMON and SPECK)

Common Sense: Explain your design!

New block ciphers should be designed in a way that allow for arguments on their security. Designers are expected to provide security arguments againt the most common attacks!

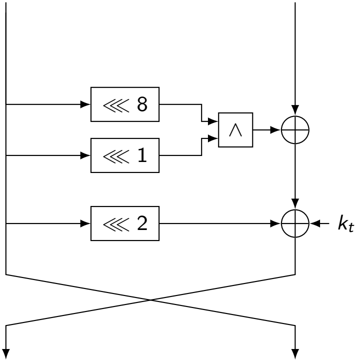
What is SIMON

- family of lightweight block ciphers designed for several block sizes and key length (10 versions in total)
- published by NSA in June 2013 on the IACR eprint archive[1]
- very simple and innovative construction

[1] R. Beaulieu et al. *The SIMON and SPECK Families of Lightweight Block Ciphers*. Cryptology ePrint Archive, Report 2013/404. `http://eprint.iacr.org/2013/404`. 2013.

Description of SIMON

- Feistel design
- A variety of block length supported (32, 48, 64, 96, 128 bit)
- The key length differs between 64 and 256 bit
- Simple round function
- 32 up to 72 rounds



New Block Cipher Designs

Common Sense: Explain your design!

New block ciphers should be designed in a way that allow for arguments on their security. Designers are expected to provide security arguments againt the most common attacks!

- Unfortunately, the designers of SIMON presented no design rationale of their ciphers.
- Lots of third-party analysis of SIMON was published. Most of the analysis is experimental.

Contribution

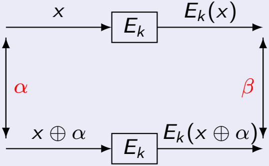
In this work, we focus on differential cryptanalysis.

- Considering differential attacks, we provide a non-experimental (pen and paper) security argument over multiple rounds of SIMON
- Thus, we contribute towards a better understanding of possible block cipher constructions.

Differential Cryptanalysis

Idea

For a function $E_k : \mathbb{F}_2^n \to \mathbb{F}_2^n$, we would like to consider a differential $\alpha \xrightarrow{E_k} \beta$.



The probability of a differential $\alpha \xrightarrow{E_k} \beta$ can be computed as

$$P(\alpha \xrightarrow{E_k} \beta) = \frac{\{x \in \mathbb{F}_2^n \mid \beta = E_k(x) \oplus E_k(x \oplus \alpha)\}}{2^n}.$$

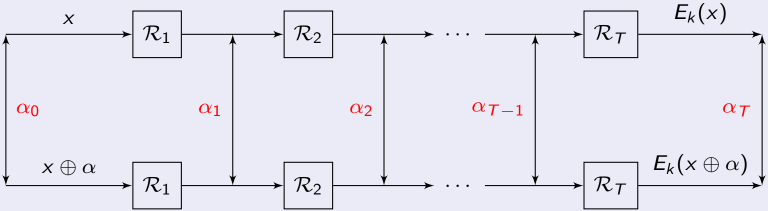
If E_k is a (round reduced) instance of a block cipher, the knowledge of a differential with high probability can be used as a distinguisher.

Considering Differential Trails

Usually, it is hard to compute the probability of multi-round differentials.

We consider differential trails

Let $\mathcal{R}_i$ denote the i-th round of a round-iterated cipher E_k. A T-round differential trail is a $(T+1)$-tuple of differential states.

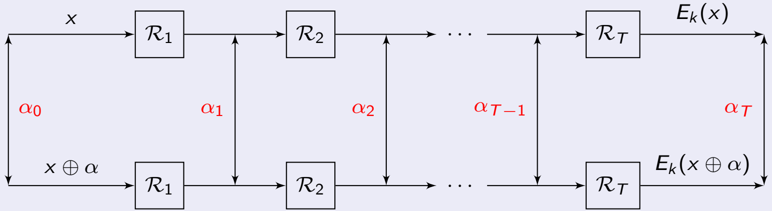


Considering Differential Trails

Usually, it is hard to compute the probability of multi-round differentials.

We consider differential trails

Let $\mathcal{R}_i$ denote the i-th round of a round-iterated cipher E_k. A T-round differential trail is a $(T+1)$-tuple of differential states.



For round-iterated ciphers, we assume that the probability of a trail is the product of its single-round differentials. Thus,

$$P(\alpha_0 \xrightarrow{\mathcal{R}_1} \alpha_1 \xrightarrow{\mathcal{R}_2} \dots \xrightarrow{\mathcal{R}_T} \alpha_T) = \prod_{i=1}^{T} P(\alpha_{i-1} \xrightarrow{\mathcal{R}_i} \alpha_i).$$

Considering Differential Trails (cont.)

Common Security Argument

- Prove an upper bound on the max. probability of any differential trail over a certain number of rounds t. (typically $\leq 2^{-\text{blocksize}}$)
- Specify the number of rounds of the primitive as $t + \kappa$ for a reasonable security margin κ.

Considering Differential Trails (cont.)

Common Security Argument

- Prove an upper bound on the max. probability of any differential trail over a certain number of rounds t. (typically $\leq 2^{-\text{blocksize}}$)
- Specify the number of rounds of the primitive as $t + \kappa$ for a reasonable security margin κ.

Two common mehtods to prove such an upper bound

- Experimental search (e.g. MILP, SAT/SMT solver): Works quite well for word-based ciphers (SPNs) and bit-based ciphers (like SIMON)
- Pen and paper proof: Works well for AES-like ciphers (Wide-trail strategy[a])

[a] J. Daemen. "Cipher and hash function design strategies based on linear and differential cryptanalysis". PhD thesis. Doctoral Dissertation, March 1995, KU Leuven, 1995.

Considering Differential Trails (cont.)

Common Security Argument

- Prove an upper bound on the max. probability of any differential trail over a certain number of rounds t. (typically $\leq 2^{-\text{blocksize}}$)
- Specify the number of rounds of the primitive as $t + \kappa$ for a reasonable security margin κ.

Two common mehtods to prove such an upper bound

- Experimental search (e.g. MILP, SAT/SMT solver): Works quite well for word-based ciphers (SPNs) and bit-based ciphers (like SIMON)
- Pen and paper proof: Works well for AES-like ciphers (Wide-trail strategy[a])

[a] J. Daemen. "Cipher and hash function design strategies based on linear and differential cryptanalysis". PhD thesis. Doctoral Dissertation, March 1995, KU Leuven, 1995.

Can we find more pen and paper arguments?

Results

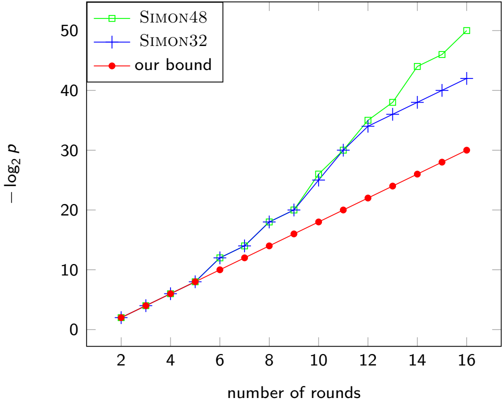
- Considering differential attacks, we provide a non-experimental security argument over multiple rounds of SIMON.
- In particular, we bound the probability of t-round differential trails below 2^{-2t+2}.

Results

- Considering differential attacks, we provide a non-experimental security argument over multiple rounds of SIMON.
- In particular, we bound the probability of t-round differential trails below 2^{-2t+2}.

- Although our bounds are (much) worse than the best experimental bounds known, our argument shows that no attack based on a single differential trail is possible for all instances of SIMON.

Results (cont.)



Comparison of the experimental bounds[2] for SIMON32 and SIMON48 and our provable bounds.

[2] S. Kölbl et al. *Observations on the SIMON Block Cipher Family*. CRYPTO 2015.

Results (cont.)

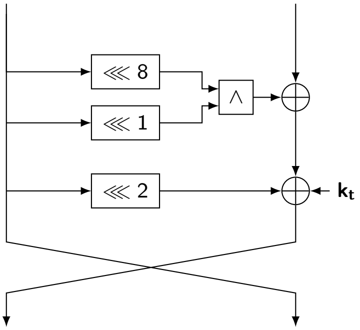
Rounds needed for bounding the differential probability by $2^{-\text{blocksize}}$

	rounds	**rounds needed**	**margin**
SIMON 32/ 64	32	17	15
SIMON 48/ 72	36	25	11
SIMON 48/ 96	36	25	11
SIMON 64/ 96	42	33	9
SIMON 64/128	44	33	11
SIMON 96/ 96	52	49	3
SIMON 96/144	54	49	5
SIMON128/128	68	65	3
SIMON128/192	69	65	4
SIMON128/256	72	65	7

Table of Contents

1. Introduction
2. Bounding the differential probability of SIMON
3. Conclusion

SIMON: linear and non-linear layer



- We seperate the Feistel function of SIMON into a non-linear part ρ and a linear part θ.

Our main result

Let $f_S(x) := (x \ggg 8) \wedge (x \ggg 1) \oplus (x \ggg 2)$ be the Feistel f-function.

Differential probability of SIMON

The probability of any t-round differential trail is upper bounded by 2^{-2t+2}.

Our main result

Let $f_S(x) := (x \ggg 8) \wedge (x \ggg 1) \oplus (x \ggg 2)$ be the Feistel f-function.

Differential probability of SIMON

The probability of any t-round differential trail is upper bounded by 2^{-2t+2}.

The main idea of the proof:

1. Show that the differential probability is low for input differences with large Hamming Weight (≥ 4)
2. Prove all other cases seperately

Some observations on the round function

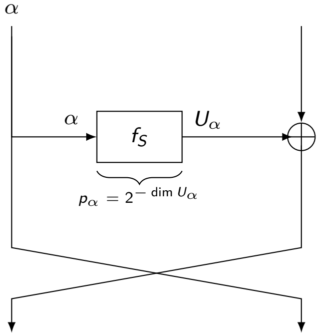
Let $f_S(x) := (x \lll 8) \wedge (x \lll 1) \oplus (x \lll 2)$

The single-round behavior is understood quite well.

Single-round propagation (Kölbl, Leander, Tiessen, 2015)

For a given (non-zero) input difference $\alpha \in \mathbb{F}_2^n$ into f_S, the set of possible output differences defines an affine subspace U_α s.t. $p_\alpha := P(\alpha \xrightarrow{f_S} \beta) \neq 0$ for all $\beta \in U_\alpha$. In particular, $p_\alpha = 2^{-d_\alpha}$ with $d_\alpha = \dim U_\alpha$.

Some observations on the round function



Why?
Because $\deg f_S = 2$ and thus $f_S(x) \oplus f_S(x \oplus \alpha)$ is linear

Some observations on the round function

$\Longrightarrow$ Observation: dim U_α (and thus the differential probability) corresponds to the Hamming weight of the input difference.

Some observations on the round function

$\Longrightarrow$ Observation: $\dim U_\alpha$ (and thus the differential probability) corresponds to the Hamming weight of the input difference.

Improving this bound

Let α be an input difference into f_S. For the differential probability over f_S it holds that

(1) if $\mathrm{wt}(\alpha) = 0$, then $p_\alpha = 1$ and $U_\alpha = \{0\}$

(2) if $\mathrm{wt}(\alpha) = 1$, then $p_\alpha \leq 2^{-2}$

(3) if $\mathrm{wt}(\alpha) \in \{2, 3\}$, then $p_\alpha \leq 2^{-3}$

(4) if $\mathrm{wt}(\alpha) \geq 4$, then $p_\alpha \leq 2^{-4}$

Proof.

Construct enough linearly independent elements U_α. $\square$

Some observations on the round function

$\Longrightarrow$ Observation: $\dim U_\alpha$ (and thus the differential probability) corresponds to the Hamming weight of the input difference.

Improving this bound

Let α be an input difference into f_S. For the differential probability over f_S it holds that

(1) if $\mathrm{wt}(\alpha) = 0$, then $p_\alpha = 1$ and $U_\alpha = \{0\}$

(2) if $\mathrm{wt}(\alpha) = 1$, then $p_\alpha \leq 2^{-2}$

(3) if $\mathrm{wt}(\alpha) \in \{2, 3\}$, then $p_\alpha \leq 2^{-3}$ Improved bound

(4) if $\mathrm{wt}(\alpha) \geq 4$, then $p_\alpha \leq 2^{-4}$

Proof.

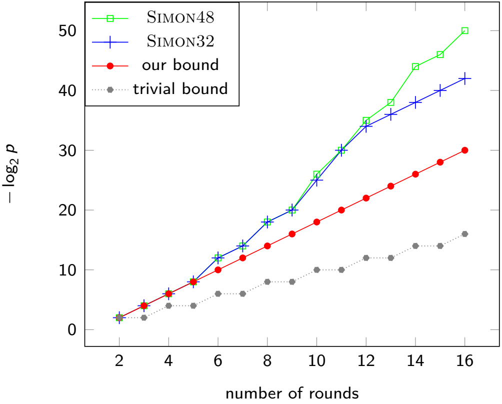
Construct enough linearly independent elements U_α. □

A Trivial Upper Bound on the Trail Probability

Worst case: The input difference into f_S of every second round is 0.

$$(0, \alpha) \to (\alpha, 0) \to (0, \alpha) \to \dots$$

If $p_\alpha = 2^{-2}$, we would obtain the *trivial bound*.



Obtaining Our Bound

For analyzing multiple rounds through the Feistel construction, we consider only trails of the form $(0, \alpha) \to \cdots \to (0, \beta)$

Observation

Let for all differences $\alpha, \beta \in \mathbb{F}_2^n \setminus \{0\}$ and all $t > 1$ the differential probability of any t-round $(0, \alpha) \to \cdots \to (0, \beta)$ trail be bounded by 2^{-2t}. Then,

$$P((\gamma_0, \delta_0) \xrightarrow{1} \ldots \xrightarrow{T} (\gamma_T, \delta_T)) \leq 2^{-2T+2}$$

for all γ_i, δ_i with $(\gamma_0, \delta_0) \neq (0, 0)$ and all $T > 0$.

Obtaining Our Bound

It is left to show that the probability of all t-round trails of the form

$$(0, \alpha) \rightarrow (\alpha, 0) \rightarrow (\gamma_2, \delta_2) \rightarrow \cdots \rightarrow (\gamma_{t-1}, \delta_{t-1}) \rightarrow (0, \beta)$$

is upper bounded by 2^{-2t}. W.l.o.g. we assume that all intermediate $\gamma_i \neq 0$.

Obtaining Our Bound

It is left to show that the probability of all t-round trails of the form

$$(0, \alpha) \to (\alpha, 0) \to (\gamma_2, \delta_2) \to \cdots \to (\gamma_{t-1}, \delta_{t-1}) \to (0, \beta)$$

is upper bounded by 2^{-2t}. W.l.o.g. we assume that all intermediate $\gamma_i \neq 0$.

Note that $p_0 = 1$, $p_\alpha \leq 2^{-2}$ and $\forall \gamma_i : p_{\gamma_i} \leq 2^{-2}$. Thus, one only has to make sure to *gain* a factor of 2^{-2} which is lost in the propagation of the 0-difference.

Obtaining Our Bound

It is left to show that the probability of all t-round trails of the form

$$(0, \alpha) \to (\alpha, 0) \to (\gamma_2, \delta_2) \to \cdots \to (\gamma_{t-1}, \delta_{t-1}) \to (0, \beta)$$

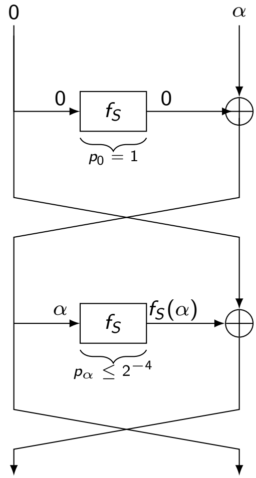
is upper bounded by 2^{-2t}. W.l.o.g. we assume that all intermediate $\gamma_i \neq 0$.

Note that $p_0 = 1$, $p_\alpha \leq 2^{-2}$ and $\forall \gamma_i : p_{\gamma_i} \leq 2^{-2}$. Thus, one only has to make sure to *gain* a factor of 2^{-2} which is lost in the propagation of the 0-difference.

We consider serveral cases for the Hamming Weight of α.

Obtaining Our Bound

- $\mathrm{wt}(\alpha) \geq 4$:



Obtaining Our Bound $[(x \ggg 8) \wedge (x \ggg 1) \oplus (x \ggg 2)]$

- $\mathrm{wt}(\alpha) = 1$: Let w.l.o.g $\alpha = (1, 0, \ldots, 0)$.

Obtaining Our Bound $[(x \ggg 8) \wedge (x \ggg 1) \oplus (x \ggg 2)]$

- $\mathrm{wt}(\alpha) = 1$: Let w.l.o.g $\alpha = (1, 0, \ldots, 0)$. Now,

$$\gamma_2 = f_S(\alpha) \oplus 0 \quad = (0, *_1, 1, 0, \ \ 0, 0, 0, 0, \ \ *_2, 0, 0, 0, \ \ 0, 0, 0, 0)$$

Obtaining Our Bound $[(x \ggg 8) \wedge (x \ggg 1) \oplus (x \ggg 2)]$

- $\mathrm{wt}(\alpha) = 1$: Let w.l.o.g $\alpha = (1, 0, \ldots, 0)$. Now,

$$\gamma_2 = f_S(\alpha) \oplus 0 \quad = (0, *_1, 1, 0, \ \ 0, 0, 0, 0, \ \ *_2, 0, 0, 0, \ \ 0, 0, 0, 0)$$

Case 1 ($*_2 = 0$):

Obtaining Our Bound $[(x \ggg 8) \wedge (x \ggg 1) \oplus (x \ggg 2)]$

- $\mathrm{wt}(\alpha) = 1$: Let w.l.o.g $\alpha = (1, 0, \ldots, 0)$. Now,

$$\gamma_2 = f_S(\alpha) \oplus 0 \quad = (0, *_1, 1, 0, \quad 0, 0, 0, 0, \quad *_2, 0, 0, 0, \quad 0, 0, 0, 0)$$

Case 1 ($*_2 = 0$): Then,

$$\gamma_3 = f_S(\gamma_2) \oplus \alpha \quad = (1, 0, *, *, \quad 1, 0, 0, 0, \quad 0, *, *, 0, \quad 0, 0, 0, 0)$$
$$\gamma_4 = f_S(\gamma_3) \oplus \gamma_2 \quad = (0, *, *, *, \quad *, *, 1, 0, \quad *, 0, *, *, \quad *, 0, 0, 0)$$

Obtaining Our Bound $[(x \lll 8) \wedge (x \lll 1) \oplus (x \lll 2)]$

- $\mathrm{wt}(\alpha) = 1$: Let w.l.o.g $\alpha = (1, 0, \ldots, 0)$. Now,

$$\gamma_2 = f_S(\alpha) \oplus 0 \quad = (0, *_1, 1, 0, \;\; 0, 0, 0, 0, \;\; *_2, 0, 0, 0, \;\; 0, 0, 0, 0)$$

Case 1 ($*_2 = 0$): Then,

$$\begin{aligned} \gamma_3 = f_S(\gamma_2) \oplus \alpha \quad &= (1, 0, *, *, \;\; 1, 0, 0, 0, \;\; 0, *, *, 0, \;\; 0, 0, 0, 0) \\ \gamma_4 = f_S(\gamma_3) \oplus \gamma_2 \quad &= (0, *, *, *, \;\; *, *, 1, 0, \;\; *, 0, *, *, \;\; *, 0, 0, 0) \end{aligned}$$

If now the weight of γ_4 is higher than 1, then $p_{\gamma_3}, p_{\gamma_4} \leq 2^{-3}$. Thus, let $\mathrm{wt}(\gamma_4) = 1$.

Obtaining Our Bound $[(x \ggg 8) \wedge (x \ggg 1) \oplus (x \ggg 2)]$

- $\mathrm{wt}(\alpha) = 1$: Let w.l.o.g $\alpha = (1, 0, \ldots, 0)$. Now,

$$\gamma_2 = f_S(\alpha) \oplus 0 \quad = (0, *_1, 1, 0, \;\; 0, 0, 0, 0, \;\; *_2, 0, 0, 0, \;\; 0, 0, 0, 0)$$

Case 1 ($*_2 = 0$): Then,

$$\begin{aligned} \gamma_3 = f_S(\gamma_2) \oplus \alpha \quad &= (1, 0, *, *, \;\; 1, 0, 0, 0, \;\; 0, *, *, 0, \;\; 0, 0, 0, 0) \\ \gamma_4 = f_S(\gamma_3) \oplus \gamma_2 \quad &= (0, *, *, *, \;\; *, *, 1, 0, \;\; *, 0, *, *, \;\; *, 0, 0, 0) \end{aligned}$$

If now the weight of γ_4 is higher than 1, then $p_{\gamma_3}, p_{\gamma_4} \leq 2^{-3}$. Thus, let $\mathrm{wt}(\gamma_4) = 1$. It follows that

$$\gamma_5 = f_S(\gamma_4) \oplus \gamma_3 \quad = (1, 0, *, *, \;\; 1, 0, 0, *, \;\; 1, *, *, 0, \;\; 0, 0, *, 0)$$

and thus $p_{\gamma_5} \leq 2^{-3}$.

Obtaining Our Bound $[(x \ggg 8) \wedge (x \ggg 1) \oplus (x \ggg 2)]$

Case 2 ($*_2 = 1$):

Obtaining Our Bound $[(x \lll 8) \wedge (x \lll 1) \oplus (x \lll 2)]$

Case 2 ($*_2 = 1$): Then $p_{\gamma_2} \leq 2^{-3}$ already holds and

$$\gamma_3 = f_S(\gamma_2) \oplus \alpha \qquad = (*, 0, *, *, \quad 1, 0, 0, 0, \quad 0, *, *, 0, \quad 0, 0, 0, 0)$$

Obtaining Our Bound $[(x \ggg 8) \wedge (x \ggg 1) \oplus (x \ggg 2)]$

Case 2 ($*_2 = 1$): Then $p_{\gamma_2} \leq 2^{-3}$ already holds and

$$\gamma_3 = f_S(\gamma_2) \oplus \alpha \qquad = (*, 0, *, *, \;\; 1, 0, 0, 0, \;\; 0, *, *, 0, \;\; 0, 0, 0, 0)$$

Again, let w.l.o.g $\mathrm{wt}(\gamma_3) = 1$. It follows that

$$\gamma_4 = f_S(\gamma_3) \oplus \gamma_2 \qquad = (0, *, 1, 0, \;\; 0, *, 1, 0, \;\; 1, 0, 0, 0, \;\; *, 0, 0, 0)$$

and thus $p_{\gamma_4} \leq 2^{-3}$.

Obtaining Our Bound $[(x \ggg 8) \wedge (x \ggg 1) \oplus (x \ggg 2)]$

Case 2 ($*_2 = 1$): Then $p_{\gamma_2} \leq 2^{-3}$ already holds and

$$\gamma_3 = f_S(\gamma_2) \oplus \alpha \qquad = (*, 0, *, *, \quad 1, 0, 0, 0, \quad 0, *, *, 0, \quad 0, 0, 0, 0)$$

Again, let w.l.o.g $\mathrm{wt}(\gamma_3) = 1$. It follows that

$$\gamma_4 = f_S(\gamma_3) \oplus \gamma_2 \qquad = (0, *, 1, 0, \quad 0, *, 1, 0, \quad 1, 0, 0, 0, \quad *, 0, 0, 0)$$

and thus $p_{\gamma_4} \leq 2^{-3}$.

All in all, we "gained" a factor of $2^{-1} \cdot 2^{-1} = 2^{-2}$.

Obtaining Our Bound

For the cases

- $\mathrm{wt}(\alpha) = 2$
- $\mathrm{wt}(\alpha) = 3$

this can be proven in a similar way!

Table of Contents

1. Introduction
2. Bounding the differential probability of SIMON
3. Conclusion

Conclusion

- We took a further step into understanding possible block cipher constructions.
- For SIMON, we were able to obtain a non-trivial upper bound on the max. probability of a differential trail using a non-experimental argument.
- One can do the analysis for other rotation constants as well. Same bound is also valid for SIMECK.[3]

[3] G. Yang et al. *The Simeck Family of Lightweight Block Ciphers*. CHES 2015.

Conclusion

- We took a further step into understanding possible block cipher constructions.
- For SIMON, we were able to obtain a non-trivial upper bound on the max. probability of a differential trail using a non-experimental argument.
- One can do the analysis for other rotation constants as well. Same bound is also valid for SIMECK.[3]

- We did not consider multi-round differentials. However, there has been shown a differential effect in SIMON. Experimental bounds are better in this case.

[3] G. Yang et al. *The Simeck Family of Lightweight Block Ciphers*. CHES 2015.

Conclusion

- We took a further step into understanding possible block cipher constructions.
- For SIMON, we were able to obtain a non-trivial upper bound on the max. probability of a differential trail using a non-experimental argument.
- One can do the analysis for other rotation constants as well. Same bound is also valid for SIMECK.[3]
- We did not consider multi-round differentials. However, there has been shown a differential effect in SIMON. Experimental bounds are better in this case.

Note

We did not show improved security of SIMON. Instead, we tried to learn more about possible block cipher constructions!

[3] G. Yang et al. *The Simeck Family of Lightweight Block Ciphers*. CHES 2015.

Thanks for your attention!
Any Questions?