OBSERVATIONS ON THE SIMON BLOCK CIPHER FAMILY

Stefan Kölbl[1] Gregor Leander[2] Tyge Tiessen[1]

August 17, 2015

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

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

LIGHTWEIGHT CRYPTOGRAPHY

What is Lightweight Cryptography?

- Design primitives for resource-constraint environments like RFID tags.
- Lot of attention over the last few years.
- NIST started to investigate the possibility to standardize primitives.

Design Criteria

- Chip-area
- Latency
- Code-size
- …

SIMON

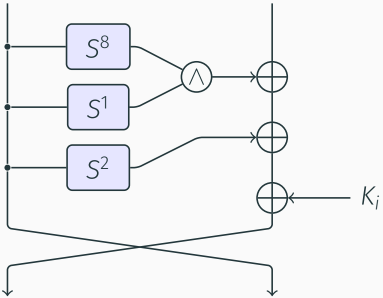
SIMON is a family of block ciphers designed by NSA.

- "Published" in 2013 on the ePrint archive.
- Lightweight design for hardware.

block size	key sizes
32	64
48	72, 96
64	96, 128
96	96, 144
128	128, 192, 256

Feistel Network

- Simple round function
- Between 32 and 72 rounds



SIMON

Cryptanalysis of SIMON

- No (public) cryptanalysis or security arguments from the designers.
- Many contributions by the cryptographic community.
- Attacks cover up to 74% of the rounds.

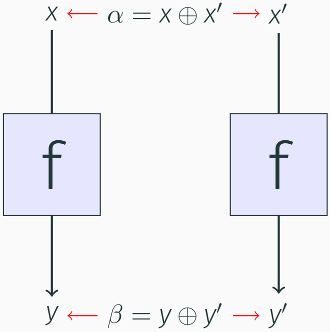
PROPERTIES OF SIMON

Any cipher should have reasonable security margin against differential and linear cryptanalysis.

- For SPN designs easier to show bounds.
- Difficult for ARX, Simon.
- Best attacks on Simon are based on differential and linear cryptanalysis.

Differential Cryptanalysis:

- Observe how difference propagate through the round function.
- Find correlations between input and output difference.



We are interested in:

- Probability for one round:

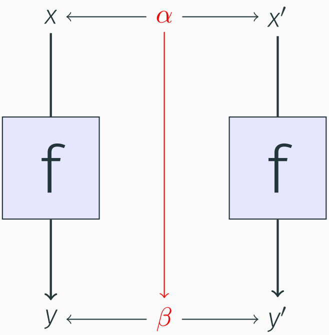
$$\Pr(\alpha \xrightarrow{f} \beta)$$

- Differential characteristics:

$$\Pr(\alpha \xrightarrow{f} \beta \xrightarrow{f} \gamma)$$

- Differentials:

$$\sum_{x} \Pr(\alpha \xrightarrow{f} x \xrightarrow{f} \gamma)$$



Differential Cryptanalysis

We are interested in:

- Probability for one round:

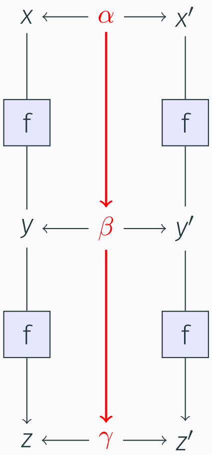
$$\Pr(\alpha \xrightarrow{f} \beta)$$

- Differential characteristics:

$$\Pr(\alpha \xrightarrow{f} \beta \xrightarrow{f} \gamma)$$

- Differentials:

$$\sum_{x} \Pr(\alpha \xrightarrow{f} x \xrightarrow{f} \gamma)$$



We are interested in:

- Probability for one round:

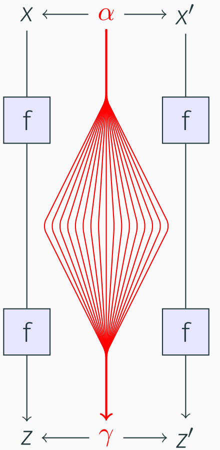
$$\Pr(\alpha \xrightarrow{f} \beta)$$

- Differential characteristics:

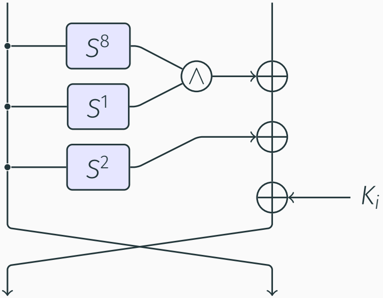
$$\Pr(\alpha \xrightarrow{f} \beta \xrightarrow{f} \gamma)$$

- Differentials:

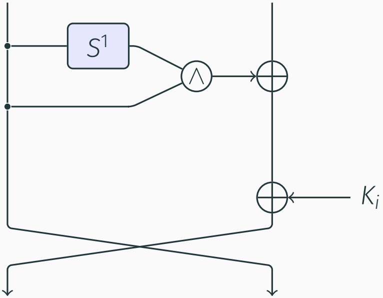
$$\sum_{x} \Pr(\alpha \xrightarrow{f} x \xrightarrow{f} \gamma)$$



For the analysis we use an equivalent representation for Simon



For the analysis we use an equivalent representation for Simon



We look at a message $m = (m_{n-1}, \ldots, m_1, m_0)$ and an input difference $d = (d_{n-1}, \ldots, d_1, d_0)$.

The output difference $f(m) \oplus f(m \oplus d)$ is then given by:

$$D_i(m, d) = \begin{cases} 0, & \text{if } d_i = 0 \text{ and } d_{i-1} = 0 \\ & \\ & \end{cases}$$

We look at a message $m = (m_{n-1}, \ldots, m_1, m_0)$ and an input difference $d = (d_{n-1}, \ldots, d_1, d_0)$.

The output difference $f(m) \oplus f(m \oplus d)$ is then given by:

$$D_i(m, d) = \begin{cases} 0, & \text{if } d_i = 0 \text{ and } d_{i-1} = 0 \\ m_i, & \text{if } d_i = 0 \text{ and } d_{i-1} = 1 \\ & \\ & \end{cases}$$

We look at a message $m = (m_{n-1}, \ldots, m_1, m_0)$ and an input difference $d = (d_{n-1}, \ldots, d_1, d_0)$.

The output difference $f(m) \oplus f(m \oplus d)$ is then given by:

$$D_i(m, d) = \begin{cases} 0, & \text{if } d_i = 0 \text{ and } d_{i-1} = 0 \\ m_i, & \text{if } d_i = 0 \text{ and } d_{i-1} = 1 \\ m_{i-1}, & \text{if } d_i = 1 \text{ and } d_{i-1} = 0 \\ & \end{cases}$$

We look at a message $m = (m_{n-1}, \ldots, m_1, m_0)$ and an input difference $d = (d_{n-1}, \ldots, d_1, d_0)$.

The output difference $f(m) \oplus f(m \oplus d)$ is then given by:

$$D_i(m, d) = \begin{cases} 0, & \text{if } d_i = 0 \text{ and } d_{i-1} = 0 \\ m_i, & \text{if } d_i = 0 \text{ and } d_{i-1} = 1 \\ m_{i-1}, & \text{if } d_i = 1 \text{ and } d_{i-1} = 0 \\ \overline{m_i \oplus m_{i-1}}, & \text{if } d_i = 1 \text{ and } d_{i-1} = 1 \end{cases} . \tag{1}$$

Let us now look at a first example. Let $n = 6$, and $d = 001010$. We then calculate $D(m, d)$ using the above bitwise definition of D:

$$\begin{array}{lcccccc} i & 5 & 4 & 3 & 2 & 1 & 0 \\ \hline d & 0 & 0 & 1 & 0 & 1 & 0 \\ S^1(d) & 0 & 1 & 0 & 1 & 0 & 0 \\ \hline D(m,d) & & & & & & \end{array} . \tag{2}$$

Let us now look at a first example. Let $n = 6$, and $d = 001010$. We then calculate $D(m, d)$ using the above bitwise definition of D:

$$
\begin{array}{lcccccc}
i & 5 & 4 & 3 & 2 & 1 & 0 \\
\hline
d & 0 & 0 & 1 & 0 & 1 & 0 \\
S^1(d) & 0 & 1 & 0 & 1 & 0 & 0 \\
\hline
D(m, d) & & & & & & 0
\end{array}
. \tag{2}
$$

Let us now look at a first example. Let $n = 6$, and $d = 001010$. We then calculate $D(m, d)$ using the above bitwise definition of D:

$$\begin{array}{lcccccc} i & 5 & 4 & 3 & 2 & 1 & 0 \\ \hline d & 0 & 0 & 1 & 0 & 1 & 0 \\ S^1(d) & 0 & 1 & 0 & 1 & 0 & 0 \\ \hline D(m, d) & & & & & m_0 & 0 \end{array} . \qquad (2)$$

Let us now look at a first example. Let $n = 6$, and $d = 001010$. We then calculate $D(m, d)$ using the above bitwise definition of D:

$$\begin{array}{l|cccccc} i & 5 & 4 & 3 & 2 & 1 & 0 \\ \hline d & 0 & 0 & 1 & 0 & 1 & 0 \\ S^1(d) & 0 & 1 & 0 & 1 & 0 & 0 \\ \hline D(m,d) & & & & m_2 & m_0 & 0 \end{array} . \tag{2}$$

Let us now look at a first example. Let $n = 6$, and $d = 001010$. We then calculate $D(m, d)$ using the above bitwise definition of D:

$$\begin{array}{lcccccc} i & 5 & 4 & 3 & 2 & 1 & 0 \\ \hline d & 0 & 0 & 1 & 0 & 1 & 0 \\ S^1(d) & 0 & 1 & 0 & 1 & 0 & 0 \\ \hline D(m,d) & & & m_2 & m_2 & m_0 & 0 \end{array} \quad . \tag{2}$$

Let us now look at a first example. Let $n = 6$, and $d = 001010$. We then calculate $D(m, d)$ using the above bitwise definition of D:

$$\begin{array}{lcccccc} i & 5 & 4 & 3 & 2 & 1 & 0 \\ \hline d & 0 & 0 & 1 & 0 & 1 & 0 \\ S^1(d) & 0 & 1 & 0 & 1 & 0 & 0 \\ \hline D(m,d) & & m_4 & m_2 & m_2 & m_0 & 0 \end{array} . \tag{2}$$

Let us now look at a first example. Let $n = 6$, and $d = 001010$. We then calculate $D(m, d)$ using the above bitwise definition of D:

$$\begin{array}{lcccccc} i & 5 & 4 & 3 & 2 & 1 & 0 \\ \hline d & 0 & 0 & 1 & 0 & 1 & 0 \\ S^1(d) & 0 & 1 & 0 & 1 & 0 & 0 \\ \hline D(m,d) & 0 & m_4 & m_2 & m_2 & m_0 & 0 \end{array} . \tag{2}$$

Resulting difference only depends on m_0, m_2, m_4. Therefore we have 8 possible output differences.

Can compute the differential probability with simple bit operations.

The bits which can be non-zero at the output:

$$\texttt{varibits} = \alpha \vee S^1(\alpha) \tag{3}$$

The bits which have to be equal to their right neighbour:

$$\texttt{doublebits} = \alpha \wedge \overline{S^1(\alpha)} \wedge S^2(\alpha) \tag{4}$$

For our previous example:

$$\texttt{varibits} = \texttt{011110}$$
$$\texttt{doublebits} = \texttt{001000}$$

Possible output differences:

```
000000
000010
001100
001110
010000
010010
011100
011110
```

For our previous example:

$$\texttt{varibits} = \texttt{011110}$$
$$\texttt{doublebits} = \texttt{001000}$$

Possible output differences:

```
000000
000010
001100
001110
010000
010010
011100
011110
```

For our previous example:

$$\texttt{varibits} = \texttt{011110}$$
$$\texttt{doublebits} = \texttt{001000}$$

Possible output differences:

```
000000
000010
001100
001110
010000
010010
011100
011110
```

A valid differential ($\alpha \to \beta$) has to satisfy:

- There can only be a difference at β_i, if $\texttt{varibits}_i$ is equal to 1.
- If $\texttt{doublebits}_i$ is 1, then $\beta_i = \beta_{i-1}$.

The probability is then given by:

$$\Pr(\alpha \to \beta) = 2^{-\operatorname{wt}(\texttt{varibits} \oplus \texttt{doublebits})} \tag{5}$$

A valid differential ($\alpha \rightarrow \beta$) has to satisfy:

- There can only be a difference at β_i, if $\texttt{varibits}_i$ is equal to 1.
- If $\texttt{doublebits}_i$ is 1, then $\beta_i = \beta_{i-1}$.

The probability is then given by:

$$\Pr(\alpha \rightarrow \beta) = 2^{-\operatorname{wt}(\texttt{varibits} \oplus \texttt{doublebits})} \tag{5}$$

Apply affine transformation for Simon round function.

- Proofs in the paper.
- Similar approach for linear cryptanalysis.

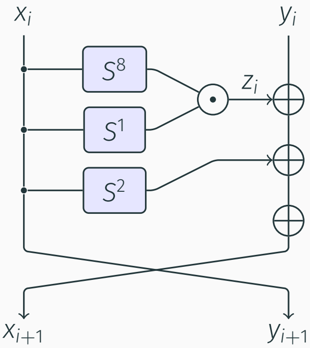
FINDING OPTIMAL DIFFERENTIAL AND LINEAR CHARACTERISTICS

Optimal Characteristics

We are interested in differential and linear characteristics with high probability.

- We use an approach based on SAT/SMT solvers, similar to results on Salsa20 [MP13] or NORX [AJN15].
- Gives upper bounds on the probability.
- Estimate probability of the differentials.
- Open Source[1]

[1] https://github.com/kste/cryptosmt



Constraints:

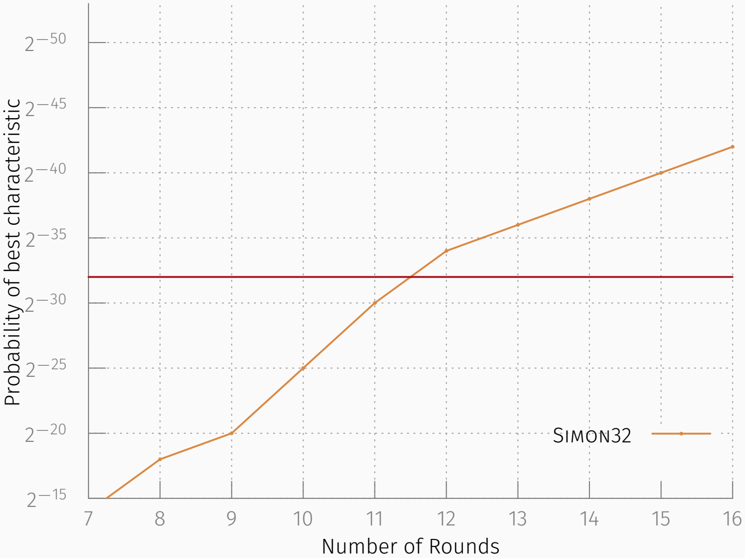
- Use our previous observations on `varibits` and `doublebits`.
- Probability for one round is $w_i = \mathrm{wt}(\texttt{varibits} \oplus \texttt{doublebits})$.

Use this to find characteristic with probability 2^{-w}:

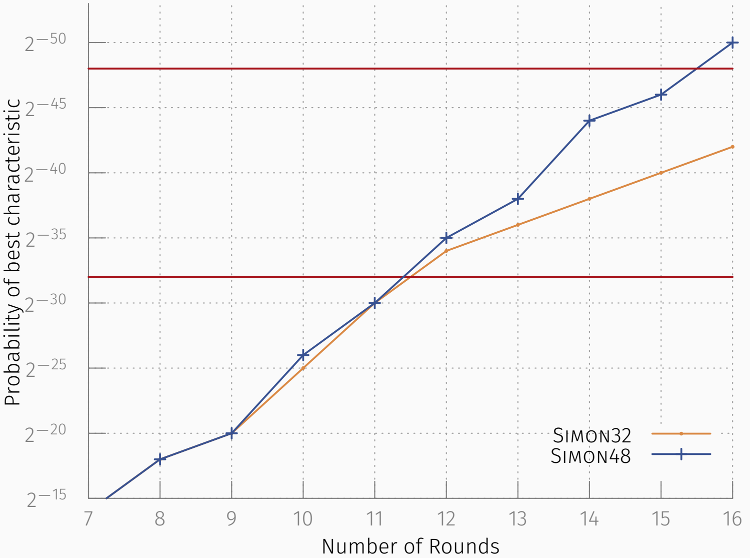
- Add constraints for each round.
- Check if $w = \sum_{i=0}^{r-1} w_i$.
- Increase w if no solution was found.

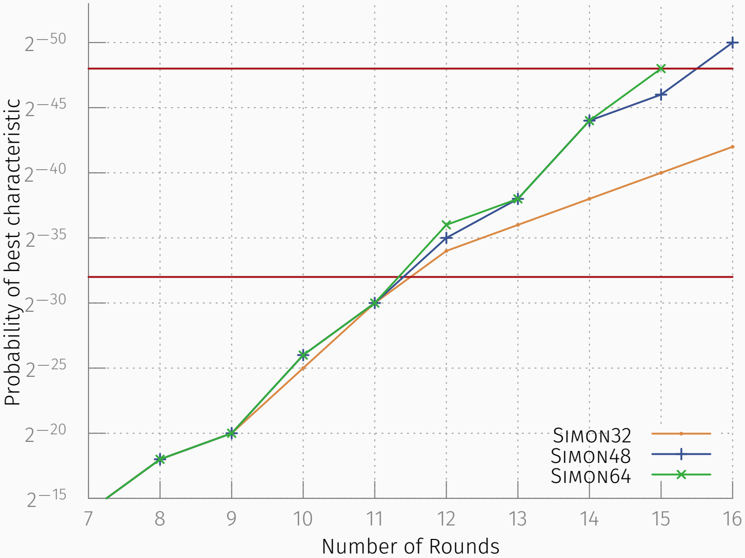
We ran experiments for Simon32, Simon48 and Simon64.

Lower Bounds



Lower Bounds




Probability of best characteristic
2^{-50}
2^{-45}
2^{-40}
2^{-35}
2^{-30}
2^{-25}
2^{-20}
2^{-15}
7 8 9 10 11 12 13 14 15 16
Number of Rounds
Simon32
Simon48
Simon64

What about differentials?

- Often assumed that probability of the best characteristics can be used to estimate probability of the best differential.
- Only inaccurate estimate for Simon.

We estimate the probability of a differential

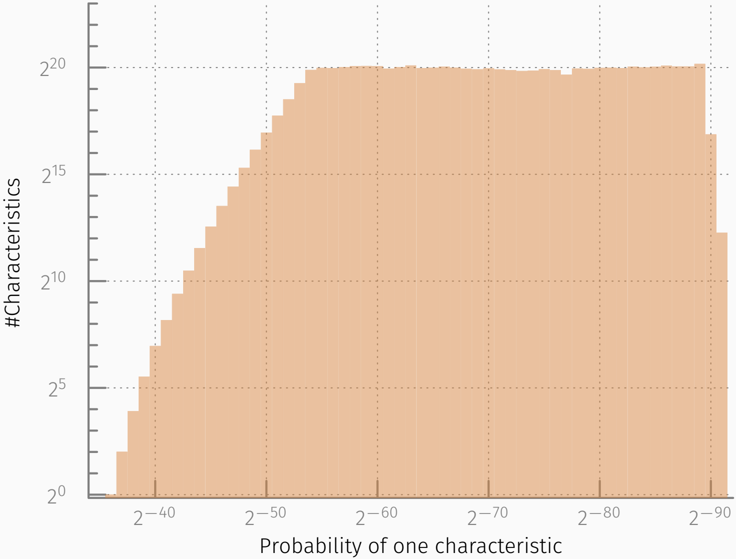
- Add constraints for each round.
- Set $(x_0, y_0) = \Delta_{\text{in}}$ and $(x_r, y_r) = \Delta_{\text{out}}$.
- Find all solutions for increasing values of w.

We can determine the interval for the characteristics contributing to a differential $[w_{\min}, w_{\max}]$.

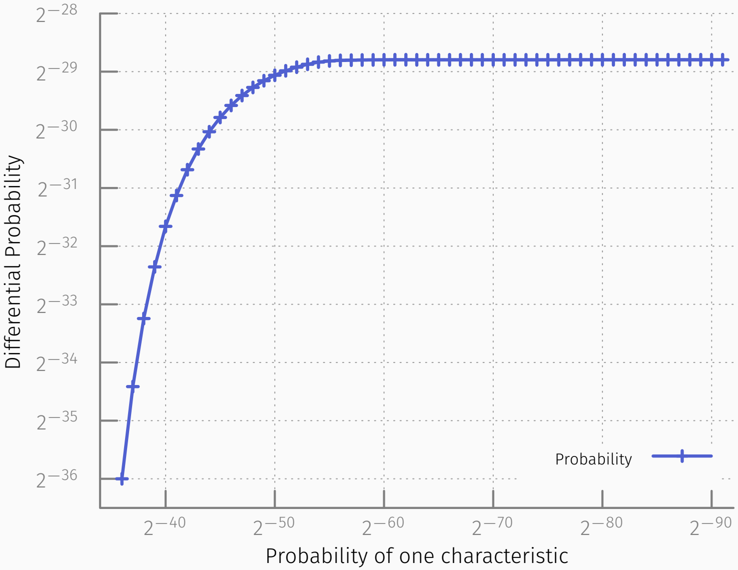
- Covering the whole interval is computationally expensive.
- Gives better estimate than previous results.

Cipher	Rounds	$w_{\min}$	$w_{\max}$	$\log_2(p)$
`Simon32`	13	36	91 (91)	−28.79
`Simon48`	16	50	256 (68)	−44.33
`Simon64`	21	68	453 (89)	−57.57

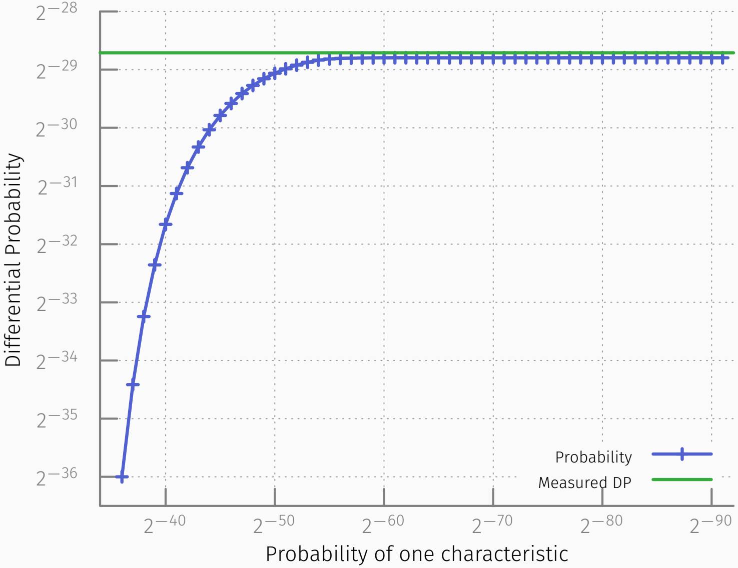
Differentials



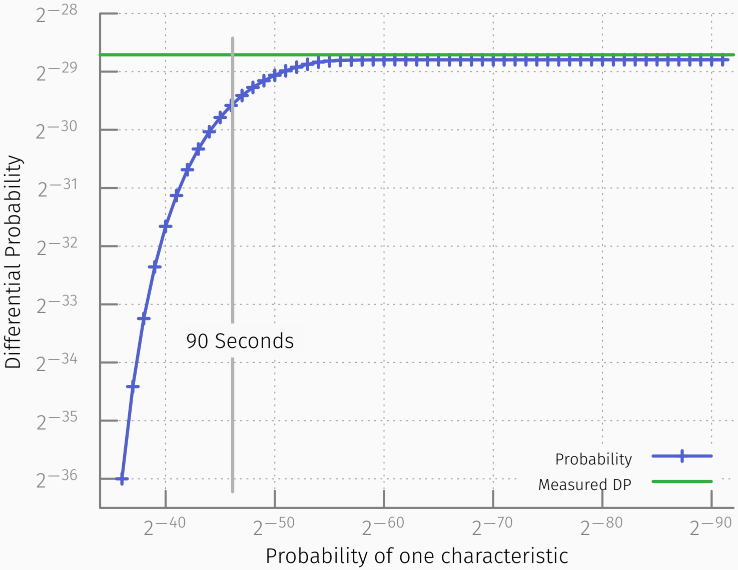
Differentials



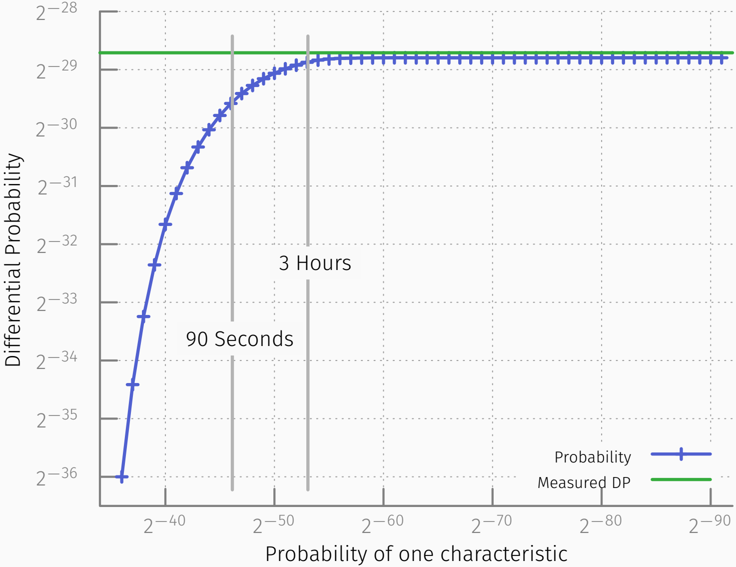
Differentials



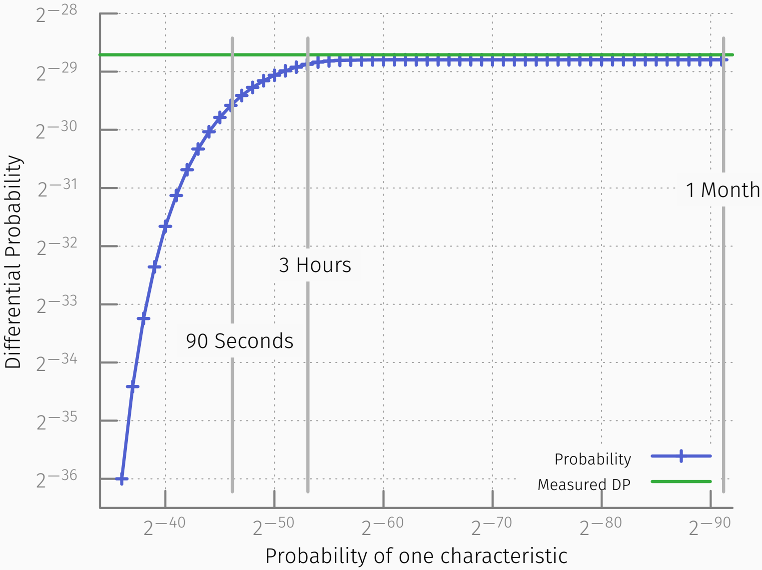
Differentials



Differentials



Differentials



ROTATION CONSTANTS

Possible Criteria:

- Simplicity
- Implementation costs
- Security?

Are there parameters which are better with regard to some metrics?

Basic test for diffusion:

Block size	32	48	64	96	128
Standard parameters	7	8	9	11	13
Best possible	6	7	8	9	10
Rank	2nd	2nd	2nd	3rd	4th

Bounds for differential and linear characteristics give us some interesting candidates:

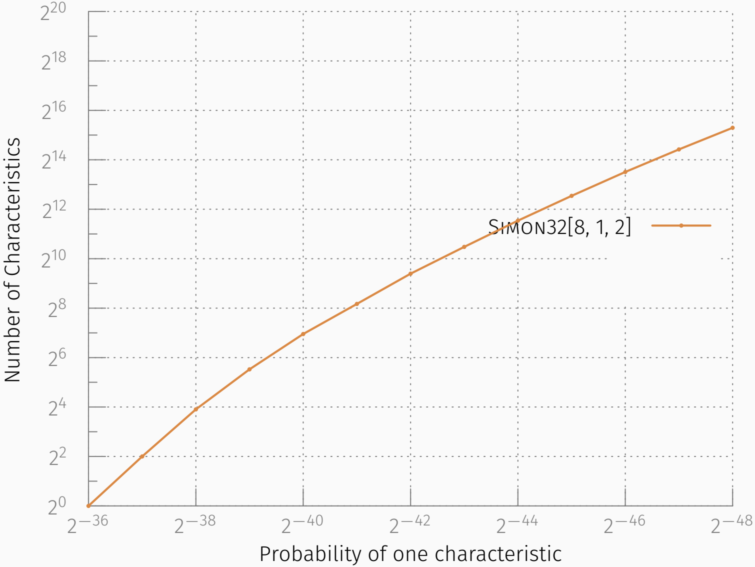
- The bounds are as good as the original parameters or slightly better.
- SIMON$[12, 5, 3]$ offers best diffusion.
- SIMON$[7, 0, 2]$ offers best diffusion, when $b = 0$.
- SIMON$[1, 0, 2]$ has bad diffusion, but good bounds.

Rotation Constants

Bounds for differential and linear characteristics give us some interesting candidates:

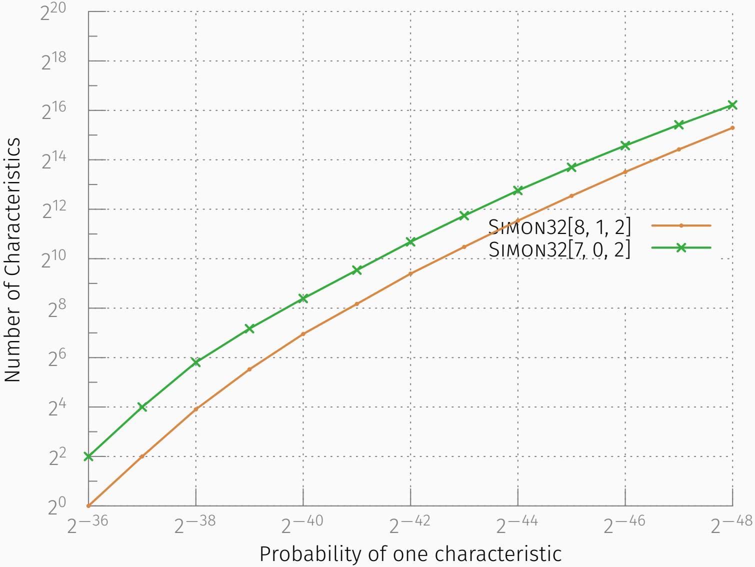
- The bounds are as good as the original parameters or slightly better.
- Simon$[12, 5, 3]$ offers best diffusion.
- Simon$[7, 0, 2]$ offers best diffusion, when $b = 0$.
- Simon$[1, 0, 2]$ has bad diffusion, but good bounds.

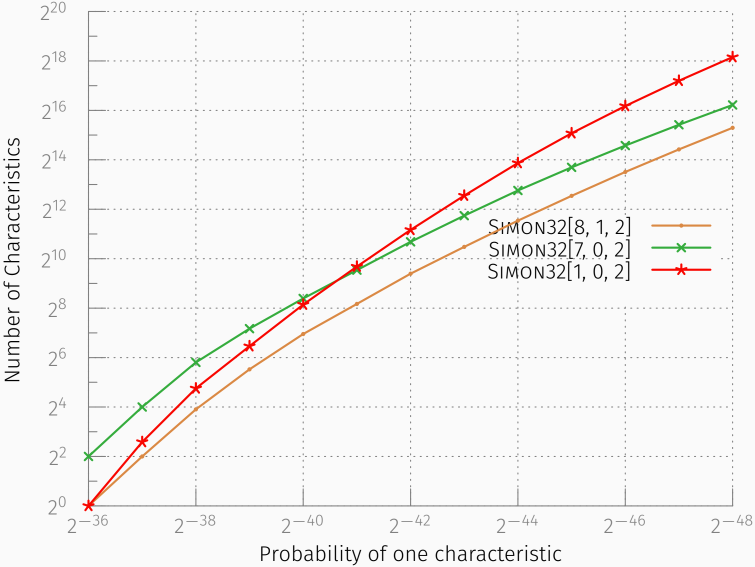
What effect do the rotations constants have on differentials?



2^{20}
2^{18}
2^{16}
2^{14}
2^{12}
2^{10}
2^{8}
2^{6}
2^{4}
2^{2}
2^{0}
Number of Characteristics
SIMON32[8, 1, 2]
2^{-36}
2^{-38}
2^{-40}
2^{-42}
2^{-44}
2^{-46}
2^{-48}
Probability of one characteristic

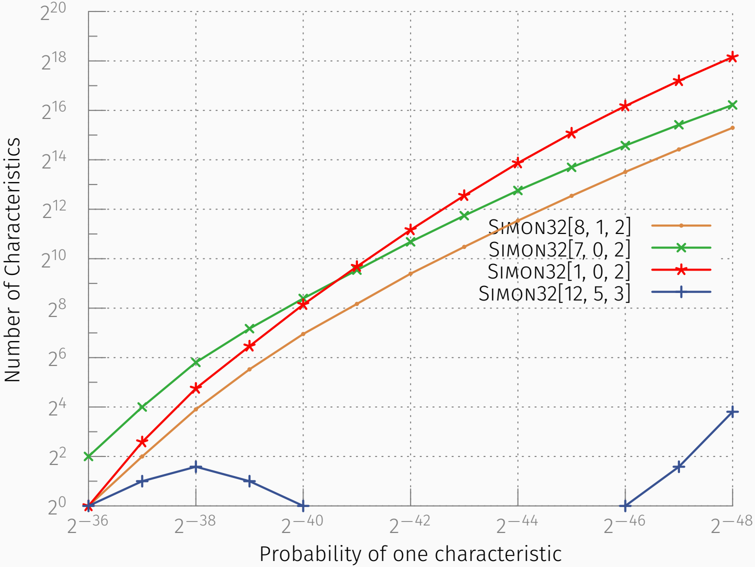
Rotation Constants





2^{20}
2^{18}
2^{16}
2^{14}
2^{12}
2^{10}
2^{8}
2^{6}
2^{4}
2^{2}
2^{0}
Number of Characteristics
2^{-36}
2^{-38}
2^{-40}
2^{-42}
2^{-44}
2^{-46}
2^{-48}
Probability of one characteristic
SIMON32[8, 1, 2]
SIMON32[7, 0, 2]
SIMON32[1, 0, 2]

Rotation Constants



Conclusion

Contributions:

- Constant time algorithm for differential probability.
- Bounds on the probability of differential/linear characteristics.
- Compared quality of rotation constants.

Open Problems:

- More refined analysis of the parameter space.
- Find efficient method to determine differential effect for different constants.

QUESTIONS?

References I

- Jean-Philippe Aumasson, Philipp Jovanovic, and Samuel Neves, *Analysis of NORX: investigating differential and rotational properties*, Progress in Cryptology - LATINCRYPT 2014 (Diego F. Aranha and Alfred Menezes, eds.), Lecture Notes in Computer Science, vol. 8895, Springer, 2015, pp. 306–324.
- 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.

Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers, *The SIMON and SPECK families of lightweight block ciphers*, Cryptology ePrint Archive, Report 2013/404, 2013, `http://eprint.iacr.org/`.

Nicky Mouha and Bart Preneel, *Towards finding optimal differential characteristics for ARX: Application to Salsa20*, Cryptology ePrint Archive, Report 2013/328, 2013, `http://eprint.iacr.org/`.