Rotational-XOR Cryptanalysis of Reduced-round SPECK

Yunwen Liu, Glenn De Witte, Adrián Ranea, Tomer Ashur

COSIC, KU Leuven, Belgium

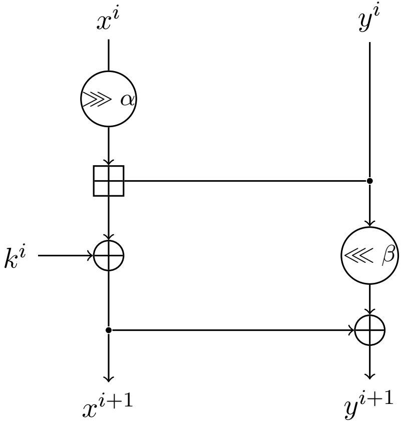
FSE, March 2018

The Block Cipher Family SPECK

- ARX ciphers designed by the NSA in 2013

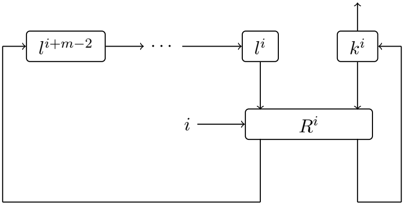
The Block Cipher Family SPECK

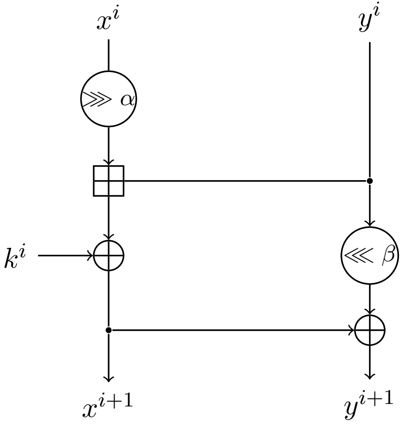
- ARX ciphers designed by the NSA in 2013
- Block size $2n$ bits, $n = 32/48/64/96/128$



The Block Cipher Family SPECK

- ARX ciphers designed by the NSA in 2013
- Block size $2n$ bits, $n = 32/48/64/96/128$
- Key size mn bits, $m = 2, 3, 4$





Overview of Distinguishers for SPECK

SPECK versions	32/64	48/96	64/128	96/144	128/256
Diff. char.	9	11	15	16	19

Overview of Distinguishers for SPECK

SPECK versions	32/64	48/96	64/128	96/144	128/256
Diff. char.	9	11	15	16	19
Lin. trail	9	10	13	15	16

- Best attacks: differential cryptanalysis [Din14][FWG+16]

Overview of Distinguishers for SPECK

SPECK versions	32/64	48/96	64/128	96/144	128/256
Diff. char.	9	11	15	16	19
Lin. trail	9	10	13	15	16

- Best attacks: differential cryptanalysis [Din14][FWG+16]
- Rotational cryptanalysis [BSS+17]

[Din14] I. Dinur. Improved differential cryptanalysis of round-reduced SPECK. SAC 2014
[FWG+16] K. Fu, M. Wang, Y. Guo, S. Sun and L. Hu. MILP-based automatic search algorithms for differential and linear trails for SPECK. FSE 2016
[BSS+17] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks and L. Wingers. Notes on the design and analysis of SIMON and SPECK, eprint 2017/560

Overview of Distinguishers for SPECK

SPECK versions	32/64	48/96	64/128	96/144	128/256
Diff. char.	9	11	15	16	19
Lin. trail	9	10	13	15	16
Ours	12	15	13	13	13

- Best attacks: differential cryptanalysis [Din14][FWG+16]
- Rotational cryptanalysis [BSS+17]

[Din14] I. Dinur. Improved differential cryptanalysis of round-reduced SPECK. SAC 2014

[FWG+16] K. Fu, M. Wang, Y. Guo, S. Sun and L. Hu. MILP-based automatic search algorithms for differential and linear trails for SPECK. FSE 2016

[BSS+17] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks and L. Wingers. Notes on the design and analysis of SIMON and SPECK, eprint 2017/560

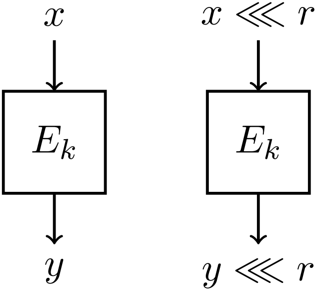
Rotational-XOR cryptanalysis

- A novel statistical cryptanalysis proposed at FSE 2017 [AL16]

[AL16] T. Ashur and Y. Liu. Rotational cryptanalysis in the presence of constants. ToSC 2016

Rotational-XOR cryptanalysis

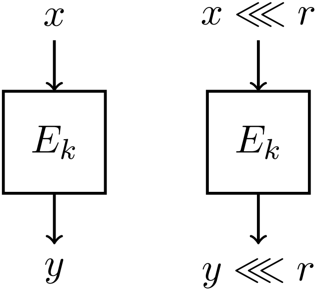
- A novel statistical cryptanalysis proposed at FSE 2017 [AL16]
- Constants involved in ARX ciphers



[AL16] T. Ashur and Y. Liu. Rotational cryptanalysis in the presence of constants. ToSC 2016

Rotational-XOR cryptanalysis

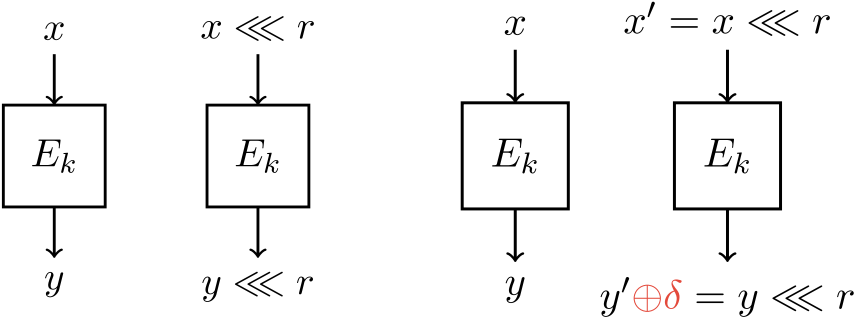
- A novel statistical cryptanalysis proposed at FSE 2017 [AL16]
- Constants involved in ARX ciphers
- Combine rotational cryptanalysis with differential cryptanalysis



[AL16] T. Ashur and Y. Liu. Rotational cryptanalysis in the presence of constants. ToSC 2016

Rotational-XOR cryptanalysis

- A novel statistical cryptanalysis proposed at FSE 2017 [AL16]
- Constants involved in ARX ciphers
- Combine rotational cryptanalysis with differential cryptanalysis



[AL16] T. Ashur and Y. Liu. Rotational cryptanalysis in the presence of constants. ToSC 2016

Rotational-XOR cryptanalysis

Define a pair with $((a_1, a_2), \gamma)$-Rotational-XOR difference:

$$(x \oplus a_1, (x \lll \gamma) \oplus a_2)$$

Rotational-XOR cryptanalysis

Define a pair with $((a_1, a_2), \gamma)$-Rotational-XOR difference:

$$(x \oplus a_1, (x \lll \gamma) \oplus a_2)$$

$\gamma = 1$: $x \lll 1 \rightarrow \overleftarrow{x}$

Rotational-XOR cryptanalysis

Define a pair with $((a_1, a_2), \gamma)$-Rotational-XOR difference:

$$(x \oplus a_1, (x \lll \gamma) \oplus a_2)$$

$\gamma = 1$: $x \lll 1 \rightarrow \overleftarrow{x}$

- Applied to $\textsc{Speck}$32/64 reduced to 7 rounds

Rotational-XOR cryptanalysis

Define a pair with $((a_1, a_2), \gamma)$-Rotational-XOR difference:

$$(x \oplus a_1, (x \lll \gamma) \oplus a_2)$$

$\gamma = 1$: $x \lll 1 \rightarrow \overleftarrow{x}$

- Applied to $\textsc{Speck}$32/64 reduced to 7 rounds
- An RX-characteristic in the key schedule

Rotational-XOR cryptanalysis

Define a pair with $((a_1, a_2), \gamma)$-Rotational-XOR difference:

$$(x \oplus a_1, (x \lll \gamma) \oplus a_2)$$

$\gamma = 1$: $x \lll 1 \to \overleftarrow{x}$

- Applied to SPECK32/64 reduced to 7 rounds
- An RX-characteristic in the key schedule
- An RX-characteristic in the round function under a weak-key space

Rotational-XOR cryptanalysis

Define a pair with $((a_1, a_2), \gamma)$-Rotational-XOR difference:

$$(x \oplus a_1, (x \lll \gamma) \oplus a_2)$$

$\gamma = 1$: $x \lll 1 \rightarrow \overleftarrow{x}$

- Applied to $\textsc{Speck}$32/64 reduced to 7 rounds
- An RX-characteristic in the key schedule
- An RX-characteristic in the round function under a weak-key space
- Proof-of-concept

Rotational-XOR cryptanalysis

Define a pair with $((a_1, a_2), \gamma)$-Rotational-XOR difference:

$$(x \oplus a_1, (x \lll \gamma) \oplus a_2)$$

$\gamma = 1$: $x \lll 1 \rightarrow \overleftarrow{x}$

- Applied to $\textsc{Speck}$32/64 reduced to 7 rounds
- An RX-characteristic in the key schedule
- An RX-characteristic in the round function under a weak-key space
- Proof-of-concept

Automatic search techniques

Automatic Search Techniques

- Widely adopted in cryptanalysis

Automatic Search Techniques

- Widely adopted in cryptanalysis
- Estimate possible attacks in designs

Automatic Search Techniques

- Widely adopted in cryptanalysis
- Estimate possible attacks in designs
- Tools currently available:

Automatic Search Techniques

- Widely adopted in cryptanalysis
- Estimate possible attacks in designs
- Tools currently available:
  - Optimised search algorithms: ARXTools, YAARX

Automatic Search Techniques

- Widely adopted in cryptanalysis
- Estimate possible attacks in designs
- Tools currently available:
  - Optimised search algorithms: ARXTools, YAARX
  - MILP + Sage : [ST17], [SHW+14]

Automatic Search Techniques

- Widely adopted in cryptanalysis
- Estimate possible attacks in designs
- Tools currently available:
  - Optimised search algorithms: ARXTools, YAARX
  - MILP + Sage : [ST17], [SHW+14]
  - CP: [SGL+17]

Automatic Search Techniques

- Widely adopted in cryptanalysis
- Estimate possible attacks in designs
- Tools currently available:
  - Optimised search algorithms: ARXTools, YAARX
  - MILP + Sage : [ST17], [SHW+14]
  - CP: [SGL+17]
  - SAT/SMT: CryptoSMT, etc

[SGL+17] S. Sun, D. Gerault, P. Lafourcade, Q. Yang, Y. Todo, K. Qiao, and L. Hu. Analysis of AES, Skinny, and others with constraint programming. ToSC 2017
[SHW+14] S. Sun, L. Hu, P. Wang, K. Qiao, X. Ma, and L. Song. Automatic security evaluation and (related-key) differential characteristic search: Application to SIMON, PRESENT, LBlock, DES (L) and other bit-oriented block ciphers. ASIACRYPT 2014
[ST17] Y. Sasaki, and Y. Todo. New impossible differential search tool from design and cryptanalysis aspects. EUROCRYPT 2017

Automatic Search Techniques

- Widely adopted in cryptanalysis
- Estimate possible attacks in designs
- Tools currently available:
    - Optimised search algorithms: ARXTools, YAARX
    - MILP + Sage : [ST17], [SHW+14]
    - CP: [SGL+17]
    - SAT/SMT: CryptoSMT, etc
- Challenge: find an efficient method to encode the cryptographic problem

[SGL+17] S. Sun, D. Gerault, P. Lafourcade, Q. Yang, Y. Todo, K. Qiao, and L. Hu. Analysis of AES, Skinny, and others with constraint programming. ToSC 2017
[SHW+14] S. Sun, L. Hu, P. Wang, K. Qiao, X. Ma, and L. Song. Automatic security evaluation and (related-key) differential characteristic search: Application to SIMON, PRESENT, LBlock, DES (L) and other bit-oriented block ciphers. ASIACRYPT 2014
[ST17] Y. Sasaki, and Y. Todo. New impossible differential search tool from design and cryptanalysis aspects. EUROCRYPT 2017

Rotational-XOR Difference

RX-difference v1

A pair with $((a_1, a_2), \gamma)$-Rotational-XOR difference:

$$(x \oplus a_1, (x \lll \gamma) \oplus a_2)$$

Rotational-XOR Difference

RX-difference v1

A pair with $((a_1, a_2), \gamma)$-Rotational-XOR difference:

$$(x \oplus a_1, (x \lll \gamma) \oplus a_2)$$

equivalent to

$$(\tilde{x}, (\tilde{x} \lll \gamma) \oplus (a_1 \lll \gamma) \oplus a_2)$$

Rotational-XOR Difference

RX-difference v1

A pair with $((a_1, a_2), \gamma)$-Rotational-XOR difference:

$$(x \oplus a_1, (x \lll \gamma) \oplus a_2)$$

equivalent to

$$(\tilde{x}, (\tilde{x} \lll \gamma) \oplus (a_1 \lll \gamma) \oplus a_2)$$

RX-difference v2

The RX-difference of a pair (x_1, x_2):

$$\Delta_\gamma(x_1, x_2) = x_1 \oplus (x_2 \lll \gamma)$$

Rotational-XOR Difference

RX-difference v1

A pair with $((a_1, a_2), \gamma)$-Rotational-XOR difference:

$$(x \oplus a_1, (x \lll \gamma) \oplus a_2)$$

equivalent to

$$(\tilde{x}, (\tilde{x} \lll \gamma) \oplus (a_1 \lll \gamma) \oplus a_2)$$

RX-difference v2

The RX-difference of a pair (x_1, x_2):

$$\Delta_\gamma(x_1, x_2) = x_1 \oplus (x_2 \lll \gamma)$$

Given an RX-difference δ, an RX-pair is $(x, (x \lll \gamma) \oplus \delta)$.

Rotational-XOR Difference

Propagation Rules of RX-differences

- Linear operations

Rotational-XOR Difference

Propagation Rules of RX-differences

- Linear operations
- Modular addition

$$\overleftarrow{(x \oplus a_1) \boxplus (y \oplus b_1) \oplus \Delta_1} = (\overleftarrow{x} \oplus a_2) \boxplus (\overleftarrow{y} \oplus b_2) \oplus \Delta_2$$

Rotational-XOR Difference

Propagation Rules of RX-differences

- Linear operations
- Modular addition

$$\overleftarrow{(x \oplus a_1) \boxplus (y \oplus b_1) \oplus \Delta_1} = (\overleftarrow{x} \oplus a_2) \boxplus (\overleftarrow{y} \oplus b_2) \oplus \Delta_2$$

$$\begin{aligned} X &= x \oplus a_1 \\ Y &= y \oplus b_1 \\ Z &= X \boxplus Y \\ d_x &= \overleftarrow{a_1} \oplus a_2 \\ d_y &= \overleftarrow{b_1} \oplus b_2 \\ d_z &= \overleftarrow{\Delta_1} \oplus \Delta_2 \end{aligned}$$

Rotational-XOR Difference

Propagation Rules of RX-differences

- Linear operations
- Modular addition

$$\overleftarrow{(x \oplus a_1) \boxplus (y \oplus b_1) \oplus \Delta_1} = (\overleftarrow{x} \oplus a_2) \boxplus (\overleftarrow{y} \oplus b_2) \oplus \Delta_2$$

$$\Bigg\downarrow \quad \begin{aligned} X &= x \oplus a_1 \\ Y &= y \oplus b_1 \\ Z &= X \boxplus Y \\ d_x &= \overleftarrow{a_1} \oplus a_2 \\ d_y &= \overleftarrow{b_1} \oplus b_2 \\ d_z &= \overleftarrow{\Delta_1} \oplus \Delta_2 \end{aligned}$$

$$\overleftarrow{Z} \oplus d_z = (\overleftarrow{X} \oplus d_x) \boxplus (\overleftarrow{Y} \oplus d_y)$$

Rotational-XOR Difference

Propagation Rules of RX-differences

- Linear operations
- Modular addition

RX-difference propagation in modular addition

Assume that input RX-differences are d_x, d_y, output RX-difference is d_z. Then,

$$\Pr[(d_x, d_y) \to d_z] =$$

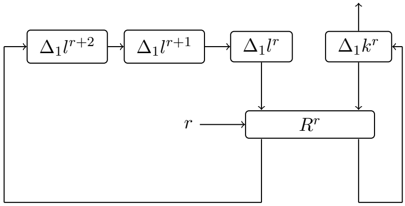
$$1_{(I\oplus SHL)(\delta_x\oplus\delta_y\oplus\delta_z)\oplus 1\preceq SHL((\delta_x\oplus\delta_z)|(\delta_y\oplus\delta_z))} \cdot 2^{-|SHL((\delta_x\oplus\delta_z)|(\delta_y\oplus\delta_z))|} \cdot 2^{-3}$$

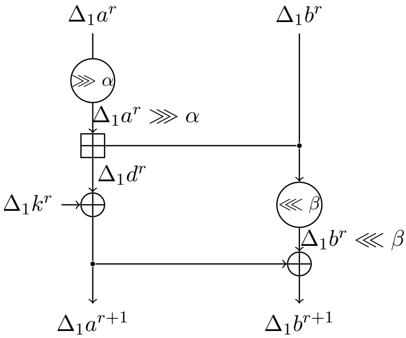
$$+1_{(I\oplus SHL)(\delta_x\oplus\delta_y\oplus\delta_z)\preceq SHL((\delta_x\oplus\delta_z)|(\delta_y\oplus\delta_z))} \cdot 2^{-|SHL((\delta_x\oplus\delta_z)|(\delta_y\oplus\delta_z))|} \cdot 2^{-1.415},$$

where

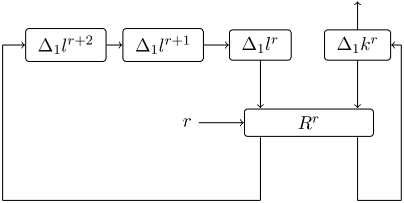
$$\delta_x = L'(d_x), \delta_y = L'(d_y), \delta_z = L'(d_z).$$

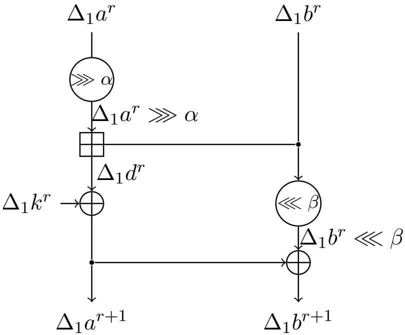
Applications to SPECK32/64





Applications to SPECK32/64





Search for RX-characteristics in the key part and data part

Application to SPECK32/64

SMT file – Modular Addition

Application to SPECK32/64

SMT file – Modular Addition

Condition 1

$$
\begin{aligned}
(I \oplus SHL)((\Delta_1 a^r \ggg \alpha) \oplus \Delta_1 b^r \oplus \Delta_1 d^r) \oplus 1 \\
\preceq SHL(((\Delta_1 a^r \ggg \alpha) \oplus \Delta_1 d^r) | (\Delta_1 b^r \oplus \Delta_1 d^r)) \\
w_r = |SHL(((\Delta_1 a^r \ggg \alpha) \oplus \Delta_1 d^r) | (\Delta_1 b^r \oplus \Delta_1 d^r))| + 3
\end{aligned}
$$

Application to SPECK32/64

SMT file – Modular Addition

Condition 1

$$
\begin{aligned}
(I \oplus SHL)((\Delta_1 a^r \ggg \alpha) \oplus \Delta_1 b^r \oplus \Delta_1 d^r) \oplus 1 & \\
\preceq SHL(((\Delta_1 a^r \ggg \alpha) \oplus \Delta_1 d^r)|(\Delta_1 b^r \oplus \Delta_1 d^r)) & \\
w_r = |SHL(((\Delta_1 a^r \ggg \alpha) \oplus \Delta_1 d^r)|(\Delta_1 b^r \oplus \Delta_1 d^r))| + 3 &
\end{aligned}
$$

Condition 2

$$
\begin{aligned}
(I \oplus SHL)((\Delta_1 a^r \ggg \alpha) \oplus \Delta_1 b^r \oplus \Delta_1 d^r) & \\
\preceq SHL(((\Delta_1 a^r \ggg \alpha) \oplus \Delta_1 d^r)|(\Delta_1 b^r \oplus \Delta_1 d^r)) & \\
w_r = |SHL(((\Delta_1 a^r \ggg \alpha) \oplus \Delta_1 d^r)|(\Delta_1 b^r \oplus \Delta_1 d^r))| + 1.415 &
\end{aligned}
$$

Application to SPECK32/64

SMT file – Modular Addition

Condition 1

$$
\begin{aligned}
&(I \oplus SHL)((\Delta_1 a^r \ggg \alpha) \oplus \Delta_1 b^r \oplus \Delta_1 d^r) \oplus 1 \\
&\qquad\qquad\qquad \preceq SHL(((\Delta_1 a^r \ggg \alpha) \oplus \Delta_1 d^r)|(\Delta_1 b^r \oplus \Delta_1 d^r))
\end{aligned}
$$

$$w_r = |SHL(((\Delta_1 a^r \ggg \alpha) \oplus \Delta_1 d^r)|(\Delta_1 b^r \oplus \Delta_1 d^r))| + 3$$

Condition 2

$$
\begin{aligned}
&(I \oplus SHL)((\Delta_1 a^r \ggg \alpha) \oplus \Delta_1 b^r \oplus \Delta_1 d^r) \\
&\qquad\qquad\qquad \preceq SHL(((\Delta_1 a^r \ggg \alpha) \oplus \Delta_1 d^r)|(\Delta_1 b^r \oplus \Delta_1 d^r))
\end{aligned}
$$

$$w_r = |SHL(((\Delta_1 a^r \ggg \alpha) \oplus \Delta_1 d^r)|(\Delta_1 b^r \oplus \Delta_1 d^r))| + 1.415$$

Total weight of a characteristic $W_{data} = \sum_r w_r$

Application to SPECK32/64

SMT file – Linear operations

Application to SPECK32/64

SMT file – Linear operations

$$\Delta_1 d^r \oplus \Delta_1 k^r \oplus \Delta_1 a^{r+1} = 0$$

$$\Delta_1 a^{r+1} \oplus (\Delta_1 b^r \lll \beta) \oplus \Delta_1 b^{r+1} = 0$$

Application to SPECK32/64

SMT file – Linear operations

$$\Delta_1 d^r \oplus \Delta_1 k^r \oplus \Delta_1 a^{r+1} = 0$$
$$\Delta_1 a^{r+1} \oplus (\Delta_1 b^r \lll \beta) \oplus \Delta_1 b^{r+1} = 0$$

Repeat the process for the key part, the total weight of an RX-characteristic is W_{key}

Application to SPECK32/64

SMT file – Linear operations

$$\Delta_1 d^r \oplus \Delta_1 k^r \oplus \Delta_1 a^{r+1} = 0$$

$$\Delta_1 a^{r+1} \oplus (\Delta_1 b^r \lll \beta) \oplus \Delta_1 b^{r+1} = 0$$

Repeat the process for the key part, the total weight of an RX-characteristic is W_{key}

SMT file – Objective functions

$$\min W_{data}$$

$$\min W_{key}$$

Search Strategy

- Optimise the key part and data part together

Search Strategy

- Optimise the key part and data part together
  - Inefficient
  - Set coefficients for the weights

Search Strategy

- Optimise the key part and data part together
  - Inefficient
  - Set coefficients for the weights
- Aim: Find a characteristic covering more rounds

Search Strategy

- Optimise the key part and data part together
    - Inefficient
    - Set coefficients for the weights
- Aim: Find a characteristic covering more rounds
- Set constraints in the weight of the data part, no constraints on key part

Search Strategy

- Optimise the key part and data part together
    - Inefficient
    - Set coefficients for the weights
- Aim: Find a characteristic covering more rounds
- Set constraints in the weight of the data part, no constraints on key part
- Fix the RX-characteristic in the data part, optimise the key part to better weak-key space

Search Strategy

- Optimise the key part and data part together
  - Inefficient
  - Set coefficients for the weights
- Aim: Find a characteristic covering more rounds
- Set constraints in the weight of the data part, no constraints on key part
- Fix the RX-characteristic in the data part, optimise the key part to better weak-key space
- Other strategy?

Search Strategy

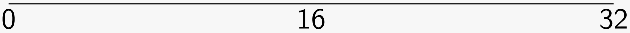
No MINIMIZE function in SAT/SMT, set the bound for objective function

Binary search

Search Strategy

No Minimize function in SAT/SMT, set the bound for objective function

Binary search

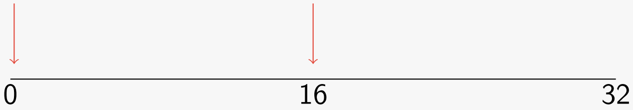


- Binary search on $[0, 32]$

Search Strategy

No MINIMIZE function in SAT/SMT, set the bound for objective function

Binary search

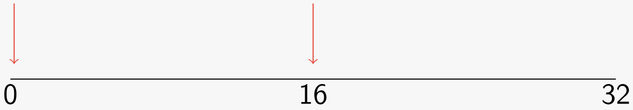


- Binary search on $[0, 32]$
- Red interval indicates the bounds for current objective function

Search Strategy

No MINIMIZE function in SAT/SMT, set the bound for objective function

Binary search

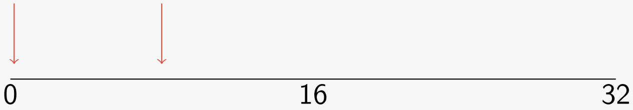


- Binary search on $[0, 32]$
- Red interval indicates the bounds for current objective function
- Search in $[0, 16]$,

Search Strategy

No MINIMIZE function in SAT/SMT, set the bound for objective function

Binary search

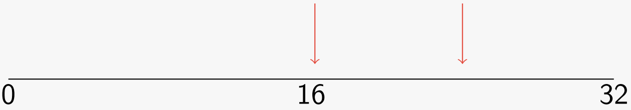


- Binary search on $[0, 32]$
- Red interval indicates the bounds for current objective function
- Search in $[0, 16]$, if solution found, search $[0, 8]$,

Search Strategy

No MINIMIZE function in SAT/SMT, set the bound for objective function

Binary search

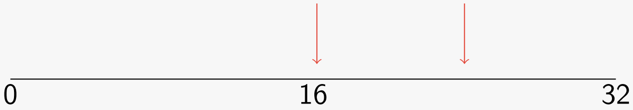


- Binary search on $[0, 32]$
- Red interval indicates the bounds for current objective function
- Search in $[0, 16]$, if solution found, search $[0, 8]$, otherwise $[16, 24]$

Search Strategy

No MINIMIZE function in SAT/SMT, set the bound for objective function

Binary search



- Binary search on $[0, 32]$
- Red interval indicates the bounds for current objective function
- Search in $[0, 16]$, if solution found, search $[0, 8]$, otherwise $[16, 24]$
- Terminate after the red interval collapsed

Results

RX-characteristics found in SPECK

Results

RX-characteristics found in SPECK

Version	Rounds	Data Prob.	Key Class Size	Ref.
32/64	9	2^{-30}	2^{64}	[Din14]
32/64	10	$2^{-19.15}$	$2^{28.10}$	This paper
32/64	11	$2^{-22.15}$	$2^{18.68}$	This paper
32/64	12	$2^{-25.57}$	$2^{4.92}$	This paper
48/96	10	2^{-40}	2^{96}	[Din14]
48/96	11	2^{-45}	2^{96}	[FWG+ 16]
48/96	11	$2^{-24.15}$	$2^{25.68}$	This paper
48/96	11	$2^{-23.15}$	$2^{14.93}$	This paper
48/96	12	$2^{-26.57}$	$2^{43.51}$	This paper
48/96	13	$2^{-31.98}$	$2^{24.51}$	This paper
48/96	14	$2^{-37.40}$	$2^{0.34}$	This paper
48/96	15	$2^{-43.81}$	$2^{1.09}$	This paper

Results

RX-characteristics found in SPECK

Results

RX-characteristics found in SPECK

Version	Rounds	Data Prob.	Key Class Size	Ref.
64/128	14	2^{-60}	2^{128}	[Din14]
64/128	15	2^{-62}	2^{128}	[FWG+16]
64/128	13	$2^{-37.98}$	$2^{21.92}$	This paper
96/144	13	2^{-84}	2^{144}	[Din14]
96/144	16	2^{-87}	2^{144}	[FWG+16]
96/144	13	$2^{-37.98}$	$2^{37.92}$	This paper
128/256	14	2^{-112}	2^{256}	[Din14]
128/256	19	2^{-119}	2^{256}	[FWG+16]
128/256	13	$2^{-31.98}$	$2^{182.51}$	This paper

[Din14] I. Dinur. Improved differential cryptanalysis of round-reduced SPECK. SAC 2014

[FWG+16] K. Fu, M. Wang, Y. Guo, S. Sun, and L. Hu. MILP-based automatic search algorithms for differential and linear trails for SPECK. FSE 2016

Conclusion

Conclusion

- An improved definition of RX-difference

Conclusion

- An improved definition of RX-difference
- Automatic search technique on RX-cryptanalysis

Conclusion

- An improved definition of RX-difference
- Automatic search technique on RX-cryptanalysis
- Distinguishers found in SPECK family, under weak-key classes

Conclusion

- An improved definition of RX-difference
- Automatic search technique on RX-cryptanalysis
- Distinguishers found in SPECK family, under weak-key classes
- RX-characteristics cover more rounds than differential characteristics, and the probability is relatively high.

Conclusion

- An improved definition of RX-difference
- Automatic search technique on RX-cryptanalysis
- Distinguishers found in SPECK family, under weak-key classes
- RX-characteristics cover more rounds than differential characteristics, and the probability is relatively high.

https://gitlab.esat.kuleuven.be/Adrian.Ranea/ArxPy

Conclusion

- An improved definition of RX-difference
- Automatic search technique on RX-cryptanalysis
- Distinguishers found in SPECK family, under weak-key classes
- RX-characteristics cover more rounds than differential characteristics, and the probability is relatively high.

https://gitlab.esat.kuleuven.be/Adrian.Ranea/ArxPy

Thank You!