Rotational Cryptanalysis in the Presence of Constants

Tomer Ashur **Yunwen Liu**

ESAT/COSIC, KU Leuven, and imec, Belgium

FSE, March 2017

Table of Contents

ARX

ARX

- Symmetric-key designs

ARX

- Symmetric-key designs
- Addition + Rotation + XOR

ARX

- Symmetric-key designs
- Addition $+$ Rotation $+$ XOR
- Differential cryptanalysis and linear cryptanalysis

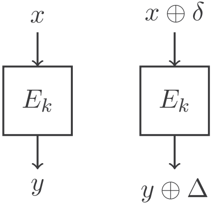
ARX

- Symmetric-key designs
- Addition + Rotation + XOR
- Differential cryptanalysis and linear cryptanalysis
- Rotational cryptanalysis

Differences

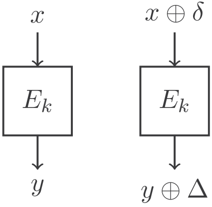
Differences

XOR difference

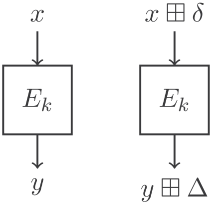


Differences

XOR difference

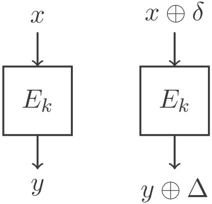


Modular difference

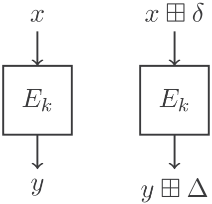


Differences

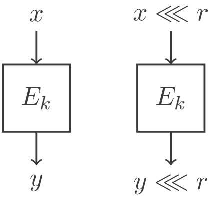
XOR difference



Modular difference



Rotational difference



Rotational Cryptanalysis

Rotational Cryptanalysis

Circular Rotation

$$(x \lll r) \lll s = x \lll (r + s)$$

Rotational Cryptanalysis

Circular Rotation

$$(x \lll r) \lll s = x \lll (r + s)$$

XOR

$$(x \lll r) \oplus (y \lll r) = (x \oplus y) \lll r$$

Rotational Cryptanalysis

Circular Rotation

$$(x \lll r) \lll s = x \lll (r + s)$$

XOR

$$(x \lll r) \oplus (y \lll r) = (x \oplus y) \lll r$$

Modular Addition

$$(x \lll r) \boxplus (y \lll r) = (x \boxplus y) \lll r \qquad \text{with probability } p$$

Rotational Cryptanalysis

Modular Addition

$$(x \lll r) \boxplus (y \lll r) = (x \boxplus y) \lll r \qquad \text{with probability } p$$

Rotational Cryptanalysis

Modular Addition

$$(x \lll r) \boxplus (y \lll r) = (x \boxplus y) \lll r \qquad \text{with probability } p$$

When $r = 1$, p achieves the maximum.

$$p = 2^{-1.415}$$

Rotational Cryptanalysis

Modular Addition

$$(x \lll r) \boxplus (y \lll r) = (x \boxplus y) \lll r \qquad \text{with probability } p$$

When $r = 1$, p achieves the maximum.

$$p = 2^{-1.415}$$

Denote $x \lll 1$ by $\overleftarrow{x}$ for simplicity.

Rotational Cryptanalysis

Rotational Cryptanalysis (v1), [KN10]

The probability that a rotational distinguisher holds for an ARX primitive is determined by the number of modular additions.

$$\mathrm{Pr} = (2^{-1.415})^{\# \boxplus}$$

[KN10]: D. Khovratovich, I. Nikolic: Rotational Cryptanalysis of ARX, FSE 2010

Rotational Cryptanalysis

Rotational Cryptanalysis (v2), [KNP+15]

The probability that a rotational distinguisher holds for an ARX primitive is dependent with the chained modular additions.

Rotational Cryptanalysis

Rotational Cryptanalysis (v2), [KNP+15]

The probability that a rotational distinguisher holds for an ARX primitive is dependent with the chained modular additions.

$$(x \lll r) \boxplus (y \lll r) = (x \boxplus y) \lll r$$

$$(x \lll r) \boxplus (y \lll r) \boxplus (z \lll r) = (x \boxplus y \boxplus z) \lll r$$

[KNP+15]: D. Khovratovich, I. Nikolic, J. Pieprzyk, P. Sokolowski, R. Steinfeld: Rotational Cryptanalysis of ARX Revisited. FSE 2015

Table of Contents

ARX with constants

ARX with constants

- Complete system ARX-C

ARX with constants

- Complete system ARX-C
- Constants come with keys and round constants

ARX with constants

- Complete system ARX-C
- Constants come with keys and round constants

XOR with a rotational variable

$$(x \lll r) \oplus (y \lll r) = (x \oplus y) \lll r$$

ARX with constants

- Complete system ARX-C
- Constants come with keys and round constants

XOR with a rotational variable

$$(x \lll r) \oplus (y \lll r) = (x \oplus y) \lll r$$

XOR with a constant

$$(x \lll r) \oplus k$$

ARX with constants

- Complete system ARX-C
- Constants come with keys and round constants

XOR with a rotational variable

$$(x \lll r) \oplus (y \lll r) = (x \oplus y) \lll r$$

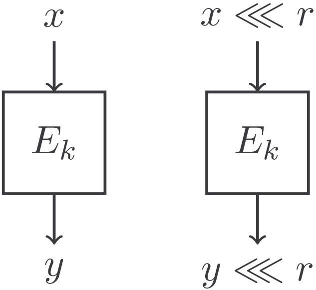
XOR with a constant

$$(x \lll r) \oplus k$$

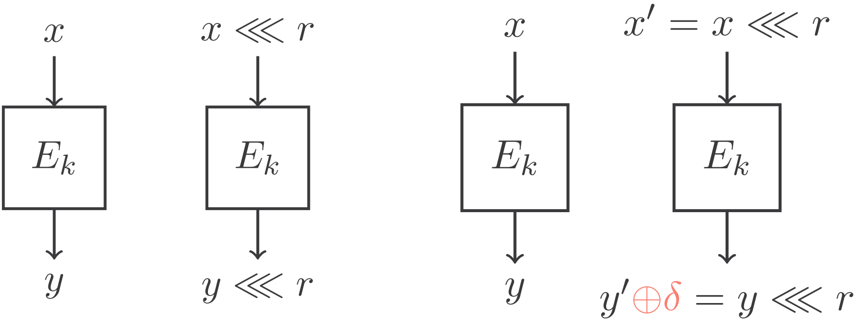
- Previous analyses: experiment

Rotational cryptanalysis on ARX-C

Rotational cryptanalysis on ARX-C



Rotational cryptanalysis on ARX-C



Rotational-XOR difference

Combine rotational difference with XOR difference

$$(x, (x \lll \gamma)$$

Rotational-XOR difference

Combine rotational difference with XOR difference

$$(x, (x \lll \gamma) \oplus a)$$

Rotational-XOR difference

Combine rotational difference with XOR difference

$$(x, (x \lll \gamma) \oplus a)$$

$((a_1, a_2), \gamma)$-Rotational-XOR difference (RX-difference)

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

Rotational-XOR difference

Combine rotational difference with XOR difference

$$(x, (x \lll \gamma) \oplus a)$$

$((a_1, a_2), \gamma)$-Rotational-XOR difference (RX-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 through ARX

Rotational-XOR difference through ARX

Rotation

$$x \xrightarrow{\lll \gamma} x \lll \gamma$$

$$\overleftarrow{x} \oplus a \xrightarrow{\lll \gamma} \overleftarrow{x \lll \gamma} \oplus (a \lll \gamma)$$

$$\Rightarrow ((0, a), 1) \xrightarrow{\lll \gamma} ((0, a \lll \gamma), 1)$$

Rotational-XOR difference through ARX

Rotation

$$x \xrightarrow{\lll \gamma} x \lll \gamma$$

$$\overleftarrow{x} \oplus a \xrightarrow{\lll \gamma} \overleftarrow{x \lll \gamma} \oplus (a \lll \gamma)$$

$$\Rightarrow ((0, a), 1) \xrightarrow{\lll \gamma} ((0, a \lll \gamma), 1)$$

XOR

$$x, y \xrightarrow{\oplus} x \oplus y$$

$$\overleftarrow{x} \oplus a, \overleftarrow{y} \oplus b \xrightarrow{\oplus} \overleftarrow{x \oplus y} \oplus (a \oplus b)$$

$$\Rightarrow ((0, a), 1), ((0, b), 1) \xrightarrow{\oplus} ((0, a \oplus b), 1)$$

Rotational-XOR difference through ARX

Modular addition

Rotational-XOR difference through ARX

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 through ARX

Modular addition

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

Sketch of proof:

Rotational-XOR difference through ARX

Modular addition

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

Sketch of proof:

$$x = \underbrace{L(x)}_{\gamma \text{ bits}} \; R(x) \;=\; L'(x) \; \underbrace{R'(x)}_{\gamma \text{ bits}}$$

Rotational-XOR difference through ARX

Modular addition

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

Sketch of proof:

$x =$	$L(x)$	$R(x)$	$=$	$L'(x)$	$R'(x)$
	γ bits				γ bits

The addition of two variables:

	$L(x)$	$R(x)$
	$L(y)$	$R(y)$
	one bit of carry	
$\boxplus$	$L(x) \boxplus L(y) \boxplus C^1_{n-\gamma}$	$R(x) \boxplus R(y)$

proof continued

LHS: $\overleftarrow{(x \oplus a_1) \boxplus (y \oplus b_1) \oplus \Delta_1}$

$$= \overleftarrow{((L(x) \oplus L(a_1)) \boxplus (L(y) \oplus L(b_1)) \boxplus C^1_{n-\gamma}) \oplus L(\Delta_1)||}$$

$$\overline{((R(x) \oplus R(a_1)) \boxplus (R(y) \oplus R(b_1))) \oplus R(\Delta_1)}$$

proof continued

LHS: $\overleftarrow{(x \oplus a_1) \boxplus (y \oplus b_1) \oplus \Delta_1}$

$$
\begin{aligned}
&= \overleftarrow{((L(x) \oplus L(a_1)) \boxplus (L(y) \oplus L(b_1)) \boxplus C^1_{n-\gamma}) \oplus L(\Delta_1)||} \\
&\qquad\qquad \overline{((R(x) \oplus R(a_1)) \boxplus (R(y) \oplus R(b_1))) \oplus R(\Delta_1)} \\
&= ((R(x) \oplus R(a_1)) \boxplus (R(y) \oplus R(b_1))) \oplus R(\Delta_1)|| \\
&\qquad\qquad ((L(x) \oplus L(a_1)) \boxplus (L(y) \oplus L(b_1)) \boxplus C^1_{n-\gamma}) \oplus L(\Delta_1).
\end{aligned}
$$

proof continued

LHS: $\overleftarrow{(x \oplus a_1) \boxplus (y \oplus b_1) \oplus \Delta_1}$

$$= \overleftarrow{((L(x) \oplus L(a_1)) \boxplus (L(y) \oplus L(b_1)) \boxplus C^1_{n-\gamma}) \oplus L(\Delta_1)||}$$
$$\overline{((R(x) \oplus R(a_1)) \boxplus (R(y) \oplus R(b_1))) \oplus R(\Delta_1)}$$
$$= ((R(x) \oplus R(a_1)) \boxplus (R(y) \oplus R(b_1))) \oplus R(\Delta_1)||$$
$$((L(x) \oplus L(a_1)) \boxplus (L(y) \oplus L(b_1)) \boxplus C^1_{n-\gamma}) \oplus L(\Delta_1).$$

RHS: $(\overleftarrow{x} \oplus a_2) \boxplus (\overleftarrow{y} \oplus b_2) \oplus \Delta_2$

$$= ((R(x) \oplus L^{'}(a_2)) \boxplus (R(y) \oplus L^{'}(b_2)) \boxplus C^2_{\gamma}) \oplus L^{'}(\Delta_2)||$$
$$((L(x) \oplus R^{'}(a_2)) \boxplus (L(y) \oplus R^{'}(b_2))) \oplus R^{'}(\Delta_2).$$

Rotational-XOR difference through ARX

proof continued

$$((L(x) \oplus L(a_1)) \boxplus (L(y) \oplus L(b_1)) \boxplus C^1_{n-\gamma}) \oplus L(\Delta_1) =$$
$$((L(x) \oplus R^{'}(a_2)) \boxplus (L(y) \oplus R^{'}(b_2))) \oplus R^{'}(\Delta_2).$$

$$((R(x) \oplus L^{'}(a_2)) \boxplus (R(y) \oplus L^{'}(b_2)) \boxplus C^2_{\gamma}) \oplus L^{'}(\Delta_2) =$$
$$(R(x) \oplus R(a_1)) \boxplus (R(y) \oplus R(b_1)) \oplus R(\Delta_1),$$

Rotational-XOR difference through ARX

proof continued

$$
\begin{aligned}
((L(x) \oplus L(a_1)) \boxplus (L(y) \oplus L(b_1)) \boxplus C^1_{n-\gamma}) \oplus L(\Delta_1) = \\
((L(x) \oplus R^{'}(a_2)) \boxplus (L(y) \oplus R^{'}(b_2))) \oplus R^{'}(\Delta_2). \\
((R(x) \oplus L^{'}(a_2)) \boxplus (R(y) \oplus L^{'}(b_2)) \boxplus C^2_{\gamma}) \oplus L^{'}(\Delta_2) = \\
(R(x) \oplus R(a_1)) \boxplus (R(y) \oplus R(b_1)) \oplus R(\Delta_1),
\end{aligned}
$$

Consider the carry

$$
\begin{aligned}
0 + 0 &= 00 \\
0 + 1 &= 01 \\
1 + 0 &= 01 \\
1 + 1 &= 10
\end{aligned}
$$

Rotational-XOR difference through ARX

proof continued

$$((L(x) \oplus L(a_1)) \boxplus (L(y) \oplus L(b_1)) \boxplus C^1_{n-\gamma}) \oplus L(\Delta_1) =$$
$$((L(x) \oplus R^{'}(a_2)) \boxplus (L(y) \oplus R^{'}(b_2))) \oplus R^{'}(\Delta_2).$$
$$((R(x) \oplus L^{'}(a_2)) \boxplus (R(y) \oplus L^{'}(b_2)) \boxplus C^2_{\gamma}) \oplus L^{'}(\Delta_2) =$$
$$(R(x) \oplus R(a_1)) \boxplus (R(y) \oplus R(b_1)) \oplus R(\Delta_1),$$

Consider the carry

$$0 + 0 = 00$$
$$0 + 1 = 01$$
$$1 + 0 = 01$$
$$1 + 1 = 10$$

Distribution of $C^1_{n-\gamma}$ and C^2_{γ}, when $\gamma = 1$

$$\Pr[C^2_{\gamma} = 0, C^1_{n-\gamma} = 0] = 2^{-1.415}$$
$$\Pr[C^2_{\gamma} = 0, C^1_{n-\gamma} = 1] = 2^{-1.415}$$
$$\Pr[C^2_{\gamma} = 1, C^1_{n-\gamma} = 0] = 2^{-3}$$
$$\Pr[C^2_{\gamma} = 1, C^1_{n-\gamma} = 1] = 2^{-3}.$$

Rotational-XOR difference through ARX

proof continued

$x \boxplus y = (x \oplus \zeta_1) \boxplus (y \oplus \zeta_2) \oplus \zeta_3$

differential probability

Rotational-XOR difference through ARX

proof continued

$x \boxplus y = (x \oplus \zeta_1) \boxplus (y \oplus \zeta_2) \oplus \zeta_3$ differential probability

$x \boxplus y \boxplus 1 = (x \oplus \zeta_1) \boxplus (y \oplus \zeta_2) \oplus \zeta_3$ See Lemma 1

Rotational-XOR difference through ARX

proof continued

$x \boxplus y = (x \oplus \zeta_1) \boxplus (y \oplus \zeta_2) \oplus \zeta_3$ differential probability

$x \boxplus y \boxplus 1 = (x \oplus \zeta_1) \boxplus (y \oplus \zeta_2) \oplus \zeta_3$ See Lemma 1

RX-difference through modular addition:

$$\Pr[\overleftarrow{(x \oplus a_1) \boxplus (y \oplus b_1) \oplus \Delta_1} = (\overleftarrow{x} \oplus a_2) \boxplus (\overleftarrow{y} \oplus b_2) \oplus \Delta_2]$$
$$= 1_{(I \oplus SHL)(\delta_1 \oplus \delta_2 \oplus \delta_3) \oplus 1 \preceq SHL((\delta_1 \oplus \delta_3)|(\delta_2 \oplus \delta_3))} \cdot 2^{-|SHL((\delta_1 \oplus \delta_3)|(\delta_2 \oplus \delta_3))|} \cdot 2^{-3}$$
$$+ 1_{(I \oplus SHL)(\delta_1 \oplus \delta_2 \oplus \delta_3) \preceq SHL((\delta_1 \oplus \delta_3)|(\delta_2 \oplus \delta_3))} \cdot 2^{-|SHL((\delta_1 \oplus \delta_3)|(\delta_2 \oplus \delta_3))|} \cdot 2^{-1.415},$$

where $\delta_1 = R(a_1) \oplus L^{'}(a_2), \delta_2 = R(b_1) \oplus L^{'}(b_2), \delta_3 = R(\Delta_1) \oplus L^{'}(\Delta_2)$

Table of Contents

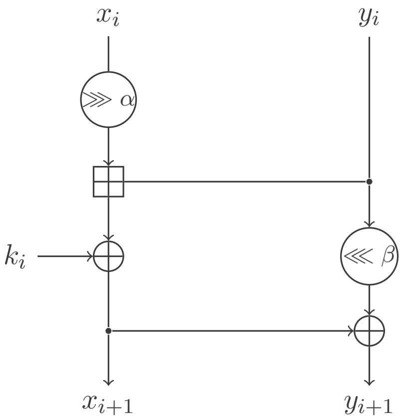
SPECK Family

SPECK Family

- NSA cipher
- block size 32/48/64/96/128 ($2n$)
- key size mn with $m = 2, 3, 4$

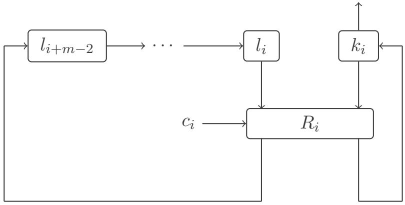
SPECK Family

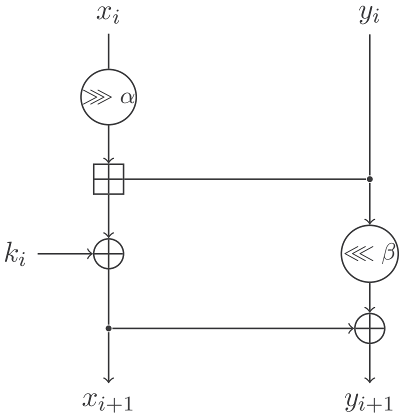
- NSA cipher
- block size 32/48/64/96/128 ($2n$)
- key size mn with $m = 2, 3, 4$



SPECK Family

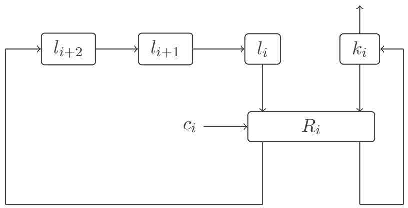
- NSA cipher
- block size 32/48/64/96/128 ($2n$)
- key size mn with $m = 2, 3, 4$

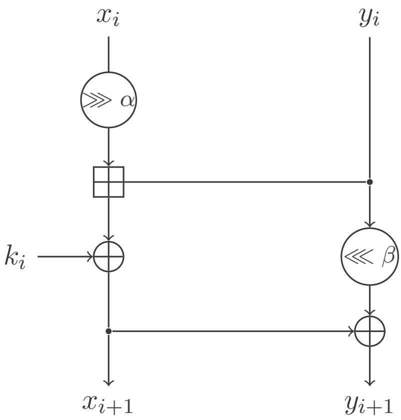




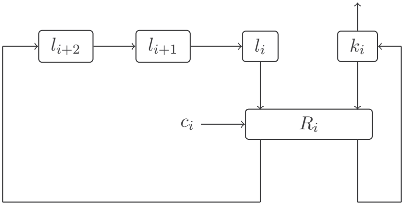
Application to SPECK32/64

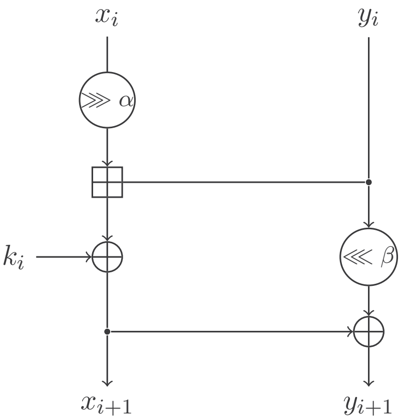
Application to SPECK32/64





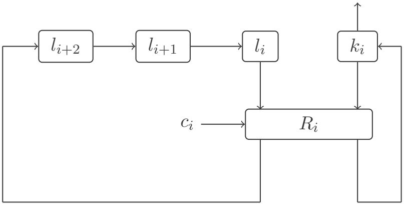
Application to SPECK32/64

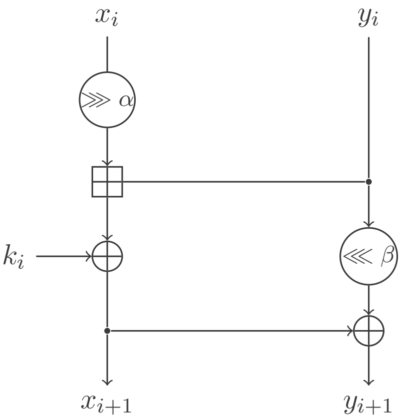




- Track RX-difference propagation in the key schedule

Application to SPECK32/64





- Track RX-difference propagation in the key schedule
- Based on the good RX-trails found in the key schedule, track the propagation of RX-differences in the encryption

Application to SPECK32/64

An RX-characteristic in the keyschedule

Round	a_1	b_1	Δ_1	a_2	b_2	Δ_2	Predicted Prob.	Empirical Prob.	Accumulated Prob.
1	0	0	0	0	0	0	$2^{-1.415}$	$2^{-1.415}$	$2^{-1.415}$
2	0	0	0	0	0	0	$2^{-1.415}$	$2^{-1.415}$	$2^{-2.83}$
3	0	1	0	0	1	2	$2^{-2.415}$	$2^{-2.415}$	$2^{-5.245}$
4	0	2	6	0	0	8	$2^{-2.415}$	$2^{-2.415}$	$2^{-7.66}$
5	0	D	C4	0	B	78	$2^{-6.415}$	$2^{-6.415}$	$2^{-14.075}$
6	0	F4	0	1000	50	1088	$2^{-7.415}$	$2^{-7.415}$	$2^{-21.49}$
Total							$2^{-21.49}$		

Application to SPECK32/64

An RX-characteristic in the keyschedule

Round	a_1	b_1	Δ_1	a_2	b_2	Δ_2	Predicted Prob.	Empirical Prob.	Accumulated Prob.
1	0	0	0	0	0	0	$2^{-1.415}$	$2^{-1.415}$	$2^{-1.415}$
2	0	0	0	0	0	0	$2^{-1.415}$	$2^{-1.415}$	$2^{-2.83}$
3	0	1	0	0	1	2	$2^{-2.415}$	$2^{-2.415}$	$2^{-5.245}$
4	0	2	6	0	0	8	$2^{-2.415}$	$2^{-2.415}$	$2^{-7.66}$
5	0	D	C4	0	B	78	$2^{-6.415}$	$2^{-6.415}$	$2^{-14.075}$
6	0	F4	0	1000	50	1088	$2^{-7.415}$	$2^{-7.415}$	$2^{-21.49}$
Total							$2^{-21.49}$		

Experimental probability: $2^{-25.046}$, leading to a weak-key class of size 2^{39}

All RX-differences are in hexadecimal notation.

Application to SPECK32/64

A corresponding RX-characteristic in the round function

Round	Input diff. (left,right)	Key diff.	Output diff. (left,right)	Predicted accumu. Prob.	Empirical accumu. Prob.
0	$0, 0$	0	$0, 0$	$2^{-1.415}$	$2^{-1.415}$
1	$0, 0$	0	$0, 0$	$2^{-2.83}$	$2^{-2.85}$
2	$0, 0$	3	$3, 3$	$2^{-4.245}$	$2^{-4.27}$
3	$3, 3$	4	$607, 60B$	$2^{-8.66}$	$2^{-8.68}$
4	$607, 60B$	11	$40E, 1C22$	$2^{-15.075}$	$2^{-15.01}$
5	$40E, 1C22$	$1B8$	$3992, 491A$	$2^{-21.49}$	$2^{-21.44}$
6	$3992, 491A$	1668	$333F, 1756$	$2^{-31.905}$	$2^{-31.6}$

All RX-differences are in hexadecimal notation.

Application to SPECK32/64

A corresponding RX-characteristic in the round function

Round	Input diff. (left,right)	Key diff.	Output diff. (left,right)	Predicted accumu. Prob.	Empirical accumu. Prob.
0	$0, 0$	0	$0, 0$	$2^{-1.415}$	$2^{-1.415}$
1	$0, 0$	0	$0, 0$	$2^{-2.83}$	$2^{-2.85}$
2	$0, 0$	3	$3, 3$	$2^{-4.245}$	$2^{-4.27}$
3	$3, 3$	4	$607, 60B$	$2^{-8.66}$	$2^{-8.68}$
4	$607, 60B$	11	$40E, 1C22$	$2^{-15.075}$	$2^{-15.01}$
5	$40E, 1C22$	$1B8$	$3992, 491A$	$2^{-21.49}$	$2^{-21.44}$
6	$3992, 491A$	1668	$333F, 1756$	$2^{-31.905}$	$2^{-31.6}$

All RX-differences are in hexadecimal notation.

Open-key model vs. Single-key model

Table of Contents

Conclusion

Conclusion

- We propose a new notion of difference: Rotational-XOR difference

Conclusion

- We propose a new notion of difference: Rotational-XOR difference
- Rotational cryptanalysis in the presence of constants can be mathematically characterised

Conclusion

- We propose a new notion of difference: Rotational-XOR difference
- Rotational cryptanalysis in the presence of constants can be mathematically characterised
- RX-distinguisher on SPECK32/64 is found

Conclusion

- We propose a new notion of difference: Rotational-XOR difference
- Rotational cryptanalysis in the presence of constants can be mathematically characterised
- RX-distinguisher on SPECK32/64 is found
- Further applications on ARX ciphers

Thank you!