Analysis of NORX

Investigating Differential and Rotational Properties

Jean-Philippe Aumasson[1] (@veorq)

Philipp Jovanovic[2] (@daeinar)

Samuel Neves[3] (@sevenps)

[1]Kudelski Security, Switzerland

[2]University of Passau, Germany

[3]University of Coimbra, Portugal

Latincrypt 2014

Florianópolis, September 17, 2014

Outline

1. Introduction: NORX
2. Differential Cryptanalysis
3. Rotational Cryptanalysis
4. Conclusion

NORX

Overview of NORX

Parameters

- *Word size:* $W \in \{32, 64\}$ bits
- *Number of rounds:* $1 \leq R \leq 63$
- *Parallelism degree:* $0 \leq D \leq 255$
- *Tag size:* $|A| \leq 10W$

Instances

Configurations submitted to CAESAR:

NORXW-R-D	Nonce size ($2W$)	Key size ($4W$)	Tag size ($4W$)	Classification
NORX64-4-1	128	256	256	Standard
NORX32-4-1	64	128	128	Standard
NORX64-6-1	128	256	256	High security
NORX32-6-1	64	128	128	High security
NORX64-4-4	128	256	256	High throughput

Overview of NORX

Parameters

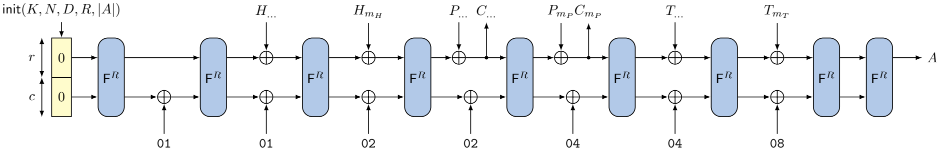
- *Word size:* $W \in \{32, 64\}$ bits
- *Number of rounds:* $1 \leq R \leq 63$
- *Parallelism degree:* $0 \leq D \leq 255$
- *Tag size:* $|A| \leq 10W$

Instances

Configurations submitted to CAESAR:

NORXW-R-D	Nonce size ($2W$)	Key size ($4W$)	Tag size ($4W$)	Classification
NORX64-4-1	128	256	256	Standard
NORX32-4-1	64	128	128	Standard
NORX64-6-1	128	256	256	High security
NORX32-6-1	64	128	128	High security
NORX64-4-4	128	256	256	High throughput

NORX Mode



NORX in Sequential Mode ($D = 1$)

Features

- (Parallel) monkeyDuplex construction (derived from Keccak/SHA-3)
- Processes header, payload and trailer data in one-pass
- Data expansion via multi-rate padding: 10^*1
- Extensible (e.g. sessions, secret message numbers)
- Parallel modes (not shown here)

The State

- NORX operates on a state of *16 W*-bit sized words

W	Size	Rate	Capacity
32	512	320	192
64	1024	640	384

- Arrangement of rate (data processing) and capacity (security) words:

s_0	s_1	s_2	s_3
s_4	s_5	s_6	s_7
s_8	s_9	s_{10}	s_{11}
s_{12}	s_{13}	s_{14}	s_{15}

Initialisation

- Load nonce, key and constants into state S:

u_0	n_0	n_1	u_1
k_0	k_1	k_2	k_3
u_2	u_3	u_4	u_5
u_6	u_7	u_8	u_9

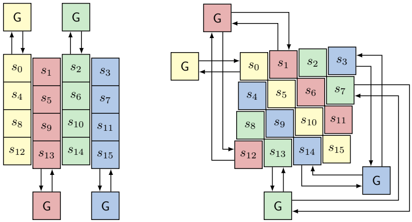
- Parameter integration:

$$s_{14} \leftarrow s_{14} \oplus (R \lll 26) \oplus (D \lll 18) \oplus (W \lll 10) \oplus |A|$$

- Apply round permutation F^R to S

The Permutation F^R

The Permutation F



The Permutation G

1: $a \longleftarrow \mathsf{H}(a, b)$
2: $d \longleftarrow (a \oplus d) \ggg r_0$
3: $c \longleftarrow \mathsf{H}(c, d)$
4: $b \longleftarrow (b \oplus c) \ggg r_1$
5: $a \longleftarrow \mathsf{H}(a, b)$
6: $d \longleftarrow (a \oplus d) \ggg r_2$
7: $c \longleftarrow \mathsf{H}(c, d)$
8: $b \longleftarrow (b \oplus c) \ggg r_3$

The Non-linear Operation H

$$\mathsf{H} : \mathbb{F}_2^{2n} \to \mathbb{F}_2^n, (x, y) \mapsto (x \oplus y) \oplus ((x \wedge y) \ll 1)$$

Rotation Offsets (r_0, r_1, r_2, r_3)

32-bit: $(8, 11, 16, 31)$ 64-bit: $(8, 19, 40, 63)$

The Permutation F^R

Features

- F and G derived from ARX-primitives ChaCha/BLAKE2
- H is an "approximation" of integer addition

$$x + y = (x \oplus y) + \big((x \wedge y) \ll 1\big)$$

  where $+$ is replaced by $\oplus$
- LRX permutation
- No SBoxes or integer additions
- SIMD-friendly
- Hardware-friendly
- High diffusion
- Constant-time

Differential Cryptanalysis

Differential Cryptanalysis

Trails

$$\delta := \delta_0 \xrightarrow[p_0]{\mathsf{F}} \delta_1 \xrightarrow[p_1]{\mathsf{F}} \dots \xrightarrow[p_{n-2}]{\mathsf{F}} \delta_{n-1} \xrightarrow[p_{n-1}]{\mathsf{F}} \delta_n$$

- Input difference: δ_0
- Output difference: δ_n
- Internal differences: δ_j $(0 < j < n)$
- Differential probability: $\mathrm{dp}(\delta) \approx \prod_{i=0}^{n-1} p_i$
- $\mathrm{dp}(\delta)$: fraction of state-pairs following the trail
- Weights: $w_i = -\log_2(p_i)$ and $w(\delta) \approx \sum_{i=0}^{n-1} w_i$

How do differences propagate through H, G and F?

Differential Cryptanalysis

Trails

$$\delta := \delta_0 \xrightarrow[p_0]{\mathsf{F}} \delta_1 \xrightarrow[p_1]{\mathsf{F}} \ldots \xrightarrow[p_{n-2}]{\mathsf{F}} \delta_{n-1} \xrightarrow[p_{n-1}]{\mathsf{F}} \delta_n$$

- Input difference: δ_0
- Output difference: δ_n
- Internal differences: δ_j $(0 < j < n)$
- Differential probability: $\mathrm{dp}(\delta) \approx \prod_{i=0}^{n-1} p_i$
- $\mathrm{dp}(\delta)$: fraction of state-pairs following the trail
- Weights: $w_i = -\log_2(p_i)$ and $w(\delta) \approx \sum_{i=0}^{n-1} w_i$

How do differences propagate through H, G and F?

XOR-Differentials

Let α, β and $\gamma \in \mathbb{F}_2^n$.

Lemma

- A *XOR-differential* $\delta := (\alpha, \beta) \longrightarrow \gamma$ with respect to H is satisfying:

$$(\alpha \oplus \beta \oplus \gamma) \wedge (\neg((\alpha \vee \beta) \ll 1)) = 0$$

- The XOR-differential probability is given by

$$\mathrm{xdp}^{\mathrm{H}}(\delta) = 2^{-w}$$

with

$$w = \mathrm{hw}((\alpha \vee \beta) \ll 1)$$

The value w is also called the *(XOR-differential) weight* of δ.

H-Differentials

Let α, β and $\gamma \in \mathbb{F}_2^n$.

Lemma

- A H-*differential* $\delta := (\alpha, \beta) \longrightarrow \gamma$ with respect to XOR, is satisfying:

$$(\alpha \oplus \beta \oplus \gamma) \wedge (\neg(\gamma \ll 1) \oplus (\alpha \ll 1)) \wedge (\neg(\beta \ll 1) \oplus (\gamma \ll 1)) = 0$$

- The H-differential probability is given by

$$\mathrm{Hdp}^{\oplus}(\delta) = 2^{-w}$$

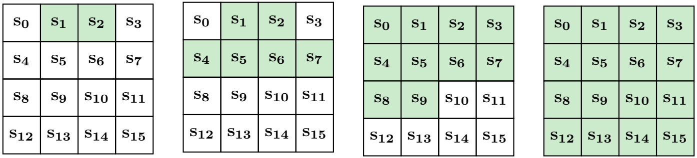
  with

$$w = \mathrm{hw}(((\alpha \oplus \gamma) \vee (\beta \oplus \gamma)) \ll 1)$$

  The value w is also called the H-*differential weight* of δ.

Differential Cryptanalysis

Settings



init_N $\text{init}_{N,K}$ rate full

- Four scenarios how an attacker can inject differences
- init_N and $\text{init}_{N,K}$: initialisation
- rate: data processing
- full: trail construction & estimation of F^R's general strength

NODE

The (NO)RX (D)ifferential Search (E)ngine

- Automatic search for XOR-differentials/differential trails in F^R.
- Based on differential propagation results of H.
- Description of the problem in CVC language.
- Uses constraint- / SAT-solvers (STP, Boolector, CryptoMiniSat).
- Available on GitHub: `https://github.com/norx/NODE`.

Bonus: Variant of NODE helped to find differentials for *practical forgery attacks* on *Wheesht* and *McMambo*, two other CAESAR candidates.

NODE

The (NO)RX (D)ifferential Search (E)ngine

- Automatic search for XOR-differentials/differential trails in F^R.
- Based on differential propagation results of H.
- Description of the problem in CVC language.
- Uses constraint- / SAT-solvers (STP, Boolector, CryptoMiniSat).
- Available on GitHub: `https://github.com/norx/NODE`.

Bonus: Variant of NODE helped to find differentials for *practical forgery attacks* on *Wheesht* and *McMambo*, two other CAESAR candidates.

NODE – Experimental Verification (full)

Settings			NORX32			NORX64		
w_e	$\#S$	v_e	v_m	$v_m - v_e$	w_m	v_m	$v_m - v_e$	w_m
12	2^{28}	65536	65652	+116	11.997	65627	+91	11.997
13	2^{29}	65536	65788	+252	12.994	65584	+48	12.998
14	2^{30}	65536	65170	−366	14.008	65476	−60	14.001
15	2^{31}	65536	65441	−95	15.002	65515	−21	15.000
16	2^{32}	65536	65683	+147	15.996	65563	+27	15.999
17	2^{33}	65536	65296	−240	17.005	65608	+72	16.998
18	2^{34}	65536	65389	−147	18.003	65565	+29	17.999

- w_e: expected weight
- $\#S$: number of samples
- $v_e = log_2(\#S) - w_e$: expected number of state-pairs adhering trail
- v_m: measured number of state-pairs adhering trail
- w_m: measured weight

Differential Cryptanalysis

Differentials of Weight 0 in G

	Differences			
δ_0	80000000	80000000	80000000	00000000
δ_1	00000000	00000001	80000000	00000000
δ_0	80000000	00000000	80000000	80000080
δ_1	80000000	00000000	00000000	00000000
δ_0	00000000	80000000	00000000	80000080
δ_1	80000000	00000001	80000000	00000000

	Differences			
δ_0	8000000000000000	8000000000000000	8000000000000000	0000000000000000
δ_1	0000000000000000	0000000000000001	8000000000000000	0000000000000000
δ_0	8000000000000000	0000000000000000	8000000000000000	8000000000000080
δ_1	8000000000000000	0000000000000000	0000000000000000	0000000000000000
δ_0	0000000000000000	8000000000000000	0000000000000000	8000000000000080
δ_1	8000000000000000	0000000000000001	8000000000000000	0000000000000000

- "Exhaustive search" for weight-0 (i.e. probability-1) trails in G.
- Exactly 3 such trails exist in 32- and 64-bit G.
- Re-used later for differential trail search in F^4.

Differential Cryptanalysis

Lower Bounds for Differential Trails

	NORX32				NORX64			
	init_N	$\text{init}_{N,K}$	rate	full	init_N	$\text{init}_{N,K}$	rate	full
$F^{0.5}$	6	2	2	0	6	2	2	0
$F^{1.0}$	(60)	22	10	2	(53)	22	12	2
$F^{1.5}$	(60)	(40)	(31)	12	(53)	(35)	(27)	12
$F^{2.0}$	(61)	(45)	(34)	(27)	(51)	(37)	(30)	(23)

- Notation:

  $w \;\hat{=}\;$ first trails for weight w

  $(w) \;\hat{=}\;$ no trails for weights $\leq w$

- Checked all trails in F under init_N with 1- and 2-bit input differences:

NORX32	NORX64
67	76

Differential Cryptanalysis

Lower Bounds for Differential Trails

	NORX32				NORX64			
	init_N	$\text{init}_{N,K}$	rate	full	init_N	$\text{init}_{N,K}$	rate	full
$F^{0.5}$	6	2	2	0	6	2	2	0
$F^{1.0}$	(60)	22	10	2	(53)	22	12	2
$F^{1.5}$	(60)	(40)	(31)	12	(53)	(35)	(27)	12
$F^{2.0}$	(61)	(45)	(34)	(27)	(51)	(37)	(30)	(23)

- Notation:

  $w \;\widehat{=}\;$ first trails for weight w

  $(w) \;\widehat{=}\;$ no trails for weights $\leq w$

- Checked all trails in F under init_N with 1- and 2-bit input differences:

NORX32	NORX64
67	76

Differential Cryptanalysis

Best Trail in F^4 (full, 32-bit), Weight 584

δ_0				w_0	δ_1				w_1
80140100	90024294	84246020	92800154		40100000	00000400	80000000	00000400	
e4548300	52240214	e0202424	d0004054	172	00100200	80000400	80000000	00000000	11
c4464046	00a08480	c1008108	90d43134		00000000	80000000	80008000	00000400	
e200c684	e2eac480	a4848881	06915342		40000200	80000000	00800000	00040400	
δ_2				w_2	δ_3				w_3
00000000	00000000	00000000	00000000		04042425	00100002	00020000	02100000	
00000000	00000000	00000000	00000000	44	04200401	42024200	20042024	20042004	357
00000000	80000000	00000000	00000000		10001002	80000200	25250504	10021010	
00000000	00000000	00000000	00000000		10020010	00001002	00000210	04252504	
δ_4									
c4001963	804da817	0c05b60e	12220503						
9072b909	185b792a	cc0d56cd	7e0ac646		total weight: 584				
80116300	100c2800	8f003320	3b270222						
01056104	88000041	92002824	04210001						

- Based on a low-weight, high-probability differential in G (32-bit).

Differential Cryptanalysis

Best Trail in F^4 (full, 64-bit), Weight 836

δ_0				w_0	δ_1				w_1
00900824010288c5	4000443880011086	224012044220ac43	e004044484049520	349	8000000800050000	8000000000000000	4000000000000000	0000001000020080	27
4080882001010885	4600841880821086	a3c0721444632c43	c224440007849504		8000000800040000	8000000000000000	c000000000040000	8000001000020080	
81600850830b0484	840080c080868000	8004449040c14400	8102101840908a80		0000000000000000	8000008000000000	c000004000040000	4000808000020080	
6191548c08000581	0200004006038044	8104f01c8702c0e0	60605084938886e3		0000000000010080	0000800000000000	8000400004040000	80808000020000c0	
δ_2				w_2	δ_3				w_3
8000000000000000	0000000000000000	0000000000000000	0000000000000000	12	0000000000000000	0000000000000000	0000100000000000	0000202000000001	448
8000000000000000	0000000000000000	0000000000000000	0000000000000000		4200404002020040	0000000000000000	0000000000000000	0000200000000021	
8000000000000000	0000000000000000	0000000000000000	0000000000000000		8000000000000010	2100000001010020	0000000000000000	0000000000000000	
0000000000000000	0000000000000000	0000000000000000	0000000000000000		0000000000000000	0000000000000010	2000000001010020	0000000000000000	
δ_4									
321a4500060e4e2e	27404405026e500e	3806422387200a08	8c40f4a0884c0820		total weight: 836				
71540fb858cb9902	ee018cc282747980	c714164174ce3eb9	1a49a091101191e1						
786680d0e46406cb	14440844013274e6	03a843203f071b7c	09a840c00c0ccc78						
4000404a22120005	07220c4202016240	2aa4200a0a041a62	84a468682000601c						

- Based on a weight-0 differential in G (64-bit).

Differential Cryptanalysis

Iterative Differentials in F^R

- Definition:

$$\delta \xrightarrow[w]{\mathsf{F}} \delta$$

- Results:

R	NORX32	NORX64	
1	(29)	(27)	verified
1	512	843	best
8	$232 \leq$	$216 \leq$	estimated
12	$348 \leq$	$324 \leq$	estimated

Differential Cryptanalysis

Equal-Column Differentials in F^R

- Based on NORX weak states:

$$\begin{pmatrix} w & w & w & w \\ x & x & x & x \\ y & y & y & y \\ z & z & z & z \end{pmatrix}$$

- Results:

R	NORX32	NORX64	
1	44	44	best
8	$352 \leq$	$352 \leq$	estimated
12	$528 \leq$	$528 \leq$	estimated

Rotational Cryptanalysis

Rotational Cryptanalysis

Lemma

- Let $x,\ y \in \mathbb{F}_2^n$. The probability that (x, y) is a rotational pair with respect to H for an offset r is

$$\Pr(\mathrm{H}(x, y) \ggg r = \mathrm{H}(x \ggg r, y \ggg r)) = \frac{9}{16}\ (\approx 2^{-0.83})$$

- Let S be a $16W$-bit NORX state, then we get

$$\Pr(\mathrm{F}^R(S) \ggg r = \mathrm{F}^R(S \ggg r)) = \left(\frac{9}{16}\right)^{4 \cdot 4 \cdot 2 \cdot R}$$

re-using the above result and a Theorem* for ARX-primitives.

* Khovratovich, D., Nikolic, I.: Rotational Cryptanalysis of ARX. In: Hong, S., Iwata, T. (eds.) FSE 2010. LNCS, vol. 6147, pp. 333–346. Springer, Heidelberg (2010)

Rotational Cryptanalysis

Consequences

- Bounds for rotational distinguishers on F^R:

R	4	6	8	12
w	106	159	212	318

- F^R on a $16W$-bit state is indistinguishable from random for

$$20 \leq R \text{ (32-bit) and } 39 \leq R \text{ (64-bit)}$$

  with weights 531 and 1035, respectively.
- However, not directly applicable to NORX due to asymmetric initialisation constants and the monkeyDuplex construction.

Paper presents more on rotational properties of NORX ...

Conclusion

Take Aways

Results

- Differential cryptanalysis:

R	type	NORX32	NORX64	
1	init_N	$60 < w \leq 67$	$53 < w \leq 76$	bound
4	full	584	836	best

NORX initialisation with $8 \leq R$ seems to have a *high security margin* against differential attacks.

- Rotational cryptanalysis:
  - Derived bounds for rot. distinguishers on F^R.
  - Not directly transferable to NORX: Protection through asymmetric init. constants and the monkeyDuplex construction.

Take Aways

Results

- Differential cryptanalysis:

R	type	NORX32	NORX64	
1	init_N	$60 < w \leq 67$	$53 < w \leq 76$	bound
4	full	584	836	best

  NORX initialisation with $8 \leq R$ seems to have a *high security margin* against differential attacks.

- Rotational cryptanalysis:
  - Derived bounds for rot. distinguishers on F^R.
  - Not directly transferable to NORX: Protection through asymmetric init. constants and the monkeyDuplex construction.

Take Aways

Results

- Differential cryptanalysis:

R	type	NORX32	NORX64	
1	init_N	$60 < w \leq 67$	$53 < w \leq 76$	bound
4	full	584	836	best

  NORX initialisation with $8 \leq R$ seems to have a *high security margin* against differential attacks.

- Rotational cryptanalysis:
  - Derived bounds for rot. distinguishers on F^R.
  - Not directly transferable to NORX: Protection through asymmetric init. constants and the monkeyDuplex construction.

Take Aways

Results

- Differential cryptanalysis:

R	type	NORX32	NORX64	
1	init_N	$60 < w \leq 67$	$53 < w \leq 76$	bound
4	full	584	836	best

NORX initialisation with $8 \leq R$ seems to have a *high security margin* against differential attacks.

- Rotational cryptanalysis:
  - Derived bounds for rot. distinguishers on F^R.
  - Not directly transferable to NORX: Protection through asymmetric init. constants and the monkeyDuplex construction.

Take Aways

Work In Progress

- Trail clustering and alignment analysis
- Differential cryptanalysis of F^R for $W \in \{8, 16\}$

Open Problems

- Linear, algebraic, (adv.) differential, (adv.) rotational cryptanalysis
- Side-channel attacks

Further Information

`https://norx.io`

Contact:
jovanovic@fim.uni-passau.de
@Daeinar

Take Aways

Work In Progress

- Trail clustering and alignment analysis
- Differential cryptanalysis of F^R for $W \in \{8, 16\}$

Open Problems

- Linear, algebraic, (adv.) differential, (adv.) rotational cryptanalysis
- Side-channel attacks

Further Information

https://norx.io

Contact:
jovanovic@fim.uni-passau.de
@Daeinar

Take Aways

Work In Progress

- Trail clustering and alignment analysis
- Differential cryptanalysis of F^R for $W \in \{8, 16\}$

Open Problems

- Linear, algebraic, (adv.) differential, (adv.) rotational cryptanalysis
- Side-channel attacks

Further Information

`https://norx.io`

Contact:
jovanovic@fim.uni-passau.de
@Daeinar