NORX8 and NORX16: AEAD for Low-End Systems

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

Rump Session

Fast Software Encryption 2015
Istanbul, Turkey

Overview

NORX32/64

- CAESAR candidate.
- Based on 32-/64-bit words.
- State sizes of 512/1024 bits.
- Proposed security levels: 128/256 bits.

NORX8/16

- New variants for low-end systems.
- Based on 8-/16-bit words.
- State sizes of 128/256 bits.
- Proposed security levels: 80/96 bits.

Overview

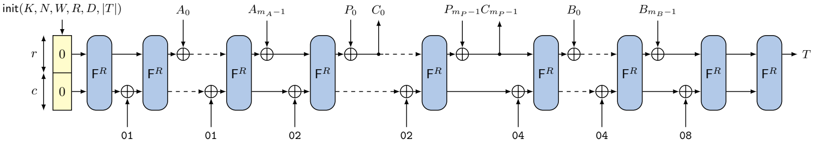
NORX32/64

- CAESAR candidate.
- Based on 32-/64-bit words.
- State sizes of 512/1024 bits.
- Proposed security levels: 128/256 bits.

NORX8/16

- New variants for low-end systems.
- Based on 8-/16-bit words.
- State sizes of 128/256 bits.
- Proposed security levels: 80/96 bits.

NORX8/16 – Layout



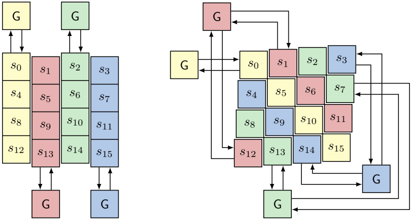
- monkeyDuplex construction.
- Process header, payload, trailer in one pass.
- Recommended parameter selections:

W	R	D	$\lvert T\rvert$	$\lvert K\rvert$	$\lvert N\rvert$	b	r	c
8	4 or 6	1	80	80	32	128	40*	88*
16	4 or 6	1	96	96	32	256	128	128

* Uses new security bounds from *Security of Keyed Sponge Constructions Using a Modular Proof Approach* by E. Andreeva, J. Daemen, B. Mennink, and G. Van Assche (FSE'15).

NORX8/NORX16 – 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

$$\mathsf{H} : \{0,1\}^{2n} \to \{0,1\}^n, \; (x, y) \mapsto (x \oplus y) \oplus ((x \wedge y) \ll 1)$$

Rotation Offsets (r_0, r_1, r_2, r_3)

8-bit: $(1, 3, 5, 7)$ 16-bit: $(8, 11, 12, 15)$

NORX8/16 – Misc

Estimations for HW Implementations

- NORX8: $\approx$ 1400 GE
- NORX16: $\approx$ 2900 GE

Preliminary Security Analysis

- Full diffusion after 2 rounds.
- No fixed-points $G(a, b, c, d) = (a, b, c, d)$ except for all-zero. Equivalently: F^R.
- Upper bounds for differential characteristics (determined with the help of SAT-/SMT-solvers):

W	F^2 (perm)	F (init)	F (init) + F^6 (perm)
8	2^{-29}	2^{-32}	$\leq 2^{-119}$
16	2^{-37}	2^{-53}	$\leq 2^{-164}$

NORX8/16 – Misc

Estimations for HW Implementations

- NORX8: ≈ 1400 GE
- NORX16: ≈ 2900 GE

Preliminary Security Analysis

- Full diffusion after 2 rounds.
- No fixed-points $G(a, b, c, d) = (a, b, c, d)$ except for all-zero. Equivalently: F^R.
- Upper bounds for differential characteristics (determined with the help of SAT-/SMT-solvers):

W	F^2 (perm)	F (init)	F (init) + F^6 (perm)
8	2^{-29}	2^{-32}	$\leq 2^{-119}$
16	2^{-37}	2^{-53}	$\leq 2^{-164}$

Conclusion

- NORX8/16: AEAD for resource-constrained systems.
- Work-in-progress paper: TRUDEVICE, Grenoble, 2015-03-13.
- Call to arms: “cryptanalyse them!”

Thank you!