NORX: Parallel and Scalable Authenticated Encryption

Jean-Philippe Aumasson
Kudelski Security
jeanphilippe.aumasson@gmail.com

Philipp Jovanovic
University of Passau
jovanovic@fim.uni-passau.de

Samuel Neves
University of Coimbra
sneves@dei.uc.pt

Overview

- **Authenticated encryption** protects payload data (integrity + authenticity + confidentiality) and associated data (integrity + authenticity).
- **NORX** is a family of authenticated encryption schemes with support for associated data (**AEAD**).
- Includes 8-, 16-, 32- and 64-bit variants.
- **NORX32/NORX64** are candidates in **CAESAR** — the **C**ompetition for **A**uthenticated **E**ncryption: **S**ecurity, **A**pplicability, and **R**obustness.
- Latest addition for low-end systems: **NORX8/NORX16**.
- **Features:**
  - Secure, fast, and scalable.
  - Based on well-analysed primitives: ChaCha/BLAKE(2)/Keccak.
  - Simple design.
  - Hardware and software friendly.
  - Parallelisable.
  - Online.
  - Side-channel robustness (constant-time operations).
  - Straightforward to implement.
  - High key agility.
  - No AES dependence.

Specification

1) Notation

W	word size	**A**	header	**S**	internal state
R	number of rounds	**B**	trailer	**b**	state size
D	parallelism degree	**P**	payload	**r**	rate
K	key	**C**	ciphertext	**c**	capacity
N	nonce	**T**	authentication tag		

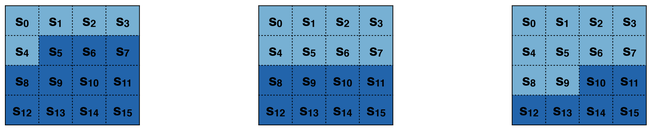
2) Parameters

- Identifying parameters of an instance: W, R, D and |T|.
- Notation: **NORXW-R-D-|T|.** Shortened to **NORXW-R-D** if default value of |T| = |K| is used (see below).
- Recommended selections:

W	R	D	|T|	|K|	|N|	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
32	4 or 6	1	128	128	64	512	320	192
64	4 or 6	1 or 4	256	256	128	1024	640	384

3) State

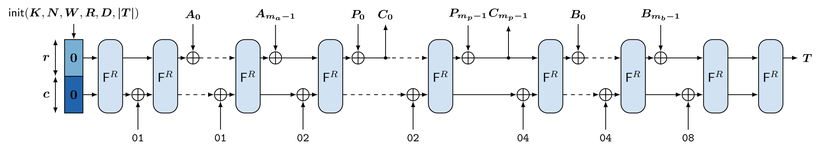
- Distribution of **rate** (data processing) and **capacity** (security) words in S:



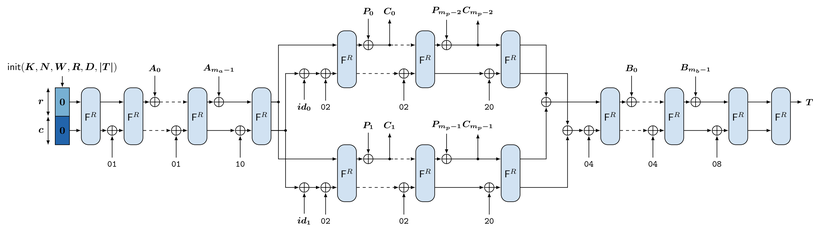
NORX8 NORX16 NORX32/64

4) Layout

- Sequential Version: D = 1, W = 8,16,32,64.

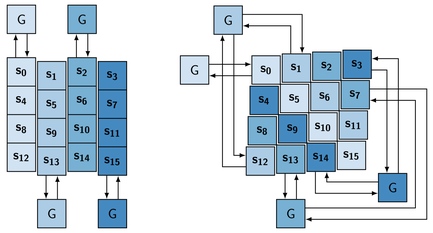


- Parallel Version: D > 1, W = 32,64.



5) Permutation F^R

- Permutation F: updates the four columns and the four diagonals of S.



a) column step b) diagonal step

- Permutation G: updates input words a,b,c,d in eight steps.

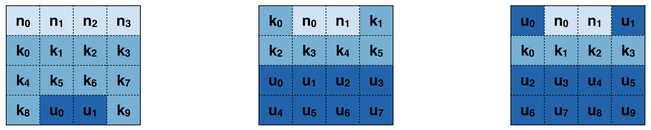
1. $a \longleftarrow (a \oplus b) \oplus ((a \wedge b) \ll 1)$
2. $d \longleftarrow (a \oplus d) \ggg r_0$
3. $c \longleftarrow (c \oplus d) \oplus ((c \wedge d) \ll 1)$
4. $b \longleftarrow (b \oplus c) \ggg r_1$
5. $a \longleftarrow (a \oplus b) \oplus ((a \wedge b) \ll 1)$
6. $d \longleftarrow (a \oplus d) \ggg r_2$
7. $c \longleftarrow (c \oplus d) \oplus ((c \wedge d) \ll 1)$
8. $b \longleftarrow (b \oplus c) \ggg r_3$

- Rotation Offsets: used for cyclic rotations in G.

W	8	16	32	64
(r_0,r_1,r_2,r_3)	(1,3,5,7)	(8,11,12,15)	(8,11,16,31)	(8,19,40,63)

6) Initialisation

- Load **nonce**, **key**, and **constants** into S. Constants u_i are generated by $(u_0,\ldots,u_{15}) \longleftarrow F^2(0,\ldots,15)$.
- Integrate parameters: XOR W, R, D, |T| to s_{12}, s_{13}, s_{14}, s_{15}, respectively.
- Update S by one application of F^R.



NORX8 NORX16 NORX32/64

Security

1) Requirements for Secure Usage

- Unique nonces.
- Abort on tag verification failure.

2) Expected Security Levels

Security Goal	NORX8	NORX16	NORX32	NORX64
Plaintext confidentiality	80	96	128	256
Plaintext integrity	80	96	128	256
Associated data integrity	80	96	128	256
Nonce integrity	80	96	128	256

3) Cryptanalytic Findings

- Conservative parameter choices. For example, NORX32/64 could increase rate by 2W for higher speeds (+16%) at no penalty for generic security.
- Parallel versions achieve generic security levels as well.
- Upper bounds for differential characteristics (determined with 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}	$\leq 2^{-164}$
32	$\leq 2^{-27}$	2^{-67}	$\leq 2^{-148}$
64	$\leq 2^{-23}$	$\leq 2^{-62}$	$\leq 2^{-131}$

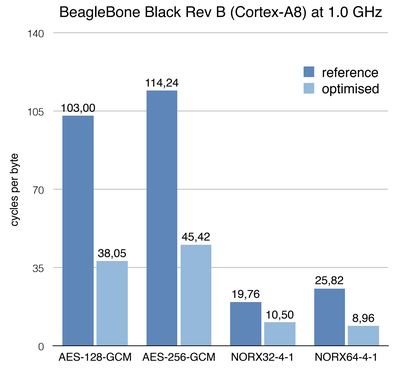
Performance

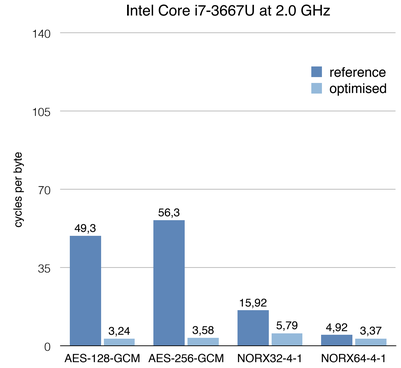
1) NORX64-4-1 in SW

Platform	Cycles per Byte	MiBps
Ivy Bridge: i7 3667U @ 2.0 GHz	3.37	**593**
Haswell: i7 4770K @ 3.5 GHz	2.51	**1390**
BeagleBone Black: Cortex-A8 @ 1.0 GHz	8.96	**111**
iPad Air: Apple A7 @ 1.4 GHz	4.07	**343**

2) NORX64-4-1 in HW (ASIC): 59 kGE, 180 nm UMC, 125 MHz, **10 Gbps**.

3) NORX vs. AES-GCM in SW





Trustworthy Manufacturing and Utilization of Secure Devices – TRUDEVICE 15, March 13, 2015, Grenoble, France