

MORUS

A Fast Authenticated Cipher

Hongjun Wu

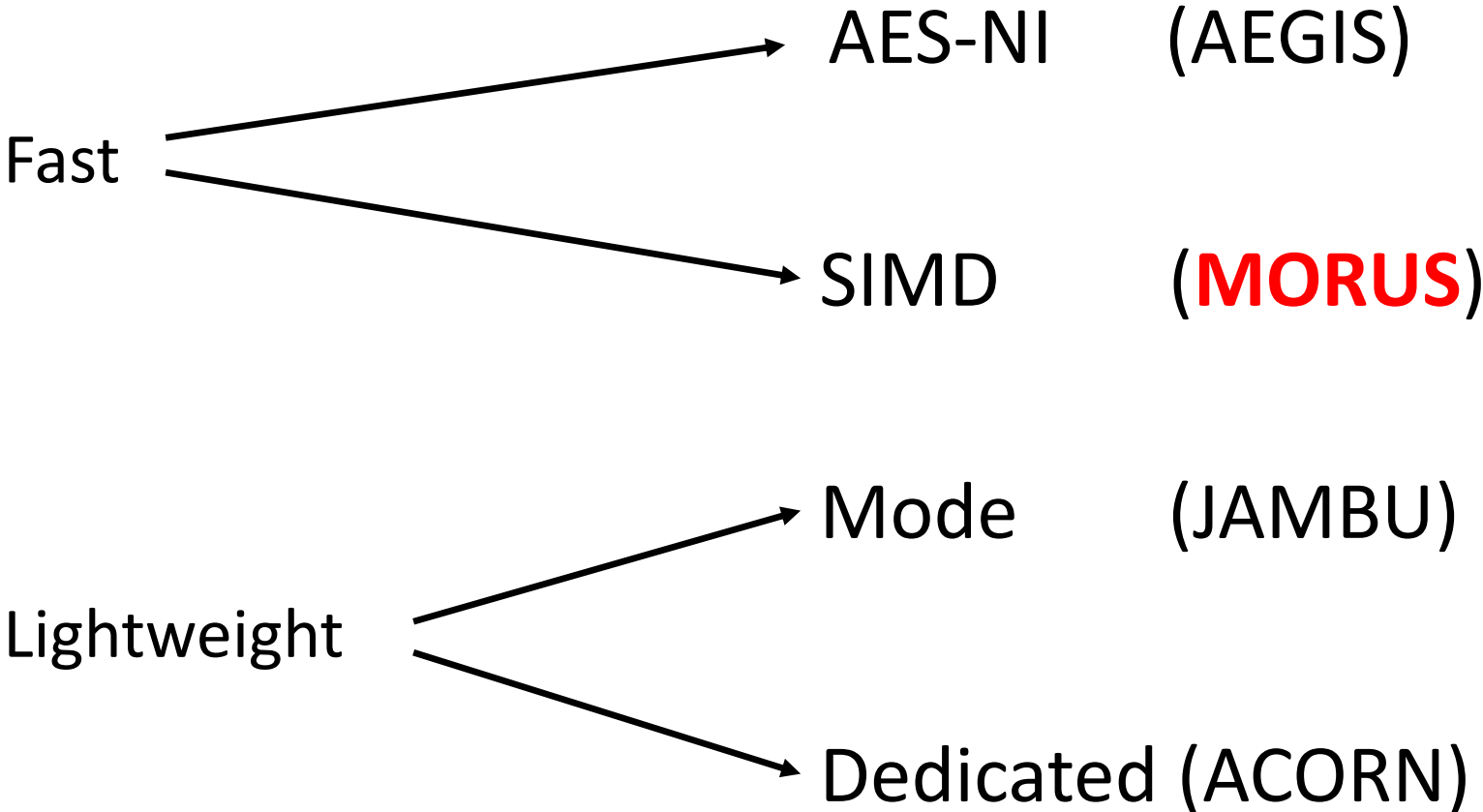
Tao Huang

Nanyang Technological University



MORUS

Different Design Approaches:



MORUS: Main features

- Fast
 - MORUS-1280 is **0.69 clock cycles/byte** on Haswell
 - **The only CAESAR candidate** which is not based on AES-NI, but faster than AES-GCM on Haswell
 - **Likely the fastest** CAESAR candidate on the processors with SIMD (SSE2, AVX2) instructions, but no AES-NI
- Nonce-based

Design software-efficient ciphers

Two general methods for designing software efficient ciphers

- Method 1:
 - reduce the number of computations in the design
- Method 2:
 - use operations that can be computed fast on CPUs

Design software-efficient ciphers

- **Method 1:**
 - reduce the number of computations in the design
- How to design a cipher using Method 1?
 - Method 1a: Proper security margin (should not be too large)
(the designers should/can analyze the security of the ciphers)
 - Method 1b: Typically stream cipher requires much less operations than block cipher (anyway, block cipher more robust than stream cipher)
 - Method 1c: Efficient design
Example: how to achieve high security with less operations

Design software-efficient ciphers

- **Method 2:**
 - use operations that can be computed fast on CPUs
- Some efficient operations on CPUs:
 - SIMD (single instruction multiple data)
 - SSE2: 128-bit registers (**available on many CPUs**)
 - AVX2: 256-bit registers (available on the latest Intel Haswell CPUs)
 - AES-NI (AES new instruction set)
 - The design of AEGIS

Design software-efficient ciphers

- Design efficient ciphers using SIMD instructions
 - Salsa (stream cipher using 128-bit SSE2 instructions, 2005)
 - Blake, JH (hash functions using 128-bit SSE2 instructions, 2008)
 - MORUS, NORX (authenticated ciphers using 256-bit AVX2 instructions, 2014)

MORUS: Design

- MORUS is a fast software cipher
 - Encryption: stream cipher
 - Authentication: almost for free
 - Use SIMD instructions

MORUS: Design

- MORUS-1280-128: 1280-bit state, 128-bit key
- MORUS-1280-256: 1280-bit state, 256-bit key
- MORUS-640-128: 640-bit state, 128-bit key

- Tag: 128-bit

- MORUS-640 benefits from 128-bit SIMD instructions
- MORUS-1280 benefits from 128/256-bit SIMD instructions

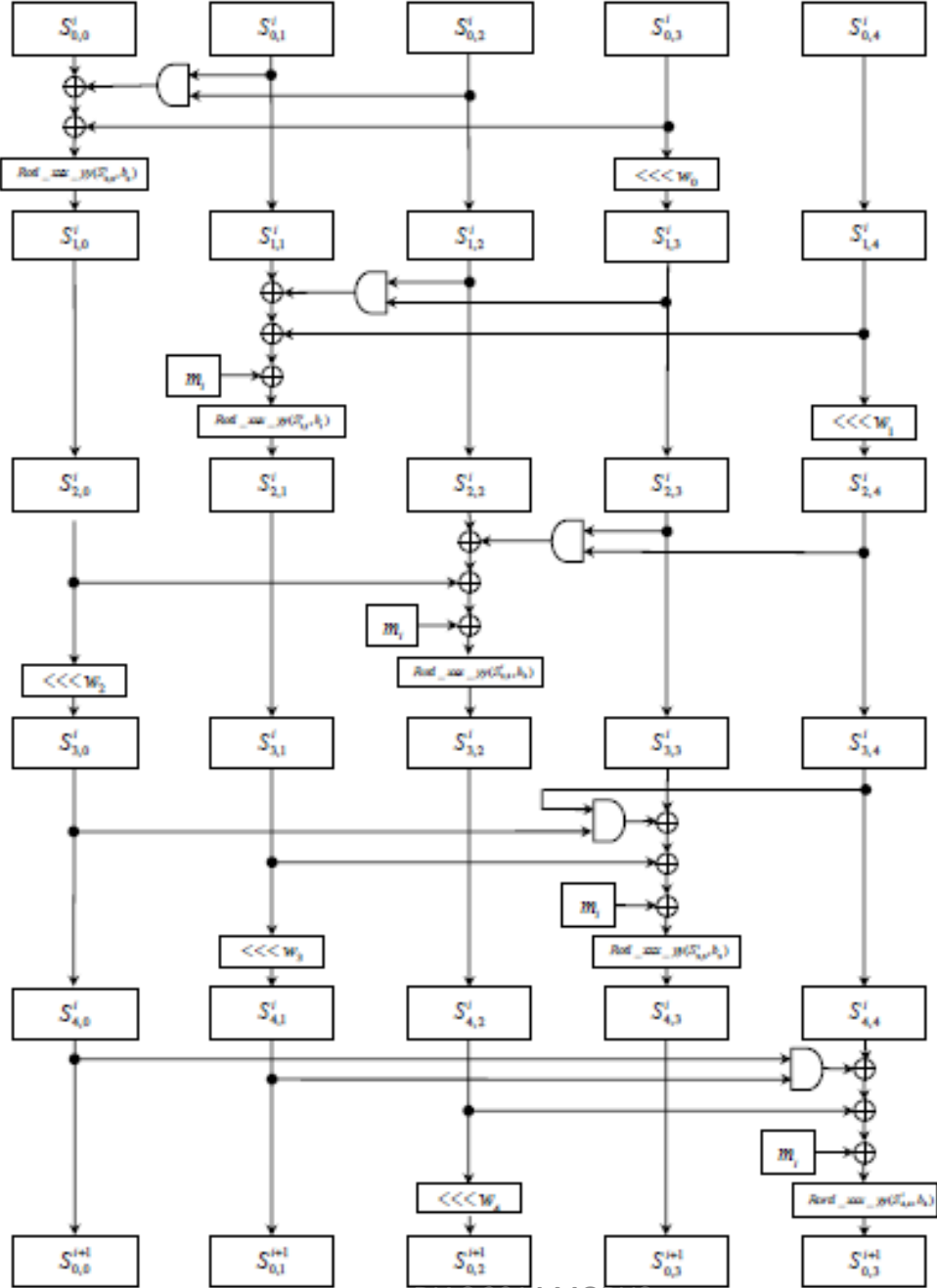
MORUS: Design

- MORUS-1280 (128-bit/256-bit key):
 - The cipher state consists of five 256-bit words
 - XOR, AND, SHIFT operations are used
- In each step,
 - 5 rounds are used to update the state, and
 - 256-bit keystream word is generated

MORUS: Design

- MORUS-640 (128-bit key):
The cipher state consists of five 128-bit words
- Each step consists of 5 rounds, and
128-bit keystream word is generated

The state update of MORUS in one step: 5 rounds



MORUS: Design

- Initialization
 - 16 steps
 - key XORed to the state at the end of the initialization
- Finalization
 - 8 steps
 - Part of secret state and length (ad, message) are used to update the state in finalization
 - Generate 128-bit tag from the state

MORUS: Security

- We analyzed differentials involving the low weight input differences
 - The probability of state collision is much less than 2^{-128} (it is tremendously difficult to eliminate the difference in the state)
- The high weight input differences likely lead to even lower probability of state collision

MORUS: Performance

Speed on Haswell

	16B	64B	512B	1024B	4096B	16384B
MORUS-640(EA)	28	7.72	1.95	1.58	1.18	1.11
MORUS-640(DV)	28	7.99	1.97	1.56	1.23	1.16
MORUS-1280(EA)	33.9	8.28	1.59	1.12	0.78	0.69
MORUS-1280(DV)	35.8	8.46	1.63	1.13	0.80	0.69

MORUS-640 is slower since it uses only 128-bit SIMD

AES-128-GCM: 1.03

MORUS: Performance

- MORUS is likely the fastest on the platforms with SIMD but no AES-NI
 - Reason 1: MORUS benefits from SIMD
 - Reason 2: We carefully removed the redundant operations in the cipher

The screenshot displays a performance comparison tool with a grid of results. The columns represent different platforms: amd, wintermute, h7green, ashr, hydra3, h7ority, hydra3, h7ry, h7ragon, foga, h7bagle, hydra3, h4400, h4400, h7bobcat, hydra3, and hydra4. The rows represent different cipher configurations, including MORUS variants like MORUS128v1, MORUS128v2, MORUS128v3, MORUS128v4, MORUS128v5, MORUS128v6, MORUS128v7, MORUS128v8, MORUS128v9, MORUS128v10, MORUS128v11, MORUS128v12, MORUS128v13, MORUS128v14, MORUS128v15, MORUS128v16, MORUS128v17, MORUS128v18, MORUS128v19, MORUS128v20, MORUS128v21, MORUS128v22, MORUS128v23, MORUS128v24, MORUS128v25, MORUS128v26, MORUS128v27, MORUS128v28, MORUS128v29, MORUS128v30, MORUS128v31, MORUS128v32, MORUS128v33, MORUS128v34, MORUS128v35, MORUS128v36, MORUS128v37, MORUS128v38, MORUS128v39, MORUS128v40, MORUS128v41, MORUS128v42, MORUS128v43, MORUS128v44, MORUS128v45, MORUS128v46, MORUS128v47, MORUS128v48, MORUS128v49, MORUS128v50, MORUS128v51, MORUS128v52, MORUS128v53, MORUS128v54, MORUS128v55, MORUS128v56, MORUS128v57, MORUS128v58, MORUS128v59, MORUS128v60, MORUS128v61, MORUS128v62, MORUS128v63, MORUS128v64, MORUS128v65, MORUS128v66, MORUS128v67, MORUS128v68, MORUS128v69, MORUS128v70, MORUS128v71, MORUS128v72, MORUS128v73, MORUS128v74, MORUS128v75, MORUS128v76, MORUS128v77, MORUS128v78, MORUS128v79, MORUS128v80, MORUS128v81, MORUS128v82, MORUS128v83, MORUS128v84, MORUS128v85, MORUS128v86, MORUS128v87, MORUS128v88, MORUS128v89, MORUS128v90, MORUS128v91, MORUS128v92, MORUS128v93, MORUS128v94, MORUS128v95, MORUS128v96, MORUS128v97, MORUS128v98, MORUS128v99, MORUS128v100.

MORUS: Performance

- MORUS is expected to be very fast on hardware
 - Critical path is very short in each step (8XOR, 3AND)
 - 128-bit (256-bit) keystream is generated for MORUS-640 (MORUS-1280)

Conclusion

- MORUS benefits from SIMD
- Likely the fastest candidate on platforms with SIMD but no AES-NI