MORUS

A Fast Authenticated Cipher

Hongjun Wu **Tao Huang**

Nanyang Technological University

DIAC 2015, Singapore
29 Sep 2015

No tweak of MORUS

for the second round

Outline

- Design Motivation and Main Features
- The MORUS Design
- Security
- Hardware and Software Performance
- Conclusion

Design Motivation and Main Features

- To design a high-speed authenticated cipher:
  - No AES-NI
  - Make use of the SIMD (SSE2, AVX2) instructions

- Features
  - Fast in software: 0.69 cpb on Haswell
  - Fast in hardware: 94.8 Gbps on high-end FPGA (non-opt)
    250 Gbps on ASIC (ETH implementation)
  - Nonce-based

Outline

- Design Motivation and Main Features
- The MORUS Design
- Security
- Hardware and Software Performance
- Conclusion

MORUS: Parameters

	State size (bits)	Key size (bits)	Tag size (bits)	Plaintext size (bits)	AD size (bits)
MORUS-1280-128	1280	128	128	$<2^{64}$	$<2^{64}$
MORUS-640-128	640	128	128	$<2^{64}$	$<2^{64}$
MORUS-1280-256	1280	256	128	$<2^{64}$	$<2^{64}$

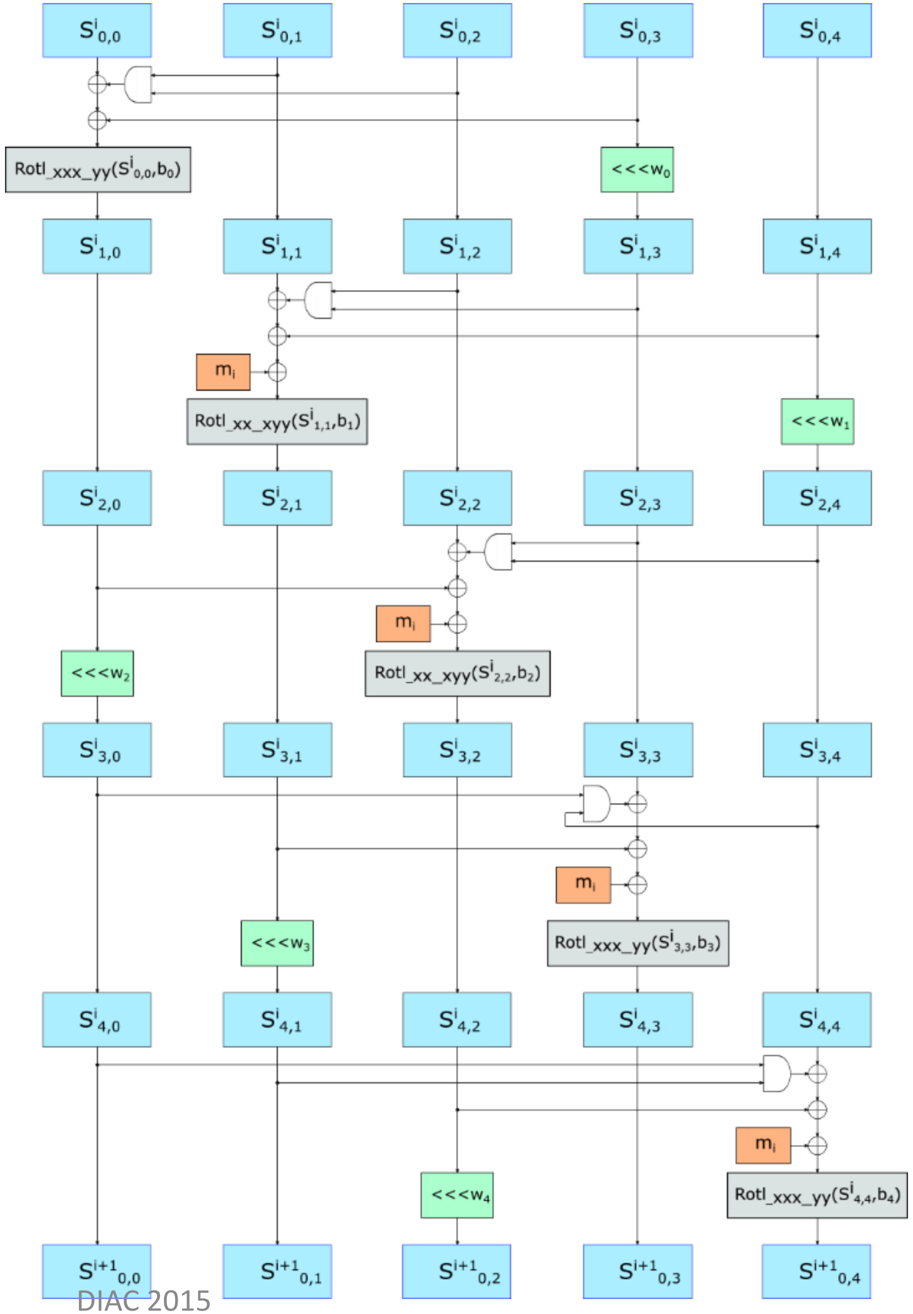
MORUS: State and Operations

- State organization
  - MORUS-1280: five 256-bit words
  - MORUS-640 : five 128-bit words

- Operations:
  - XOR, AND, SHIFT
  - Rotl_128_32(x,n): Divide a 128-bit block *x* into 4 32-bit words, rotate each word left by *n* bits.
  - Rotl_256_64(x,n): Divide a 256-bit block *x* into 4 64-bit words, rotate each word left by *n* bits.

MORUS: State Update (Overview)

One step: 5 rounds



MORUS: Initialization

- Load IV, key and constants into the initial state
- Update state: 16 steps
- Key is XORed to the state at the end of the initialization

MORUS: Keystream Generation

- State S = {S_0, S_1, S_2, S_3, S_4}
- For MORUS-640:
  - $keystream = S_0 \oplus (S_1 <<< 96) \oplus S_2 \,\&\, S_3$
- For MORUS-1280
  - $keystream = S_0 \oplus (S_1 <<< 192) \oplus S_2 \,\&\, S_3$

MORUS: Finalization

- Update state: 8 steps
- Part of secret state (S_3) and length ($adlen$, $msglen$) are used to form the message register in state update
- Generate 128-bit tag from the state

Outline

- Design Motivation and Main Features
- The MORUS Design
- Security
- Hardware and Software Performance
- Conclusion

MORUS: Security

	Confidentiality (bits)	Integrity (bits)
MORUS-640-128	128	128
MORUS-1280-128	128	128
MORUS-1280-256	256	128

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
- After one and half years, no published attacks against our security claims

Outline

- Design Motivation and Main Features
- The MORUS Design
- Security
- Hardware and Software Performance
- Conclusion

MORUS: Hardware Performance

- State update function of MORUS is designed to be fast in hardware
  - AND and XOR gates are used
  - Short critical path

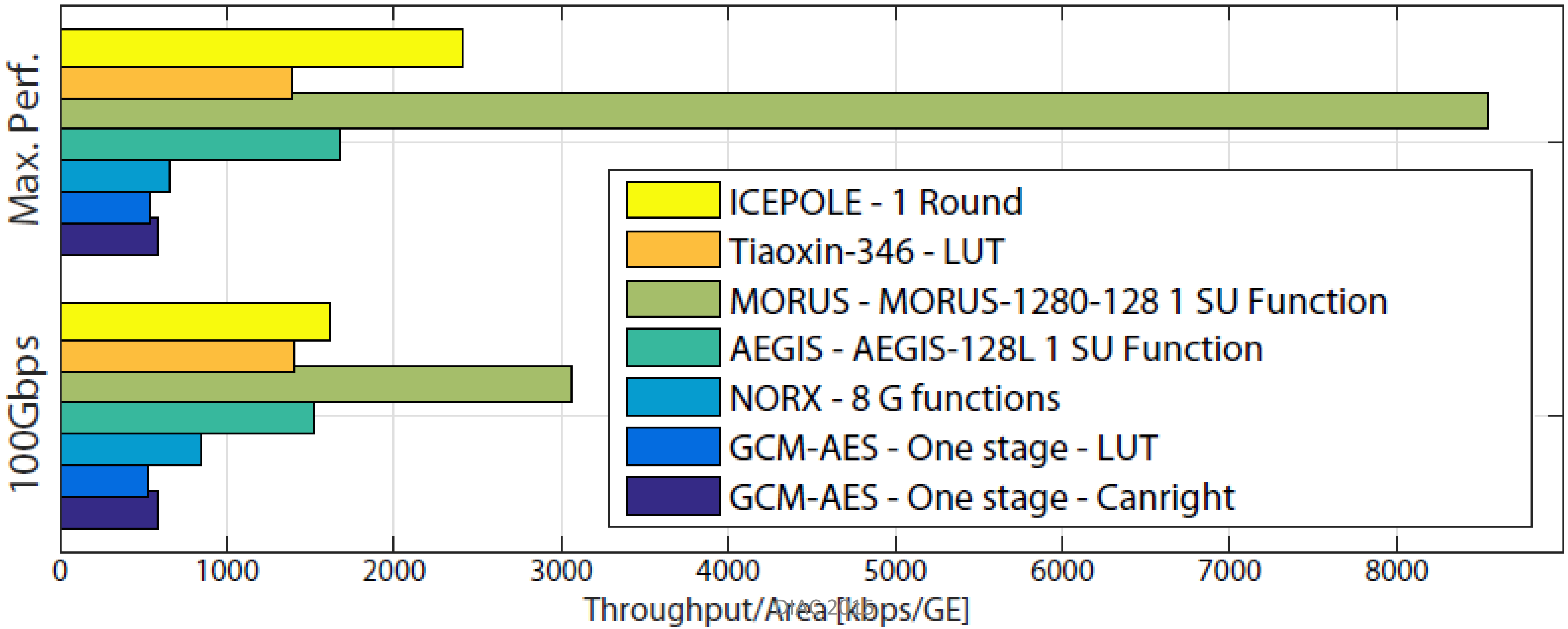
MORUS: Hardware Performance

- Non-optimized implementation on FPGA
  - Virtex 7, Xilinx Vivado

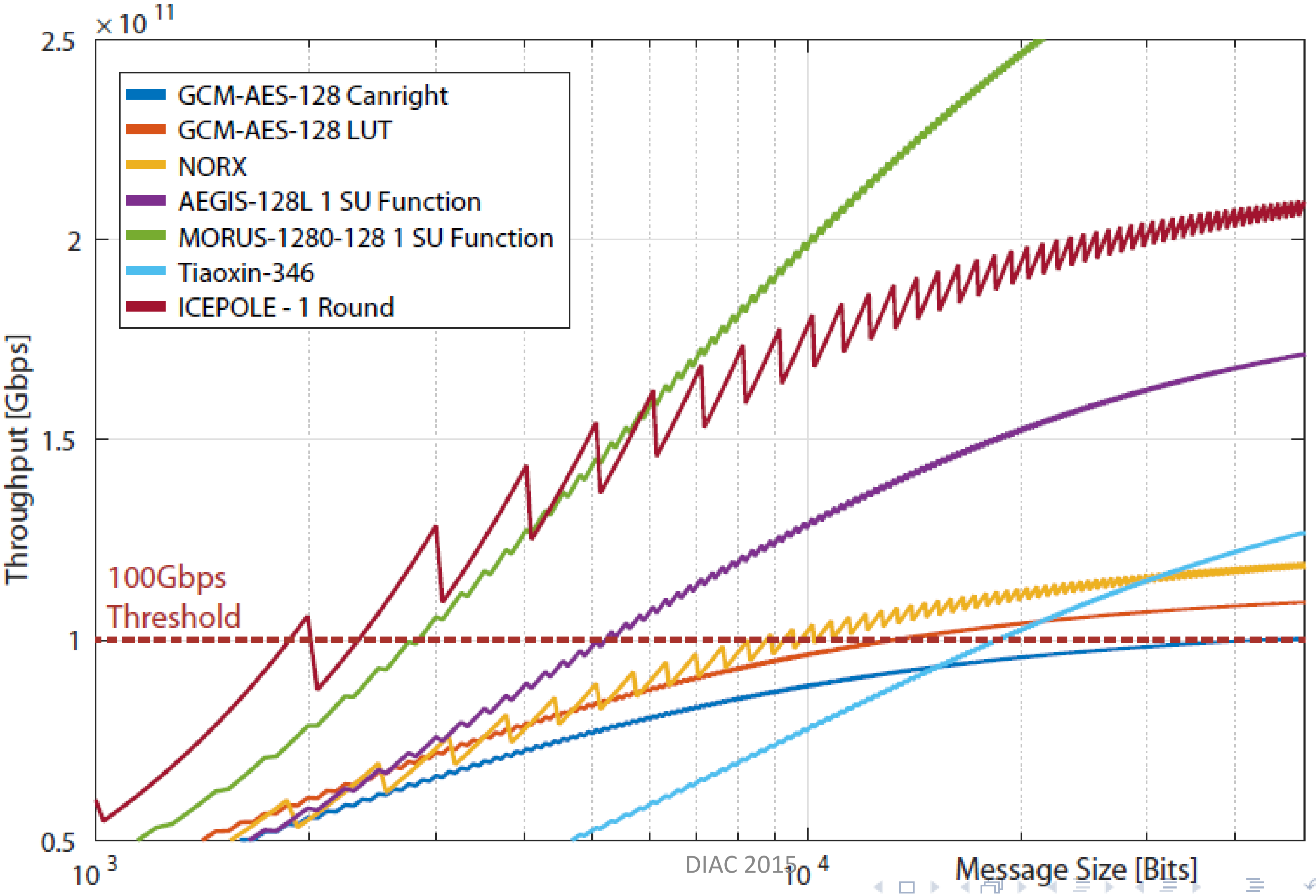
	Area (Slice)	Frequency (MHz)	Throughput (Gbps)
MORUS-640	485	425	54.4
MORUS-1280	879	370.4	**94.8**

MORUS: Hardware Performance

- Performance on ASIC: high throughtput/area
  (Michael Muehlberghuber and Frank K. Gürkaynak, DIAC 2015)



- Performance on ASIC: high throughput (250Gbps)
  (Michael Muehlberghuber and Frank K. Gürkaynak, DIAC 2015)



MORUS: Software Performance

- Speed on Haswell, AVX2 is used in MORUS-1280

	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: Software Performance

- Faster than AES-GCM on Haswell (1.03 cpb)
- Likely the fastest on the platforms with SIMD but no AES-NI
- Reasons:
  - Benefits from SIMD
  - Removed the redundant operations in the cipher

Outline

- Design Motivation and Main Features
- The MORUS Design
- Security
- Hardware and Software Performance
- Conclusion

Conclusion

- No tweak in the second-round submission
- Remain as the fastest candidate on the platforms with SIMD but no AES-NI
- MORUS is very fast in hardware