AEGIS

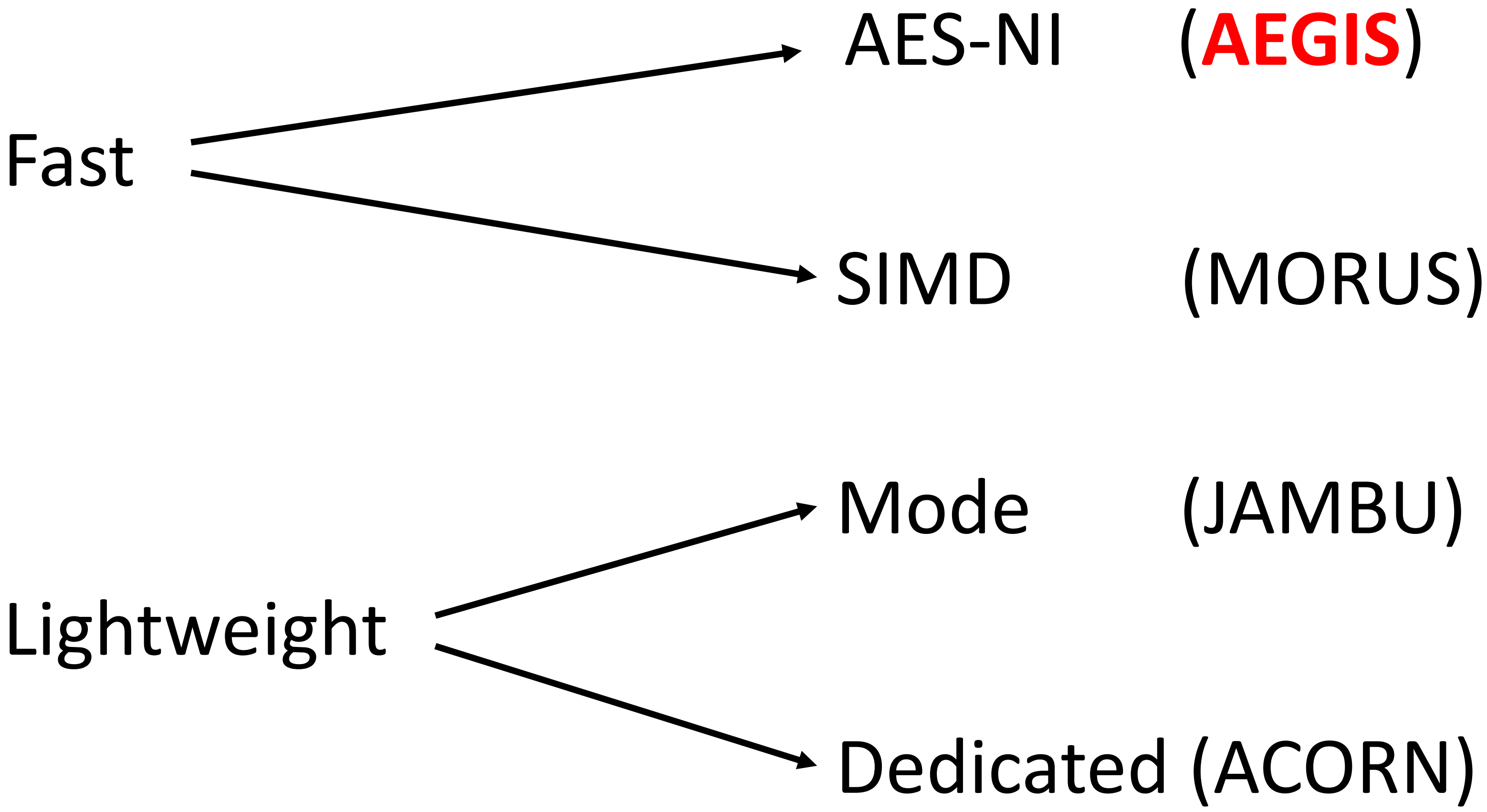
A Fast Authenticated Encryption Algorithm

Hongjun Wu   Bart Preneel

Nanyang Technological University
KU Leuven and iMinds

AEGIS: A shield carried by Athena and Zeus

Different Design Approaches:



Fast

AES-NI (**AEGIS**)

SIMD (MORUS)

Lightweight

Mode (JAMBU)

Dedicated (ACORN)

AEGIS: Main features

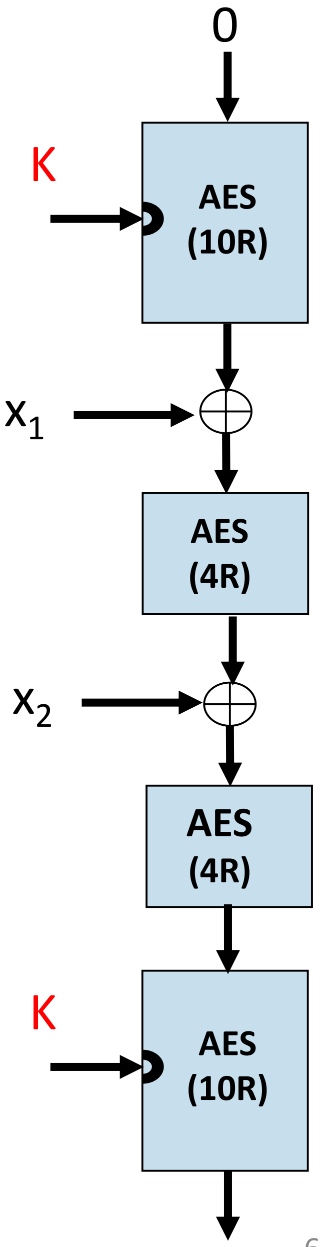
- Fast
  - AEGIS-128L is **0.30 clock cycles/byte** on Haswell (16KB messages)
    - Fully use the pipeline of AES-NI
    - **Likely the fastest** CAESAR candidate on Intel Haswell processors
- Nonce-based

AEGIS: Properties

- Properties
  - **Parallelizable: locally**
  - **No security reduction but easy to analyze**
  - Not resistant to nonce reuse
  - Performance: size/speed tradeoff

AEGIS

- Design Rationale
  - Inspiration **Pelican MAC**
    - [Daemen-Rijmen'05]
    - 128-bit secret state
    - easy to analyze
    - secure up to birthday bound
    - 2.5 times faster than AES
  - Our design: **Save the state after each AES round**, then construct stream cipher from MAC



AEGIS

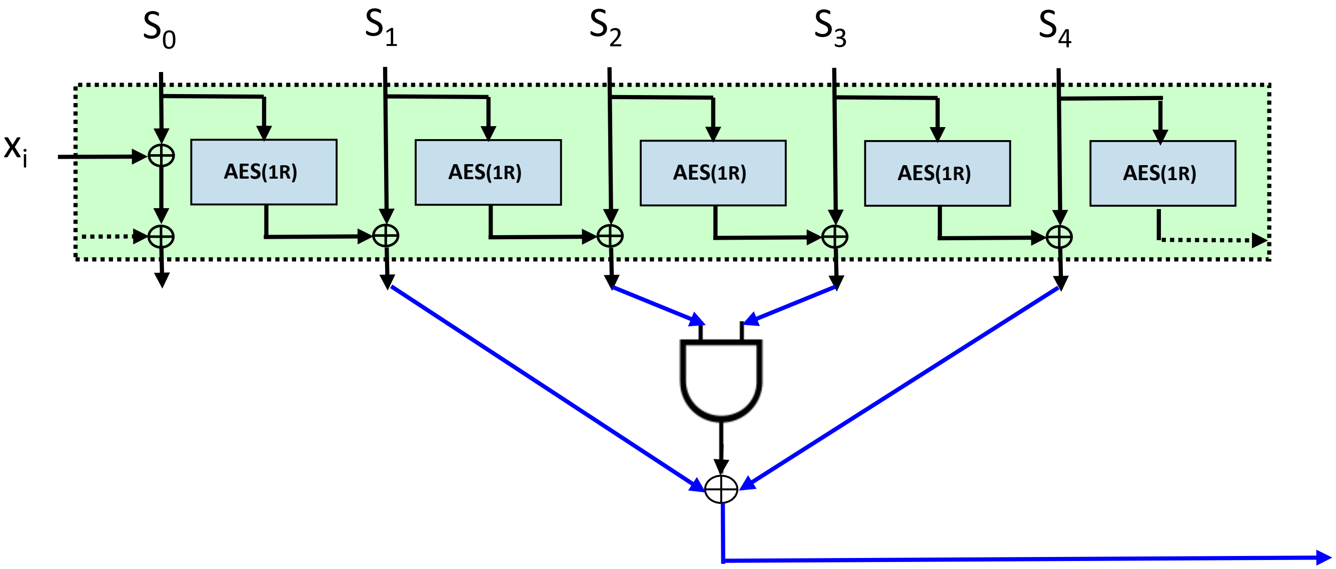
- Design Rationale (2)
  - **Parallel AES round functions in each step** so as to fill the AES instruction pipeline
  - AEGIS-128L can make full use of the 8-stage AES instruction pipeline of Haswell processor

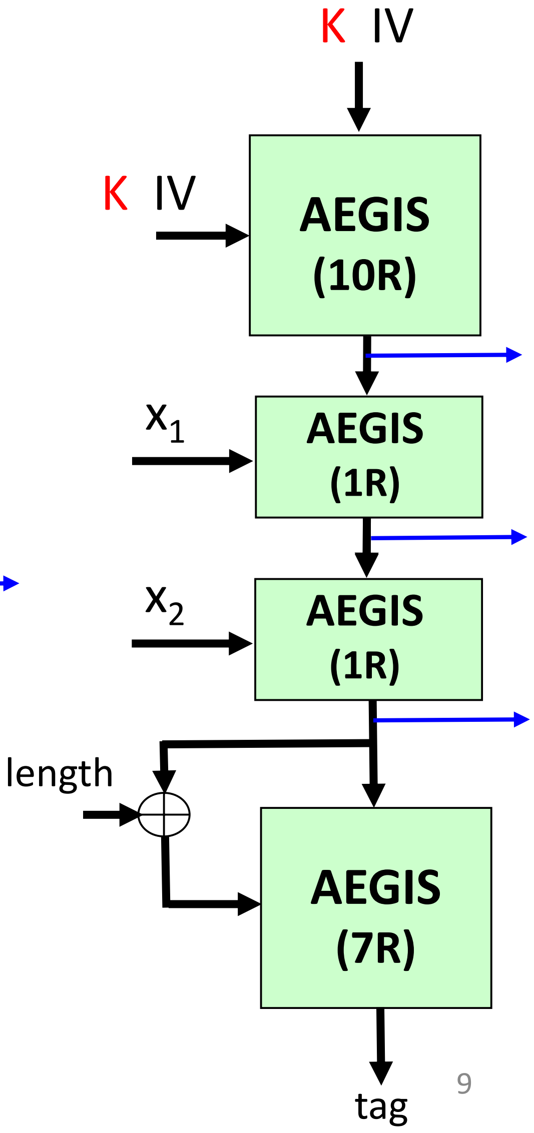
AEGIS

- AEGIS-128L
  - 128-bit key, 1024-bit state
- AEGIS-128
  - 128-bit key, 640-bit state
- AEGIS-256
  - 128-bit key, 756-bit state

- Tag: 128-bit

AEGIS-128





- larger state: 5 x 128 bits
- but simpler operation: 1 AES round
- still easy to analyze

AEGIS: Security Claims

- Requirements for secure implementation
  - each key and nonce pair can be used only once
  - if verification fails, the decrypted message and wrong message authentication tag should not be given as output

- Forgery attack: success prob. 2^{-t} with t the tag size
- Key and state cannot be recovered faster than brute force if forgery attack is not successful
  - 128-bit tags strongly recommended

AEGIS: Security Analysis

- Authentication
- Encryption
- Does authentication affect encryption?
  - short tag → easy forgery, and results in chosen ciphertext attack against encryption
- Does encryption weaken authentication?
  - ciphertext leaks state information, which may benefit a forgery attack
    - such as partial state value, state collision

AEGIS: Security

- Authentication
  - a difference in ciphertext passes through at least 4 AES rounds
    - stronger than Pelican MAC (4 AES rounds) since difference being distributed to at least 4 words
- Encryption
  - AEGIS encryption is a stream cipher with **nonlinear** state update function
    - differential and linear analysis is precluded

AEGIS: Security
Does authentication affect encryption?

- AEGIS without MAC is vulnerable to a chosen ciphertext attack
- To preclude chosen ciphertext attack
  1) if tag verification fails, the decrypted plaintext should not be given as output
  2) the tag size should be sufficiently large to resist a chosen-ciphertext attack
     (128-bit tag recommended)

AEGIS: Security
Does encryption weaken authentication?

- At each step, AEGIS leaks 128-bit keystream, i.e., 128-bit state information
- The overall differential probability of the forgery attack against AEGIS increases
- But the differential probability that a difference propagates through 5 AES rounds is not affected
  - reason: at each step, the information leaked on $S_{i,j}$ is of the form:

$$S_{i,1} \oplus (S_{i,2} \,\&\, S_{i,3}) \oplus S_{i,4}$$

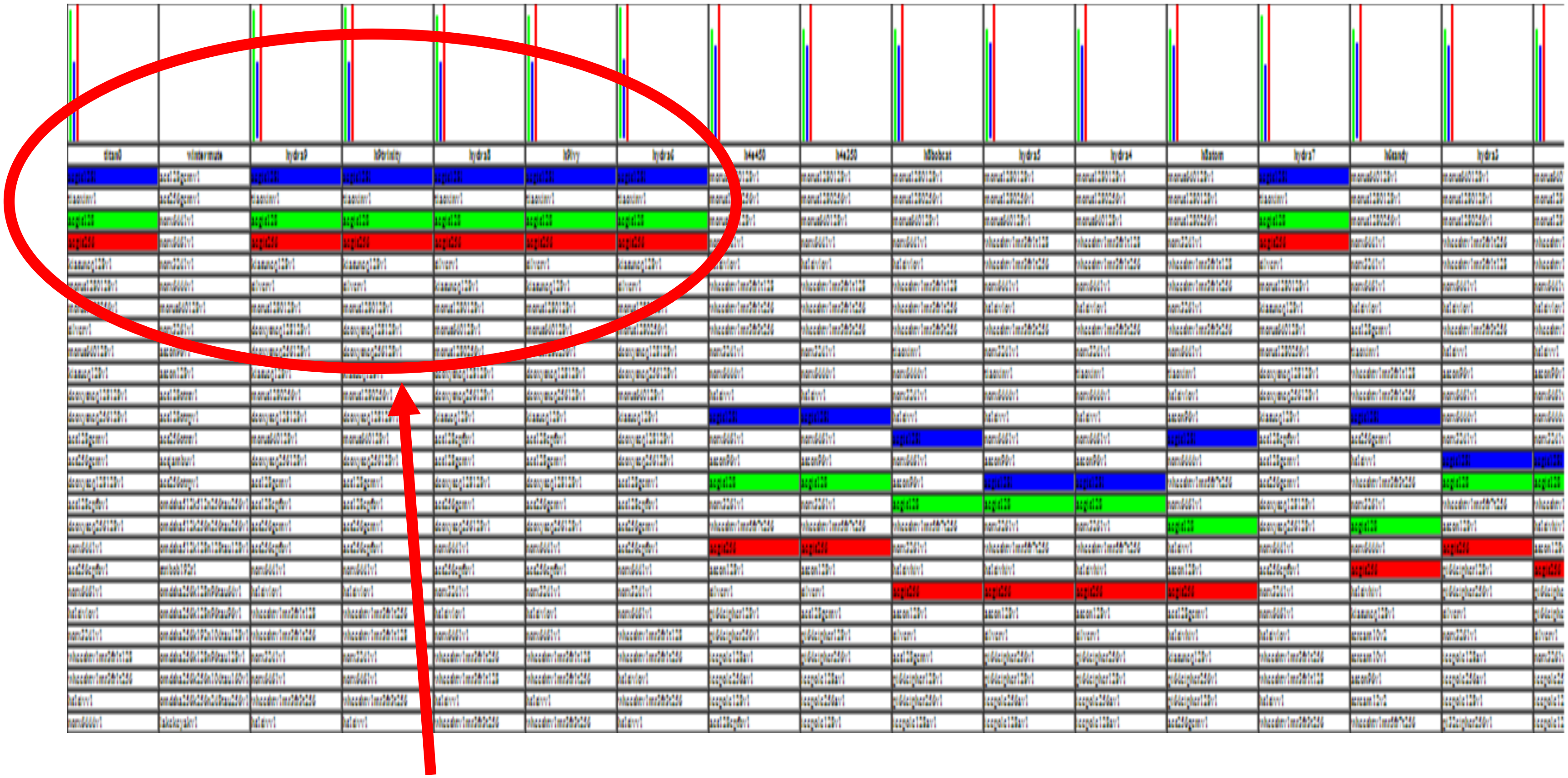
AEGIS: Security
Randomness of keystream

- Recent results (Minaud, SAC 2014)
  - AEGIS-128
    - 2^{130+} keystream bits for distinguishing
  - AEGIS-256
    - 2^{180+} keystream bits for distinguishing
  - AEGIS-128L
    - So far, no results (expected to be strong)

Performance

- Speed on haswell processor (AEGIS-128L)
  - 0.30 cycles/byte (16KB messages)
  - 0.37 cycles/byte (4KB messages)
  - 0.51 cycles/byte (1KB messages)
  - 1.11 cycles/byte (256B messages)
  - 3.44 cycles/byte (64B messages)

Performance



- Likely the fastest on Haswell
- Quite fast on platforms with no AES-NI

Conclusions

- Simple design
- Likely the fastest on Haswell processors
  - Targeting platforms with AES-NI
  - Also fast for short messages
- Strong in security