AEGIS

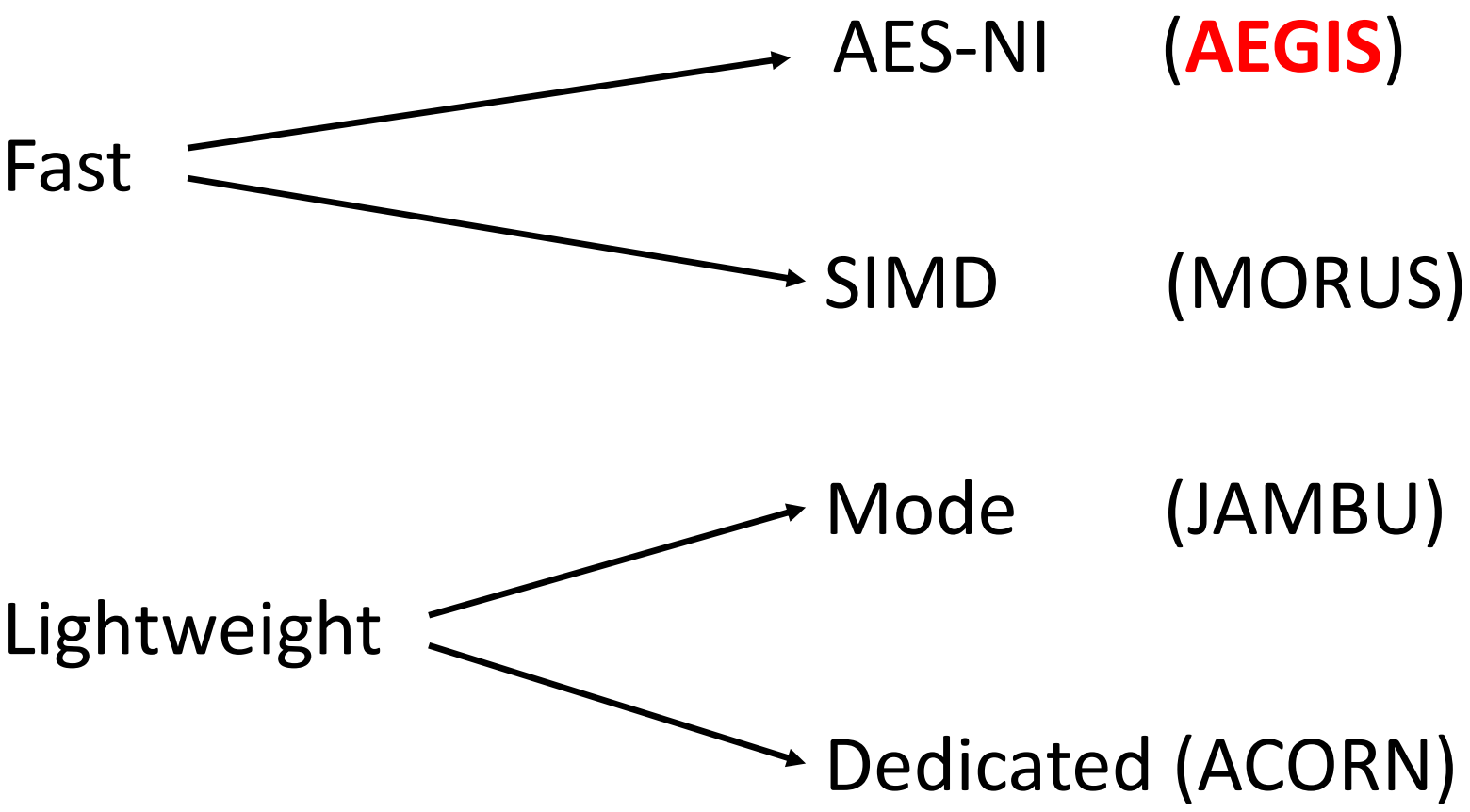
A Fast Authenticated Encryption Algorithm

Hongjun Wu **Bart Preneel**

Nanyang Technological University
KU Leuven and iMinds

AEGIS: A shield carried by Athena and Zeus

Different Design Approaches:



No tweak for the second and third rounds

AEGIS: Main features

- Simple
- Fast
  - AEGIS-128L is **0.25 clock cycles/byte** on Intel Skylake (long messages)
    - Fully use the pipeline of AES-NI
- Nonce is used only once

AEGIS

- AEGIS-128L
  - 128-bit key, 1024-bit state
- AEGIS-128
  - 128-bit key, 640-bit state
- AEGIS-256
  - 256-bit key, 768-bit state

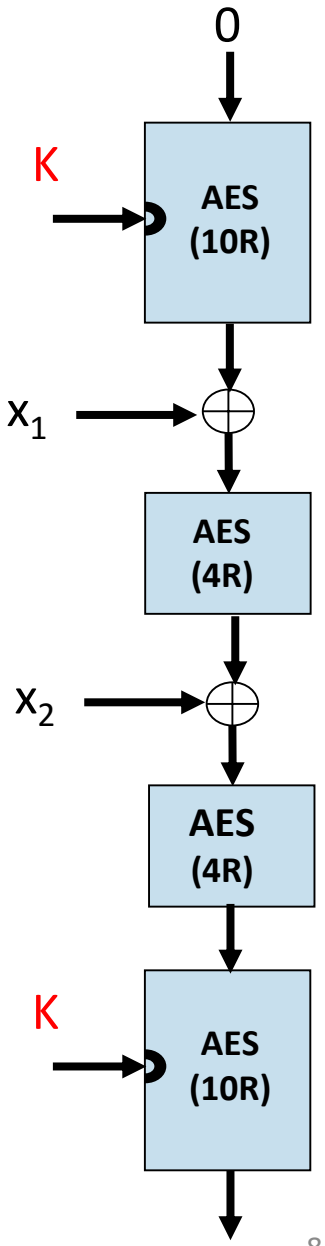
- Tag: 128-bit

AEGIS: Properties

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

AEGIS

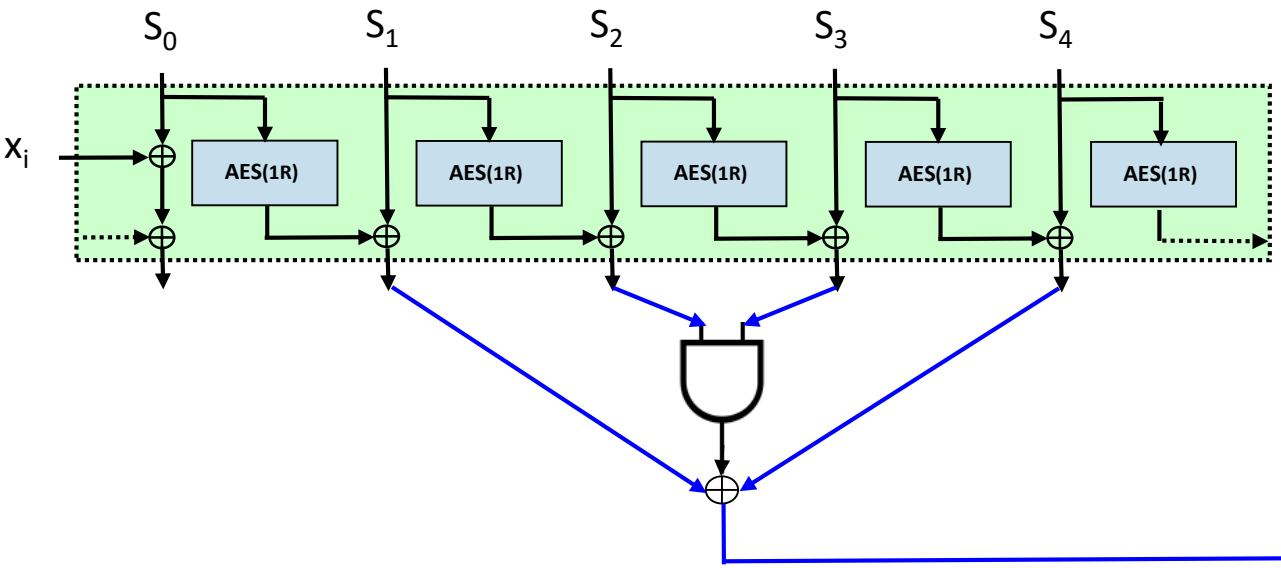
- Design Rationale
  - Inspiration: **Pelican MAC**
    - [Daemen-Rijmen'05]
    - 128-bit secret state
    - easy to analyze
    - secure up to birthday bound
    - 2.5 times faster than AES
  - Our design: **Save the state after each AES round**, then construct stream cipher from MAC

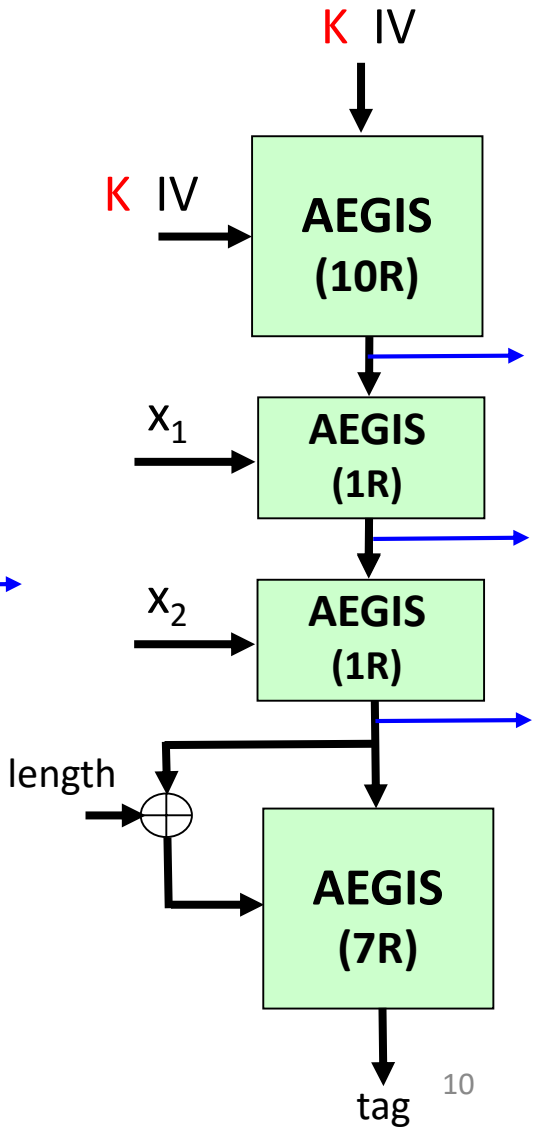


AEGIS

- 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 AES instruction pipeline of Intel Haswell and Skylake processors

AEGIS-128





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

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
Randomness of keystream

- Recent results (Minaud, SAC 2014)
  - AEGIS-128
    - 2^{130+} keystream bits for distinguishing
  - AEGIS-256
    - 2^{180+} keystream bits for distinguishing

Performance

- Speed on Intel Skylake processor Core i5-6600 (Supercop-2016-08-06) No associated data.

	Very Long	1536B	64B
AEGIS-128L(EA)	0.25	0.34	2.50
AEGIS-128L(DV)	0.25	0.37	3.16
AEGIS-128(EA)	0.43	0.51	2.22
AEGIS-128(DV)	0.41	0.49	2.41
AEGIS-256(EA)	0.47	0.59	3.19
AEGIS-256(DV)	0.46	0.57	3.31

Performance

- Compare to the performance of Tiaoxin
  - Tiaoxin extends AEGIS to larger state with more complicated state update function
    - state size of Tiaoxin: 1664 bits (60% more)
    - state size of AEGIS-128L: 1024 bits
  - Larger state size in stream cipher design normally leads to faster speed
  - Long message (on Skylake, Supercop-2016-08-06)
    - Tiaoxin: encryption 0.21 cpb; decryption 0.34 cpb
    - AEGIS-128L: encryption 0.25 cpb; decryption 0.25 cpb
  - 1536-byte message (on Skylake, Supercop-2016-08-06)
    - Tiaoxin: encryption 0.36 cpb; decryption 0.48 cpb
    - AEGIS-128L: encryption 0.34 cpb; decryption 0.37 cpb

Performance

- Hardware
  - FPGA implementation of AEGIS-128L (Tao Huang)
    - **For throughput optimized: 78.3 Gbps, 2424 slices**
  - 65 nm ASIC implementation of AEGIS-128
    (Debjyoti Bhattacharjee, Anupam Chattopadhyay, DIAC 2015)
    - **For throughput optimized: 121 Gbps, 173 KGE**
    - For Low area optimized: 1.32 Gbps, 18.72 KGE
    - We expect that **AEGIS-128L is about twice as fast as AEGIS-128 on ASIC, with larger area (60% more)**

Discussions

- We restrict the disclosure of plaintext when authentication failed. **What would happen if the attacker knows the decrypted plaintext when authentication fails**?
  - For AEGIS, the secret key remains strong, so there is **little compromise of encryption security** (since the attacker can access the decrypted plaintext, the encryption security of a single message is not a concern here)

Discussions

- We restrict the disclosure of plaintext when authentication failed. **What would happen if the attacker knows the decrypted plaintext when authentication fails**?
  - If the communication protocol terminates/restarts when authentication fails, then there is no compromise of authentication security

Conclusions

- Simple design
- Fast
  - Software: targeting platforms with AES-NI
  - Also fast in hardware
- Strong in security