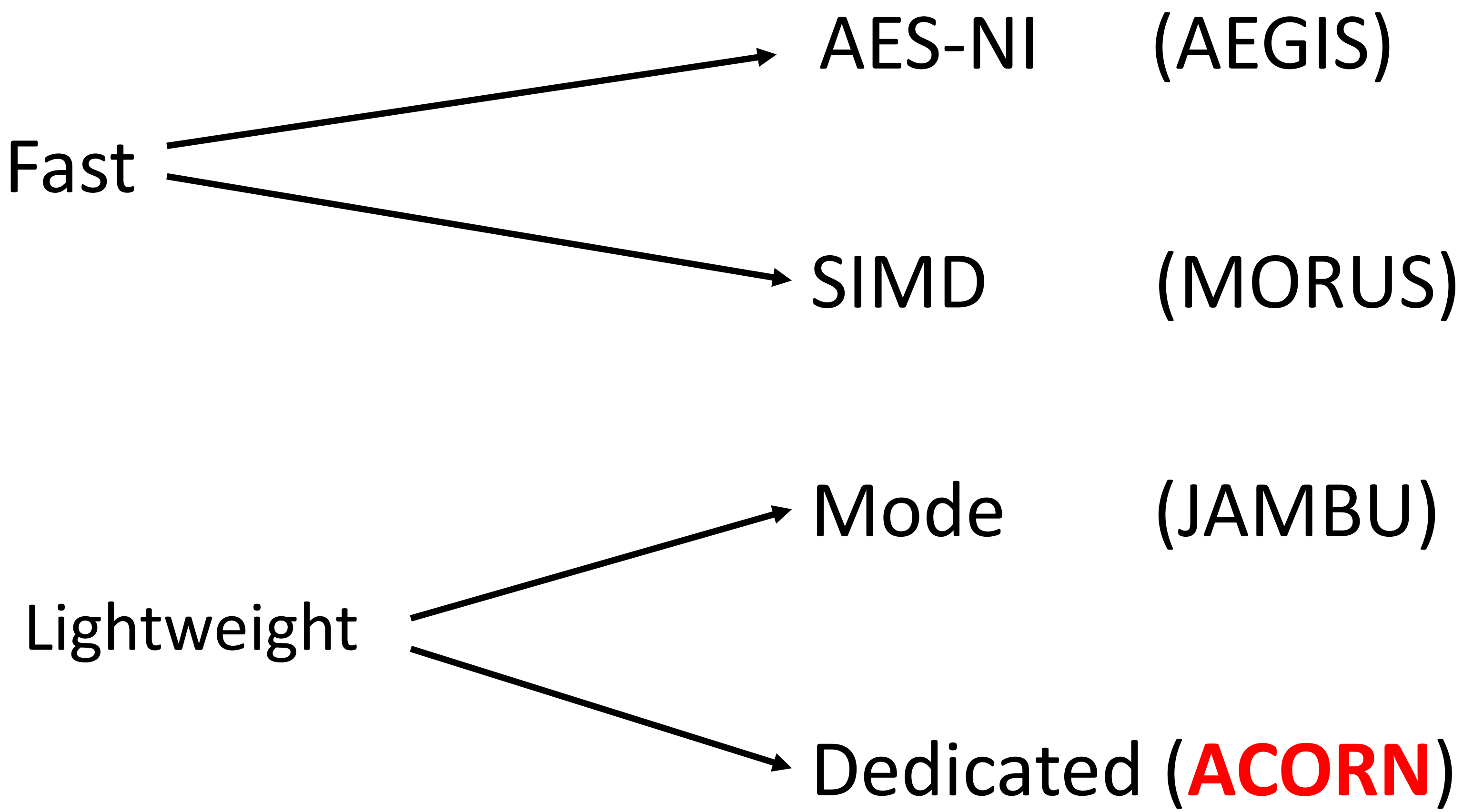
ACORN
A Lightweight Authenticated Cipher

Hongjun Wu

Nanyang Technological University

ACORN

Different Design Approaches:



Fast

AES-NI (AEGIS)

SIMD (MORUS)

Lightweight

Mode (JAMBU)

Dedicated (**ACORN**)

How to design a lightweight authenticated cipher?

Design lightweight authenticated ciphers

- Methods
  - Method 1. Reduce the state size (general)
    - 2n-bit state for n-bit key (stream cipher)
    - 2n-bit state for full n-bit authentication security
  - Method 2. Encryption and authentication share operations and state
  - Method 3. Use **bit-based** feedback shift register
    - Process message bit-by-bit
    - Simple circuit of bit-based feedback shift register

Design lightweight authenticated ciphers

- Challenge in the design

When 1) encryption and authentication share operations and state, and
2) bit-based feedback shift register is used,

How to analyze the differential propagation in a bit-based feedback shift register? (how to convince myself that the authentication part is strong?)

Design lightweight authenticated ciphers

- Challenge in the design

How to analyze the differential propagation in a bit-based feedback shift register?

Our solutions: 1) use **the concatenation of several LFSRs** in the state --> easy to analyze (linear), and each difference being injected into the state causes many differences in the state before being eliminated

(The idea here is somehow related to those convolutional codes whose free distance can be easily analyzed)

2) use an **overall nonlinear feedback structure** to provide strong encryption and authentication security

ACORN: design

- ACORN
  - Based on stream cipher
  - Encryption and authentication share the same state
- ACORN-128
  - Small state
    - 293-bit (the minimum is 256-bit)
  - Sequential design
    - At each step only one message bit is processed
  - 128-bit key, 128-bit IV, 128-bit tag

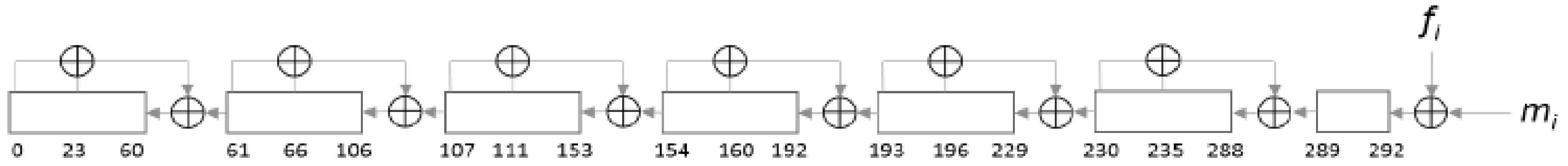
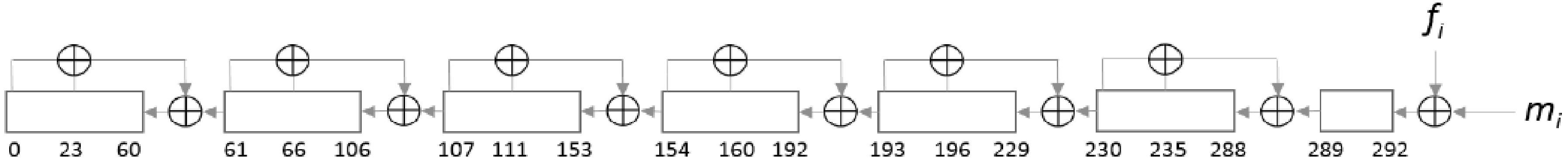


Figure 1.1: The concatenation of 6 LFSRs in ACORN-128. f_i indicates the overall feedback bit for the ith step; m_i indicates the message bit for the ith step.

- Initialization
  - Key and IV are injected into the state bit by bit
  - Consists of 1536 steps
- Process associated data
  - Each step one bit
  - Padding is fixed as 512 bits: 1 0^{511} (without padding to fixed length block)
- Process plaintext
  - Each step one bit
  - Padding is fixed as 512 bits: 1 0^{511}
- Finalization
  - Run the cipher for 512 steps
  - The last 128 keystream bits are the tag
- **Two control bits are applied to the cipher to separate associated data, plaintext and the finalization**

ACORN: Security

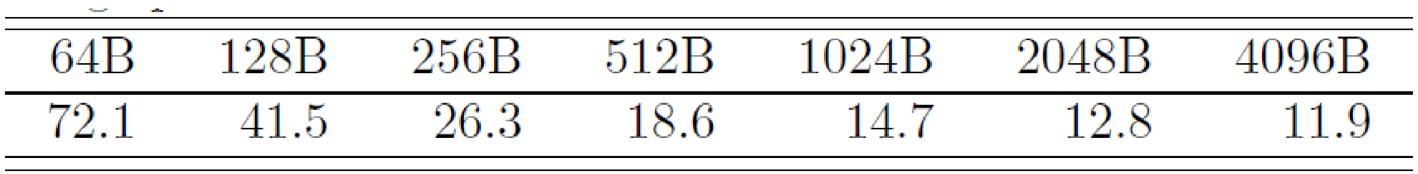
- Encryption: analysis is the same as stream cipher analysis
- Authentication: with the use of the concatenated LFSRs, the security analysis of authentication can be done much easier
  - To eliminate the difference being injected into the state, the success rate is 2^{-189}



ACORN: Performance

- Hardware
  - Expected to be slightly more costly than Trivium (hardware area)
    - To implement it in hardware for verification …
  - Fast implementation is possible due to 32 parallel steps

- Software speed on Sandy Bridge



64B	128B	256B	512B	1024B	2048B	4096B
72.1	41.5	26.3	18.6	14.7	12.8	11.9

Conclusions

- ACORN
  - A new design very different from the other candidates
  - Lightweight
    - Is ACORN the most compact design among those candidates which offer 128-bit full encryption and authentication security? (implementation is needed)
  - Reasonably fast due to 32 parallel steps
  - ACORN-128 provides 128-bit encryption and authentication security
- ACORN provides a new approach to design lightweight MAC (using bit-based registers)