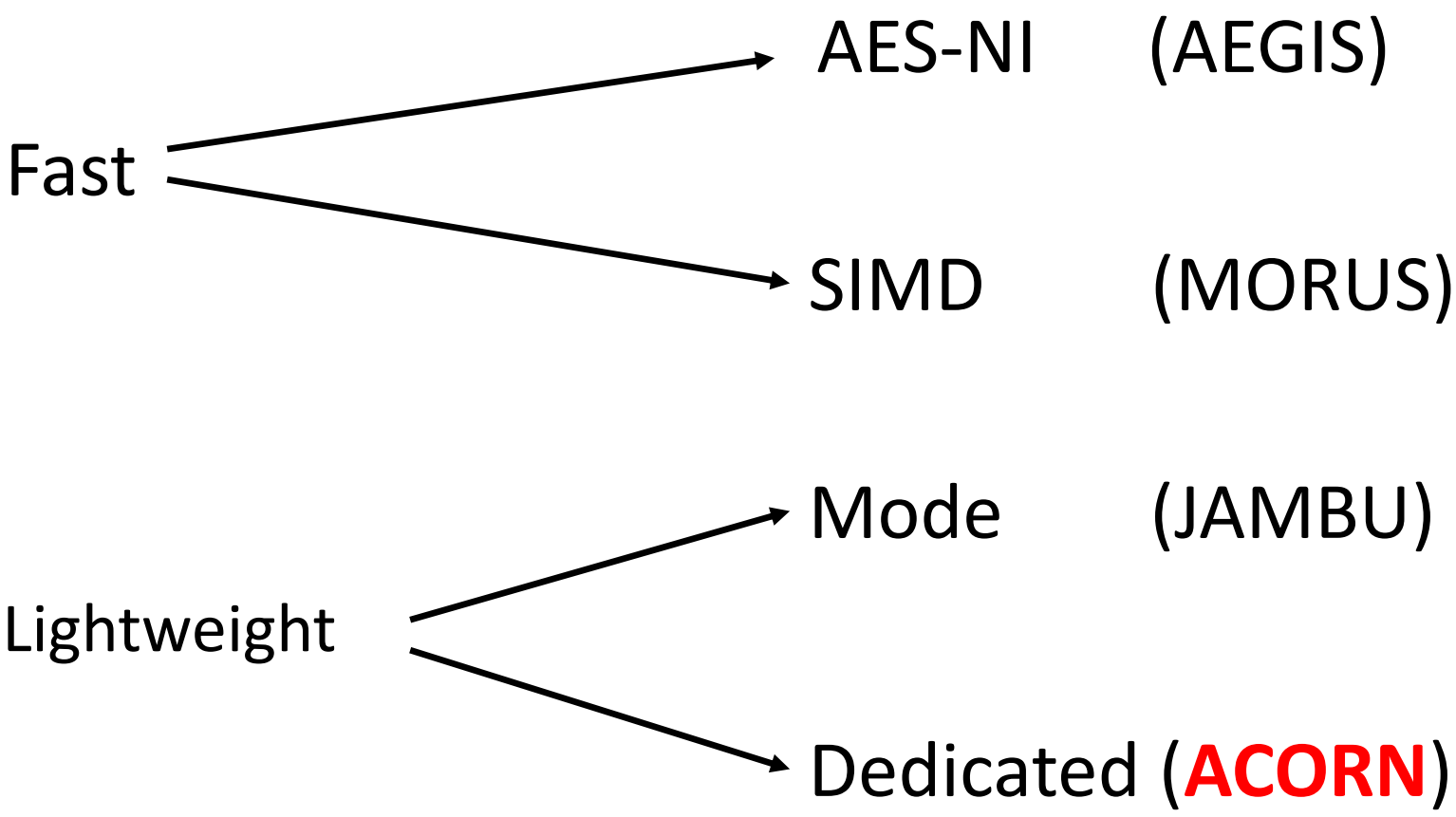
ACORN v3

A Lightweight Authenticated Cipher

Hongjun Wu

Nanyang Technological University

Different Design Approaches:



ACORN

ACORN: design

- ACORN-128
  - Based on **bit-oriented stream cipher**
  - **Encryption and authentication share the same state**
  - Small state
    - 293-bit (37 bits more than the minimum 256-bit)
  - IV should not be reused
  - 128-bit key, 128-bit IV, 128-bit tag

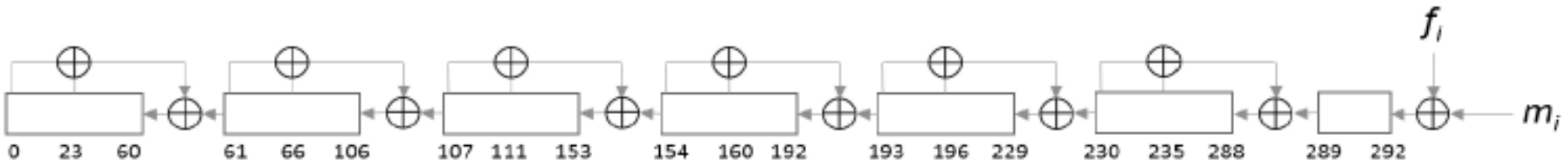


Figure 1.1: The concatenation of 6 LFSRs in ACORN-128. f_i indicates the overall feedback bit for the ith step; m_i indicates the message bit for the ith step.

ACORN: design

- Tweak for Round 3
  - Function *ch* is moved from the nonlinear feedback function to the output filtering function

$$ks_i = S_{i,12} \oplus S_{i,154} \oplus maj(S_{i,235}, S_{i,61}, S_{i,193}) \oplus ch(S_{i,230}, S_{i,111}, S_{i,66});$$
$$f_i = S_{i,0} \oplus (\sim S_{i,107}) \oplus maj(S_{i,244}, S_{i,23}, S_{i,160}) \oplus (ca_i \& S_{i,196}) \oplus (cb_i \& ks_i) \ ;$$

- Rationale for the tweak:
  - Better balance between the feedback function and the output filtering function
    - The feedback function consists of 6 LFSRs and the overall nonlinear feedback.
  - Larger security margin against guess-and-determine attack

- Initialization
  - Key and IV are injected into the state bit by bit
  - Consists of 1792 steps
- Process associated data
  - Each step one bit
  - Padding is fixed as 256 bits: $1\ 0^{255}$ (without padding to fixed length block, so suitable for bit-oriented hardware implementation)
- Process plaintext
  - Each step one bit
  - Padding is fixed as 256 bits: $1\ 0^{255}$
- Finalization
  - Run the cipher for 768 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

- Security of initialization (1792 steps)
  - Strong against differential analysis
    - probability is less than 2^{-200} for 400 steps

ACORN: Security

- Security of initialization (1792 steps)
  - Strong against cube analysis (as the cube size *n* increases from 17 to 32, the number of steps increases from 931 to 974, less than 3 steps per one cube increment)

Table 3.1: The minimum number of steps for every state bit being affected by $iv_{128-n} \cdot iv_{128-n+1} \cdots iv_{127}$

n	steps	n	steps	n	steps	n	steps
1	669	9	891	17	931	25	955
2	736	10	894	18	933	26	957
3	781	11	894	19	933	27	961
4	796	12	896	20	938	28	964
5	806	13	906	21	942	29	965
6	843	14	912	22	949	30	966
7	852	15	923	23	950	31	972
8	869	16	931	24	954	32	974

ACORN: Security

- Security of encryption
  - Strong against statistical analysis
    - nonce used only once
    - nonlinear state update function
  - Strong against guess-and-determine attack
    - Complexity larger than 2^{200} (of the attack that attempts to recover the state from linear equations)

ACORN: Security

- Authentication
  - with the use of 6 concatenated LFSRs, it is expensive to eliminate a difference in the state.
  - To eliminate the difference being injected into the state through ciphertext or associated data, the success rate is 2^{-181}

ACORN: Performance

- Hardware performance on FPGA Virtex 7 (Tao Huang)
  - 499 LUTs, 3.4 Gbps (implementing 8 steps)
    - **Currently much smaller than other CAESAR candidates**
    - About the same speed of AES-GCM, but 7 times smaller than AES-GCM.
  - 979 LUTs, 11.3 Gbps (implementing 32 steps)

ACORN: Performance

- Software speed on Intel Skylake (Intel Core i7-6550U, ultrabook cpu)
  - Faster than AES-GCM on the microprocessors with no AES instructions

	64B	128B	256B	512B	1024B	2048B	4096B
encryption	38.2	23.2	15.4	11.8	11.2	8.8	8.2
decryption	37.8	22.1	14.3	10.5	8.4	7.5	7.1

ACORN: Features

- Lightweight
  - Based on bit-oriented stream cipher (small data path)
  - Message length is not needed for authentication and verification
    - Do not need to implement circuits to count the message length
    - Do not need to pad the message to full blocks
- 32 steps can be computed in parallel in software and hardware
- High security
  - 128-bit encryption security
  - 128-bit authentication security

Conclusions

- ACORN
  - Lightweight
  - Reasonably fast due to 32 parallel steps
  - 128-bit encryption and authentication security