JAMBU

A Lightweight Authenticated Encryption Mode

HONGJUN WU TAO HUANG

NANYANG TECHNOLOGICAL UNIVERSITY

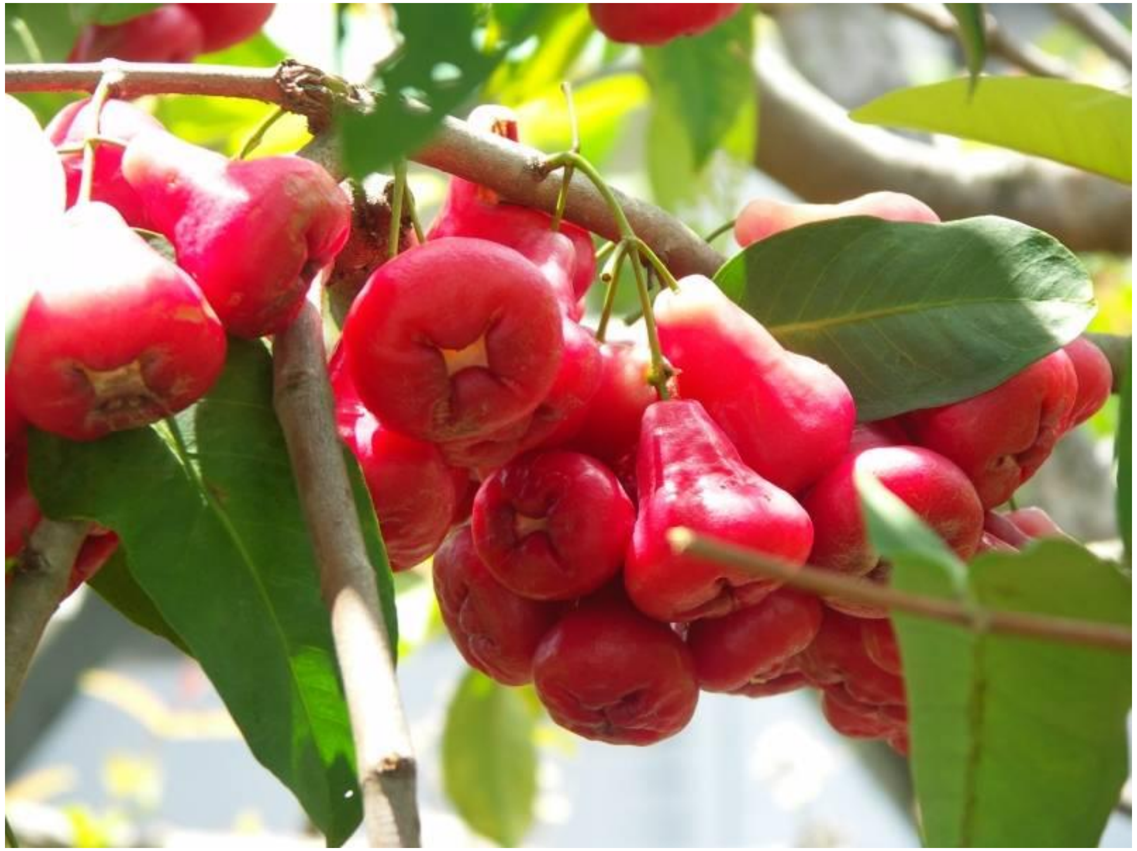
LIGHTWEIGHT CRYPTOGRAPHY WORKSHOP

20 JUL 2015

Outline

- Design Goal
- The JAMBU Authenticated Encryption Mode
- JAMBU Features
- Examples of JAMBU
- Security of JAMBU
- Performance of JAMBU
- Conclusion

JAMBU



Design Goal

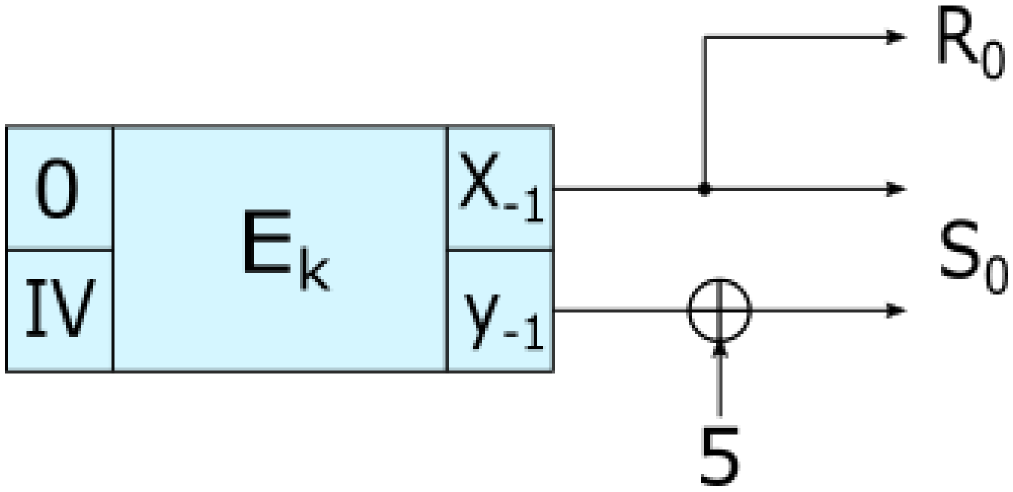
- To design a lightweight AE mode
  - Introduce small extra state size
    - For n-bit block size, the extra state sizes are

CCM	n-bit (authenticate-then-encrypt)
GCM	2n-bit
OCB3	2n-bit
EAX	3n-bit
JAMBU	0.5n-bit

Design Goal

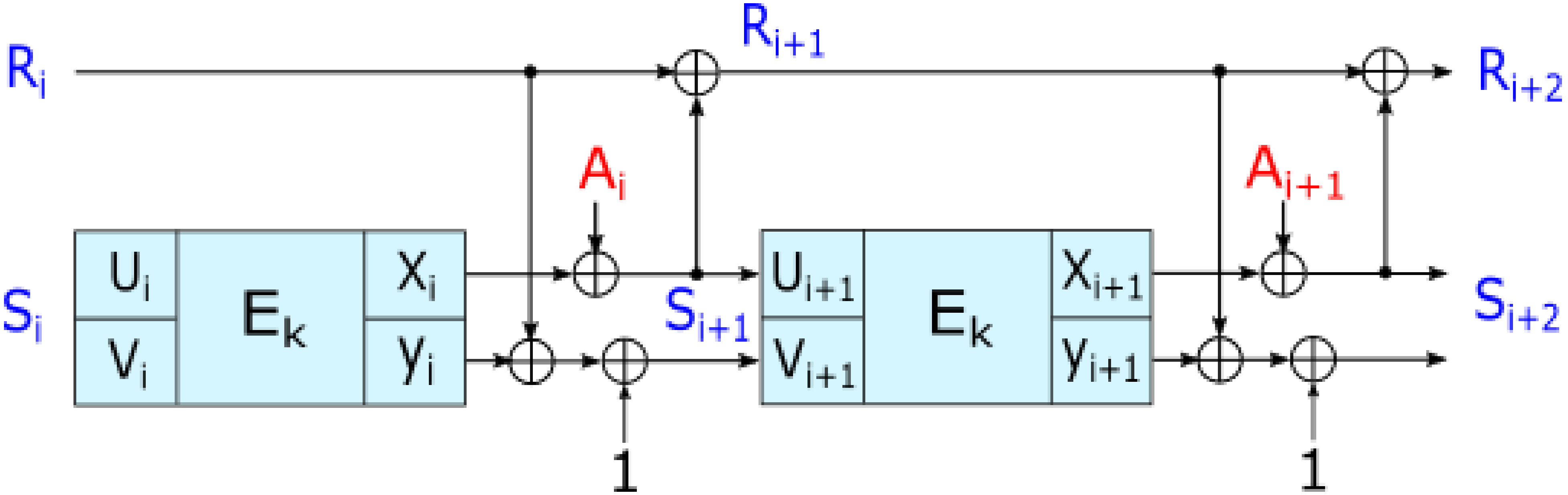
- To design a lightweight AE mode
  - Use simple operations
    - Only XOR is used other than the block cipher call
- Reasonably secure when IV is misused

The JAMBU Mode:
– Initialization



Block cipher: n-bit block size
IV: n/2-bit

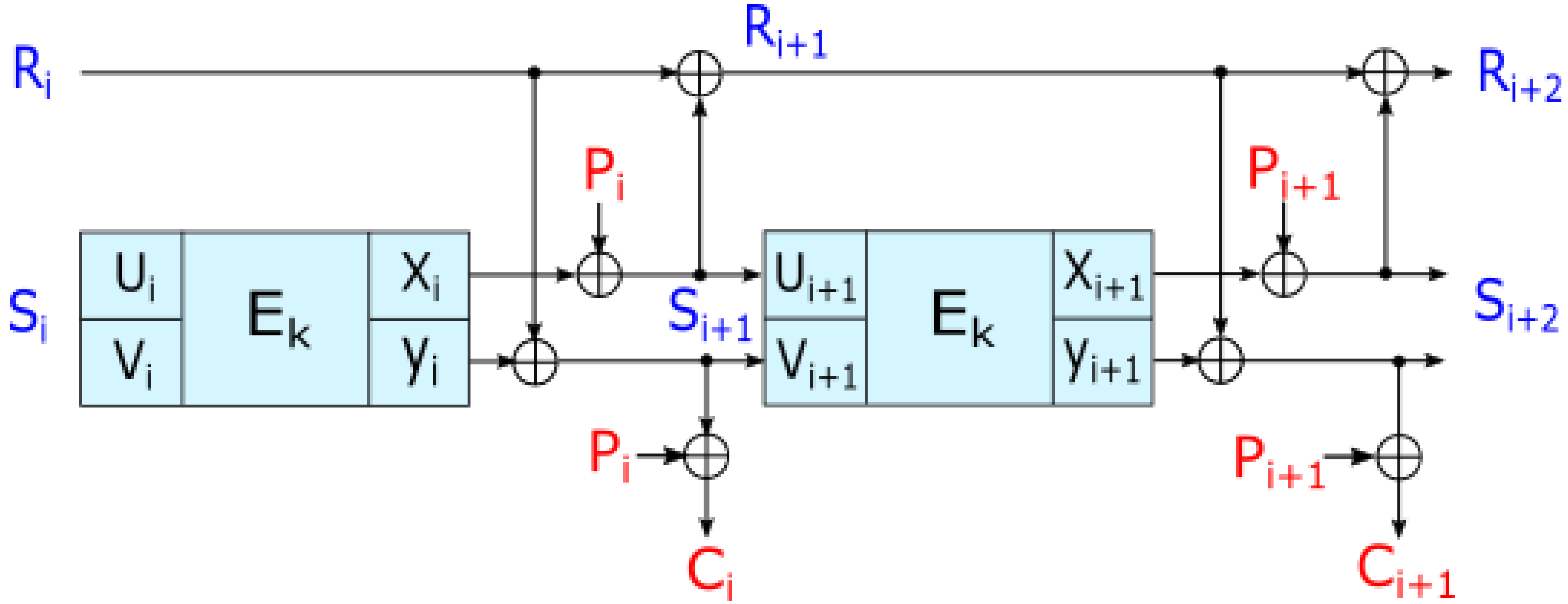
The JAMBU Mode:
– Process Associated Data



Data block size: n/2 bits

Pad the associated data with: 10^*

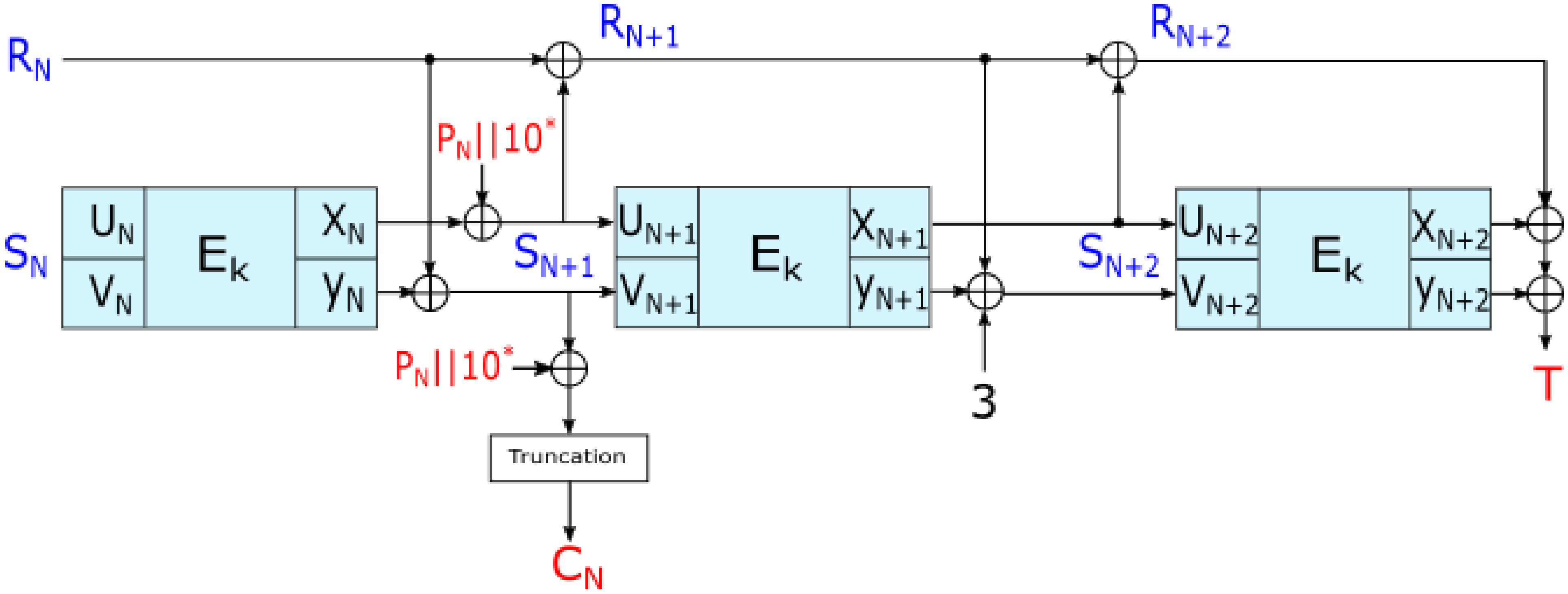
The JAMBU Mode:
– Process Plaintext



Data block size: n/2 bits

Pad the plaintext with: 10^*

The JAMBU Mode:
– Finalization



Tag: n/2-bit

JAMBU Features

- Use the existing block ciphers directly
- Lightweight mode
  - Only **n/2 extra state** is introduced (for n-bit block size)
  - Only simple XORs are introduced at each step
- Reasonably strongly when IV is misused
- Use only block cipher encryption in both authenticated encryption and decryption

The JAMBU Example: AES-JAMBU

- Use the currently most widely implemented block cipher AES
- Recommended parameters:
  - 128-bit block size
  - 128-bit key
  - 64-bit tag

The JAMBU Example: SIMON-JAMBU

- Use the lightweight block cipher SIMON proposed by NSA
- Flexible parameters:
  - 128-bit block size, 128-bit key, 64-bit tag
  - 96-bit block size, 96/128-bit key, 48-bit tag
  - 64-bit block size, 96/128-bit key, 32-bit tag

Security of JAMBU

- Encryption
  - When IV is unique
    - similar to the CFB mode
  - When IV is reused
    - if the first n plaintext blocks are the same, then the blocks after the (n+2)-th plaintext blocks are secure. (The (n+2)-th block is insecure according to the analysis by Thomas Peyrin, Siang Meng Sim, Lei Wang, and Guoyan Zhang)

Security of JAMBU

- Authentication
  - n/2-bit tag
  - Provide **n/2-bit security** when **$2^{n/2}$ message blocks** get protected
  - We analyzed the forgery probability, and it is upper bounded by $O(2^{-n/2})$

Performance of JAMBU

- Software
  - Around half of the underlying block cipher for long messages
    - Tested with AES-JAMBU and SIMON-JAMBU
- Hardware
  - The hardware area cost of JAMBU is very close to that of the underlying block cipher

Conclusion

- JAMBU: A lightweight authenticated encryption mode
  - Reasonably strong when nonce is misused
  - Probably the most compact authenticated encryption mode

Thank you!

Questions?