JAMBU

A Lightweight Authenticated Encryption Mode

Hongjun Wu **Tao Huang**

Nanyang Technological University

DIAC 2015, Singapore

29 Sep 2015

No tweak to the JAMBU mode for the second round

More security analysis provided

Lightweight block cipher SIMON is added

Security claim on encryption security for nonce reuse is slightly changed

Outline

- Design Motivation
- The JAMBU Authenticated Encryption Mode
- JAMBU Features
- AES-JAMBU and SIMON-JAMBU
- Security of JAMBU
- Performance of JAMBU
- Conclusion

Design Motivation

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

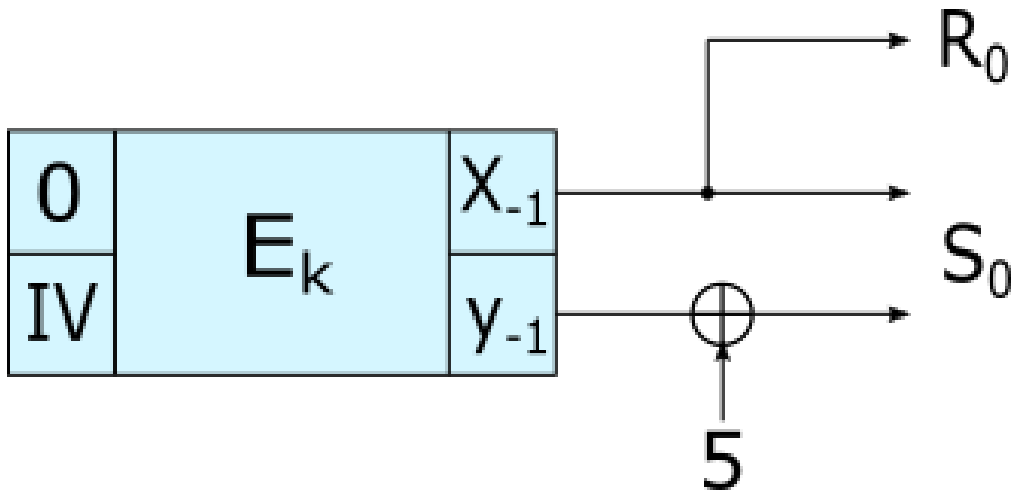
	CCM	GCM	OCB3	EAX	COPA	CPFB	ELmD	SILC	CLOC	JAMBU
State Size	2n	3n	3n	4n	3n	3n	4n	2n	2n	1.5n
Increments	n	2n	2n	3n	2n	2n	3n	n	n	0.5n

smallest

Design Motivation

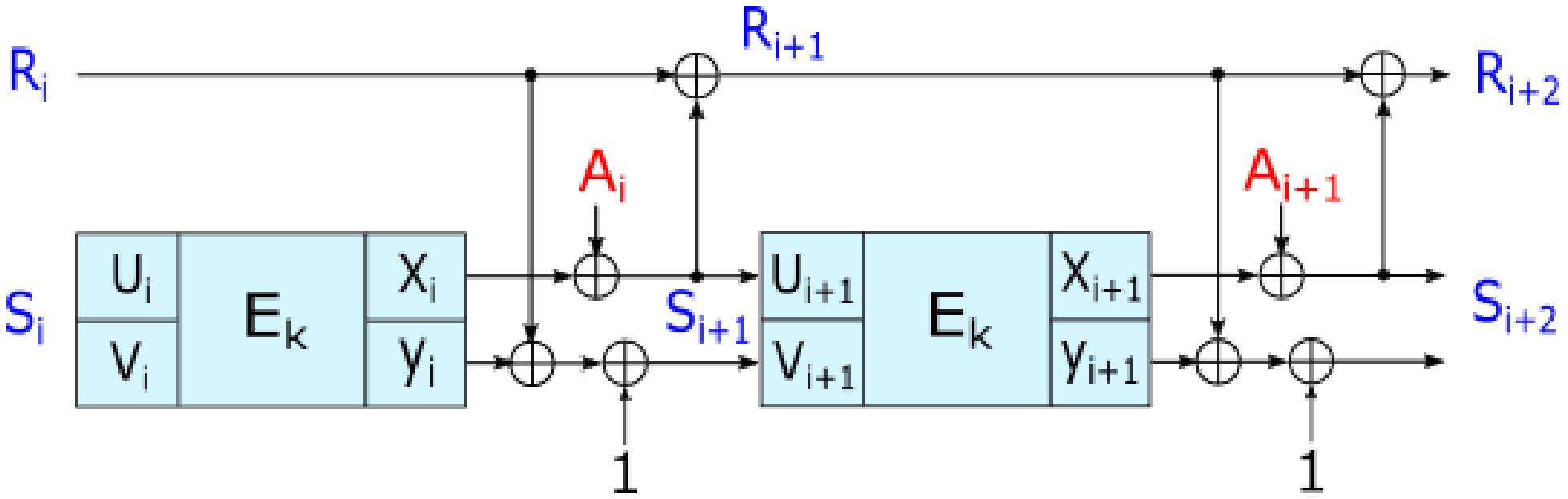
- To design a lightweight AE mode
  - Use simple operations
    - Only XOR is used other than the block cipher call

The JAMBU Mode: – Initialization



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

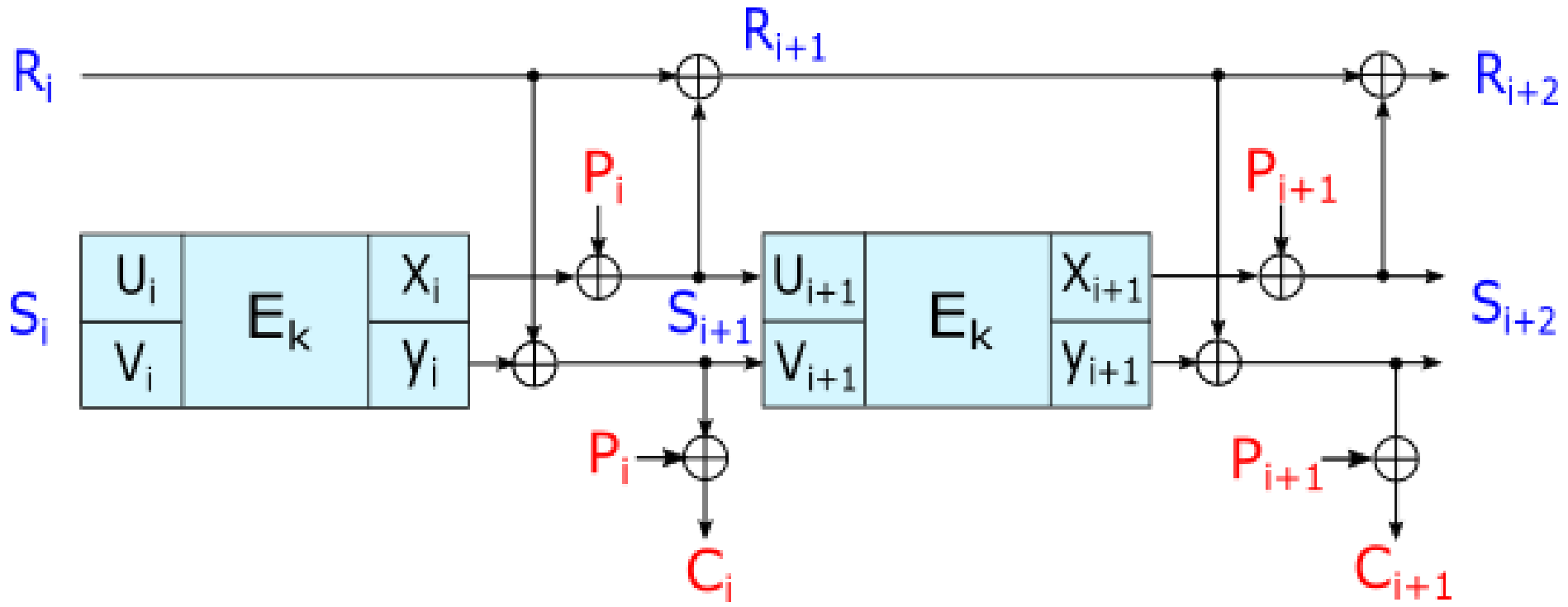
The JAMBU Mode:
– Process Associated Data



Data block size: n/2 bits

Pad the associated data with: 10^*

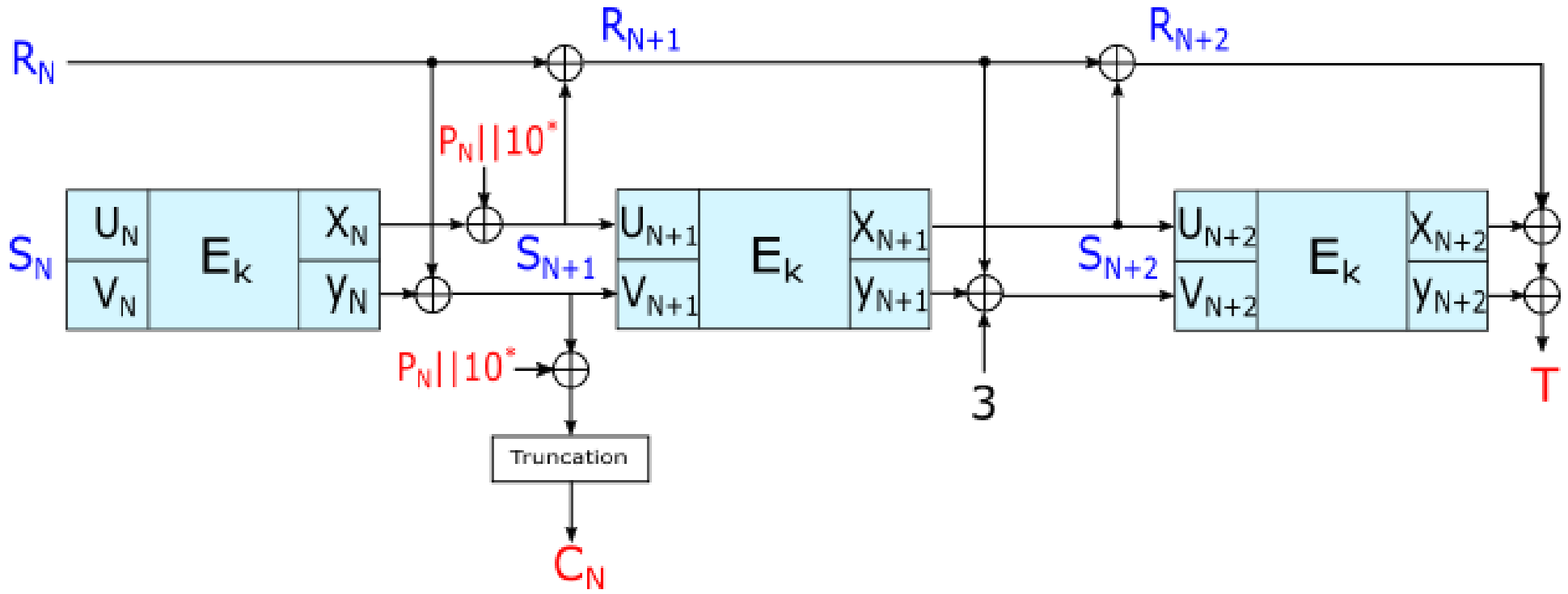
The JAMBU Mode: – Process Plaintext



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 encryption and decryption

SIMON-JAMBU

- Use the recent proposed lightweight block cipher SIMON
- With flexible parameters:
  - 96-bit block size, 96-bit key, 48-bit tag (Primary)
  - 64-bit block size, 96-bit key, 32-bit tag
  - 128-bit block size, 128-bit key, 64-bit tag

AES-JAMBU

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

Security of JAMBU: Encryption

- When IV is unique: similar to the CFB mode
- When IV is reused and first i plaintext blocks are the same:
  - the (i+1)-th plaintext block is insecure (obviously, 1 more query)
  - the (i+2)-th block is insecure according to the analysis by Thomas Peyrin, Siang Meng Sim, Lei Wang, and Guoyan Zhang. (by repeating same nonce and chosen plaintext for $2^{n/2}$ times).
  - the blocks after (i+2)-th plaintext blocks are secure (changed from the first version)

Security of JAMBU: Authentication

- n/2-bit tag
- Provide **n/2-bit security** when **$2^{n/2}$ message blocks** get protected

Performance of JAMBU

- Software
  - Around half of the underlying block cipher for long messages
    - Tested with AES-JAMBU and SIMON-JAMBU

	64B	128B	256B	512B	1024B	4096B
AES-128-CTR	1.71	1.52	1.13	1.09	1.00	0.97
AES-128-CCM	6.62	5.56	5.03	4.76	4.63	4.53
AES-128-GCM	5.93	3.84	2.91	2.46	2.24	2.07
AES-128-OCB3	3.46	2.15	1.43	1.09	0.93	0.78
SIMON-JAMBU64/96	83.24	62.78	57.21	54.79	53.21	51.94
SIMON-JAMBU96/96	124.72	95.67	84.93	79.67	76.93	75.08
SIMON-JAMBU128/128	76.11	58.26	49.55	45.61	43.06	41.45
AES-JAMBU	24.41	17.08	13.41	11.57	10.65	9.98

Performance of JAMBU

- Hardware
  - JAMBU mode requires **the least amount of extra state** comparing to other AE modes
  - Implementation results will be provided in the future

Conclusion

- Main features of JAMBU
  - Reasonably strong when nonce is misused
  - Probably the most compact authenticated encryption mode

Conclusion

- Changes in the second-round submission
  - No tweak to the JAMBU mode
  - More security analysis
  - Add SIMON-JAMBU
  - Slightly modified the security claim

Thank you!
Questions?