JAMBU
A Lightweight Authenticated Encryption Mode

Hongjun Wu **Tao Huang**

Nanyang Technological University

DIAC 2016, Nagoya

26 Sep 2016

JAMBU

Comparison between AEGIS, MORUS, JAMBU, ACORN

Fast → AES-NI (AEGIS)

Fast → SIMD (MORUS)

Lightweight → Mode (**JAMBU**)

Lightweight → Dedicated (ACORN)

No tweak to the JAMBU mode for the third round

Update **in JAMBU v2.1 document**

- Add authentication security proof for nonce reused in JAMBU
- Add hardware performance of JAMBU

Outline

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

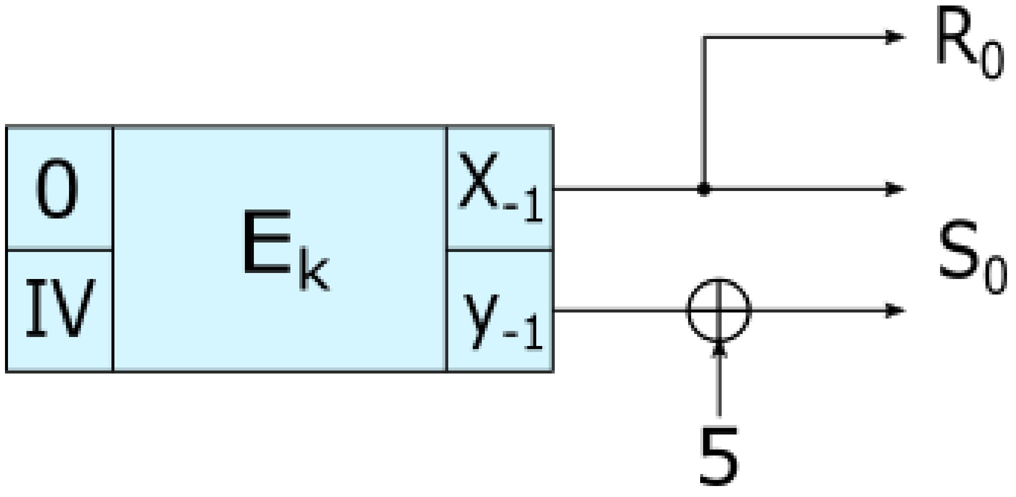
Design Motivation

- To design a lightweight AE mode
  - Use simple operations
    - Only **XOR** is used
  - Introduce small extra state size.
  - For $2n$-bit block size, the extra state sizes are

	CCM	GCM	OCB3	EAX	CPFB	COLM	SILC	CLOC	JAMBU
State Size	4n	6n	6n	8n	6n	8n	4n	4n	3n
Increments	2n	4n	4n	6n	4n	6n	2n	2n	n

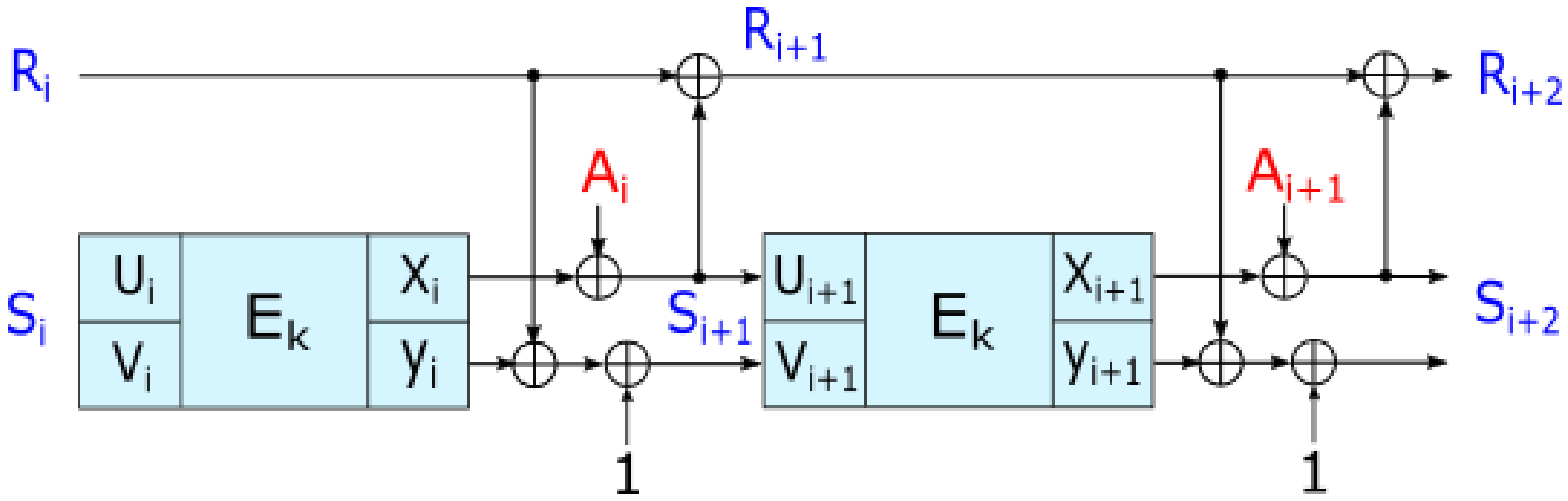
smallest

The JAMBU Mode:
– Initialization



Block cipher: $2n$ bits block size
IV: n bits

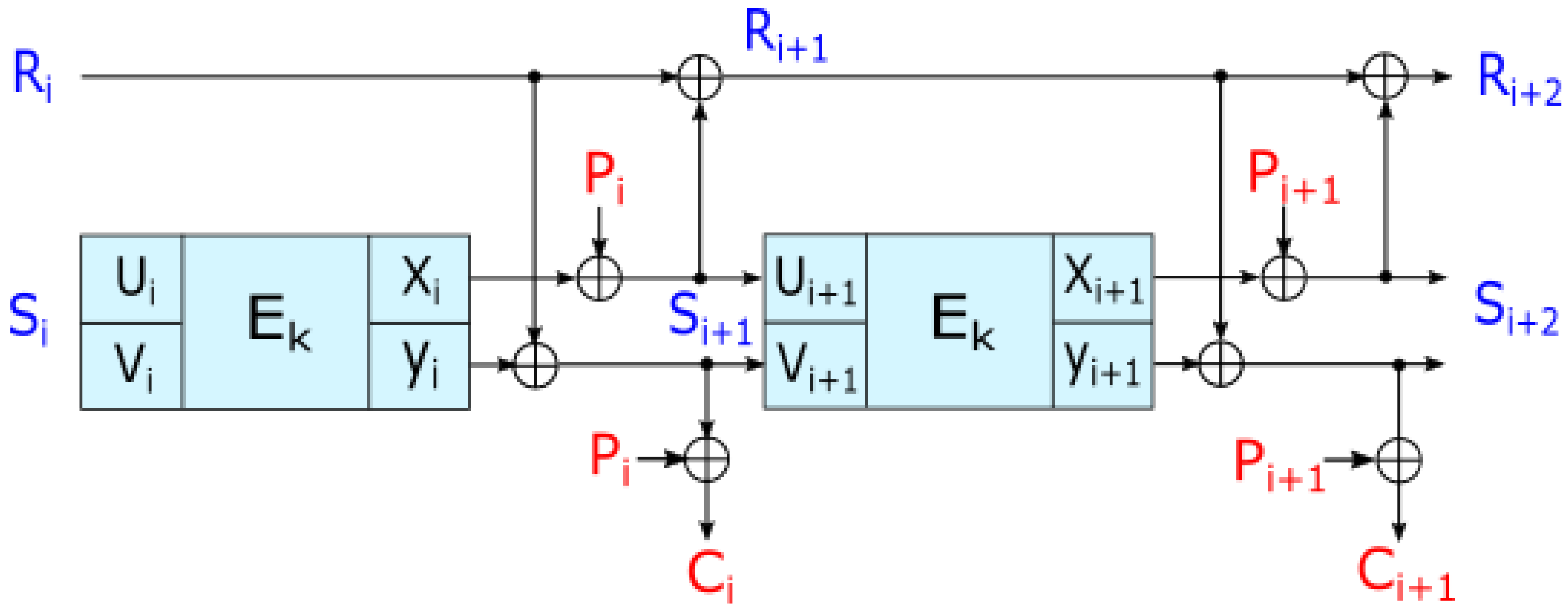
The JAMBU Mode: – Process Associated Data



Data block size: n bits

Pad the associated data with: 10^*

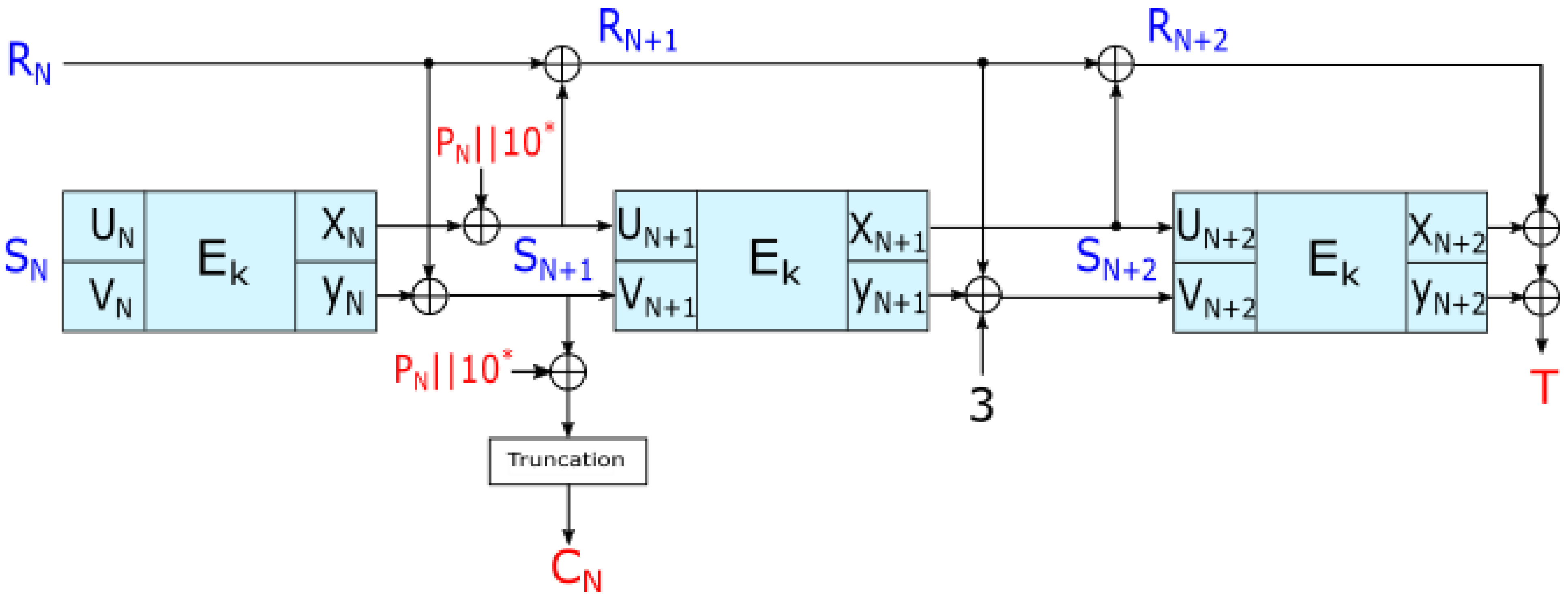
The JAMBU Mode: – Process Plaintext



Data block size: n bits

Pad the plaintext with: 10^*

The JAMBU Mode:
– Finalization



Tag: n bits

Parameter sets

Order	Name	Key size (bits)	IV size (bits)	State size (bits)	Tag size (bits)	Use cases
Primary	SIMON-JAMBU96/96	96	48	144	48	Lightweight/Defense in depth
Secondary	SIMON-JAMBU64/96	96	32	96	32	Lightweight/Defense in depth
Tertiary	SIMON-JAMBU128/128	128	64	192	64	Lightweight/Defense in depth
Quaternary	AES-JAMBU	128	64	192	64	Defense in depth/Lightweight

JAMBU Features

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

Security of JAMBU

- Encryption
  - **When IV is unique**
    - similar to the CFB mode
  - **When IV is reused and** the **first i plaintext blocks are the same**
    - it is obvious that the security of the $(i+1)$-th plaintext block is insecure when nonce is reused.
    - the $(i+2)$-th block is also insecure according to the analysis by ***Thomas Peyrin***, ***Siang Meng Sim***, ***Lei Wang***, *and* ***Guoyan Zhang*** (FSE 2015)
    - the blocks after $(i+2)$-th plaintext blocks are secure

Security of JAMBU

- Authentication
  - n-bit tag
  - Provide **n-bit security** when message size is no more than $\mathbf{2^{n/2}}$ bits and nonce is misused
    - Note that the nonce reuse security for spongeWrap with $2n$-bit permutation, n-bit message block size, the authentication security is $n/2$-bit when nonce is misused.
  - We show in our security proof that for adversary making at most q queries with at most l blocks of message in each query

$$Adv_{JAMBU}^{auth} \leq \frac{3q^2l^2}{2^{2n}} + \frac{2q^2l}{2^{2n}} + \frac{5q^2}{2^{2n+1}} + \frac{q(l+2)}{2^{2n+1}}$$

Performance of JAMBU

- Software
  - Around half of the speed of underlying block cipher
  - JAMBU is not designed for high-speed applications

Table. Software performance of JAMBU (Intel Core i7-4770 Haswell)

	64B	128B	256B	512B	1024B	4096B
SIMON-JAMBU96/96	83.24	62.78	57.21	54.79	53.21	51.94
SIMON-JAMBU64/96	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

- Hardware
  - JAMBU mode requires **the least amount of extra state** comparing to other AE modes
  - FPGA results of SIMON-JAMBU96/96 on Xilinx Virtex-7 (CAESAR hardware API)

Frequency	434 MHz
Area in Slices	375 Slices
Area in LUTs	1254 LUTs
Throughput	385 Mbits/s
Throughput/slice	1.028 Mbits/Slice
Throughput/LUT	0.307 Mbits/LUT

Conclusion

- Main features of JAMBU
  - Strong authentication security when nonce is misused
  - CFB-type encryption security when nonce is misused
  - Probably the most compact authenticated encryption mode
- **No tweak** to the JAMBU mode in the third round
- Update
  - Authentication security proof in the nonce-reuse cases
  - FPGA performance of JAMBU

Thanks for your attention!