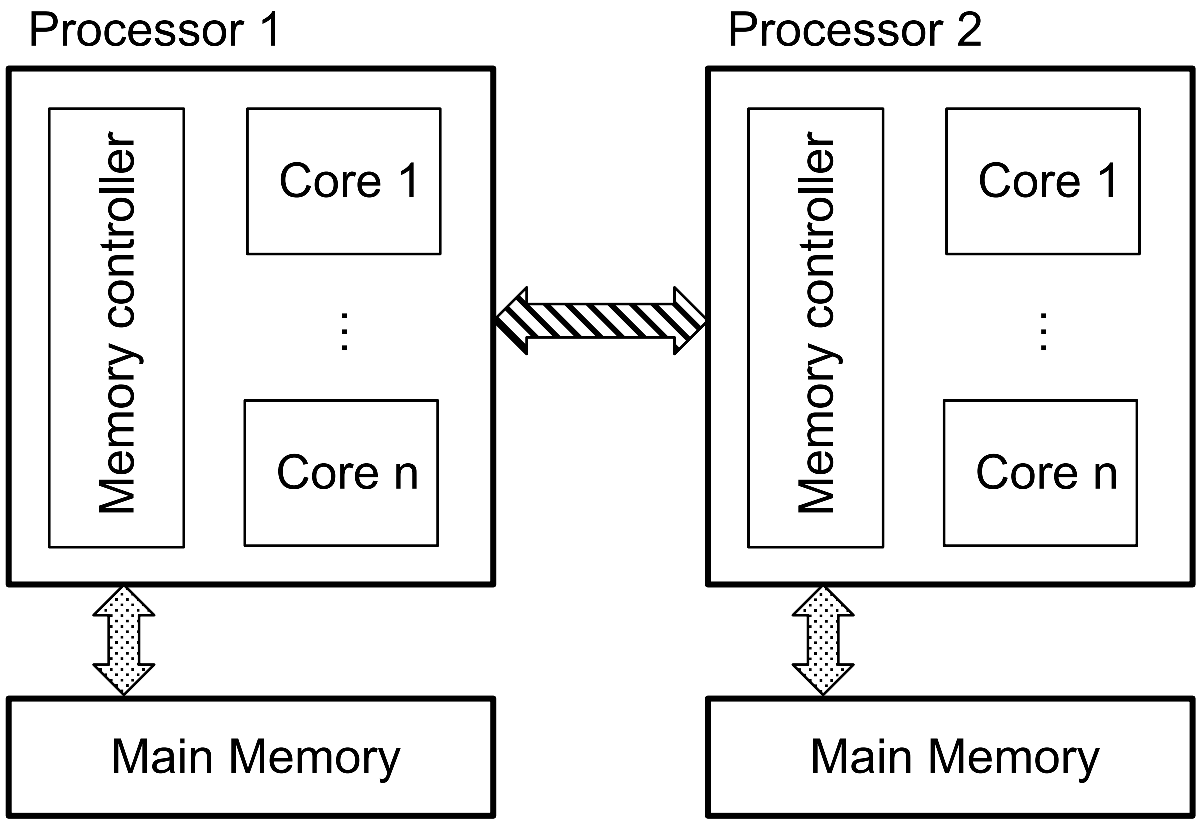
Securing the Processor-to-Processor and Processor-to-Memory Communication Links

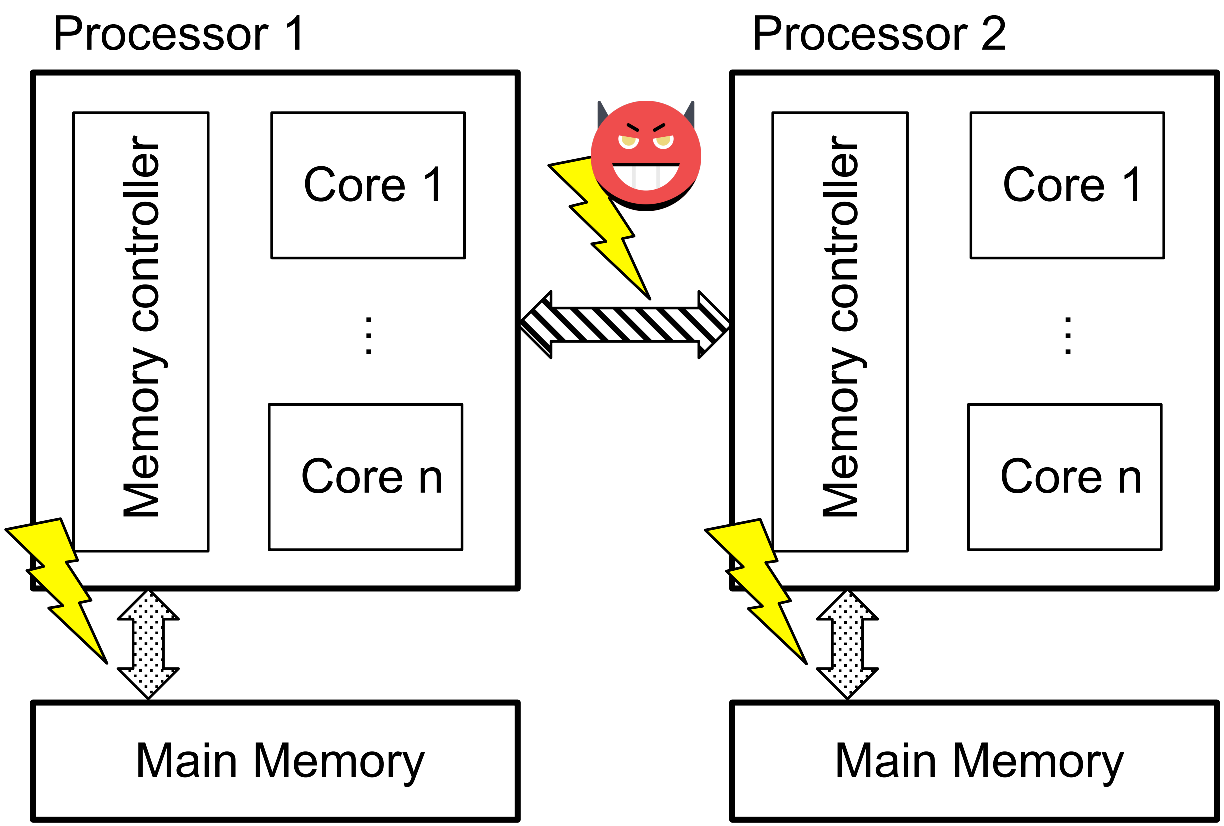
George Angelopoulos, C. Barner,
R. Kessler
(georgiosa@marvell.com)

BARC 2019

Security Challenges



Security Challenges



Motivation

- New computing paradigms
  - Cloud and IaaS computing
- New technologies
  - Non-volatile memories
- New attacks
  - Foreshadow, Rowhammer variants
- Security primitives can be area, performance and power hungry

Security Objectives

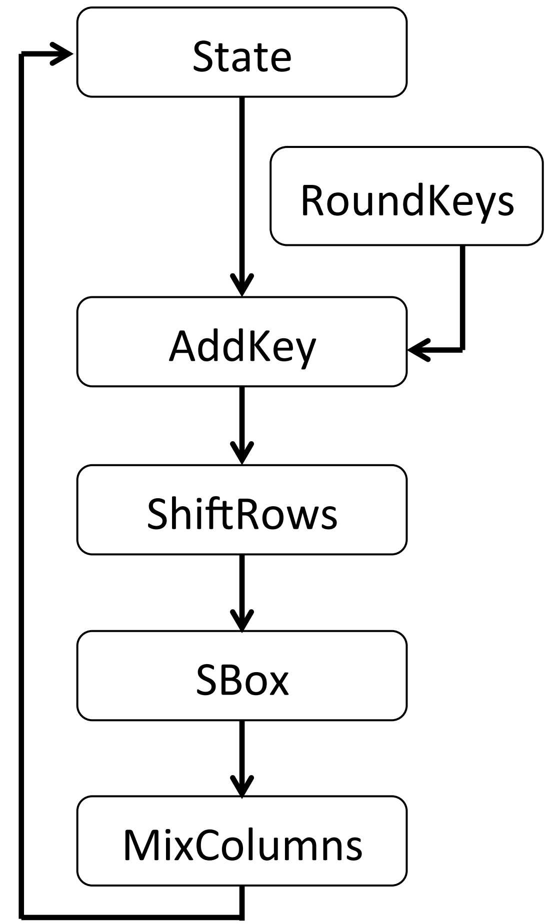
- Confidentiality
  - Prevents eavesdropping
- Authentication
  - Active attacks to tamper data
- Replay attacks
  - Capture now, inject later
- Ciphers, hashes and anti-replay mechanisms are employed to secure our platforms

Advanced Encryption Standard

- AES: ‘Golden standard’ for ~2 decades
- AES-256 is quantum-resistant
- Widespread support

Advanced Encryption Standard

- AES: ‘Golden standard’ for ~2 decades
- AES-256 is quantum-resistant
- Widespread support
- Sbox’es consume large area
- Key expansion
- Secure, but not designed with modern computing requirements in mind



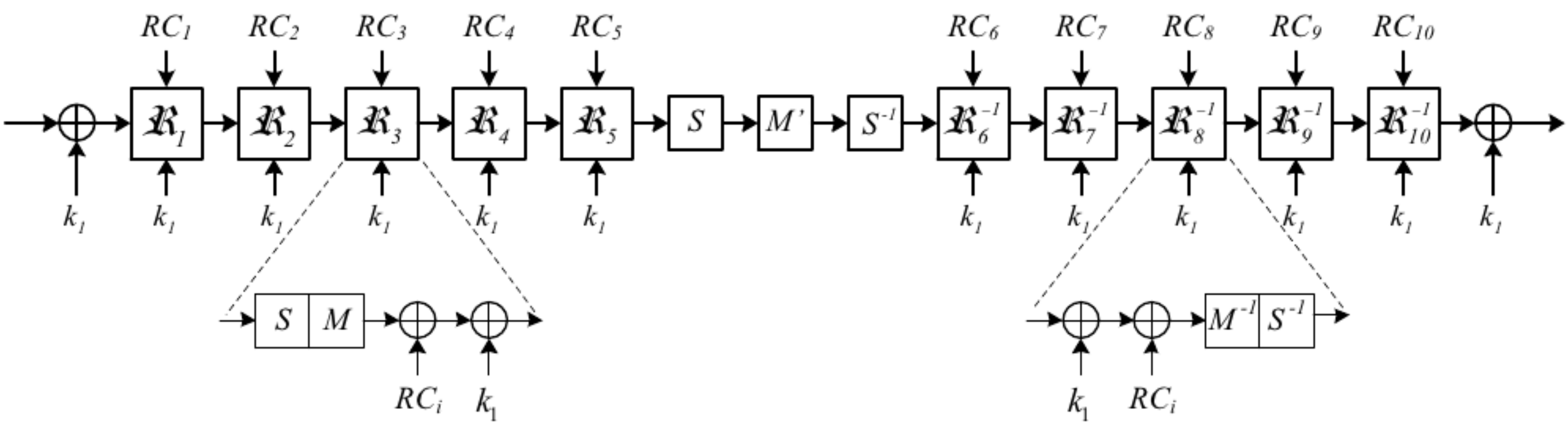
AES round

Lightweight Crypto

- New crypto primitives
- ‘Friendlier’ to SW/HW implementations
- No compromises on security
- IoT is main driver in this space
- Plethora of ciphers
  - SIMON, PRESENCE, PRINCE, …
  - Trivium, Grain, ChaCha, …
- Same applies for authentication algos

PRINCE cipher

- 64-bit block, 128-bit key
- 11 rounds (5 forward, 1 middle, 5 reverse)
- Low latency and low area



[1] Borghoff et al, "PRINCE – A low-latency block cipher for pervasive computing applications", 2012

PRINCE cipher

- Almost-instantaneous key expansion
  - 128 → 196bits $(k_0 \| k_1) \rightarrow (k_0 \| k_0' \| k_1)$

$$k_0' = (k_0 >>> 1) \oplus (k_0 >> 63)$$

- Low latency
  - Few rounds, each round with short logic-depth
- Low area
  - 4-bit Sbox
  - α-reflection property

$$D_{(k_0 \| k_0' \| k_1)}(\cdot) = E_{(k_0' \| k_0 \| k_1 \oplus \alpha)}(\cdot)$$

PRINCE cipher

Cipher	Area (kGE)	Latency (cycles)	Normalized Power
AES	78	20	23
PRINCE	4.5	5	1

- Fully pipelined design, 2.6GHz, 14nm
- Almost free expansion
- Very low latency for ECB mode
- No RAMs required to store expanded keys
- Significantly lower power than AES

[2] Horowitz, "Computing's Energy Problem (and what we can do about it)", ISSCC, 2012

Data Authentication

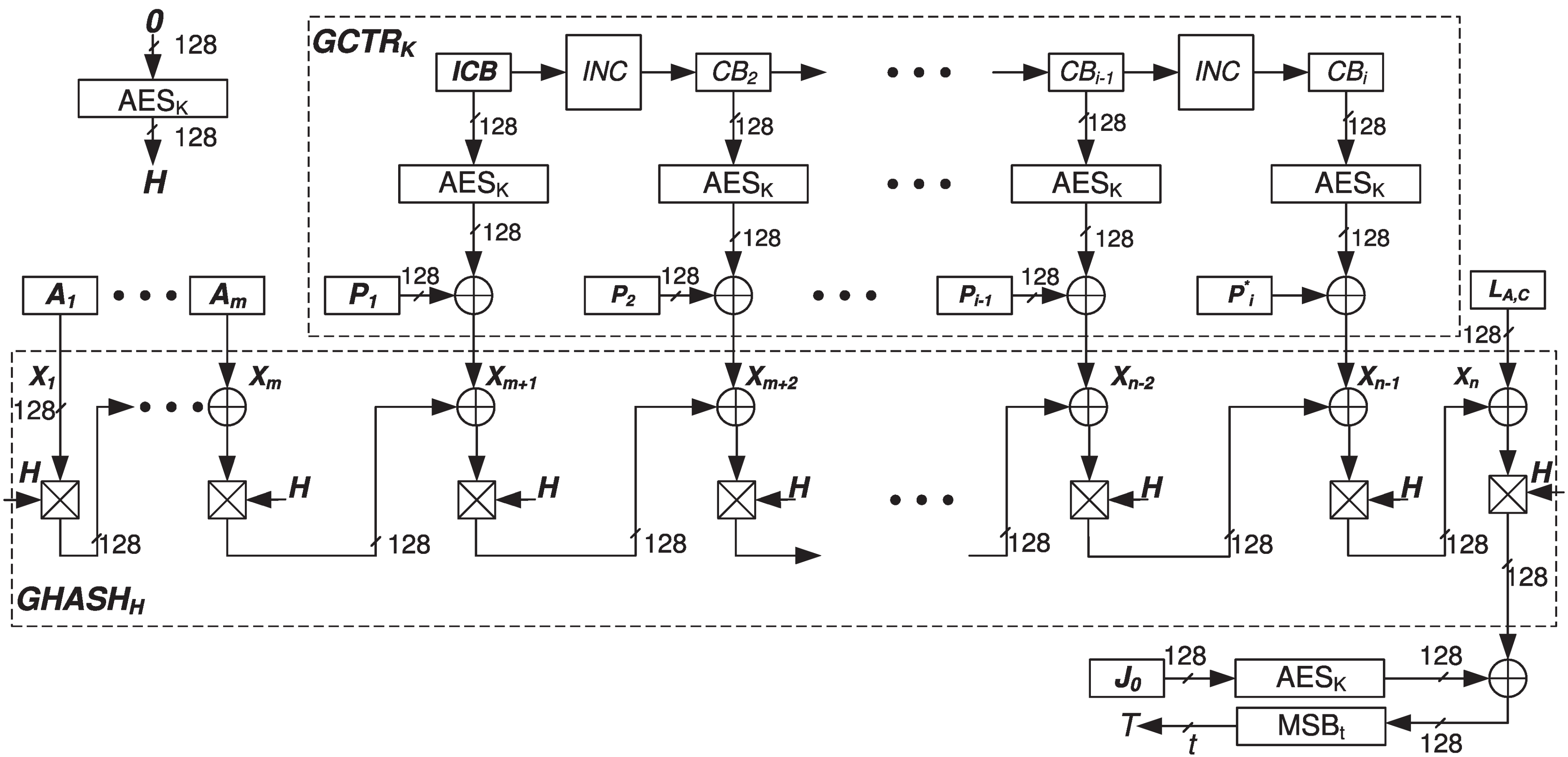
- Encryption is not enough!

Data Authentication

- Encryption is not enough!
- Hash function for MAC-tag generation
- Galois counter mode (GCM)
  - Encryption with CTR/authentication with GHASH
  - Since ~2016, GCM performance is equal to ECB in some modern CPUs
- 64-bit and 128-bit tags
- AES-GCM well understood and used, eg MEE

[3] Gueron, "A memory encryption engine suitable for general purpose processors",ePrint, 2016

Data Authentication



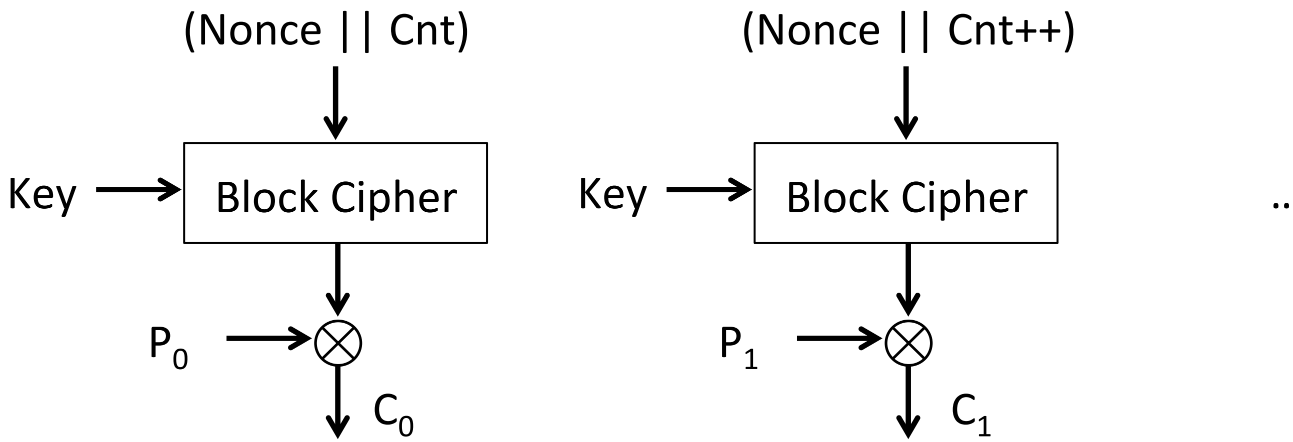
Data Authentication

- GF(2^{128}) multiplication
  - No overflows, wide-expansion
- Recursive Karatsuba algorithm
  - Sub-quadratic complexity

Cipher	Area (kGE)	Latency (cycles)	Normalized Power
AES	78	20	23
PRINCE	4.5	5	1
GHASH	1.6	2	0.4

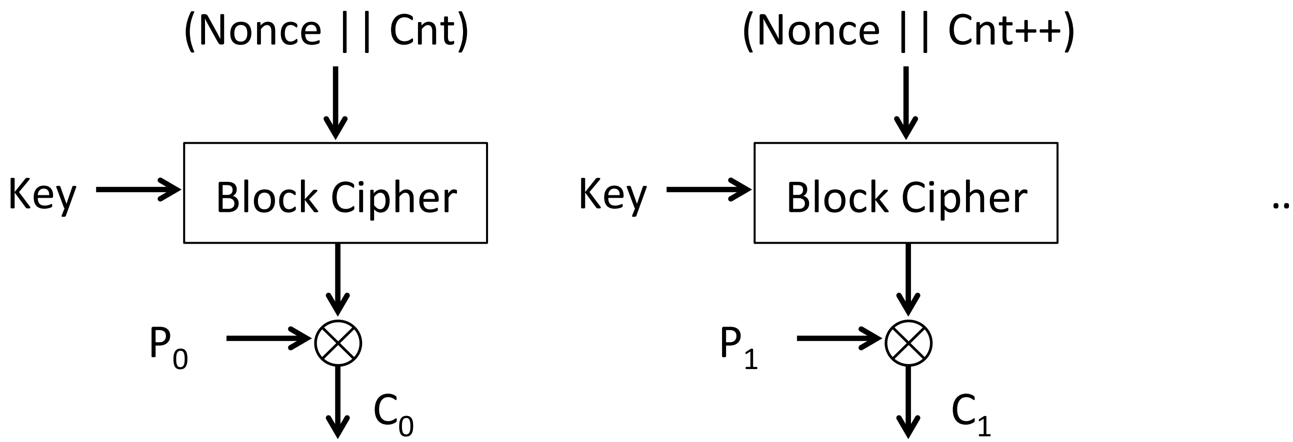
Anti-replay Protection

- Counter mode (CTR)



Anti-replay Protection

- Counter mode (CTR)



- Reusing the same IV can be catastrophic
- Lost confidentiality of few msgs, integrity for whole session
- Should use temporal and special info in IV

Anti-replay Protection

- Maintaining counters is not trivial!
- Leverage information from multi-socket CPU protocols
- CCPI (Cavium Coherent Processor Interconnect)
- Sequence number for in order reception
- Retransmission buffers
- Joint operation increases complexity but saves a lot of area

Conclusions

- Integrity, authentication and replay are of equal importance
- Promising new crypto primitives
- PRINCE is an ideal cipher candidate
- Synthesized at 14nm, 2.6 GHz
- Unnoticeable area and power increase
- Negligible latency overhead

Questions?