PMAC-Double: Doubling PMAC with a Single Key

(in progress)

Nilanjan Datta, Avijit Dutta, Mridul Nandi, Goutam Paul and Liting Zhang

ISI, ISCAS and NTU

ASK 2015 @ NTU, Singapore

Sep. 30th - Oct. 3rd 2015

Outline

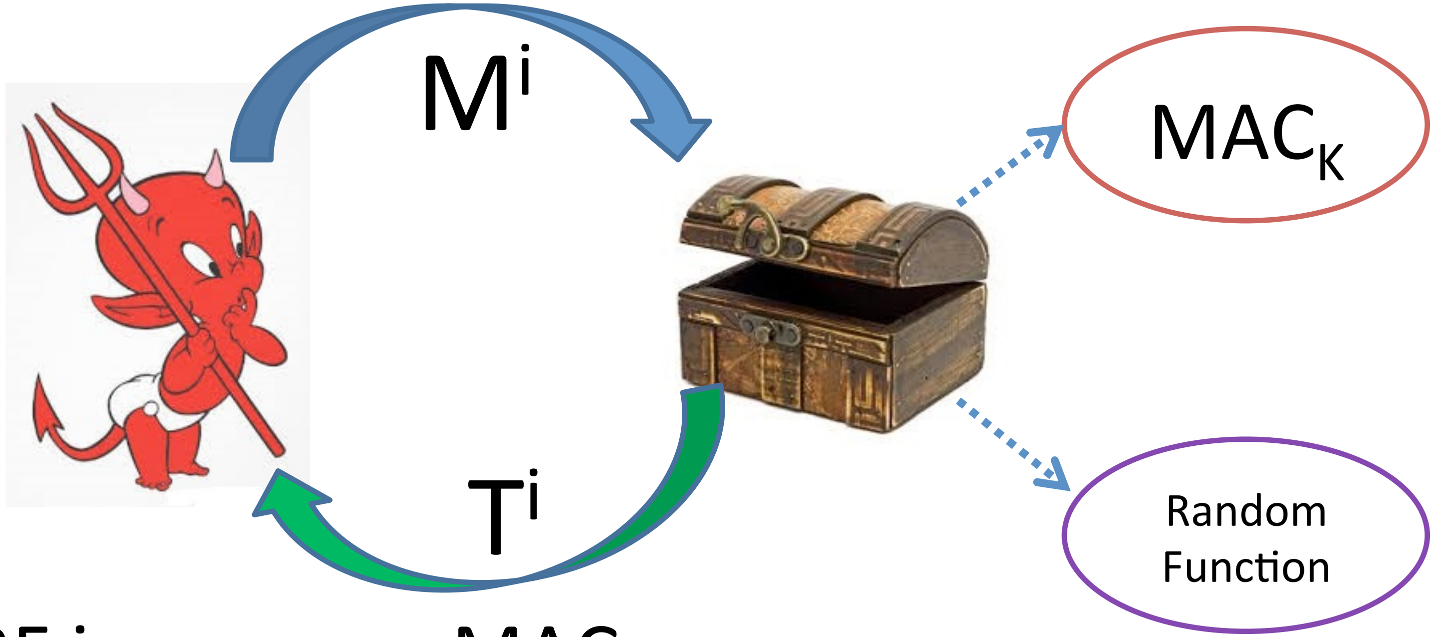
- Review on MAC, PMAC and PMAC_Plus
- Birthday bound and beyond
- PMAC-Double
  - Illustration
  - Comparison with PMAC_Plus
  - Proof sketch
  - Bad events and solutions

MAC

- Message Authentication Code
  - Data integrity and data origin authentication
- Constructions
  - Block cipher-based: CBC-MACs, PMAC, …
  - Hash-function-based: HMAC, NMAC, …
  - Universal-hash-function-based: UMAC, …
  - Dedicated: Alpha-MAC, …

MAC Security

- Unpredictability, Pseudorandomness



M^i

T^i

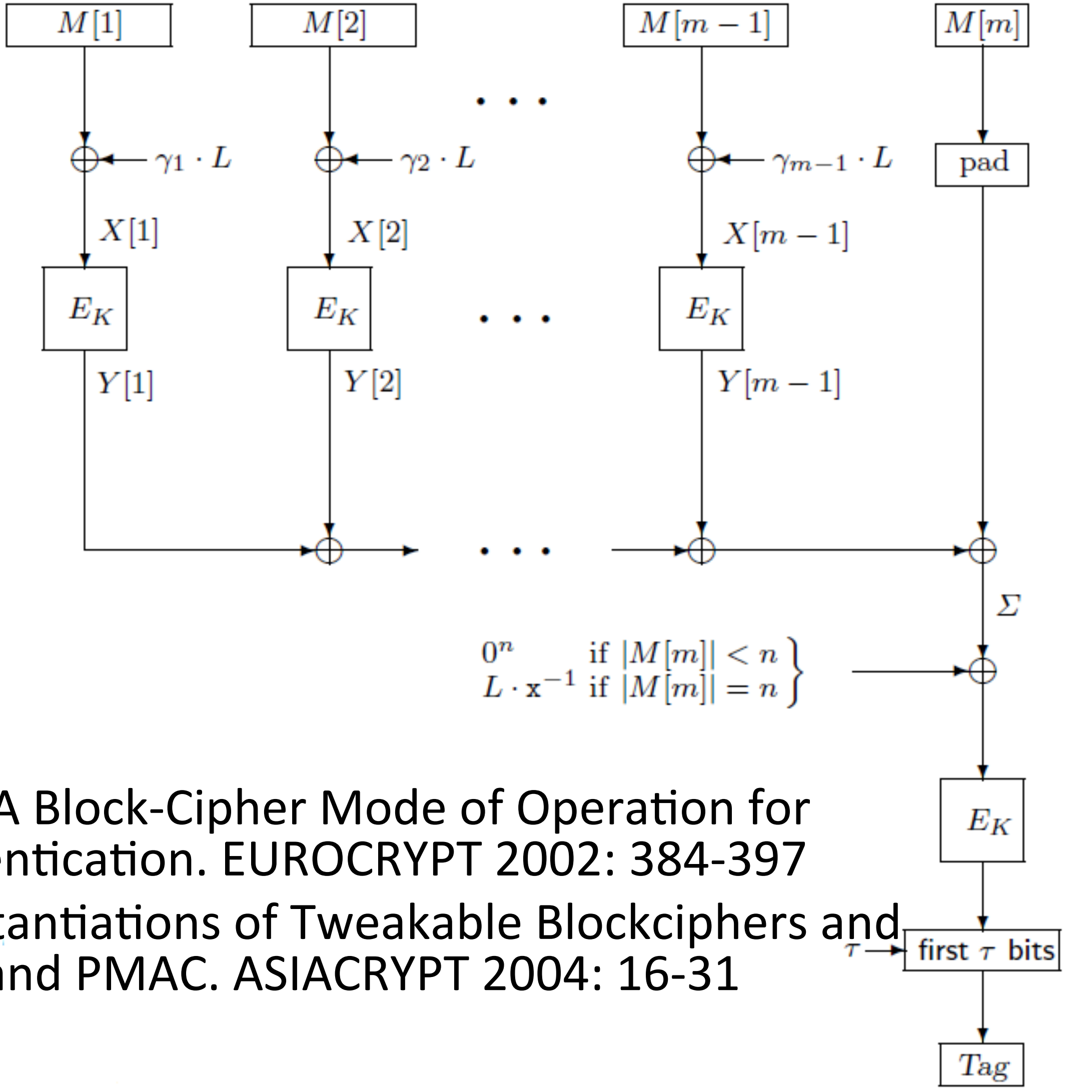
MAC_K

Random Function

- A PRF is a secure MAC

PMAC

- Fully parallel
- One block cipher key
- n-bit internal state
- PRF secure up to $O(2^{n/2})$



- John Black, Phillip Rogaway: A Block-Cipher Mode of Operation for Parallelizable Message Authentication. EUROCRYPT 2002: 384-397
- Phillip Rogaway: Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC. ASIACRYPT 2004: 16-31

PMAC Security

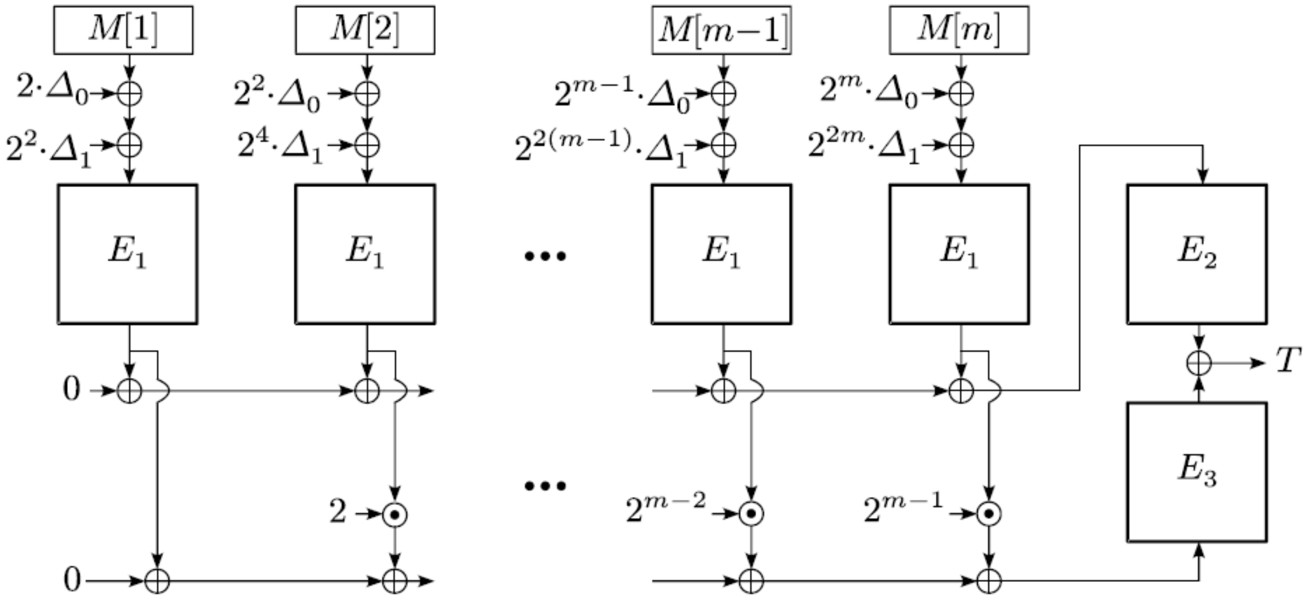
- $O(q^2L^2/2^n)$ → $O(q^2L/2^n)$

- PMAC is less sensitive for L

- John Black, Phillip Rogaway: A Block-Cipher Mode of Operation for Parallelizable Message Authentication. EUROCRYPT 2002: 384-397
- Kazuhiko Minematsu, Toshiyasu Matsushima: New Bounds for PMAC, TMAC, and XCBC. FSE 2007: 434-451
- Mridul Nandi: A Unified Method for Improving PRF Bounds for a Class of Blockcipher Based MACs. FSE 2010: 212-229

PMAC_Plus

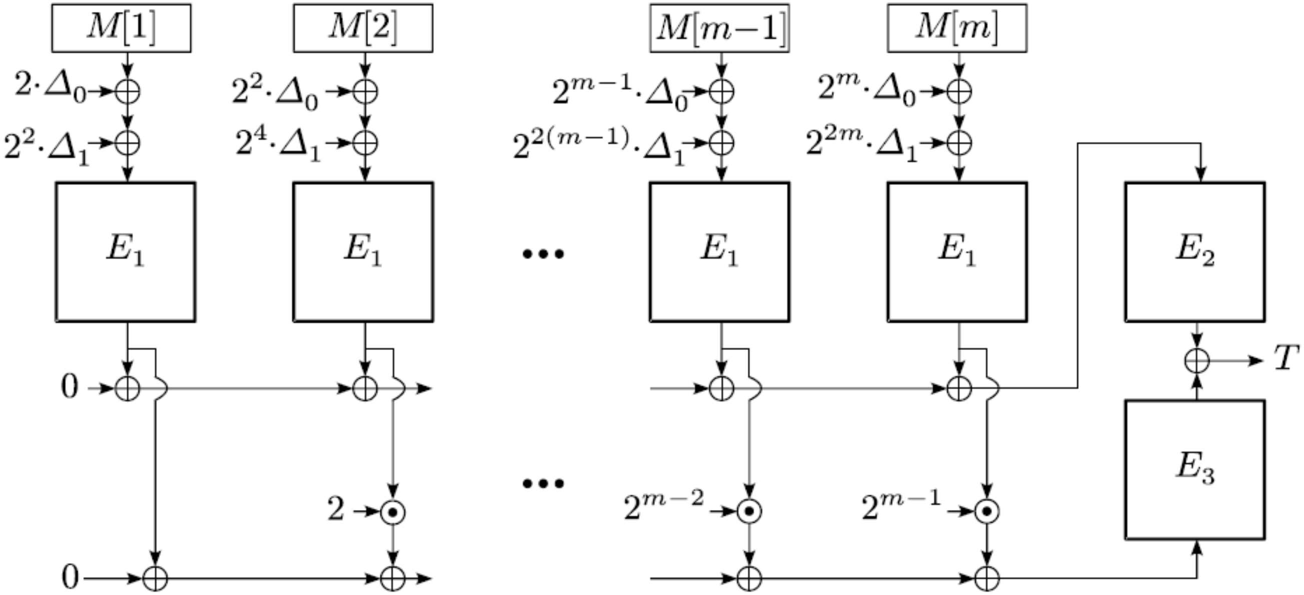
- 3 block cipher keys, essentially serial
- 2n-bit internal state, PRF secure up to $O(2^{2n/3})$



- Kan Yasuda: A New Variant of PMAC: Beyond the Birthday Bound. CRYPTO 2011: 596-609

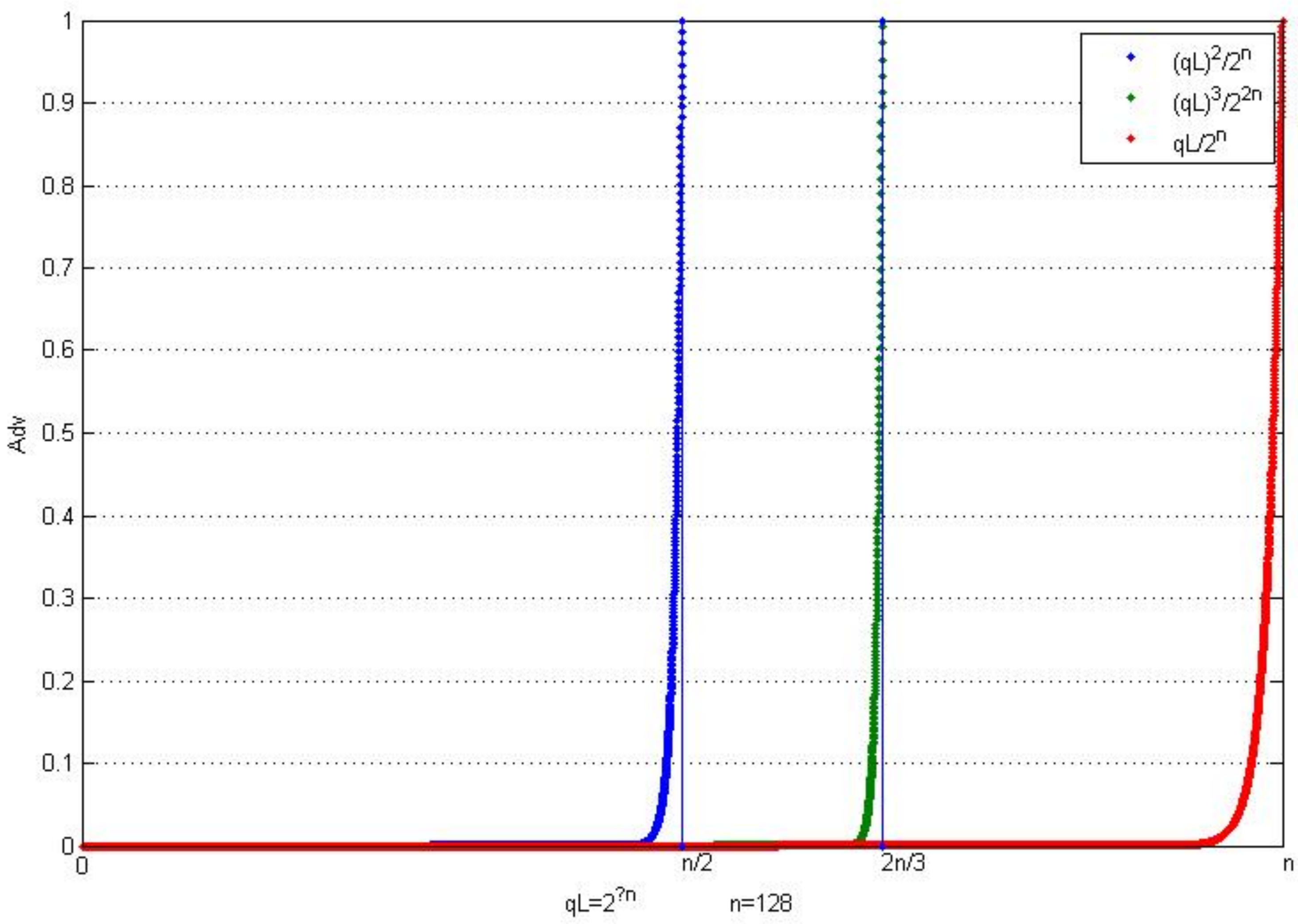
PMAC_Plus Security

- $O(qL/2^n+q^3L^3/2^{2n})$



- S_1 is new, S_2 is new
- S_1 is old, S_2 is new
- S_1 is new, S_2 is old
- S_1 is old, S_2 is old

Birthday bound and beyond



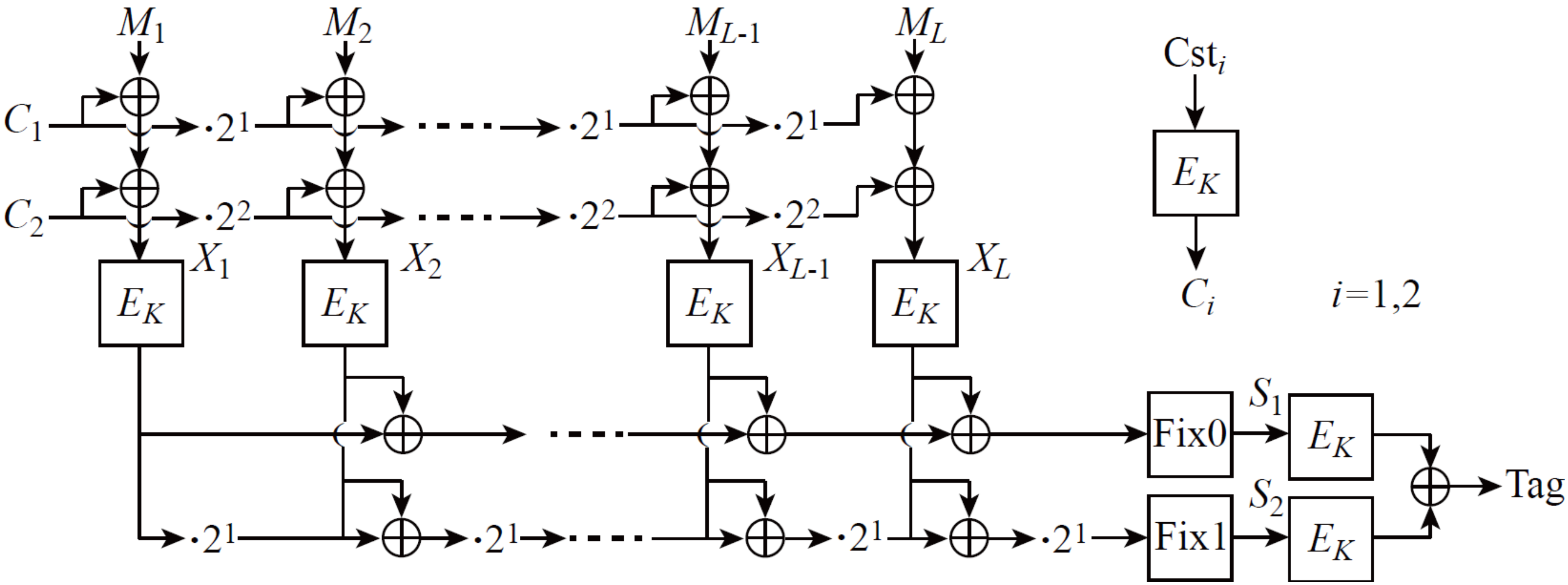
Birthday bound and beyond

Upper bounds	n=64	n=128	n=256
$(qL)^2/2^n$	32	64	128
$(qL)^3/2^{2n}$	42.7	85.3	170.7
…			
$(qL)^{d+1}/2^{dn}$	$64d/(d+1)$	$128d/(d+1)$	$256d/(d+1)$
…			
$qL/2^n$	64	128	256

Reducing Key Size

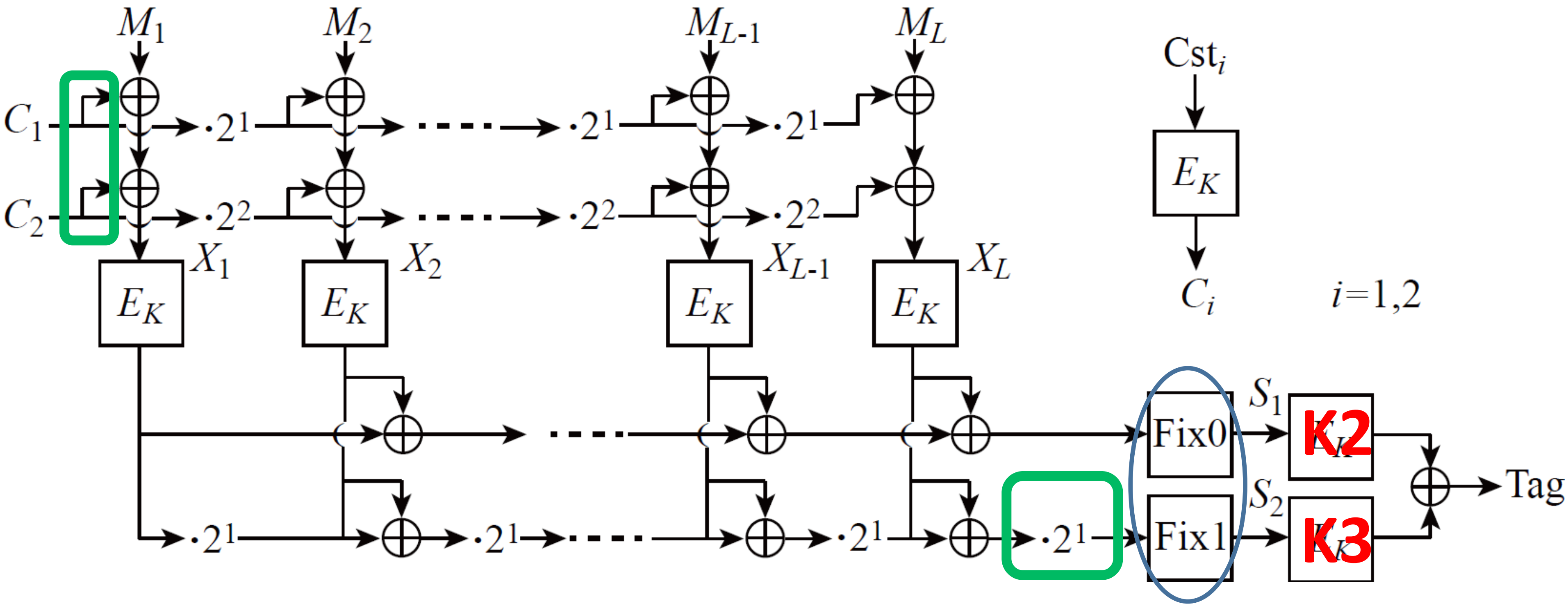
- Introducing a key generation function
  - K1, K2, K3← f(masker Key)
    - Extra costs
    - Pseudorandomness of f
- Using tweakable block ciphers
  - Dedicated construction no provable security
  - Beyond-birthday-bound design
    - Key size
    - Several normal BC calls

PMAC-Double: Illustration



- One key by minor changes on PMAC_Plus
- PRF secure up to $O(qL/2^n+q^3L^3/2^{2n}+q^4L^2/2^{3n})$

Comparison with PMAC_Plus



- Two less keys, -3+1 double operations
- Introducing Fix0, Fix1

Thanks

Q&A