On Beyond-Birthday-Bound Security: Revisiting the Development of ISO/IEC 9797-1 MACs

Yaobin Shen and Lei Wang

Shanghai Jiao Tong University

November 09, FSE 2020

Outline

Message Authentication Code (MAC)

- Provide integrity and authenticity of messages
- Three ways to build a MAC
  - blockcipher-based
  - universal-hash-function-based
  - hash-function-based
- Blockcipher-based MACs
  - CBC-MAC, CMAC, PMAC, LightMAC

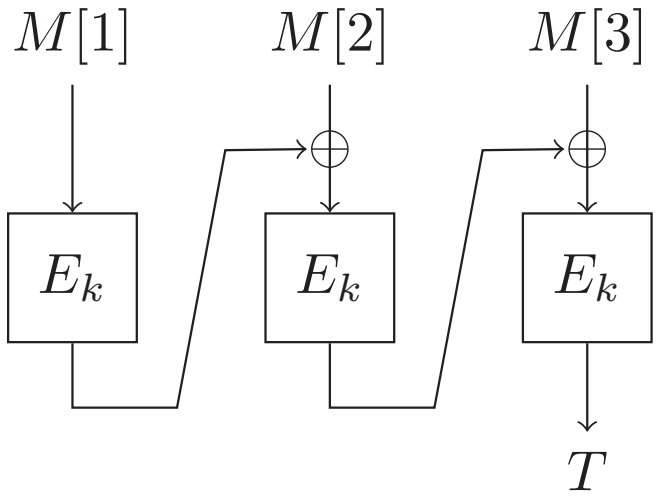


Illustration of CBC-MAC

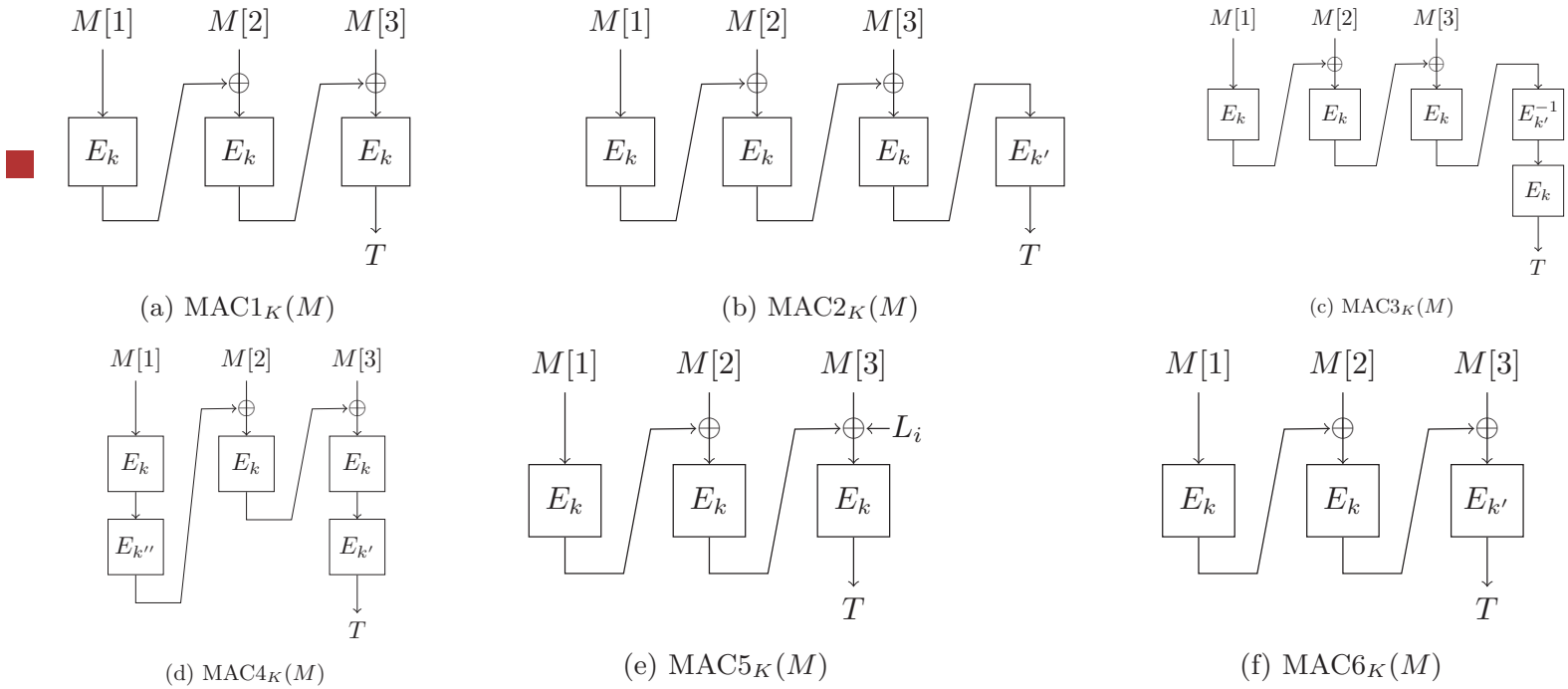
ISO/IEC 9797-1:2011

- ISO/IEC 9797-1:2011, an international standard for blockcipher-based MAC:

Reference number
ISO/IEC 9797-1:2011(E)

- Specifies 6 different variants of CBC MACs
- Provides with four padding schemes

ISO/IEC 9797-1:2011



(a) $\mathrm{MAC1}_K(M)$ (b) $\mathrm{MAC2}_K(M)$ (c) $\mathrm{MAC3}_K(M)$

(d) $\mathrm{MAC4}_K(M)$ (e) $\mathrm{MAC5}_K(M)$ (f) $\mathrm{MAC6}_K(M)$

Illustration of the ISO/IEC 9797-1:2011 MACs.

- Padding schemes:
  - **pad1**: $X \,\|\, 0^*$ (insecure)
  - **pad2**: $X \,\|\, 10^*$
  - **pad3**: $\mathrm{bin}_n(|X|) \,\|\, X \,\|\, 0^*$
  - **pad4**: X if $|X| \mod n = 0$, otherwise $X \,\|\, 10^*$ (only MAC5)

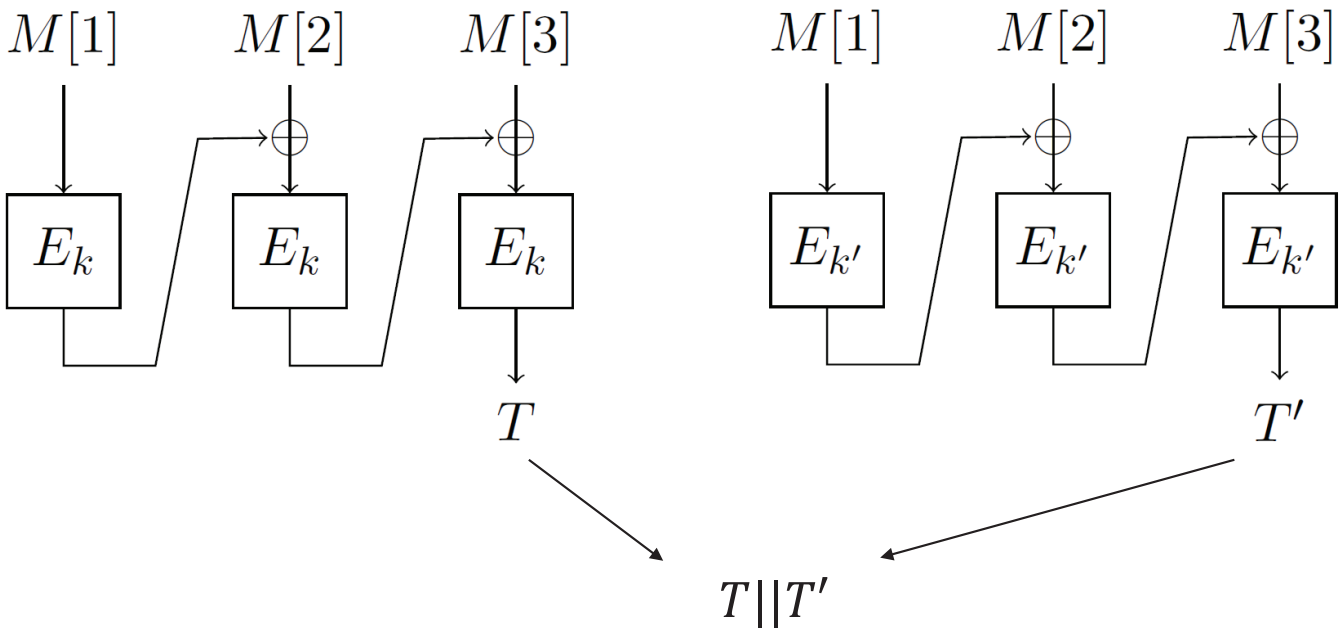
Birthday Bound Security

- Single-pass CBC-like MAC structures
  - suffer from birthday attacks [PvO95, PvO99]
  - capped at the birthday bound security
- Birthday-bound security is not always enough
  - lightweight blockciphers (HIGHT, PRESENT, PRINCE), TDES
  - $n = 64, 2^{n/2} = 2^{32}$ is somewhat small
  - two practical attacks exploit collision on short blockcipher [BL16]

ISO/IEC 9797-1:2011's Recommendation

- ISO/IEC 9797-1:2011 Annex C:

  if a MAC algorithm with a higher security level is needed, it is recommended to perform two MAC calculations with independent keys and concatenate the results (rather than XORing them).

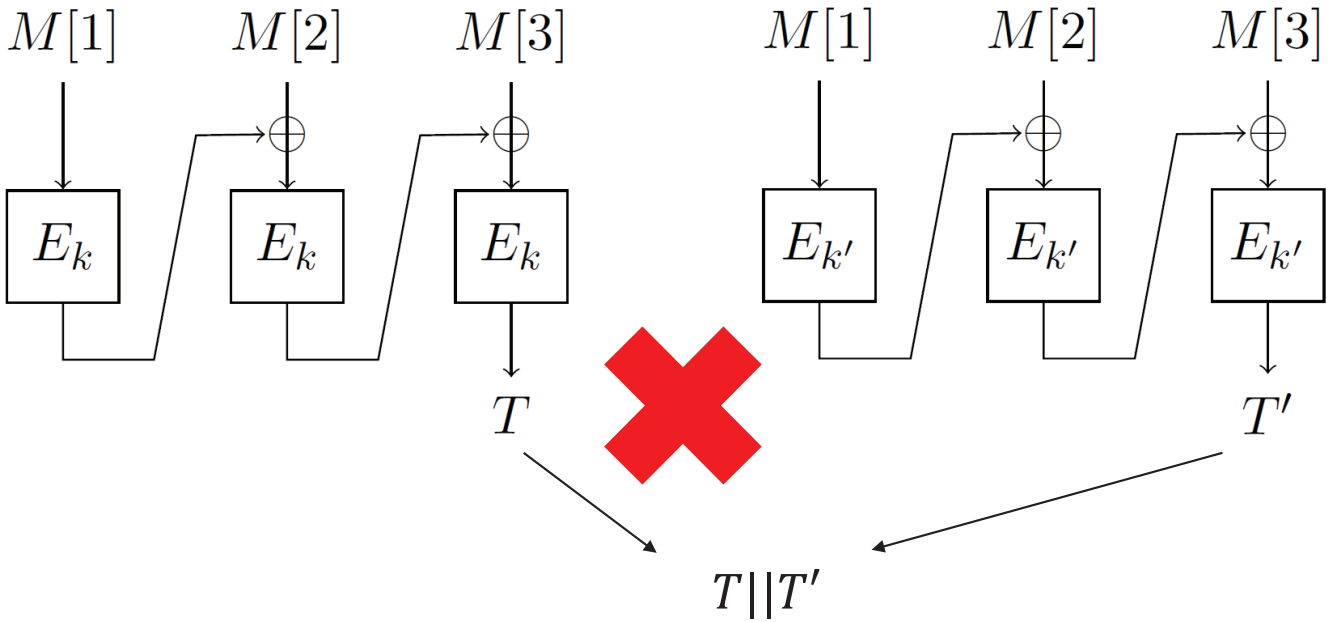


The concatenation combiner of two MACs

Outline

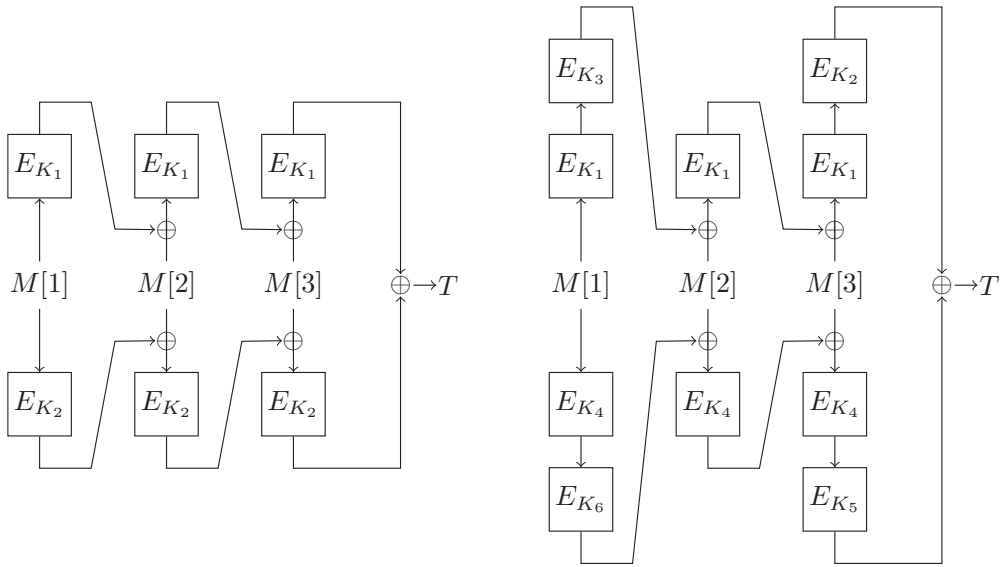
Forgery Attack on the Concatenation Combiner

- Our attacks:
  - birthday-bound forgery attack on the concatenation combiner of any two MACs in ISO/IEC 9797-1:2011
  - Notably, 3 queries attack on the concatenation combiner of two MAC algorithm 1 with $\mathbf{pad2}$
- Invalidate the suggestion in ISO/IEC 9797-1:2011
  - the concatenation combiner cannot be secure beyond birthday bound



Look for Patches

- Development of ISO/IEC 9797-1
  - ISO/IEC 9797-1:1999 used XOR combiner: $\mathtt{MAC}_5, \mathtt{MAC}_6$
  - Joux et al.'s [JPS03] birthday forgery on $\mathtt{MAC}_5$ with $\mathbf{pad2}$
  - Yasuda [Yas10] proved $\mathtt{MAC}_6$ achieves beyond-birthday-bound (BBB) security
  - Provable-security analysis is absent, for $\mathtt{MAC}_5$ with $\mathbf{pad3}$ or even with $\mathbf{pad2}$



$\mathtt{MAC}_5$ and $\mathtt{MAC}_6$ in ISO/IEC 9797-1:1999

Our Patches

- Revisit the impact of the XOR combiner of two MACs on ISO/IEC 9797-1:2011
  - XOR combiner of two $\mathrm{MAC1}$ ($\mathtt{MAC}_5$ in v1999) is BBB secure with $\mathbf{pad3}$
  - XOR combiner of two $\mathrm{MAC5}$ is BBB secure
  - XOR combiner of two $\mathrm{MAC1}$ is birthday-bound secure with $\mathbf{pad2}$ [1]

Algorithm	#keys	BBB	Ref
$\mathtt{MAC}_6$	6	✓	[Yas10]
SUM-ECBC	4	✓	[Yas10]
3kf9	3	✓	[ZWSW12]
XMAC1 with $\mathbf{pad3}$	2	✓	this paper
XMAC5	2	✓	this paper

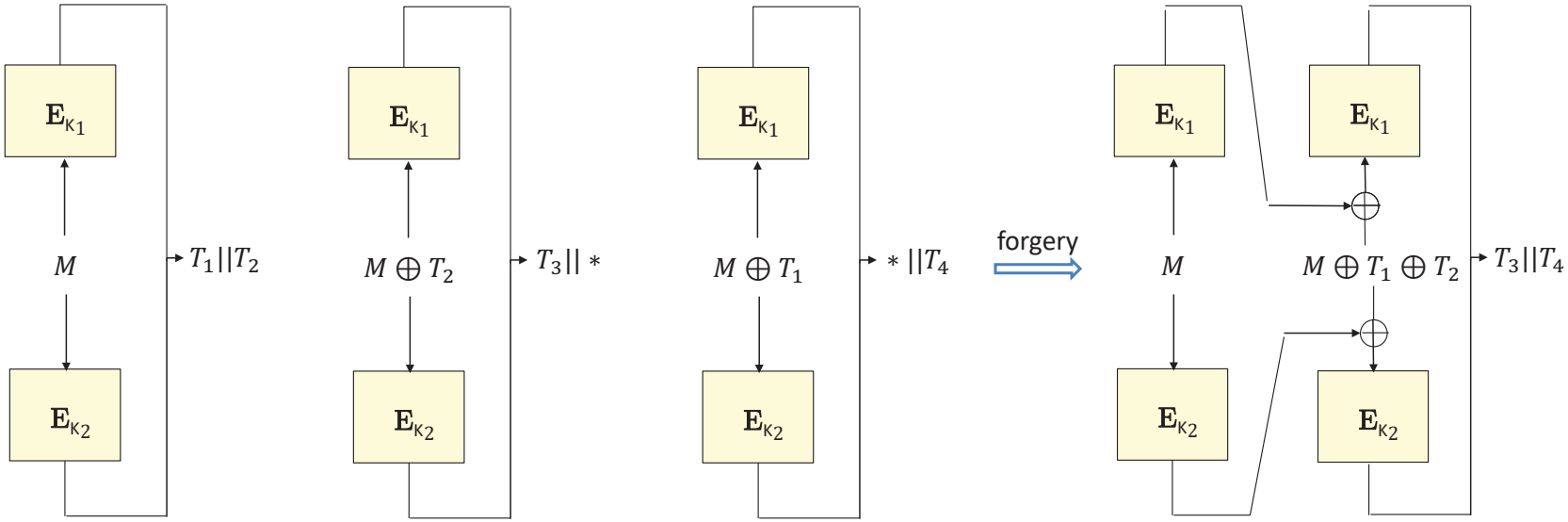
XMAC1, XMAC5 and other CBC-type MACs with BBB security

[1] Concatenation of two $\mathrm{MAC1}$ with $\mathbf{pad2}$ can be broken with just 3 queries

Outline

Attack on the Concatenation of two MAC1

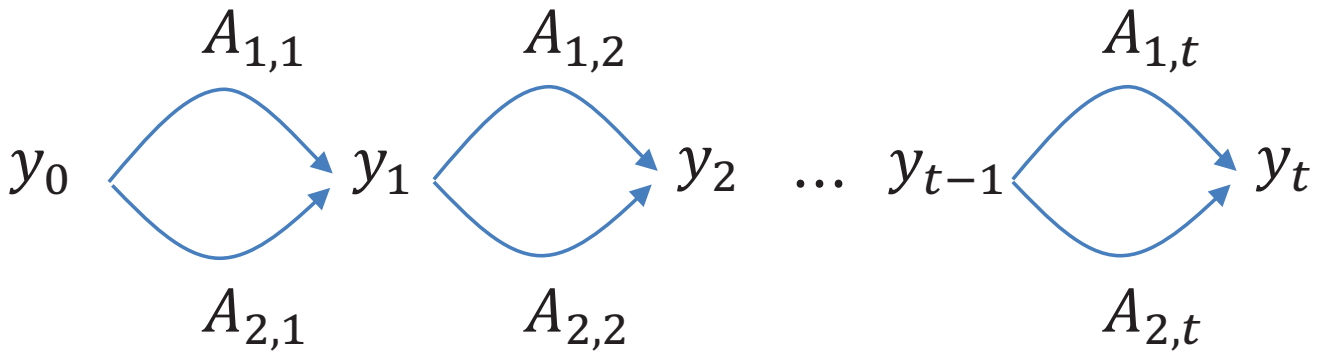
- $\mathrm{MAC1}_{K_1}(M) \,\|\, \mathrm{MAC1}_{K_2}(M)$ with **pad2** $(M \,\|\, 10^*)$
- Forgery attack:



- 3 queries, succeeds with probability 1

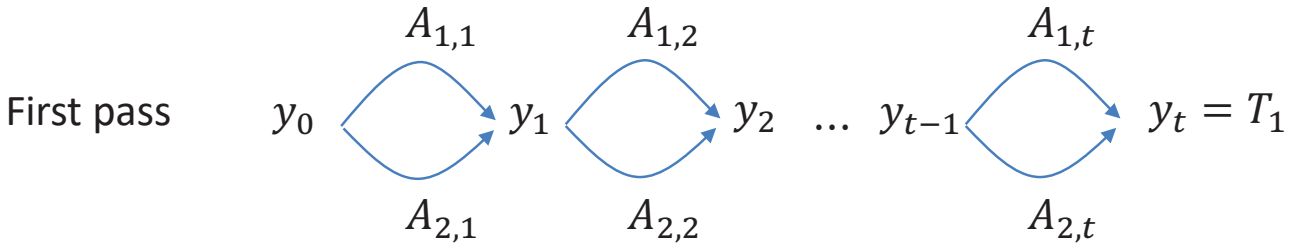
Attack on the Concatenation of any two MACs

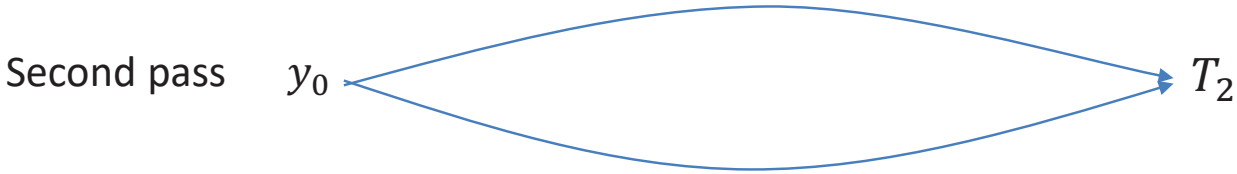
- $\mathrm{MAC}i_{K_1}(M) \,\|\, \mathrm{MAC}j_{K_2}(M)$ with $\mathbf{pad2}$ or $\mathbf{pad4}$
- Multi-collision attack for iterated hash function [Jou04]
  - if find one collision with complexity $2^{n/2}$, then
  - find 2^t messages colliding to one value with complexity $t2^{n/2}$



Attack on the Concatenation of any two MACs

- $\mathrm{MAC}i_{K_1}(M) \,\|\, \mathrm{MAC}j_{K_2}(M)$ with $\mathbf{pad2}$ or $\mathbf{pad4}$
- Our attack





- There exists a collision for the second pass among these 2^t messages $(t \geq n/2)$
- Complexity $O(n2^{n/2})$

Attack on the Concatenation of any two MACs

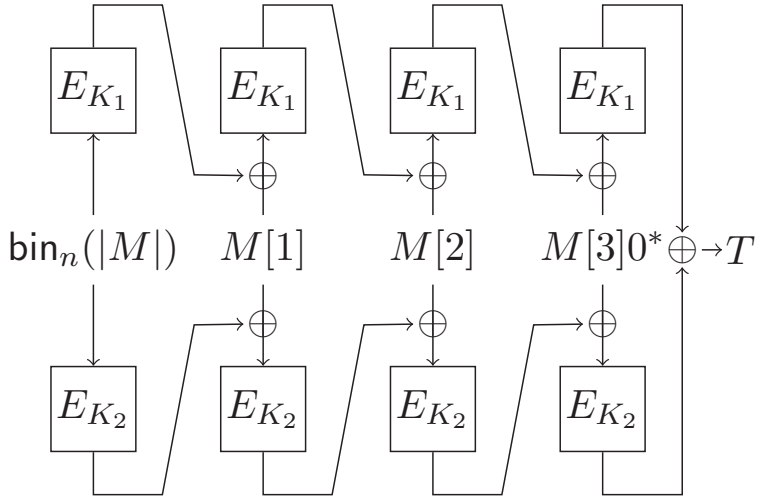
- $\mathrm{MAC}i_{K_1}(M) \,\|\, \mathrm{MAC}j_{K_2}(M)$ with $\mathbf{pad3}$
- $\mathbf{pad3}$: $\mathrm{bin}_n(|M|) \,\|\, M \,\|\, 0^*$, length padded at the first block
- Append zeros to each of 2^t messages to have the same bit-length ℓ

$$\begin{aligned} &\mathrm{MAC}i_{K_1}(|\ell|_n \,\|\, a_{1,1} \,\|\, r_{1,1} \,\|\, 0^n \,\|\, \ldots \,\|\, 0^n) \\ =\, &\mathrm{MAC}i_{K_1}(|\ell|_n \,\|\, a_{2,1} \,\|\, r_{2,1} \,\|\, 0^n \,\|\, \ldots \,\|\, 0^n) \end{aligned}$$

- The same procedure as before

Our Patches

- XOR combiner of two $\mathrm{MAC1}$ with $\mathbf{pad3}$



Theorem 1

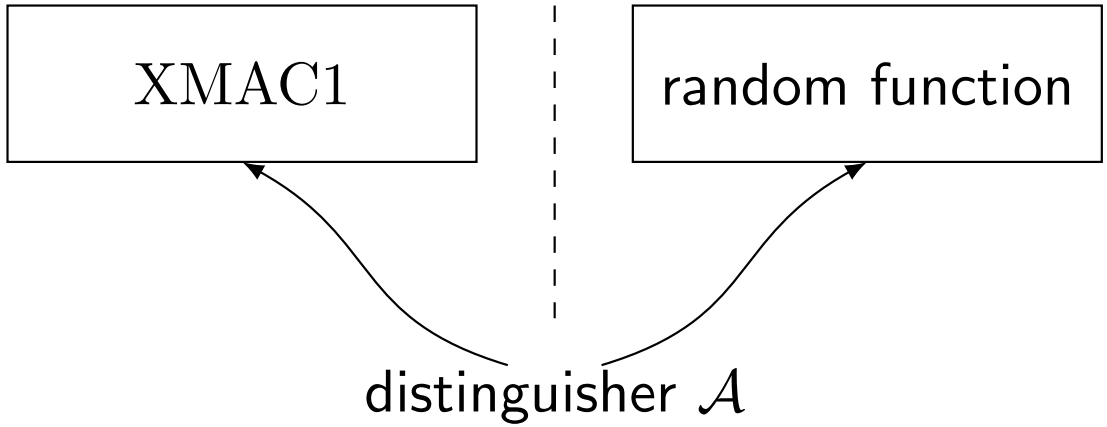
With $\mathbf{pad3}$*, one has*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{XMAC1}[E]}(\mathcal{A}) \leq \frac{844\sigma q^2 \ell}{2^{2n}} + \mathbf{Adv}^{\mathrm{prp}}_{E}(\mathcal{B}),$$

when $\ell \leq 2^{n/3}$*, where* q *is the number of queries,* ℓ *is the largest block length,* σ *is the total number of blocks.*

Proof Sketch

- Indistinguishability of two systems



- Game-playing technique by Bellare and Rogaway [BR06]
- Fundamental lemma of game-playing [BR06]

Let G_0 and G_1 be identical-until-bad games and let $\mathcal{A}$ be a distinguisher. Then

$$\mathbf{Adv}(\mathcal{A}^{G_0}, \mathcal{A}^{G_1}) \leq \Pr[\mathcal{A}^{G_1} \textit{ sets bad}]$$

Proof Sketch

- A framework by [Yas10] for SUM-ECBC

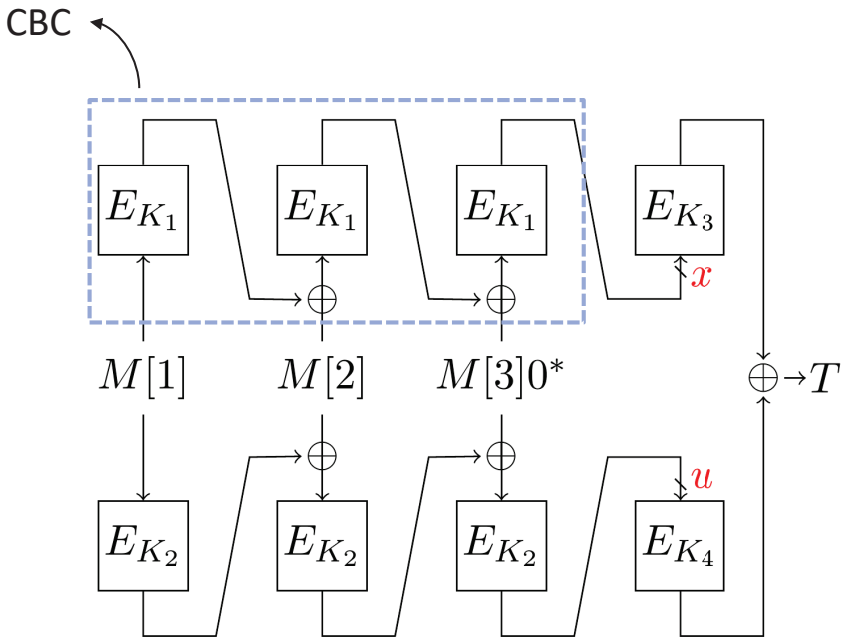


Illustration of SUM-ECBC

- Classify bad events according to whether the collision happens
  - neither x nor u collides with previous CBC outputs
  - only one of x and u collides with previous CBC outputs
  - both of x and u collide with previous CBC outputs

Proof Sketch

- Our proof for XMAC1

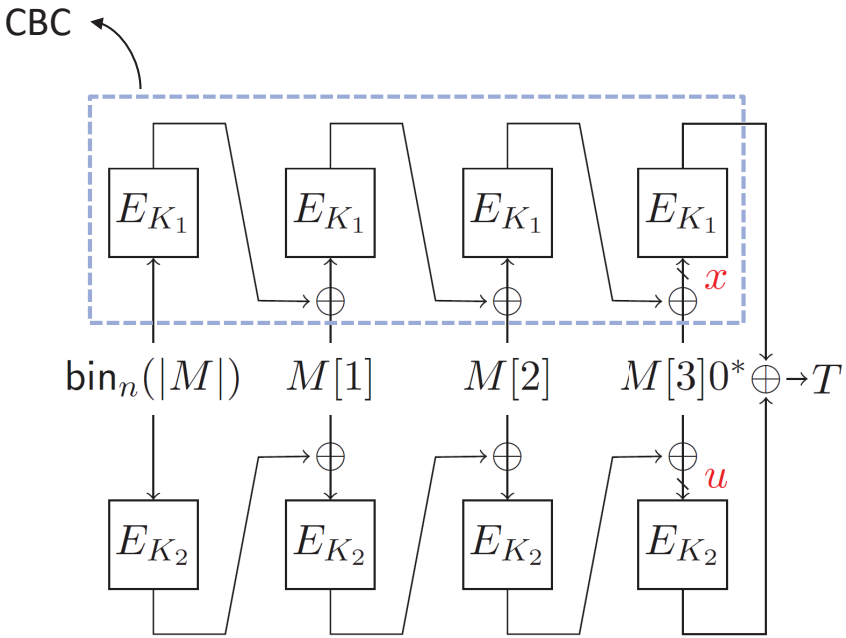
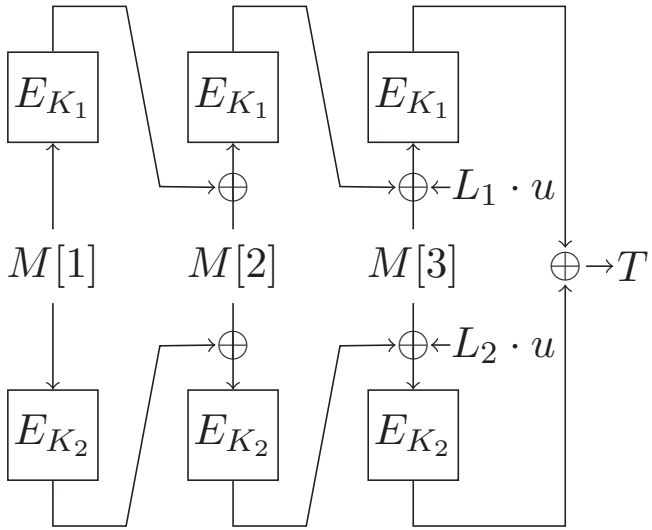


Illustration of XMAC1

- only use two keys instead of four keys
- analyze the impact of the last blockcipher call
- more involved internal collisions in CBC instead of only considering the outputs of CBC

Our Patches

- XOR combiner of two MAC5 (aka CMAC)



Theorem 2

For $\ell \leq 2^{n/3}$, one has

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{XMAC5}[E]}(\mathcal{A}) \leq \frac{4}{2^n} + \frac{58\sigma^2 q}{2^{2n}} + \frac{841\sigma q^2 \ell}{2^{2n}} + 2\mathbf{Adv}^{\mathrm{prp}}_{E}(\mathcal{B}),$$

where q is the number of queries, ℓ is the largest block length, σ is the total number of blocks.

Proof Sketch

- XMAC5 uses masks $L_1 = E_{K_1}(0^n)$ and $L_2 = E_{K_2}(0^n)$ to keep messages to be prefix-free

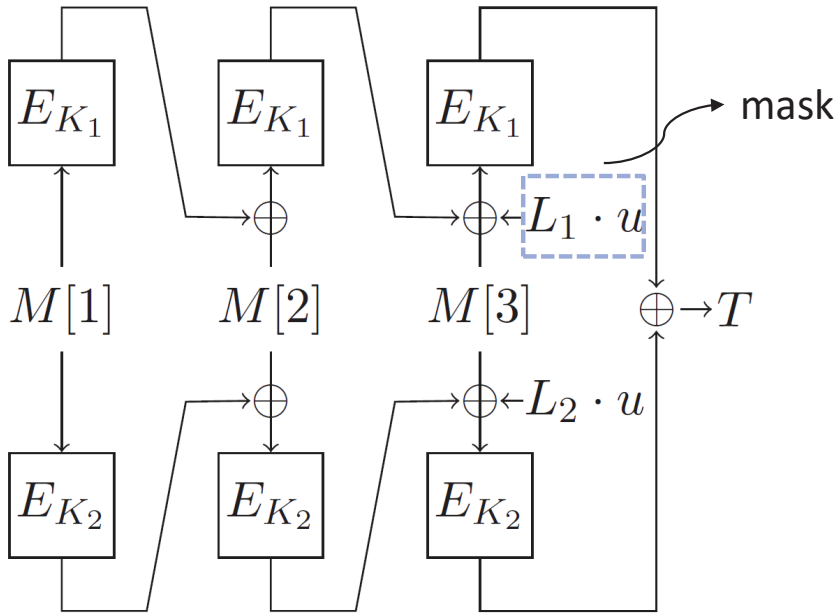


Illustration of XMAC5

- The proof for XMAC5 is similar to that for XMAC1, except to bound the probability when masks do not work

Outline

Conclusion

- Our attacks:
  - birthday-bound forgery attack on the concatenation combiner of any two MACs in ISO/IEC 9797-1:2011
  - 3 queries attack on the concatenation combiner of two MAC algorithm 1 with $\mathbf{pad2}$
- Invalidate the suggestion in ISO/IEC 9797-1:2011
  - the concatenation combiner cannot be beyond birthday bound (BBB) secure
- Our patches: the XOR combiner can be BBB secure
  - the XOR combiner of two $\mathrm{MAC1}$ is BBB secure with $\mathbf{pad3}$
  - the XOR combiner of two $\mathrm{MAC5}$ is BBB secure

Thanks for your attention!