Impact of ANSI X9.24-1:2009 Key Check Value on ISO/IEC 9797-1:2011 MACs

Tetsu Iwata, Nagoya University
Lei Wang, Nanyang Technological University

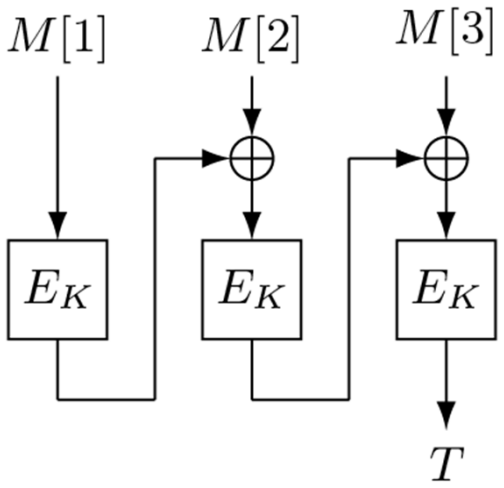
FSE 2014
March 4, 2014, London, UK

Overview

- ANSI X9.24-1:2009, Annex C specifies “the key check value”
- ISO/IEC 9797-1:2011, Annex C specifies a total of ten variants of CBC MAC
- We derive the quantitative impact of using the key check value on the security of ISO/IEC 9797-1:2011 CBC MACs

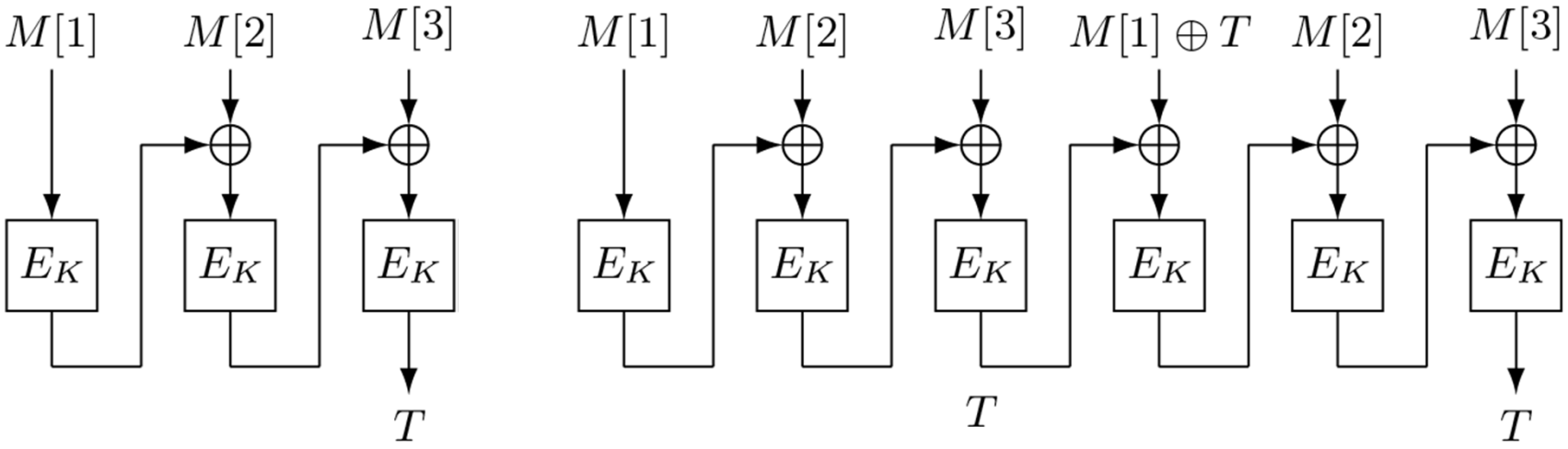
CBC MAC

- M = (M[1], M[2], . . . , M[m]): input message, T: tag
- Fixed-Input-Length PRF if E is a PRP [BKR ’94, BPR ’05]
  - Provably implies that it is a secure MAC (over fixed-length messages)
- It allows forgery attacks for variable-length messages



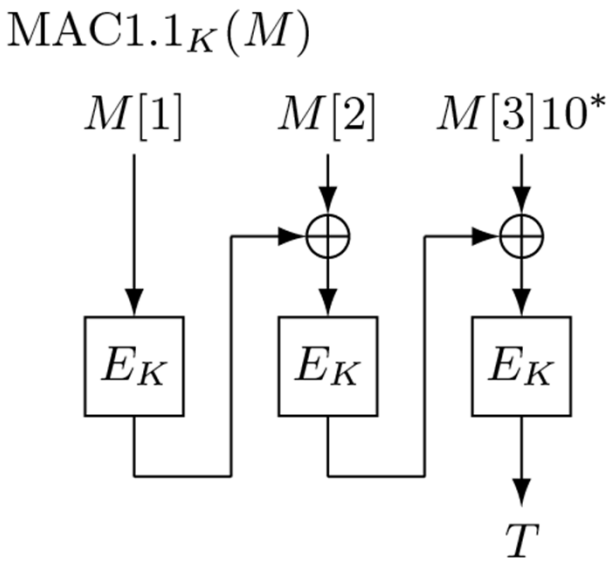
Length-Extension Attack on CBC MAC

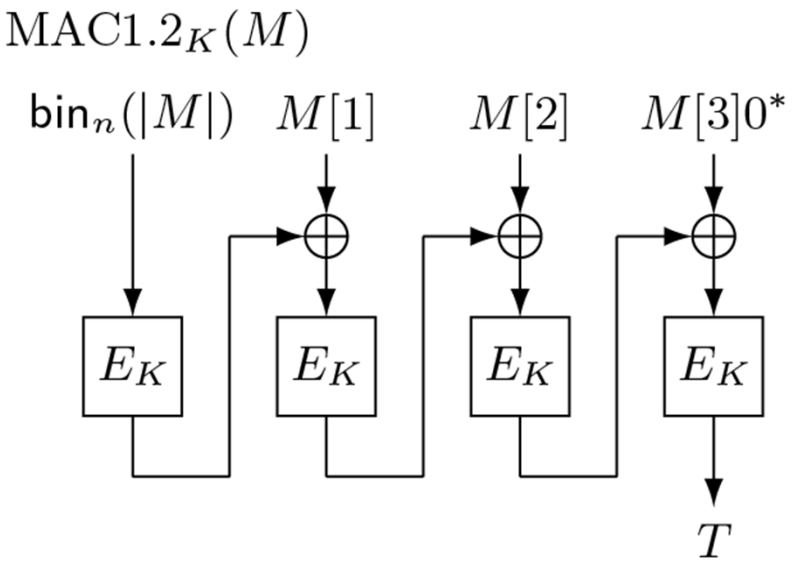
- Given (M[1], M[2], M[3]) and T,
  (M[1], M[2], M[3], M[1] xor T, M[2], M[3]) and T
  is a valid (message, tag) pair



CBC MAC Variants in ISO/IEC 9797-1:2011

- MAC1.1 -- basic CBC MAC
- MAC1.2 -- CBC MAC w/ prefix-free padding

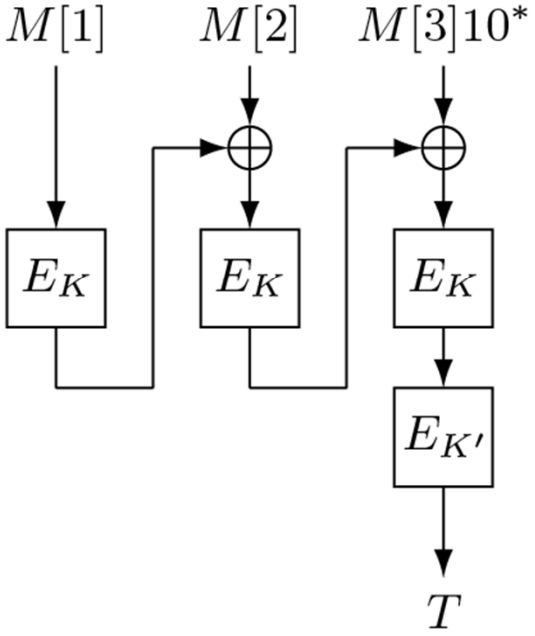




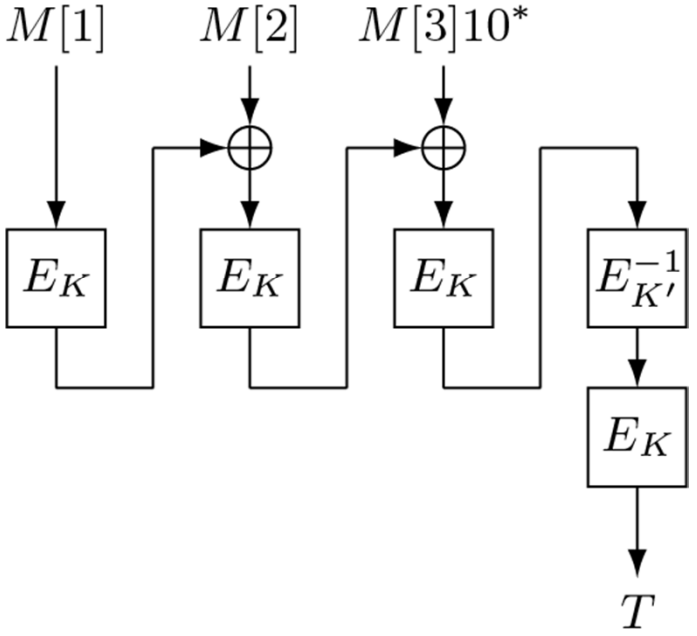
CBC MAC Variants in ISO/IEC 9797-1:2011

- MAC2.1 -- EMAC w/ a related key, K’ = K xor 0xf0f0 . . . f0
- MAC2.2 -- EMAC w/ two independent keys
- MAC3 -- ANSI retail MAC, two independent keys

$\mathrm{MAC2.1}_K(M)/\mathrm{MAC2.2}_{K,K'}(M)$

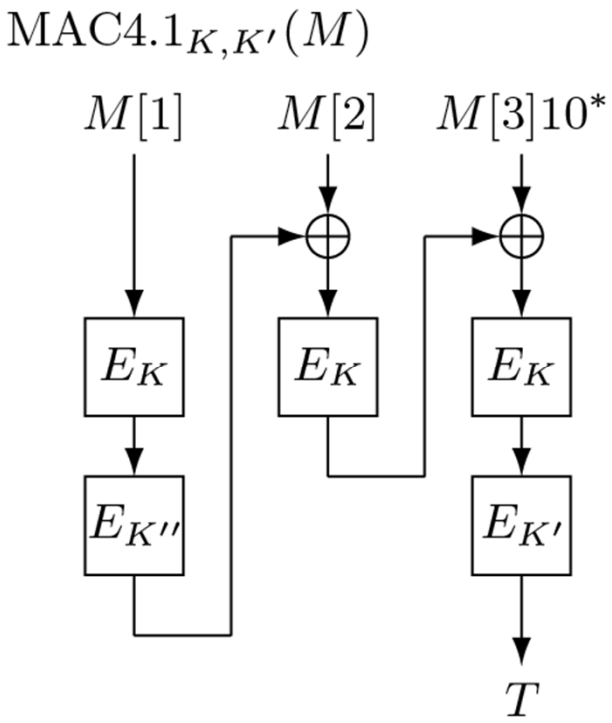


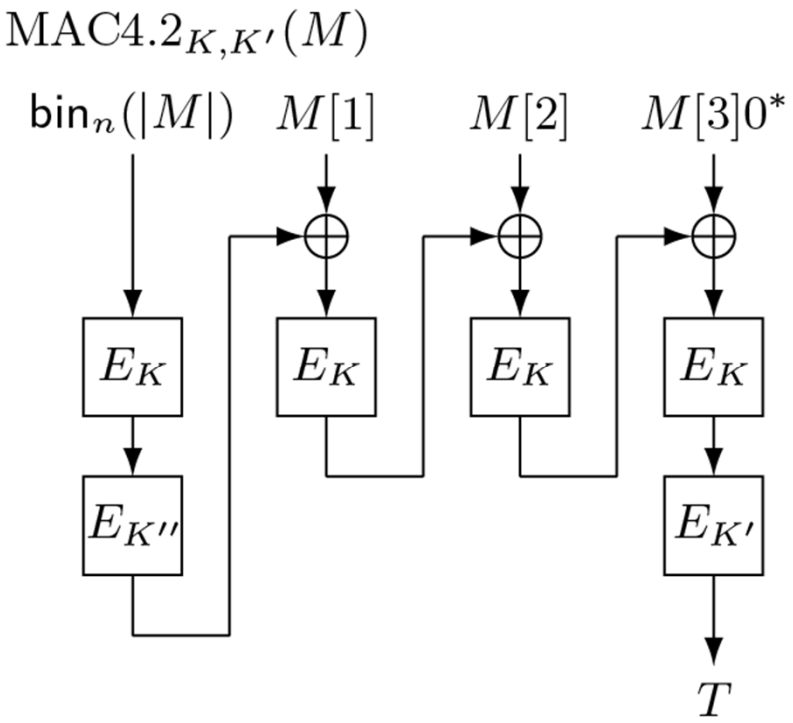
$\mathrm{MAC3}_{K,K'}(M)$



CBC MAC Variants in ISO/IEC 9797-1:2011

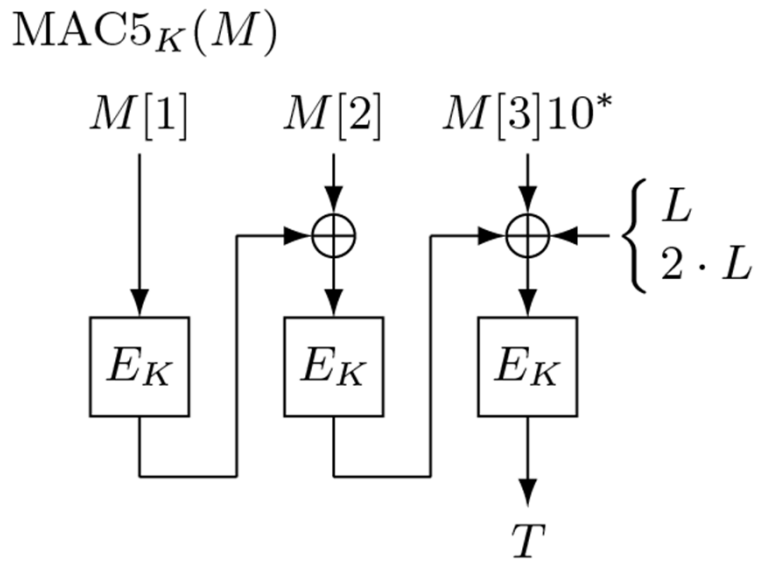
- MAC4.1 -- MacDES, K'' = K' xor 0xf0f0 . . . f0
- MAC4.2 -- MacDES w/ the same K'' and prefix-free padding
  - K and K' are two independent keys





CBC MAC Variants in ISO/IEC 9797-1:2011

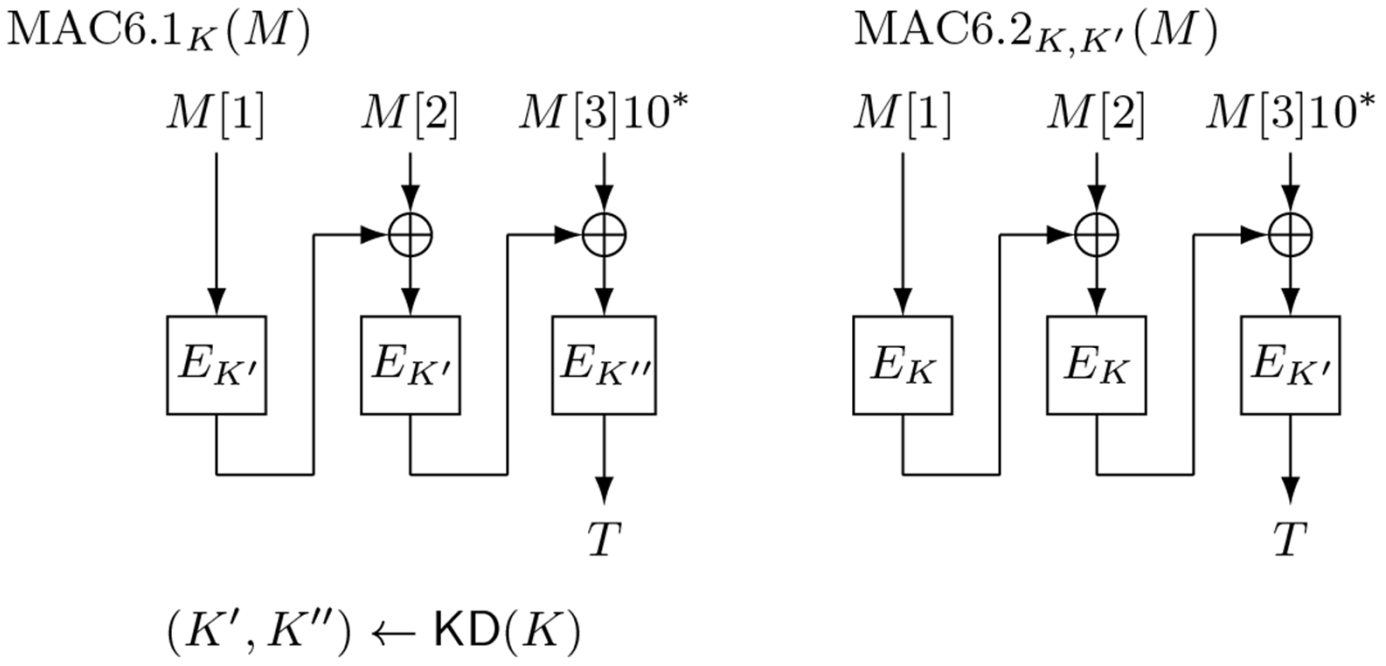
- MAC5 -- CMAC



$L \leftarrow 2 \cdot E_K(0^n)$

CBC MAC Variants in ISO/IEC 9797-1:2011

- MAC6.1 -- FCBC w/ a key derivation function
- MAC6.2 -- FCBC w/ two independent keys

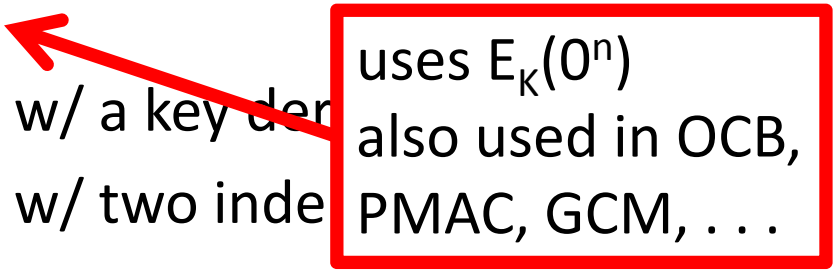


CBC MAC Variants in ISO/IEC 9797-1:2011

- MAC1.1 -- a basic CBC MAC
- MAC1.2 -- CBC MAC w/ prefix-free padding
- MAC2.1 -- EMAC w/ a related key, K’ = K xor 0xf0f0 . . . f0
- MAC2.2 -- EMAC w/ two independent keys
- MAC3 -- ANSI retail MAC
- MAC4.1 -- MacDES, K’’ = K’ xor 0xf0f0 . . . f0
- MAC4.2 -- MacDES w/ the same K’’ and prefix-free padding
- MAC5 -- CMAC
- MAC6.1 -- FCBC w/ a key derivation function
- MAC6.2 -- FCBC w/ two independent keys

CBC MAC Variants in ISO/IEC 9797-1:2011

- MAC1.1 -- a basic CBC MAC
- MAC1.2 -- CBC MAC w/ prefix-free padding
- MAC2.1 -- EMAC w/ a related key, K’ = K xor 0xf0f0 . . . f0
- MAC2.2 -- EMAC w/ two independent keys
- MAC3 -- ANSI retail MAC
- MAC4.1 -- MacDES, K’’ = K’ xor 0xf0f0 . . . f0
- MAC4.2 -- MacDES w/ the same K’’ and prefix-free padding
- MAC5 -- CMAC
- MAC6.1 -- FCBC w/ a key der
- MAC6.2 -- FCBC w/ two inde



ANSI X9.24-1:2009

- “Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques”
- specifies the management of keying material used for financial services
  - POS transactions, transactions in banking systems, . . .

Key Check Value

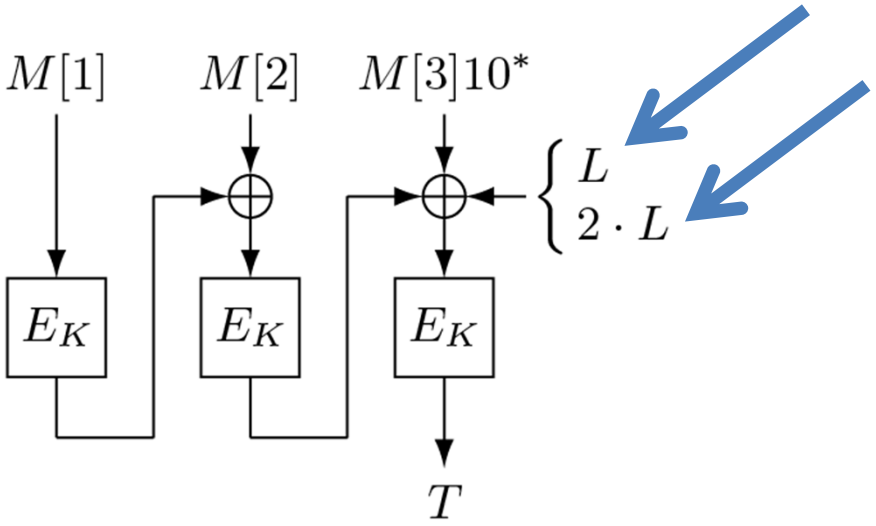
- ANSI X9.24-1:2009, Annex C:
- “The optional check values, as mentioned in notes 2 and 3 above, are the left-most six hexadecimal digits from the ciphertext produced by using the DEA in ECB mode to encrypt to 64-bit binary zero value with the subject key or key component. The check value process may be simplified operationally, while still retaining reliability, by limiting the check value to the left-most four or six hexadecimal digits of the ciphertext. (Using the truncated check value may provide additional security in that the ciphertext which could be used for exhaustive key determination would be unavailable.)”

Key Check Value

- KCV = msb(s, $E_K(0^n)$)
- s = 16 or 24 (for n = 64), defined only for DES and Triple-DES
- used as the ID for the key K in financial services
- inherently public data, as it is used for verification
  - transmitted, sent, or stored in clear
  - the adversary may learn this value
  - special case of leakage of the internal state
- CMAC uses $E_K(0^n)$
- CMAC has a proof of security, but the proof does not take KCV into account
- What is the impact on the security of the use of KCV?

Case s = n, MAC5 (CMAC)

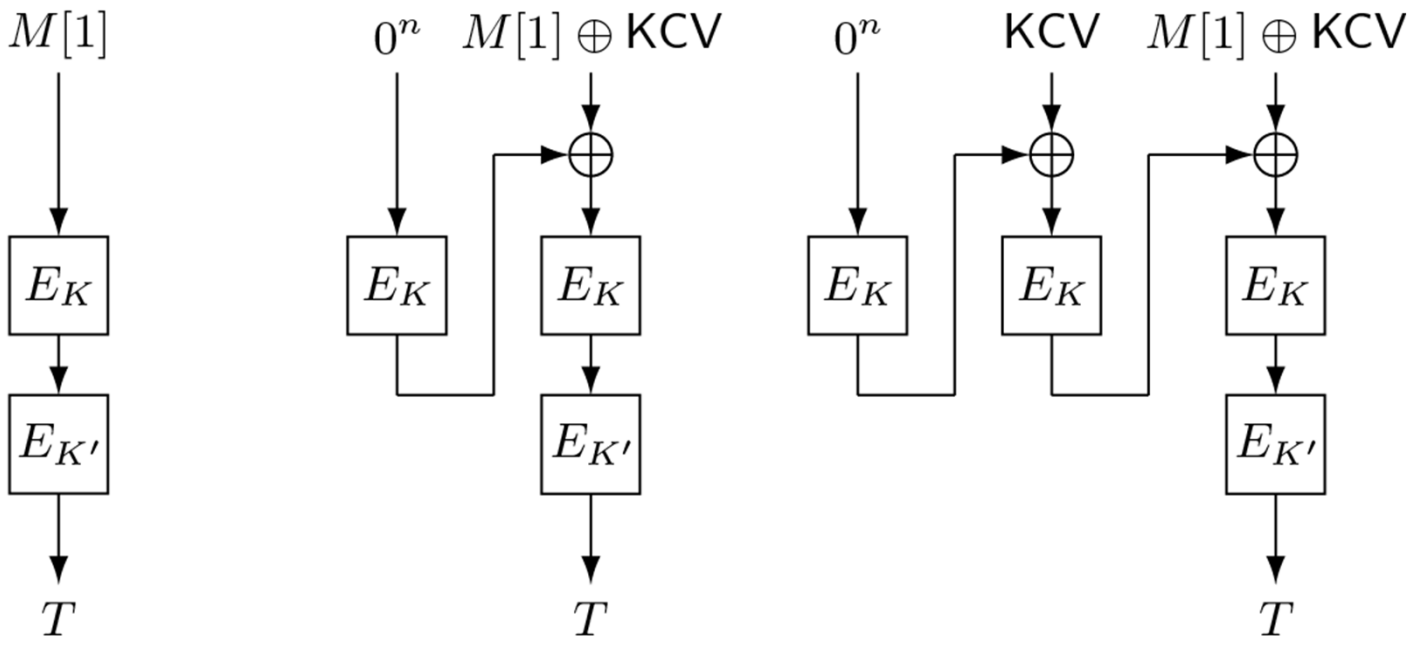
- KCV = msb(s, $E_K(0^n)$)
- $E_K(0^n)$ is known, then $L = 2 \cdot E_K(0^n)$ and $2 \cdot L$ are known
- reduces to CBC MAC
- length-extension attack



$$L \leftarrow 2 \cdot E_K(0^n)$$

Case s = n, MAC2.1 (EMAC)

- K is the key, K’ = K xor 0xf0f0 . . . f0
  - KCV = $E_K(0^n)$

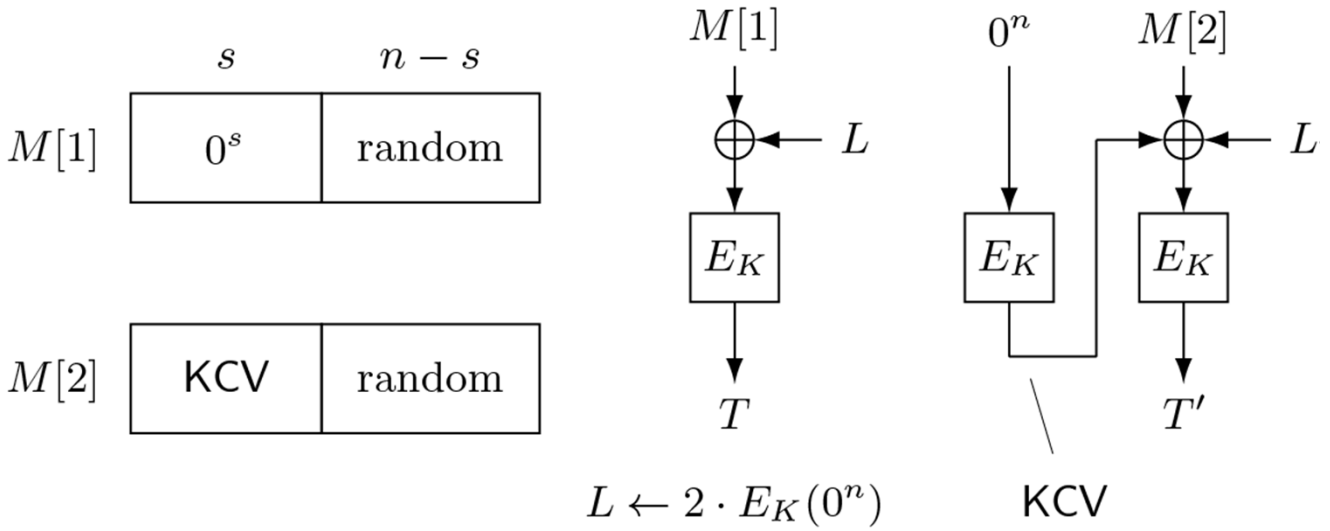


Case s < n, MAC5 (CMAC)

- Trivial attack:
  - guess the missing n-s bits of $E_K(0^n)$ and try the length-extension attack
  - Pr[success] = $1/2^{n-s}$

Case s < n, MAC5 (CMAC)

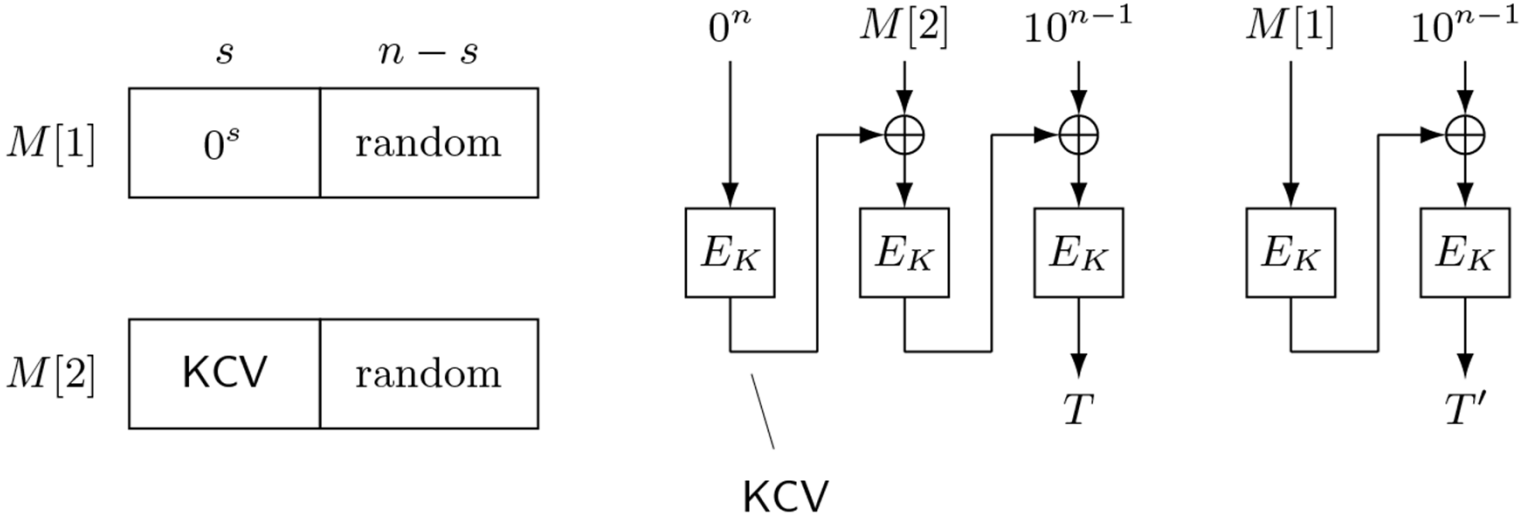
- Birthday attack, similar to [Knudsen, ’97]



- ask $2^{(n-s)/2}$ different M[1]’s and $2^{(n-s)/2}$ different (0^n, M[2])’s
  - with a high probability, T = T’
- distinguishing attack with $O(2^{(n-s)/2})$ queries
- $E_K(0^n)$ (= M[1] xor M[2]) is known, length-extension attack

Case s < n, MAC2.1 (EMAC)

- The same attack can be used



- ask $2^{(n-s)/2}$ different M[1]'s and $2^{(n-s)/2}$ different (0^n, M[2])'s
  - with a high probability, T = T'
- distinguishing attack with $O(2^{(n-s)/2})$ queries
- $E_K(0^n)$ (= M[1] xor M[2]) is known, forgery attack

CBC MAC Variants in ISO/IEC 9797-1:2011

- MAC1.1 O(1): folklore
- MAC1.2
- MAC2.1 $O(2^{(n-s)/2})$
- MAC2.2
- MAC3
- MAC4.1
- MAC4.2
- MAC5 $O(2^{(n-s)/2})$
- MAC6.1
- MAC6.2

CBC MAC Variants in ISO/IEC 9797-1:2011

- MAC1.1 $O(1)$: folklore
- MAC1.2
- MAC2.1 $O(2^{(n-s)/2})$
- MAC2.2 $O(2^{(n-s)/2})$ 
- MAC3 $O(2^{(n-s)/2})$ 
- MAC4.1
- MAC4.2
- MAC5 $O(2^{(n-s)/2})$
- MAC6.1
- MAC6.2 $O(2^{(n-s)/2})$ 

- The same attack applies

CBC MAC Variants in ISO/IEC 9797-1:2011

- MAC1.1 $O(1)$: folklore
- MAC1.2 $O(2^{n/2})$ ←
- MAC2.1 $O(2^{(n-s)/2})$
- MAC2.2 $O(2^{(n-s)/2})$
- MAC3 $O(2^{(n-s)/2})$
- MAC4.1 $O(2^{n/2})$ ←
- MAC4.2 $O(2^{n/2})$ ←
- MAC5 $O(2^{(n-s)/2})$
- MAC6.1 $O(2^{n/2})$ ←
- MAC6.2 $O(2^{(n-s)/2})$

- Attacks with the birthday complexity are known [ISO/IEC 9797-1, PO99]

CBC MAC Variants in ISO/IEC 9797-1:2011

- MAC1.1 $O(1)$: folklore
- MAC1.2 $O(2^{n/2})$
- MAC2.1 $O(2^{(n-s)/2})$
- MAC2.2 $O(2^{(n-s)/2})$
- MAC3 $O(2^{(n-s)/2})$
- MAC4.1 $O(2^{n/2})$
- MAC4.2 $O(2^{n/2})$
- MAC5 $O(2^{(n-s)/2})$
- MAC6.1 $O(2^{n/2})$
- MAC6.2 $O(2^{(n-s)/2})$

- Can we improve these attacks?

CBC MAC Variants in ISO/IEC 9797-1:2011

- MAC1.1 $O(1)$: folklore
- MAC1.2 $O(2^{n/2})$
- MAC2.1 $O(2^{(n-s)/2})$
- MAC2.2 $O(2^{(n-s)/2})$
- MAC3 $O(2^{(n-s)/2})$
- MAC4.1 $O(2^{n/2})$
- MAC4.2 $O(2^{n/2})$
- MAC5 $O(2^{(n-s)/2})$
- MAC6.1 $O(2^{n/2})$
- MAC6.2 $O(2^{(n-s)/2})$

- Can we improve these attacks?

  No, we cannot

Provable Security Results

- PRF-KCV: a variant of PRF notion that captures KCV
  - The adversary is given KCV
  - Then the adversary is asked to distinguish between the MAC oracle and the random oracle
- Let $M_{K1, \ldots, Kw}$ be a MAC based on E: $\{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$
  - the key space is $(\{0,1\}^k)^w$ for some integer $w > 0$, and uses $(K_1, \ldots, K_w)$ as a key
  - KCV = $(\text{msb}(s, E_{K1}(0^n)), \ldots, \text{msb}(s, E_{Kw}(0^n)))$

$$\mathbf{Adv}_{\mathcal{M}}^{\text{prf-kcv}}(\mathcal{A}) = \Pr\left[\mathcal{A} \leftarrow \text{KCV}, \mathcal{A}^{\mathcal{M}_{K_1,\ldots,K_w}(\cdot)} \Rightarrow 1\right] - \Pr\left[\mathcal{A} \leftarrow \text{KCV}, \mathcal{A}^{\mathcal{R}(\cdot)} \Rightarrow 1\right]$$

Theorem

Theorem 1. *Fix t, q, and σ, where $q, \sigma \geq 1$. Then the following bounds hold.*

$$\mathbf{Adv}^{\text{prf-kcv}}_{\text{MAC1.2}[E]}(t,q,\sigma) \leq \mathbf{Adv}^{\text{prp}}_{E}(t',\sigma+1) + n/2^{n/2} + 7.5\sigma^2/2^n,$$

$$\mathbf{Adv}^{\text{prf-kcv}}_{\text{MAC2.1}[E]}(t,q,\sigma) \leq \mathbf{Adv}^{\text{prp-rka}}_{E}(t',q+\sigma+1) + 3.5\sigma^2/2^{n-s},$$

$$\mathbf{Adv}^{\text{prf-kcv}}_{\text{MAC2.2}[E]}(t,q,\sigma) \leq 2\mathbf{Adv}^{\text{prp}}_{E}(t',\sigma+1) + 8\sigma^2/2^{n-s},$$

$$\mathbf{Adv}^{\text{prf-kcv}}_{\text{MAC3}[E]}(t,q,\sigma) \leq 2\mathbf{Adv}^{\text{sprp}}_{E}(t',q+\sigma+1) + 23.5\sigma^2/2^{n-s},$$

$$\mathbf{Adv}^{\text{prf-kcv}}_{\text{MAC4.1}[E]}(t,q,\sigma) \leq 2\mathbf{Adv}^{\text{prp-rka}}_{E}(t',2\sigma+1) + 11.5\sigma^2/2^n,$$

$$\mathbf{Adv}^{\text{prf-kcv}}_{\text{MAC4.2}[E]}(t,q,\sigma) \leq 2\mathbf{Adv}^{\text{prp-rka}}_{E}(t',2\sigma+1) + 11.5\sigma^2/2^n,$$

$$\mathbf{Adv}^{\text{prf-kcv}}_{\text{MAC5}[E]}(t,q,\sigma) \leq \mathbf{Adv}^{\text{prp}}_{E}(t',\sigma+1) + 5\sigma^2/2^{n-s},$$

$$\mathbf{Adv}^{\text{prf-kcv}}_{\text{MAC6.1}[E]}(t,q,\sigma) \leq 2\mathbf{Adv}^{\text{prp}}_{E}(t',\sigma+1) + \mathbf{Adv}^{\text{prp}}_{E}(t'',2\ell+1) + 8\sigma^2/2^n + 4.5\ell^2/2^n,$$

$$\mathbf{Adv}^{\text{prf-kcv}}_{\text{MAC6.2}[E]}(t,q,\sigma) \leq 2\mathbf{Adv}^{\text{prp}}_{E}(t',\sigma+1) + 8\sigma^2/2^{n-s},$$

where $t' = t + O(\sigma)$, $t'' = t + O(\ell+\sigma)$, and $\ell = \lceil k/n \rceil$.

Theorem

MAC	attack	bound	assumption
MAC1.2	$O(2^{n/2})$	$O(\sigma^2/2^n)$	PRP
MAC2.1	$O(2^{(n-s)/2})$	$O(\sigma^2/2^{n-s})$	PRP-RKA
MAC2.2	$O(2^{(n-s)/2})$	$O(\sigma^2/2^{n-s})$	PRP
MAC3	$O(2^{(n-s)/2})$	$O(\sigma^2/2^{n-s})$	SPRP
MAC4.1	$O(2^{n/2})$	$O(\sigma^2/2^n)$	PRP-RKA
MAC4.2	$O(2^{n/2})$	$O(\sigma^2/2^n)$	PRP-RKA
MAC5	$O(2^{(n-s)/2})$	$O(\sigma^2/2^{n-s})$	PRP
MAC6.1	$O(2^{n/2})$	$O(\sigma^2/2^n)$	PRP
MAC6.2	$O(2^{(n-s)/2})$	$O(\sigma^2/2^{n-s})$	PRP

Theorem

MAC	attack	bound	assumption
MAC1.2	$O(2^{n/2})$	$O(\sigma^2/2^n)$	PRP
MAC2.1	$O(2^{(n-s)/2})$	$O(\sigma^2/2^{n-s})$	PRP-RKA
MAC2.2	$O(2^{(n-s)/2})$	$O(\sigma^2/2^{n-s})$	PRP
MAC3	$O(2^{(n-s)/2})$	$O(\sigma^2/2^{n-s})$	SPRP
MAC4.1	$O(2^{n/2})$	$O(\sigma^2/2^n)$	PRP-RKA
MAC4.2	$O(2^{n/2})$	$O(\sigma^2/2^n)$	PRP-RKA
MAC5	$O(2^{(n-s)/2})$	$O(\sigma^2/2^{n-s})$	PRP
MAC6.1	$O(2^{n/2})$	$O(\sigma^2/2^n)$	PRP
MAC6.2	$O(2^{(n-s)/2})$	$O(\sigma^2/2^{n-s})$	PRP

- obtained a complete quantitative characterization of using KCV on ISO/IEC 9797-1:2011 MACs

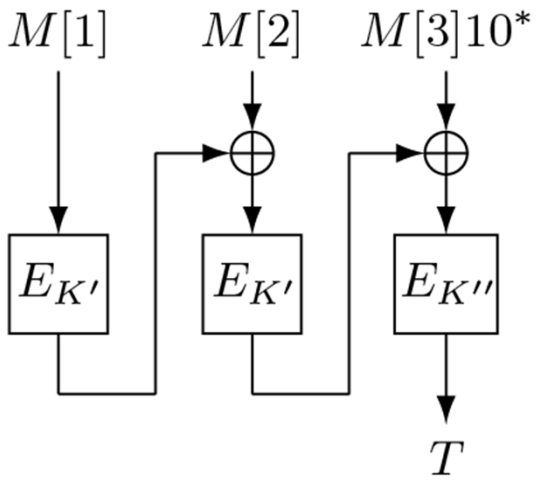
Theorem

MAC	attack	bound	assumption
MAC1.2	$O(2^{n/2})$	$O(\sigma^2/2^n)$	PRP
MAC2.1	$O(2^{(n-s)/2})$	$O(\sigma^2/2^{n-s})$	PRP-RKA
MAC2.2	$O(2^{(n-s)/2})$	$O(\sigma^2/2^{n-s})$	PRP
MAC3	$O(2^{(n-s)/2})$	$O(\sigma^2/2^{n-s})$	SPRP
MAC4.1	$O(2^{n/2})$	$O(\sigma^2/2^n)$	PRP-RKA
MAC4.2	$O(2^{n/2})$	$O(\sigma^2/2^n)$	PRP-RKA
MAC5	$O(2^{(n-s)/2})$	$O(\sigma^2/2^{n-s})$	PRP
MAC6.1	$O(2^{n/2})$	$O(\sigma^2/2^n)$	PRP
MAC6.2	$O(2^{(n-s)/2})$	$O(\sigma^2/2^{n-s})$	PRP

- obtained a complete quantitative characterization of using KCV on ISO/IEC 9797-1:2011 MACs

Example: MAC6.1

- FCBC w/ a key derivation function
- KCV = msb(s, $E_K(0^n)$)
- (K', K'') <- KD(K)
  - when k = n, K' = $E_K(0^{n-1}1)$ and K'' = $E_K(0^{n-2}10)$
  - KCV, K', and K'' are random and independent if E is a PRP



Implication

- The use of KCV in these MACs does not result in “total security loss”
- security is lost by s/2 bits in some cases, and there is almost no security loss in other cases
- The impact is limited in practice if s is not large
  - say 16 bits or 24 bits as suggested in ANSI X9.24-1:2009

Implication

- for n = 64,
  - if s = 0, then the best attack needs 2^{32}
  - if s = 16 2^{24}
  - if s = 24 2^{20}
- for n = 128 (not defined in ANSI X9.24, Annex C),
  - if s = 0, then the best attack needs 2^{64}
  - if s = 16 2^{56}
  - if s = 24 2^{52}
  - if s = 32 2^{48}
  - if s = 48 2^{40}
- can still be used in practice (depending on applications)

Possible Fixes

- Option 1: Always use the key derivation function of MAC6.1
  - even if the MAC uses one key
  - KCV = msb(s, $E_K(0^n)$)
  - K’ <- KD(K), when k = n, K’ = $E_K(0^{n-1}1)$
  - use K’ in the MAC computation
  - KCV and K’ are random and independent if E is a PRP

Possible Fixes

- Option 1: Always use the key derivation function of MAC6.1
  - even if the MAC uses one key
  - KCV = msb(s, $E_K(0^n)$)
  - K' <- KD(K), when k = n, K' = $E_K(0^{n-1}1)$
  - use K' in the MAC computation
  - KCV and K' are random and independent if E is a PRP
- Two more options in the paper
  - based on the theory of a tweakable blockcipher
  - removes the key scheduling process

Conclusions

- We analyzed the impact of using the key check value on the security of ISO/IEC 9797-1:2011 CBC MACs
  - obtained a complete quantitative characterization
  - the impact is limited in practice (if s is not very large)
  - suggested possible fixes
- In general, KCV affects the security of blockcipher modes
  - Question: impact on other modes?
    - OCB, PMAC, GCM, and MAC5 and MAC6 in older version of ISO/IEC 9797-1: 1999