Revisiting the Security of DbHtS MACs: Beyond-Birthday-Bound in the Multi-User Setting

Yaobin Shen[1], Lei Wang[1], Dawu Gu[1], and Jian Weng[2]

[1]Shanghai Jiao Tong University

[2]Jinan University

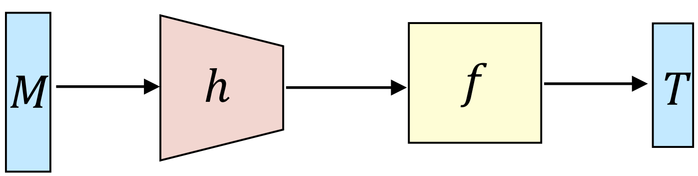
CRYPTO 2021

August 19, 2021

Contents

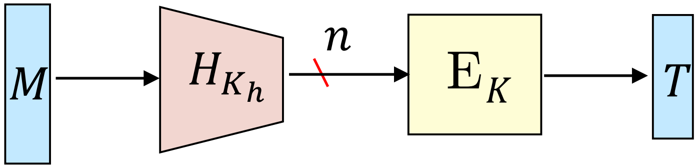
Message Authentication Code

- MAC: ensure integrity and authenticity of messages
- Two ways to build a MAC
  - using a blockcipher (CBC-MAC, OMAC, LightMAC)
  - using a hash function (HMAC, NMAC, NI-MAC)
- Following the Hash-then-PRF paradigm



Birthday Bound Security

- Hash-then-PRF

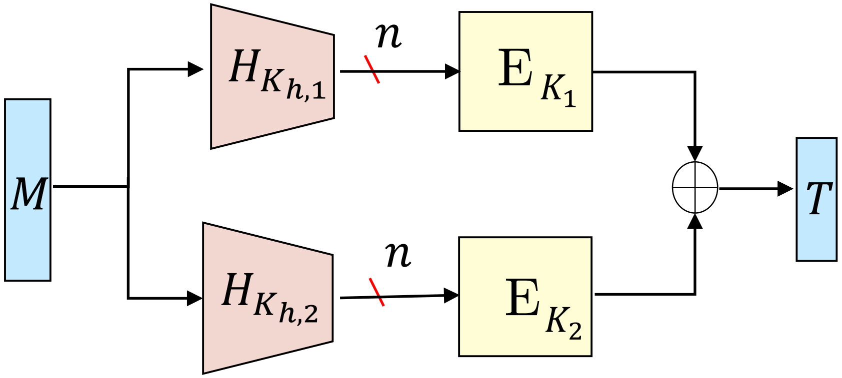


  - $H_{K_h}(M_1) = H_{K_h}(M_2) \Rightarrow T_1 = T_2$
  - Birthday-bound security $O(2^{\frac{n}{2}})$
- Birthday-bound security is not always enough
  - lightweight blockciphers (HIGHT, PRESENT, GIFT), or TDES
  - $n = 64, 2^{\frac{n}{2}} = 2^{32}$ is somewhat small
  - practical attacks exploit collision on short blockcipher [BL16]

[BL16] Karthikeyan Bhargavan, Gaëtan Leurent: On the Practical (In-)Security of 64-bit Block Ciphers: Collision Attacks on HTTP over TLS and OpenVPN. CCS 2016: 456-467

DbHtS MACs

- A class of MACs that aim for BBB security
  - SUM-ECBC [Yas10], PMAC_Plus [Yas11]
  - 3kf9 [Zha12]
  - LightMAC_Plus [Nai17]
- **D**ouble-**b**lock **H**ash-**t**hen-**S**UM (DbHtS) [DDNP19]



[DDNP19] Nilanjan Datta, Avijit Dutta, Mridul Nandi, Goutam Paul: Double-block Hash-then-Sum: A Paradigm for Constructing BBB Secure PRF. IACR Trans. Symmetric Cryptol. 2018(3) (FSE 2019): 36-92 (2018)
[Yas10] Kan Yasuda:The Sum of CBC MACs Is a Secure PRF. CT-RSA 2010: 366-381
[Yas11] Kan Yasuda: A New Variant of PMAC: Beyond the Birthday Bound. CRYPTO 2011: 596-609
[Zha12] Liting Zhang, Wenling Wu, Han Sui, Peng Wang: 3kf9: Enhancing 3GPP-MAC beyond the Birthday Bound. ASIACRYPT 2012: 296-312
[Nai17] Yusuke Naito: Blockcipher-Based MACs: Beyond the Birthday Bound Without Message Length. ASIACRYPT (3) 2017: 446-470

DbHtS MACs

- BBB security $\frac{q^3}{2^{2n}}$ [DDNP19]
- Forgery attack with complexity $2^{\frac{3n}{4}}$ [LNS18]
- Tight security bound $\frac{q^{\frac{4}{3}}}{2^n}$ [KLL20]

[DDNP19] Nilanjan Datta, Avijit Dutta, Mridul Nandi, Goutam Paul: Double-block Hash-then-Sum: A Paradigm for Constructing BBB Secure PRF. IACR Trans. Symmetric Cryptol. 2018(3) (FSE 2019): 36-92 (2018)
[LNS18] Gaëtan Leurent, Mridul Nandi, Ferdinand Sibleyras: Generic Attacks Against Beyond-Birthday-Bound MACs. CRYPTO (1) 2018: 306-336
[KLL20] Seongkwang Kim, ByeongHak Lee, Jooyoung Lee: Tight Security Bounds for Double-Block Hash-then-Sum MACs. EUROCRYPT (1) 2020: 435-465

Multi-User(mu) Security

- The above BBB results only consider a single user (su)
- In practice, the adversary can attack multiple users, adaptively distributing its resource
  - MAC: core element of real-world security protocols

SSL SSH IPSec

  - billions of daily active users
- Question: can DbHtS MACs still achieve BBB security in the multi-user setting?

Mu Security of DbHtS

- Generic reduction: su × #users [CMS11,MPS20]
  - mu security of DbHtS: $\frac{uq^3}{2^{2n}}$ or $\frac{uq^{\frac{4}{3}}}{2^n}$
  - u is the number of users, q is the number of queries
  - if one query per user, then $\frac{q^4}{2^{2n}}$ or $\frac{q^{\frac{7}{3}}}{2^n}$
  - $q = 2^{\frac{n}{2}}$ or $q = 2^{\frac{3n}{7}}$ is still (or even worse than) birthday bound
- A direct analysis of mu security of DbHtS is much desired

[CMS11] Sanjit Chatterjee, Alfred Menezes, Palash Sarkar: Another Look at Tightness. Selected Areas in Cryptography 2011: 293-319
[MPS20] Andrew Morgan, Rafael Pass, Elaine Shi: On the Adaptive Security of MACs and PRFs. ASIACRYPT (1) 2020: 724-753

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

Our Contributions

- Propose a generic mu framework for DbHtS MACs
  - usability: prove H is ϵ_1-regular and ϵ_2-almost universal
  - high security: BBB security $\frac{q^3}{2^{2n}}$

$\Pr[H(M_1) = H(M_2)] \leq \epsilon_1$

$\Pr[H(M) = y] \leq \epsilon_1$

- Applications to key-reduced variants of DbHtS MACs
  - 2k-SUM-ECBC
  - 2k-PMAC_Plus
  - 2k-LightMAC_Plus

Our Contributions

- Point out a critical flaw in 2kf9 [DDNP19]
  - one query forgery attack
  - birthday attack on several variants of 2kf9

[DDNP19] Nilanjan Datta, Avijit Dutta, Mridul Nandi, Goutam Paul: Double-block Hash-then-Sum: A Paradigm for Constructing BBB Secure PRF. IACR Trans. Symmetric Cryptol. 2018(3) (FSE 2019): 36-92 (2018)

BBB Security of DbHtS MACs

- Main theorem:

$$\mathsf{Adv}^{\mathsf{prf}}_{\mathsf{DbHtS}}(A) \leq \frac{qp\ell}{2^{k+n}} + \frac{q^3}{2^{2n}} + \frac{q^2p + qp^2}{2^{2k}}$$

  - assume H is $\frac{1}{2^n}$-regular and $\frac{1}{2^n}$-almost universal, omit lower-order terms and small constant factors
  - q the number of MAC queries, p the number of ideal-cipher queries, n the length of block size, k the length of key
- Independent of the number of users u, which can be as large as q

Our Bound vs Generic Reduction

- Generic reduction: $\frac{q^4}{2^{2n}}$
  - when $q = 2^{\frac{n}{2}}$, it becomes vanished
- Our bound: $\frac{qp\ell}{2^{k+n}} + \frac{q^3}{2^{2n}} + \frac{q^2 p + qp^2}{2^{2k}}$
  - when $q = 2^{\frac{n}{2}}$, it is still reasonably small

$$\frac{p\ell}{2^{k+\frac{n}{2}}} + \frac{1}{2^{\frac{n}{2}}} + \frac{p}{2^{2k-n}} + \frac{p^2}{2^{2k-\frac{n}{2}}}$$

  - $n = 64, k = 128, q = 2^{32}$, querying 32GB online data, the terms containing p become

$$\frac{p\ell}{2^{160}} + \frac{p}{2^{192}} + \frac{p^2}{2^{224}}$$

Security Model

procedure INITIALIZE
$(K_h^1, K_1), (K_h^2, K_2), \cdots, \leftarrow_\$ \mathcal{K}_h \times \mathcal{K}$
$f_1, f_2, \cdots, \leftarrow_\$ \mathrm{Func}(\mathcal{M}, \{0,1\}^n)$
$b \leftarrow_\$ \{0,1\}$

procedure PRIM(J, X)
if $X = (+, x)$ **then return** $E_J(x)$
if $X = (-, y)$ **then return** $E_J^{-1}(y)$

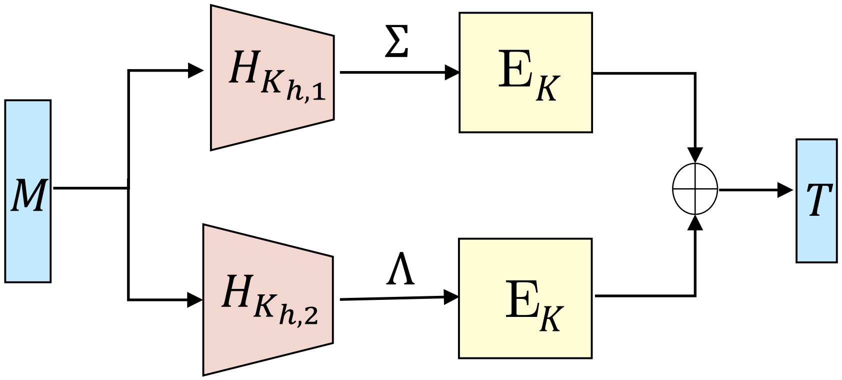
procedure EVAL(i, M)
$T_1 \leftarrow \mathsf{DbHtS}[H, E](K_h^i, K_i, M)$
$T_0 \leftarrow f_i(M)$
return T_b

procedure FINALIZE(b')
return $(b' = b)$

Game $\mathrm{G}^{\mathsf{prf}}_{\mathsf{DbHtS}}$ defining the multi-user prf security of DbHtS construction

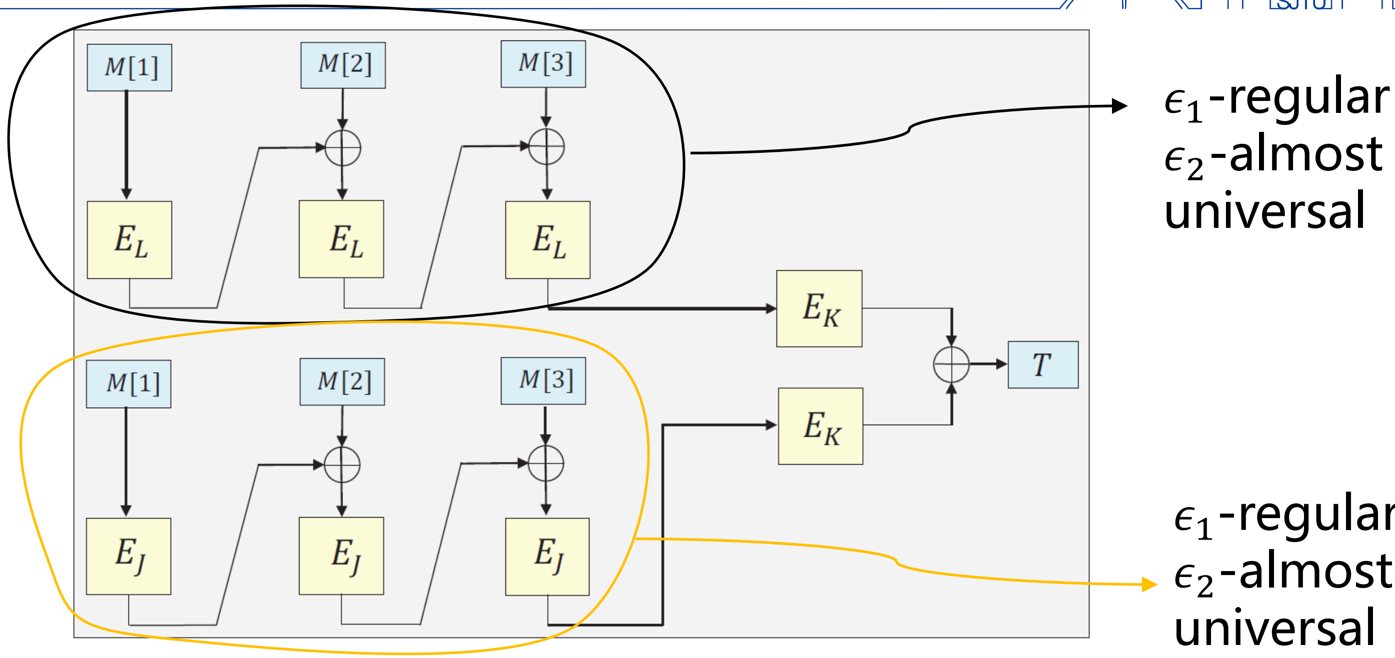
- Ideal-cipher model
  - better capture the local computation of the adversary
  - use n-bit keys to go beyond the birthday bound

Overview of The Proof



- Define bad events to guarantee:
  - For each user, at least one of (K_h^i, K_i) is fresh
  - For queries to the same user, at least one of (Σ, Λ) is fresh
  - For queries to different users, if K_i collides with other keys, then the input to E_{K_i} is fresh

Application to 2k-SUM-ECBC



2k-SUM-ECBC, hash key $K_{h,1} = L,\ K_{h,2} = J$

- Hash function: the concatenation of two CBC MACs

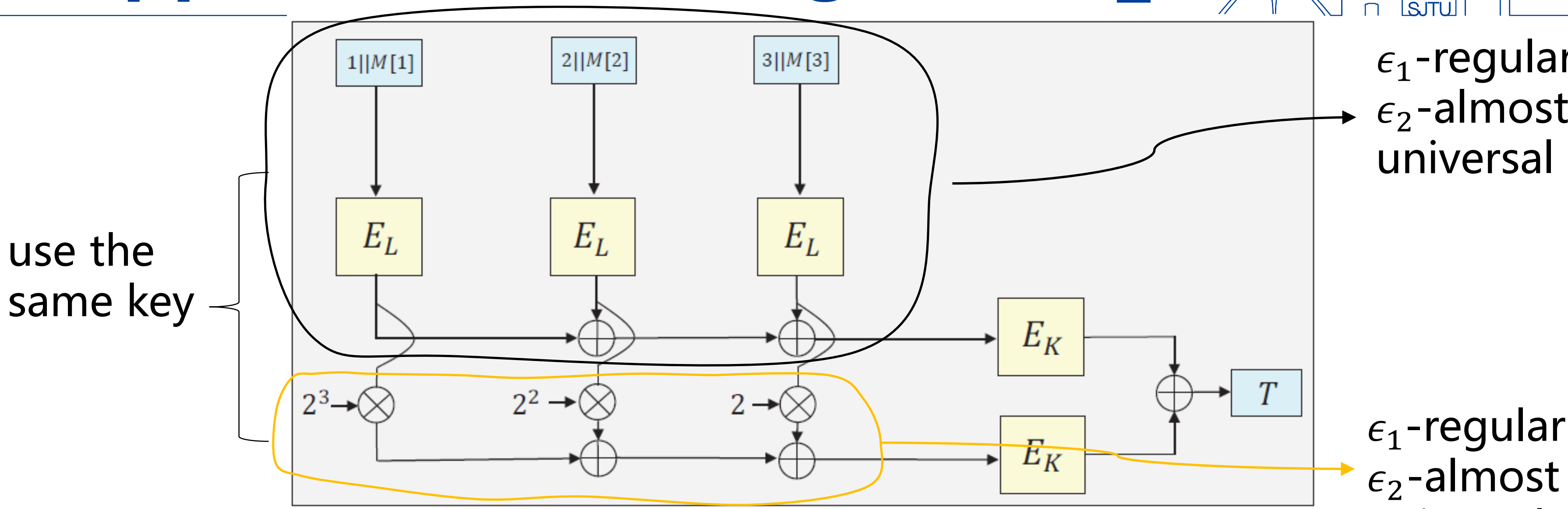
$$H_{K_h}(M) = (H^1_{K_{h,1}}(M), H^2_{K_{h,2}}(M)) = (\text{CBC}[E](K_{h,1}, M), \text{CBC}[E](K_{h,2}, M))$$

Application to 2k-SUM-ECBC

- Mu security of 2k-SUM-ECBC

$$\mathsf{Adv}^{\mathrm{prf}}_{\mathsf{2k\text{-}SUM\text{-}ECBC}}(A) \leq \frac{2q}{2^k} + \frac{q(3q+p)(6q+2p)}{2^{2k}} + \frac{6qp\ell}{2^{k+n}} + \frac{64q^2}{2^{n+k}} + \frac{36qp}{2^{n+k}} + \frac{44q^2\ell^{\frac{3}{2}}}{2^{n+k}} + \frac{576q^3\ell}{2^{2n}} + \frac{2304q^3}{2^{2n}} \ ,$$

Application to 2k-LightMAC_Plus



2k-LightMAC_Plus, hash key $K_{h,1} = K_{h,2} = L$

- Hash function: $H_L^1 = \Sigma, H_L^2 = \Lambda$

procedure $H(L, M)$

$M[1] \parallel \ldots \parallel M[\ell] \leftarrow M$

for $i \leftarrow 1$ **to** ℓ **do**

  $Y_i \leftarrow \langle i \rangle_m \parallel M[i]$; $Z_i \leftarrow E_L(Y_i)$

$\Sigma = Z_1 \oplus Z_2 \oplus \cdots \oplus Z_\ell$; $\Lambda = 2^\ell \cdot Z_1 \oplus 2^{\ell-1} \cdot Z_2 \oplus \cdots \oplus 2 \cdot Z_\ell$

return (Σ, Λ)

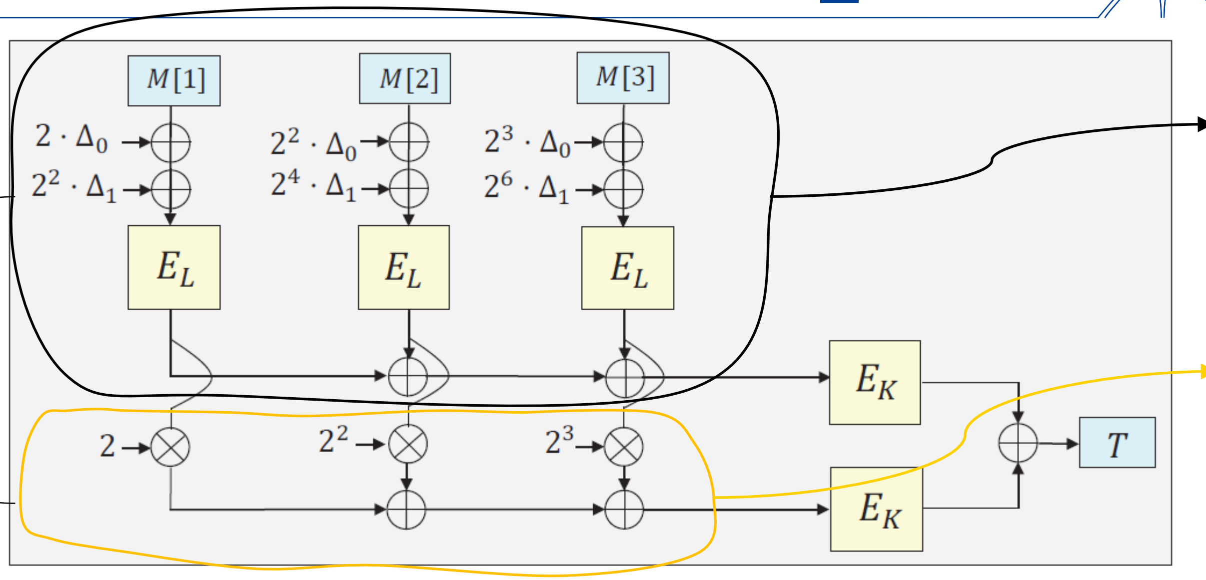
Application to 2k-LightMAC_Plus

- Mu security of 2k-LightMAC_Plus

$$\mathrm{Adv}^{\mathrm{prf}}_{\text{2k-LightMAC\_Plus}}(A) \leq \frac{2q}{2^k} + \frac{q(3q+p)(6q+2p)}{2^{2k}} + \frac{2qp\ell}{2^{k+n}} + \frac{8qp}{2^{k+n}} + \frac{8q^2}{2^{k+n}} + \frac{4q^2\ell}{2^{k+n}} + \frac{70q^3}{2^{2n}} ,$$

Application to 2k-PMAC_Plus

use the same key



ϵ_1-regular
ϵ_2-almost
universal

ϵ_1-regular
ϵ_2-almost
universal

2k-PMAC_Plus, hash key $K_{h,1} = K_{h,2} = L$

- Hash function: $H_L^1 = \Sigma, H_L^2 = \Lambda$

procedure $H(L, M)$
$M[1] \parallel \ldots \parallel M[\ell] \leftarrow M;\ \Delta_0 \leftarrow E_L(0);\ \Delta_1 \leftarrow E_L(1)$
for $i \leftarrow 1$ **to** ℓ **do**
  $Y_i \leftarrow M[i] \oplus 2^i \cdot \Delta_0 \oplus 2^{2i} \cdot \Delta_1;\ Z_i \leftarrow E_L(Y_i)$
$\Sigma = Z_1 \oplus Z_2 \oplus \cdots \oplus Z_\ell;\ \Lambda = 2 \cdot Z_1 \oplus 2^2 \cdot Z_2 \oplus \cdots \oplus 2^\ell \cdot Z_\ell$
return (Σ, Λ)

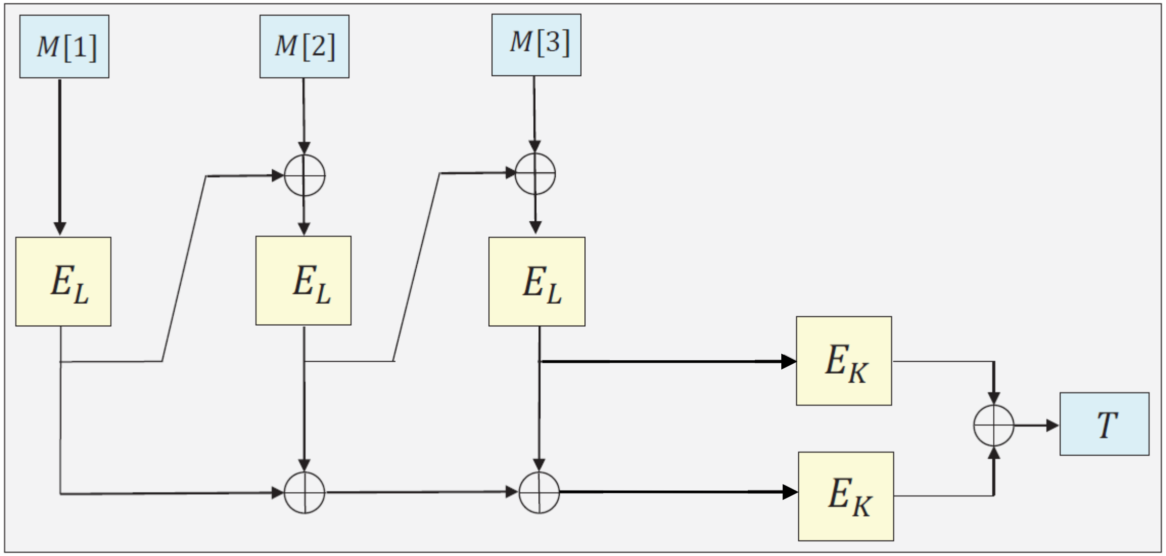
Application to 2k-PMAC_Plus

- Mu security of 2k-PMAC_Plus

$$\mathsf{Adv}^{\mathrm{prf}}_{\text{2k-PMAC\_Plus}}(A) \leq \frac{2q}{2^k} + \frac{q(3q+p)(6q+2p)}{2^{2k}} + \frac{6qp\ell^2}{2^{n+k}} + \frac{4qp}{2^{n+k}} + \frac{20q^2\ell^3}{2^{n+k}} + \frac{200q^3\ell^2}{2^{2n}} + \frac{8q\ell}{2^n} + \frac{6q^3}{2^{2n}} ,$$

Attack on 2kf9

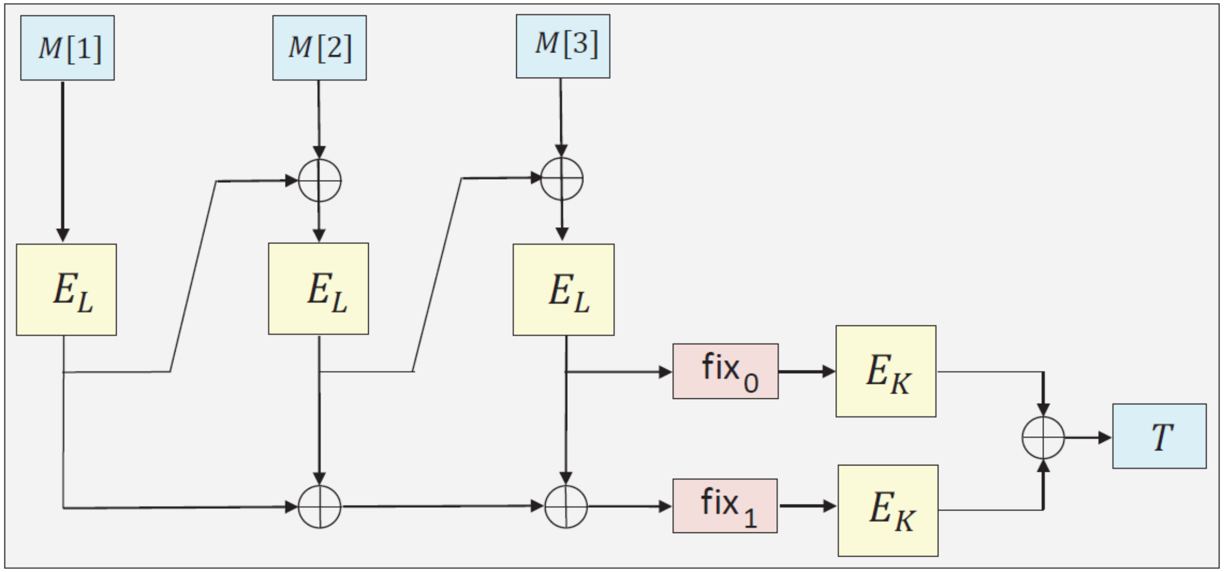
- 2kf9: BBB security $\frac{q^3}{2^{2n}}$ [DDN19]



- Attack: for any short message M with $|M| < n$, $(M, 0^n)$ is a valid forgery

[DDNP19] Nilanjan Datta, Avijit Dutta, Mridul Nandi, Goutam Paul: Double-block Hash-then-Sum: A Paradigm for Constructing BBB Secure PRF. IACR Trans. Symmetric Cryptol. 2018(3) (FSE 2019): 36-92 (2018)

Attack on 2kf9 with Domain Separation



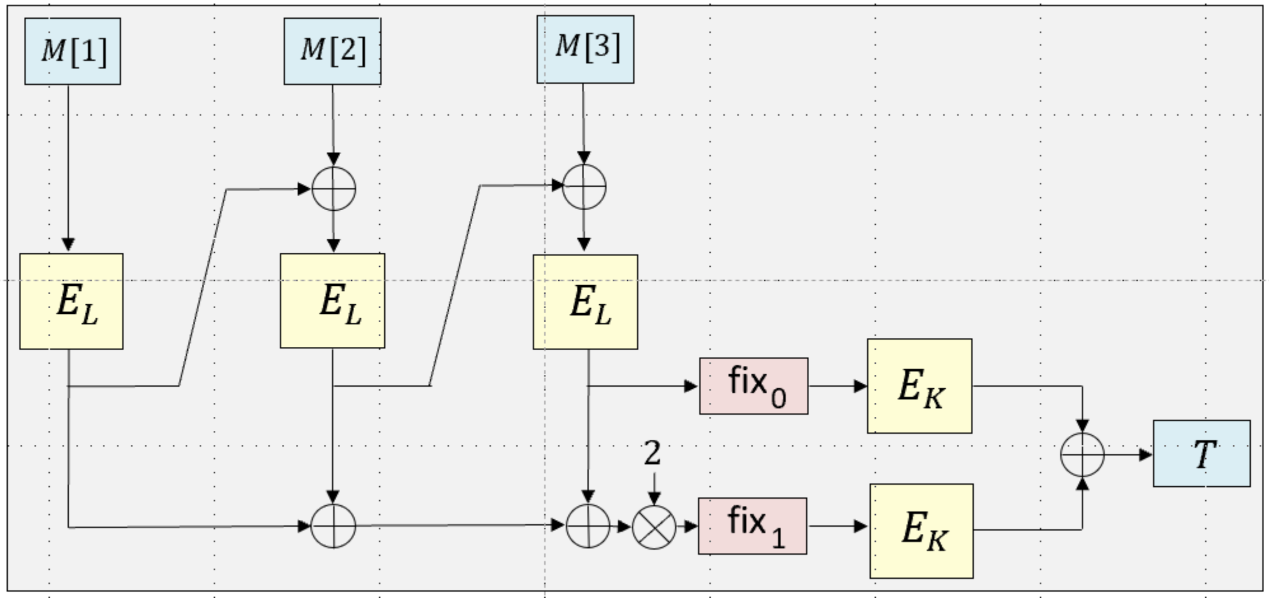
2kf9 with domain separation

- For any two messages $M_1 = x||z$ and $M_2 = y||z \oplus 0^{n-1}1$

$$E_L(x) \oplus E_L(y) = 0^{n-1}1 \quad \Rightarrow \quad T_1 = T_2$$

- Find (x, y) with birthday-bound complexity

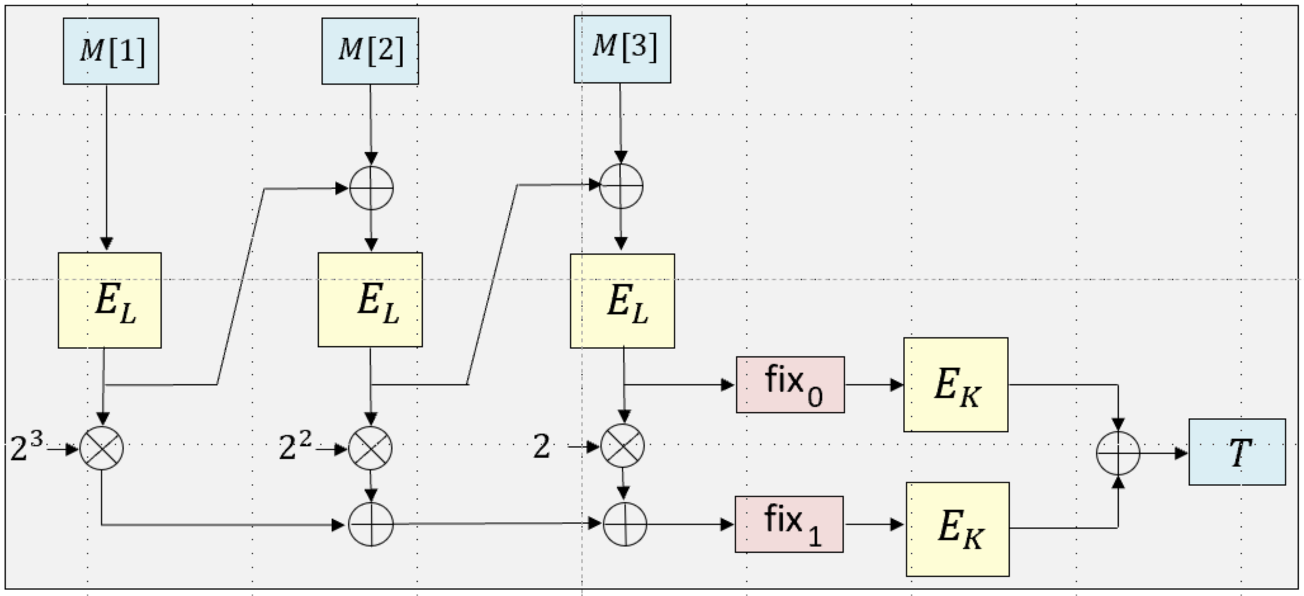
Attack on other variant of 2kf9



variant of 2kf9, multiply by 2 before fix_1

- Similar birthday-bound attack works

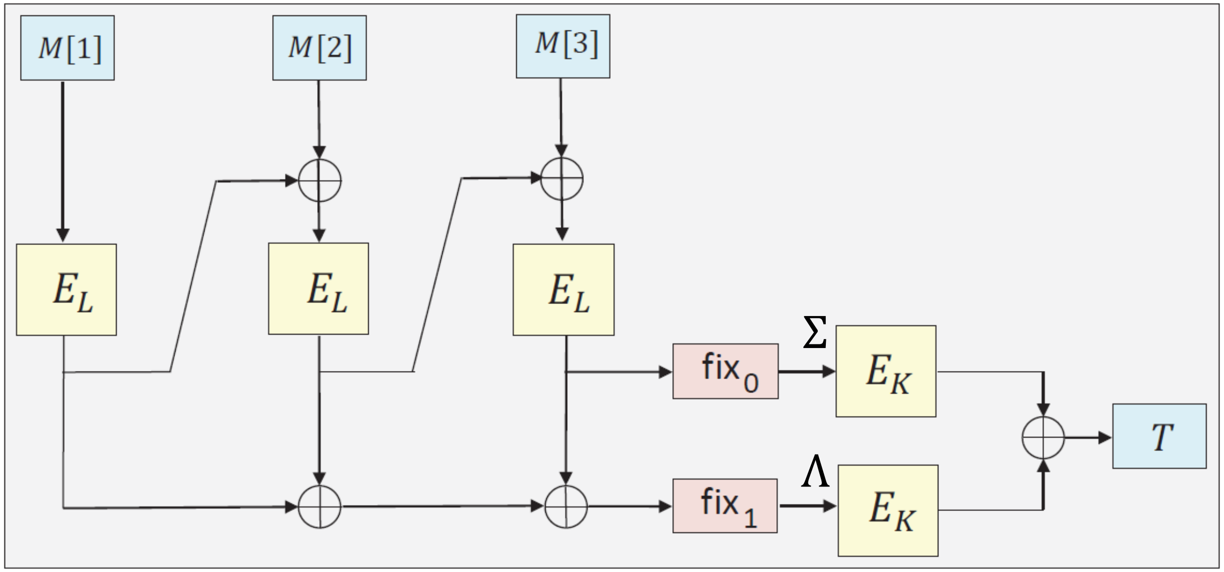
Attack on Other Variant of 2kf9



variant of 2kf9, multiply by 2 per block as in 2k-LightMAC_Plus

- Similar birthday-bound attack works

Reason behind This Flaw



2kf9 with domain separation

- We can always find a relation between Σ and Λ
  - if $\Sigma_i = \Sigma_j$, then $\Lambda_i = \Lambda_j$
- Such relation does not exit in 2k-SUM-ECBC, 2k-LightMAC_Plus, or 2k-PMAC_Plus

Conclusion

- BBB secure multi-user framework for DbHtS MACs
  - 2k-SUM-ECBC (✓)
  - 2k-PMAC_Plus (✓)
  - 2k-LightMAC_Plus (✓)
  - 2kf9 (×), insecure
- Future works
  - fix 2kf9 to go beyond the birthday bound?
  - 3n/4-bit security for DbHtS MACs in the multi-user setting?

Thanks for your attention!

Q&A?: yaobins180@gmail.com