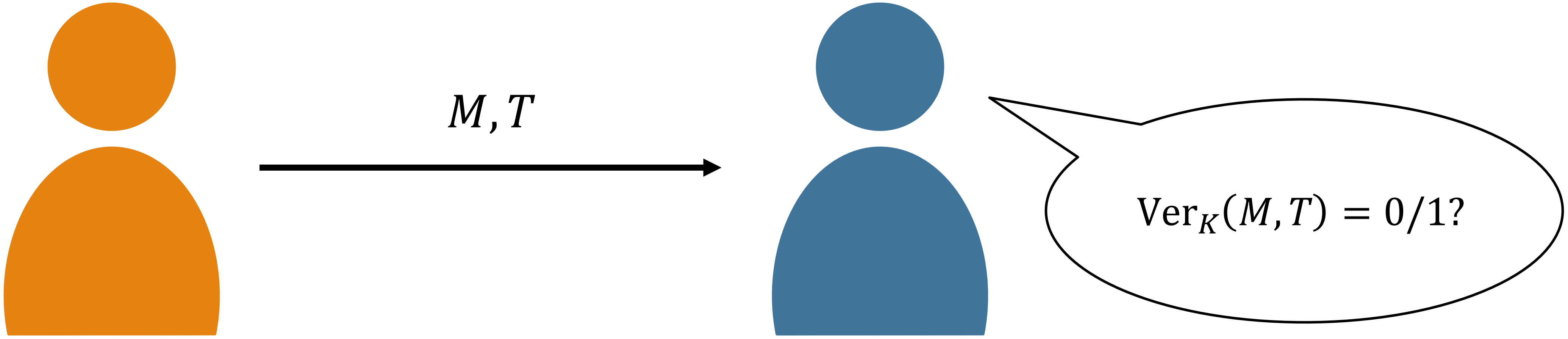
Toward Full n-bit Security and Nonce Misuse Resistance of Block Cipher-based MACs

Wonseok Choi[1], Jooyoung Lee[2], **Yeongmin Lee[3]**

[1]Purdue University
[2]KAIST
[3]DESILO Inc.

ASIACRYPT 2024

Message Authentication Codes (MACs)



For a shared key K, $T = \mathrm{MAC}_K(M)$ where M is a message and T is a tag

$\mathrm{Ver}_K(M, T) = 1$ if it is valid

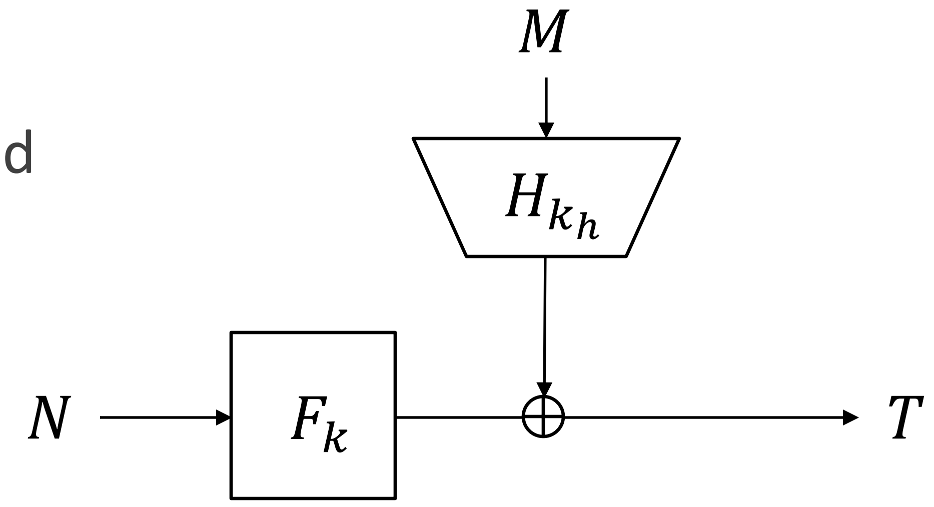
Nonce-based MAC

Wegman-Carter (WC)[WC81] : $T = H_{k_h}(M) \oplus F_k(N)$

- H is a universal hash function and F is a pseudorandom function (PRF)
- The forging advantage is $v\epsilon$ in nonce respecting setting
  - v = # of verification queries, ϵ = collision probability of H

This is vulnerable if a single nonce is repeated

- This is called nonce misuse



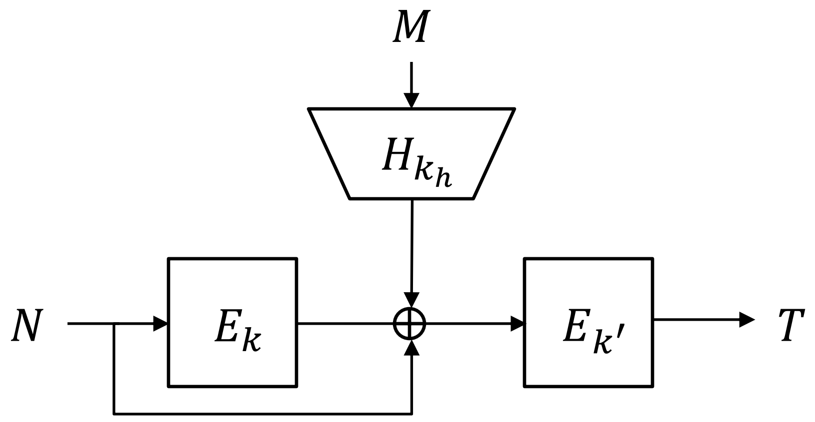
WC MAC

Nonce-misuse Resistant MACs

Cogliati and Seurin [CS16] proposed EWCDM which is secure up to $O\left(2^{2n/3}\right)$ MAC queries and $O(2^n)$ verification queries in nonce-respecting setting

- n is size of block cipher
- EWCDM is birthday bound secure in nonce-misuse setting, which is tight

Datta et al. [DDD21] improved its $\frac{3n}{4}$ bit MAC security



EWCDM

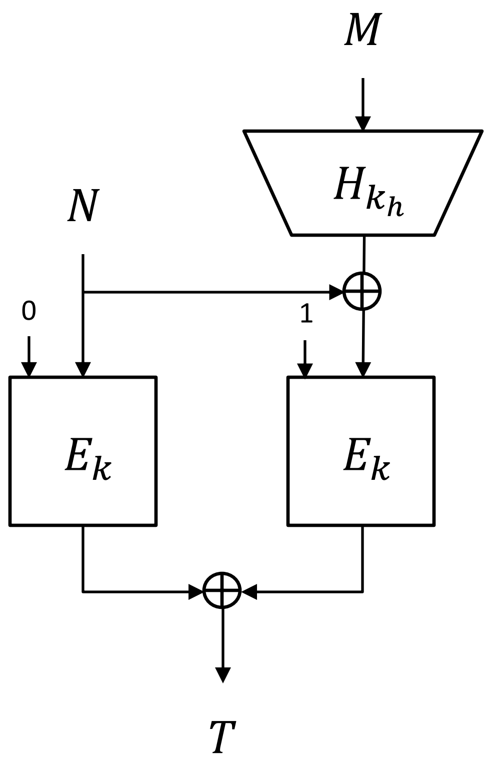
Faulty Nonce Model

Dutta et al. proposed nEHtM [DNT19] which is secure up to $O\left(2^{2n/3}\right)$ MAC queries and $O(2^n)$ verification queries in nonce-respecting setting

In nonce-misuse setting, it enjoys graceful degradation with respect to the number of faulty queries

- A MAC query is called faulty query if the nonce is reused
- μ : # of faulty queries

Choi et al. proved its $\frac{3n}{4}$-bit MAC security [CLLL20]



Generalized MAC Constructions

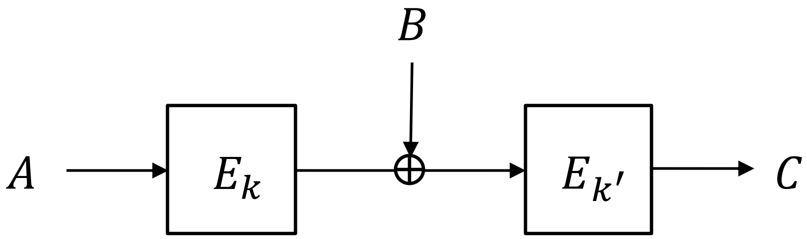
Chen et al. [CMP21] categorized nonce-based MACs that use two block cipher calls and one universal hash function call

- $C = E_{k'}(E_k(A) \oplus B)$
- A, B, C are functions of $H_{k_h}(M)$, N and T

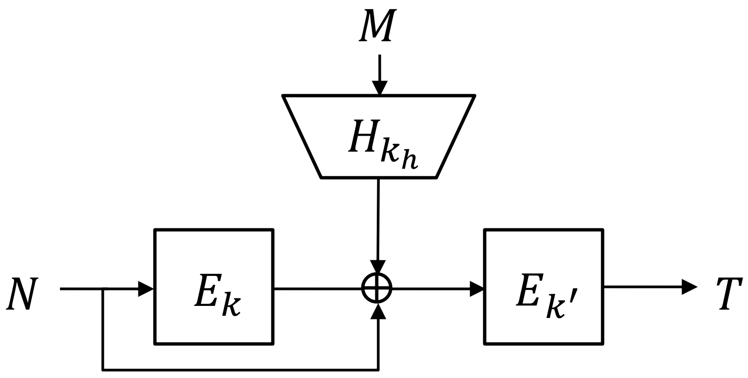
They proved six constructions has $\frac{3n}{4}$-bit PRF security in nonce-respecting setting

- $F_{B_2}^{\mathrm{EDM}}$, $F_{B_3}^{\mathrm{EDM}}$, $F_{B_4}^{\mathrm{EDM}}$, $F_{B_5}^{\mathrm{EDM}}$, $F_{B_2}^{\mathrm{SoP}}$ and $F_{B_3}^{\mathrm{SoP}}$
- Four constructions still achieve beyond birthday bound in nonce-misuse setting

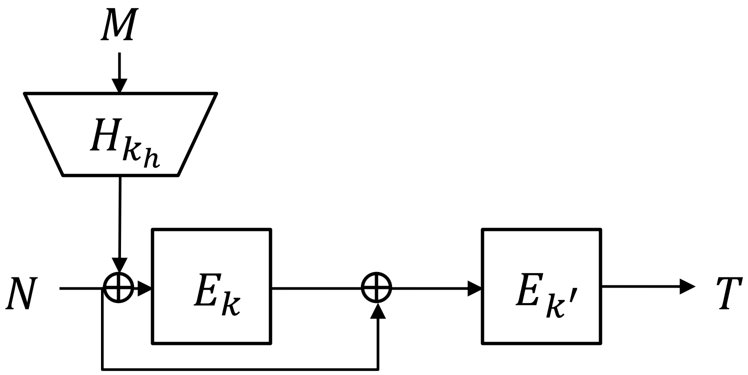
However, security tightness is still open



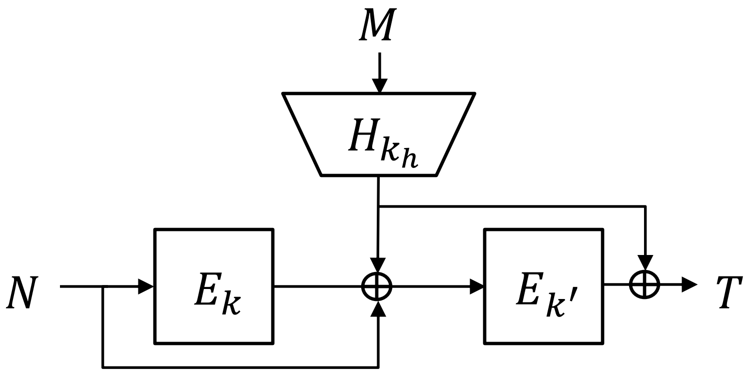
BBB Nonce-based MACs



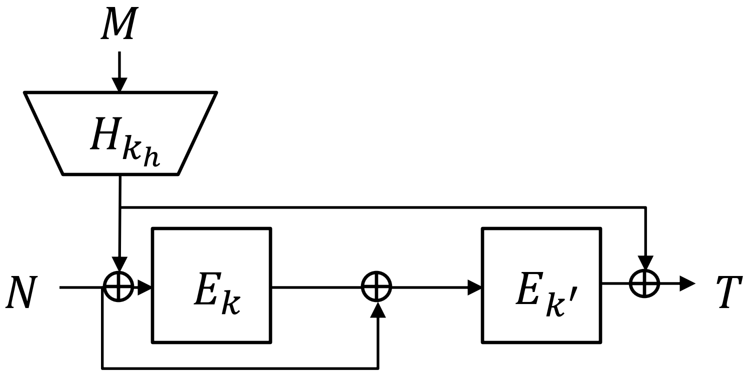
$F_{B_2}^{\mathrm{EDM}}$ (EWCDM)



$F_{B_4}^{\mathrm{EDM}}$

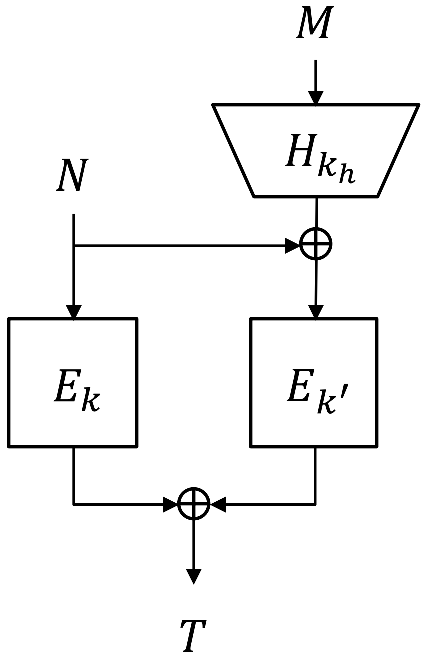


$F_{B_3}^{\mathrm{EDM}}$

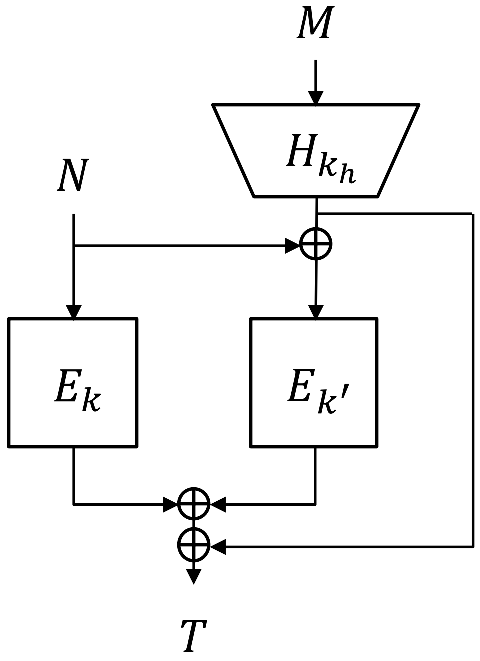


$F_{B_5}^{\mathrm{EDM}}$

BBB Nonce-based MACs



$F_{B_2}^{\mathrm{SoP}}$ (nEHtM$_2$)



$F_{B_3}^{\mathrm{SoP}}$

Contributions

MAC	NR	NM	Tightness	Hash assumption	References
WC	2^n	0	tight	CR	[29]
EWCDM	$2^{3n/4}$	$2^{n/2}$	-	CR	[12,13]
$F_{B_3}^{\mathrm{EDM}}$	$2^{3n/4}$	$2^{n/2}$	-	CR	[9]
$F_{B_2}^{\mathrm{SoP}}$	$2^{3n/4}$	$2^{3n/4}$ $(\mu \leq 2^{n/4})$	-	CR	[9]
$F_{B_3}^{\mathrm{SoP}}$	$2^{3n/4}$	$2^{3n/4}$ $(\mu \leq 2^{n/4})$	-	CR	[9]
$F_{B_4}^{\mathrm{EDM}}$	$2^{3n/4}$	$2^{3n/4}$ $(\mu < 2^{n/2})$	**tight**	CR	[9], Section 6
$F_{B_5}^{\mathrm{EDM}}$	$2^{3n/4}$	$2^{3n/4}$ $(\mu < 2^{n/2})$	**tight**	CR	[9], Section 6
EWCDM	$\mathbf{2^n}$	$\mathbf{2^{n/2}}$	**tight**	CR	Section 4
$F_{B_3}^{\mathrm{EDM}}$	$\mathbf{2^n}$	$\mathbf{2^{n/2}}$	**tight**	CR	Section 4
$F_{B_2}^{\mathrm{SoP}}$	$\mathbf{2^n}$	$\mathbf{2^n/\mu}$ $(\mu \leq 2^{n/2})\dagger$	**tight (NR)**	MCR	Section 5
$F_{B_3}^{\mathrm{SoP}}$	$\mathbf{2^n}$	$\mathbf{2^n/\mu}$ $(\mu \leq 2^{n/2})\dagger$	**tight (NR)**	MCR	Section 5

† In this paper, we proved the security bound for $\mu \leq 2^{n/4}$, while the same bound is obtained when $2^{n/4} \leq \mu \leq 2^{n/2}$ in a similar way to [15].

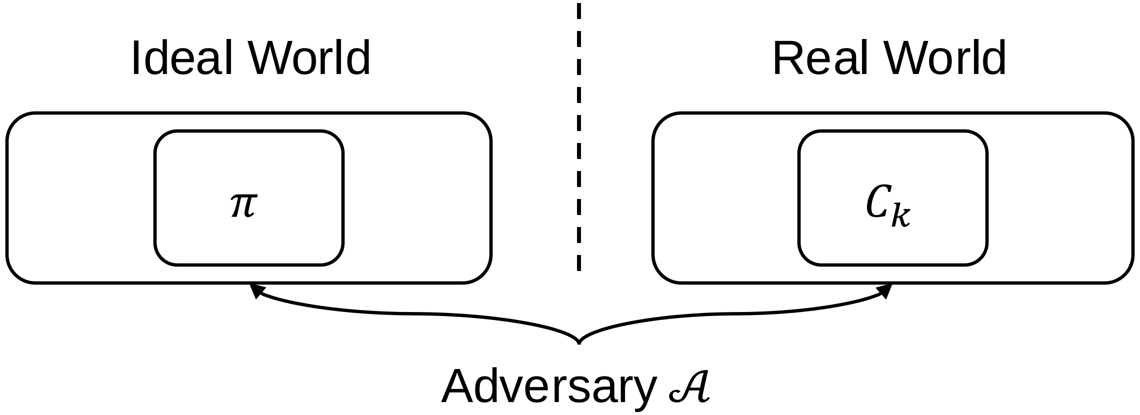
Security of Pseudorandom Function

A keyed function $C : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$

C is secure PRF if it cannot be distinguished from a random function

- Adversary $\mathcal{A}$ interacts with oracle (C_k with random k or a random function)

$$\mathrm{Adv}_C^{\mathrm{PRF}}(\mathcal{A}) = \Pr[k \leftarrow_\$ \mathcal{K} : \mathcal{A}^{C_k} = 1] - \Pr[\pi \leftarrow_\$ \mathrm{Func}(\mathcal{X}, \mathcal{Y}) : \mathcal{A}^{\pi} = 1]$$



MAC Security

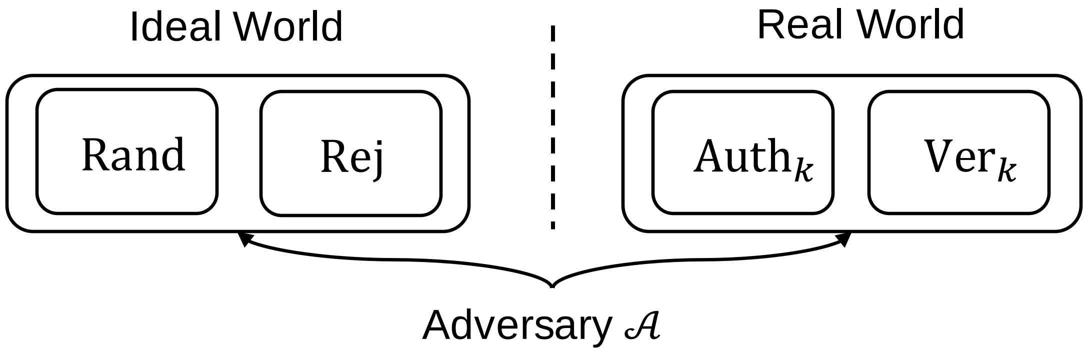
A MAC algorithm $F : \mathcal{K} \times \mathcal{N} \times \mathcal{M} \to \mathcal{T}$

F is a secure MAC if an adversary cannot forge a tag of an arbitrary message

- Adversary $\mathcal{A}$ interacts with oracle Auth_k and Ver_k with random key k
- Goal of an adversary is to get accept from the verification algorithm (no redundant query!)

$\mathrm{Adv}_F^{\mathrm{MAC}}(\mathcal{A}) = \Pr[\mathcal{A}^F \text{ forges}]$

- Upper bound: a distinguishing advantage between $S_0 = (\mathrm{Rand}, \mathrm{Rej})$ and $S_1 = (\mathrm{Auth}_k, \mathrm{Ver}_k)$
- Rand : random oracle
- Rej : always return reject



Coefficient-H Technique

Adversary records all information from the oracle in a transcript τ

- A transcript τ is called attainable transcript when $\mathrm{p}_{S_0}(\tau) > 0$
- Θ : set of attainable transcript

Coefficient-H Technique (informal)

If there exists ϵ_{bad}, ϵ_{good} such that

1) *for a set of bad transcripts $\Theta_{bad} \subset \Theta$, $\sum_{\tau \in \Theta_{bad}} \mathrm{p}_{S_0}(\tau) \leq \epsilon_{bad}$*

2) *with $\tau \notin \Theta_{bad}$, $\frac{\mathrm{p}_{S_1}(\tau)}{\mathrm{p}_{S_0}(\tau)} \geq 1 - \epsilon_{good}$*

Then,

$$\left\| P_{S_0} - P_{S_1} \right\| \leq \epsilon_{bad} + \epsilon_{good}$$

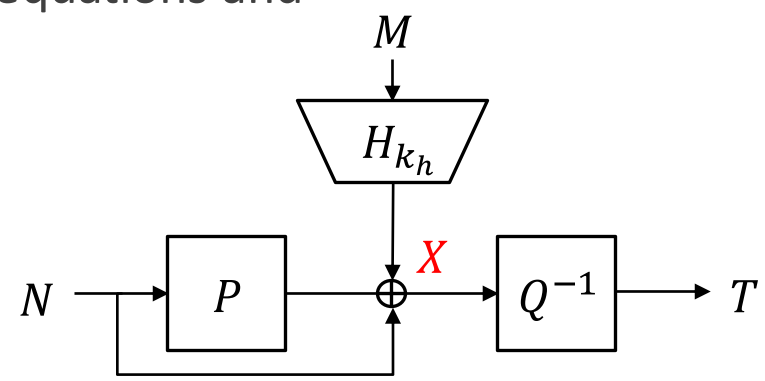
Mirror Theory

From the transcript τ, we obtain

$$\gamma^{=} = \begin{cases} P(N_1) \oplus Q(T_1) = X_1 \\ \vdots \\ P(N_q) \oplus Q(T_q) = X_q \end{cases} \text{ and } \gamma^{\neq} = \begin{cases} P(N_1') \oplus Q(T_1') \neq X_1' \\ \vdots \\ P(N_v') \oplus Q(T_v') \neq X_v' \end{cases}$$

Mirror theory: estimate the number of solutions to system of equations and inequalities

$$\mathrm{p}_{S_1}(\tau) = \frac{h(\gamma^{=},\gamma^{\neq}) = (\#\text{ of } P \text{ and } Q \text{ satisfying } \gamma^{=} \text{ and } \gamma^{\neq})}{(\#\text{ of } P \text{ and } Q)}$$

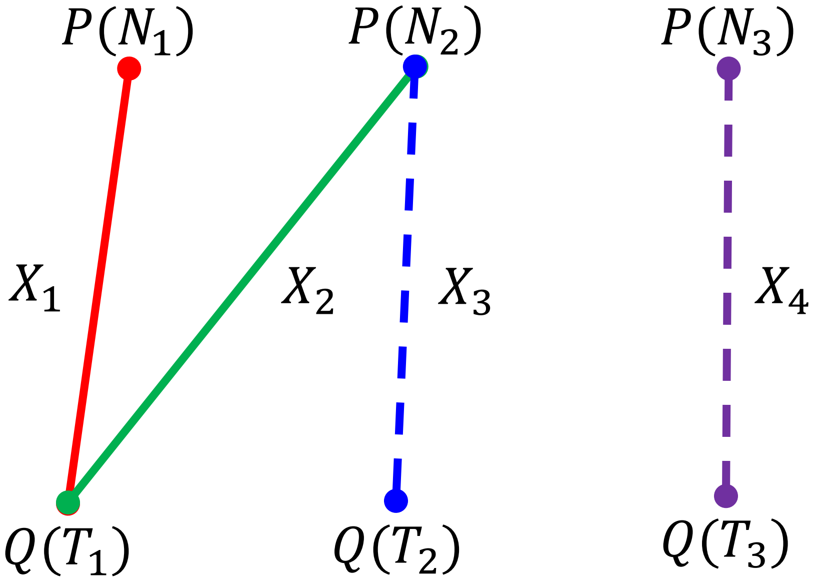


Transcript Graph

From a transcript τ, we construct a graph $\mathcal{G} = (\mathcal{V} = \mathcal{V}_1 \sqcup \mathcal{V}_2, \mathcal{E}^{=} \sqcup \mathcal{E}^{\neq})$

An equation is represented by a solid edge and an inequality is represented by a dotted edge

$\xi_{\max}$: the maximum component size



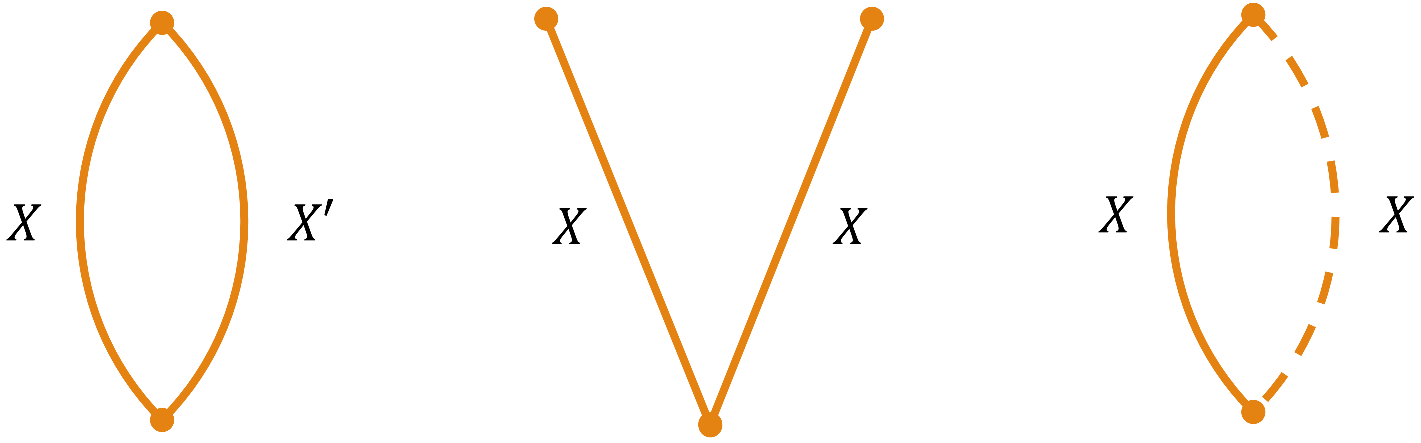
$$P(N_1) \oplus Q(T_1) = X_1$$
$$P(N_2) \oplus Q(T_1) = X_2$$

$$P(N_2) \oplus Q(T_2) \neq X_3$$
$$P(N_3) \oplus Q(T_3) \neq X_4$$

Transcript Graph

Some transcript graph might lead to contradiction

- The graph contains a cycle such that label sum is not 0 → non-cyclic
- The graph contains a path such that label sum is 0 → non-degeneracy
- If the graph contains too long trail, it is hard to analyze
- The graph contains a cycle with one inequality with label sum is 0



Mirror Theory for two permutations

In EC23, Cogliati et al. improved mirror theory for one permutation with only equations [CDN23]

- We refined the mirror theory for two permutations

If $\gamma^=$ is non-cyclic and non-degeneracy, $\xi_{\max}^2 \leq 2^{n/2}$ and $q\xi_{\max}^2 \leq 2^n$, then

$$h(\gamma^=) \geq \frac{(2^n-2)_{|\mathcal{V}_1|}(2^n-2)_{|\mathcal{V}_2|}}{(2^n)^q}$$

Adding Inequalities

From the transcript τ, we obtain

$$\gamma^{=} = \begin{cases} P(N_1) \oplus Q(T_1) = X_1 \\ \vdots \\ P(N_q) \oplus Q(T_q) = X_q \end{cases} \text{ and } \gamma^{\neq} = \begin{cases} P(N_1') \oplus Q(T_1') \neq X_1' \\ \vdots \\ P(N_v') \oplus Q(T_v') \neq X_v' \end{cases}$$

If $\gamma^{=}$ and $\gamma^{\neq}$ contains no contradiction, then

$$\frac{h(\gamma^{=}, \gamma^{\neq})}{h(\gamma^{=})} \geq 1 - \frac{2v}{2^n}$$

Bad events

We define bad events if transcript τ violate the condition

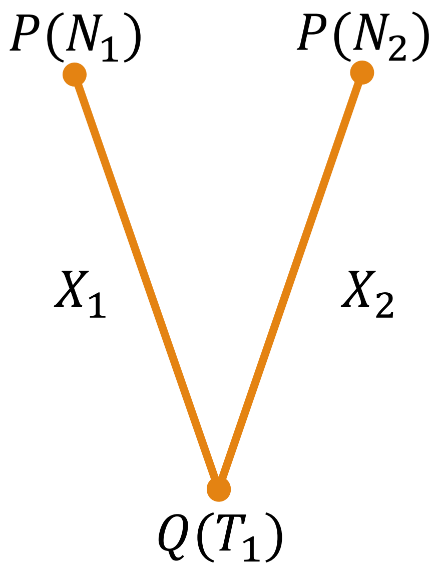
- bad1 $\leftrightarrow$ $\xi_{\max}^2 \leq 2^{n/2}$ and $q\xi_{\max}^2 \leq 2^n$
- bad2 $\leftrightarrow$ non-cyclic
- bad3 $\leftrightarrow$ non-degeneracy

In the nonce respecting setting, there is no cycle

- There is no bad2

In the nonce respecting setting, there is no length 3 path

- The probability that there exists a length 2 path such that label sum is 0

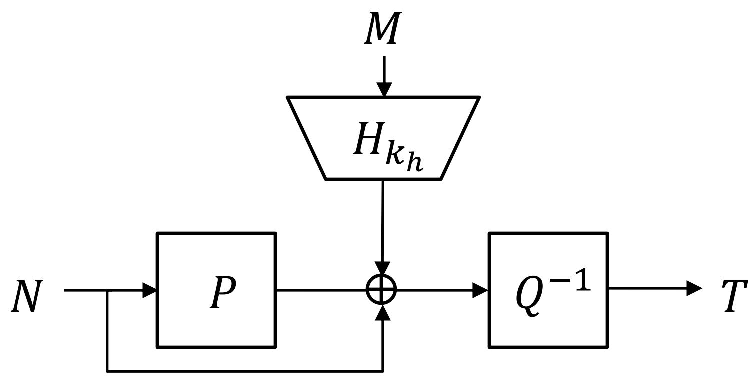


Bad events

What is the probability to have bad1?

In case of EWCDM and $F^{\mathrm{EDM}}_{B_3}$
- bad1: n multi-collision of T

In the ideal world, T is output of random function
- It is easy to compute



$F^{\mathrm{EDM}}_{B_2}$ (EWCDM)

Multi-xor collision Resistance

In case of nEHtM_2 and $F^{\mathrm{SoP}}_{B_3}$,

- bad1: n multi-collision of $H_{k_h}(M) \oplus N$

Bottleneck: we generally assume H is xor universal hash function

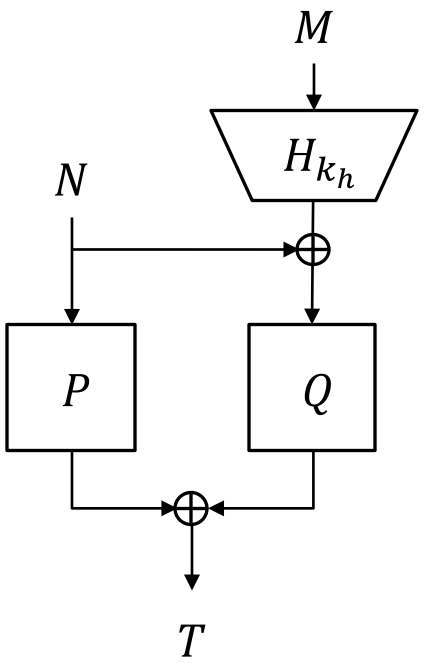
- $\Pr\left[k_h \leftarrow \mathcal{K}_h : H_{k_h}(x) \oplus H_{k_h}(x') = y\right] \le \epsilon$ for small ϵ

However, we need multi-xor-universality

- $\Pr\left[k_h \leftarrow \mathcal{K}_h : H_{k_h}(x_1) \oplus y_1 = \cdots = H_{k_h}(x_n) \oplus y_n\right] \le \epsilon'$ for small ϵ'
- We want $\epsilon' \approx \epsilon^n$ but it does not hold generally

We proved the ISO standard CBC hash function enjoys $\epsilon' \approx \epsilon^n$

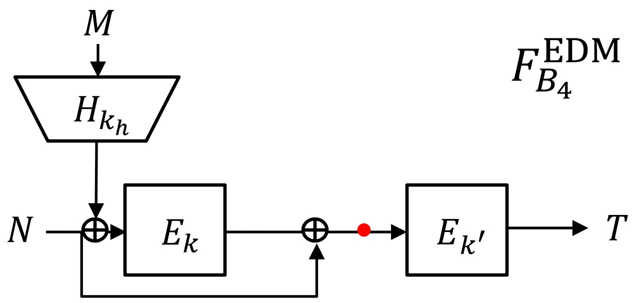
- structure graph technique [JN16]



$F^{\mathrm{SoP}}_{B_2}$ (nEHtM_2)

Attack Sketch

Collect $2^{n/2}$ pairs of (N_i, M, T_i) and (N_i', M', T_i') such that $N^* = N_i \oplus N_i'$ is same



If $H_{k_h}(M) \oplus H_{k_h}(M') = N^*$, then $T_i = T_j \Rightarrow T_i' = T_j'$

- $H_{k_h}(M) \oplus N_i = H_{k_h}(M') \oplus N_i'$ and $H_{k_h}(M) \oplus N_j = H_{k_h}(M') \oplus N_j'$
- Adversary can find (i, j) with high probability

If $H_{k_h}(M) \oplus H_{k_h}(M') \neq N^*$

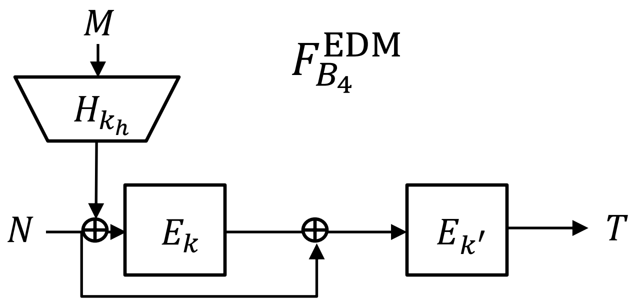
- The probability that finds (i, j) is negligible

By using $2 * 2^{3n/4}$ queries, the adversary can collect 2^n such pairs

Attack Sketch

Consider an adversary know the hash difference between two message M and M'

- $H_{k_h}(M) \oplus H_{k_h}(M') = Y$



1. Find two queries (N_1, M, T) and (N_2, M, T) by using $2^{n/2}$ queries
   - $E_k\left(N_1 \oplus H_{k_h}(M)\right) \oplus N_1 = E_k\left(N_2 \oplus H_{k_h}(M)\right) \oplus N_2$
2. Obtain $(N_1 \oplus Y, M', T')$
3. Output a valid forgery $(N_2 \oplus Y, M', T')$ since

$$E_k\left(N_1 \oplus Y \oplus H_{k_h}(M')\right) \oplus N_1 \oplus Y = E_k\left(N_2 \oplus Y \oplus H_{k_h}(M')\right) \oplus N_2 \oplus Y$$

Summary

Proved full security of nonce-based MACs

- n-bit MAC security of EWCDM and $F_{B_3}^{\mathrm{EDM}}$ in nonce respecting setting
- n-bit MAC security of nEHtM_2 and $F_{B_3}^{\mathrm{SoP}}$ in nonce respecting setting by assuming multi-xor-collision resistance
- graceful degradation for nEHtM_2 and $F_{B_3}^{\mathrm{SoP}}$ in nonce misuse setting

Presented a matching forgery attack on $F_{B_4}^{\mathrm{EDM}}$ and $F_{B_5}^{\mathrm{EDM}}$ using $O\left(2^{3n/4}\right)$ MAC queries

Thank you