On the Composition of Single-Keyed Tweakable Even-Mansour for Achieving BBB Security

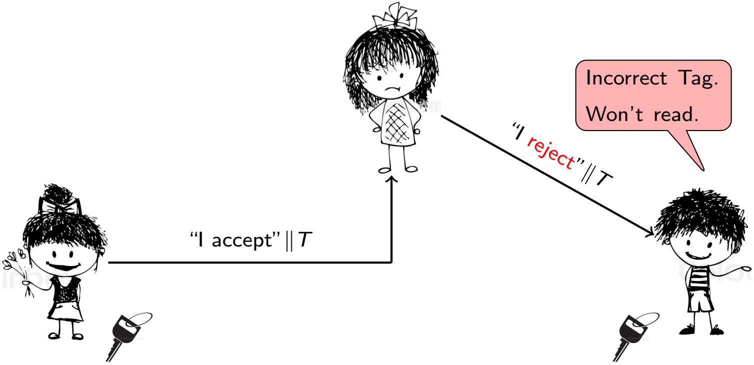
Avik Chakraborti, Mridul Nandi, **Suprita Talnikar**, Kan Yasuda

Message Authentication Codes (MAC)

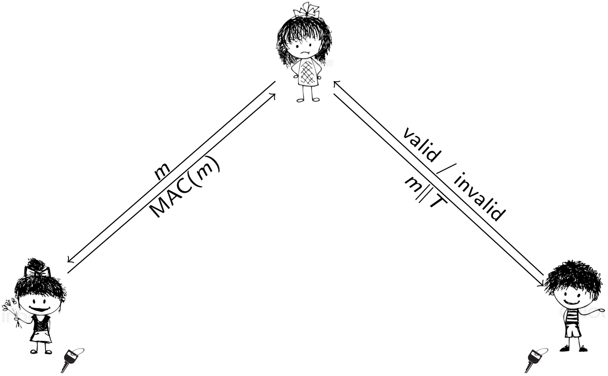
- **Symmetric Key:** Alice and Bob share the same secret key.
- **Active Attacker:** Eve may intercept and manipulate the message.
- **Authentication:** Alice computes and appends a tag, which Bob recomputes and matches with the received tag.

Message Authentication Codes (MAC)

- **Verification:** Bob verifies the tag with the shared key and only reads the message if tags match.
- **Forgery:** Eve cannnot modify the message without forging a new and correct tag.



Forgery Game



q_m = number of authentication queries

q_v = number of verification queries

Can Eve forge a valid tag for a message that Alice never saw?

Why is Beyond Birthday Security Required?

- BBB security is useful in lightweight cryptography.
- Consider the following security advantages for $\epsilon = 2^{-10}$, $n = 64$ and $\ell = 2^{16}$ blocks.

Construction	Security	# of queries
ECBC	$16q_m^2/2^n$	$\approx 2^{25}$
PMAC	$5\ell q_m^2/2^n$	$\approx 2^{18}$

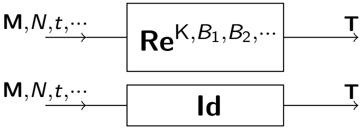
Table: Data limit of constructions acheiving birthday bound security.

BBB security allows processing of a larger number of blocks per session key.

Block-Ciphers Vs Random Permutations as Primitives

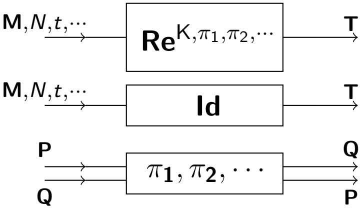
Block Ciphers or Tweakable Block Ciphers

Oracles:



Random Permutations

Oracles:



Even-Mansour, with and without Tweak

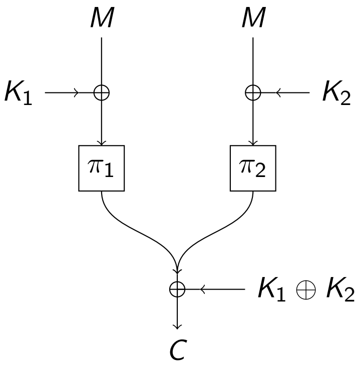
$$\mathrm{EM}_K[\pi](M) := \pi(M \oplus K_1) \oplus K_2$$

Round keys replaced by functions $f_i(K_i, t)$ of *tweaks* t, resulting in the tweakable Even-Mansour (TEM) construction:

$$\begin{tikzcd}
 & 2^t \cdot K \arrow[d] & & & 2^t \cdot K \arrow[d] & \\
M \arrow[r] & \oplus \arrow[r] & \boxed{\pi} \arrow[rr] & & \oplus \arrow[r] & C
\end{tikzcd}$$

Figure: $\mathrm{TEM}[\pi](M) := \pi(M \oplus 2^t \cdot K) \oplus 2^t \cdot K$.

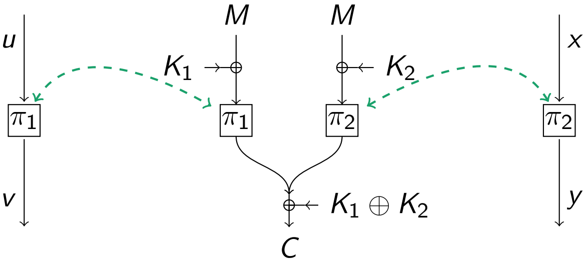
Sum of Even-Mansour



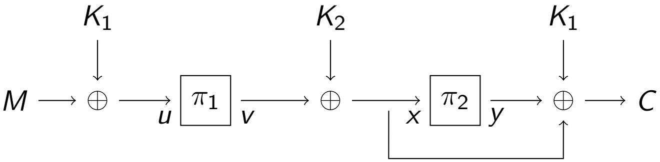
Attack on SoEM

Key-recovery attack on SoEM22:
Verify keys by repeatedly checking –

$$C \oplus C' = v \oplus v' \oplus y \oplus y'.$$



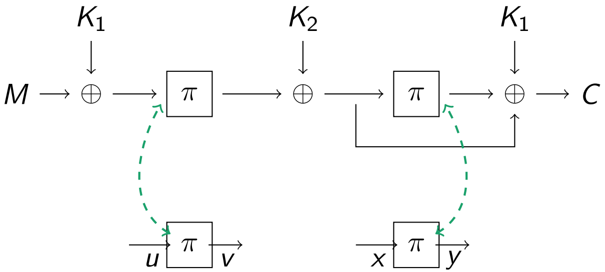
Sum of Key Alternating Ciphers



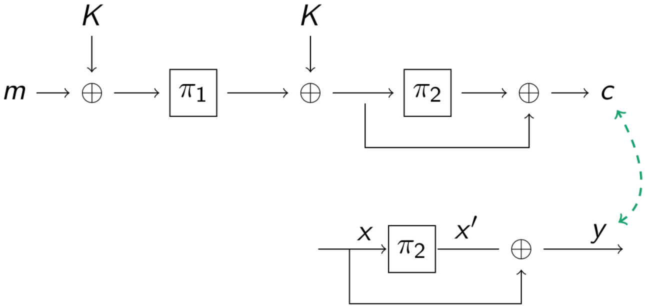
Attack on SoKAC1

Check the following for each key value:

$$v \oplus x \oplus v' \oplus x' = 0.$$



Attack on SoKAC21



Comparision with Existing Constructions

Construction	#Key Instances	#Primitive Instances	MAC Security in n-bits (tightness)	Nonce Based	Multi-Block Inputs
Based on permutations					
PDMMAC [**This work**]	1	1	$2n/3$ (tight)		
PDM*MAC [**This work**]	1 + 1 (hash key)	1	$2n/3$ (tight)	✓	✓
1K-PDM*MAC [**This work**]	1	1	$2n/3$ (tight)	✓	✓
SoEM1	2	1	- (birthday attack)		
SoEM21	1	2	- (birthday attack)		
SoEM22	2	2	$2n/3$ (tight)		
SoKAC1	2	1	- (birthday attack)		
SoKAC21	1	2	- (birthday attack)		
Based on Block Ciphers					
EDM	2	2	$2n/3$ (not tight)		
EWCDM	2 + 1 (hash key)	2	$2n/3$ (not tight)	✓	✓
DWCDM	1 + 1 (hash key)	1	$2n/3$ (not tight)	✓	✓
1K-DWCDM	1	1	$2n/3$ (not tight)	✓	✓

PDMMAC

Constructions with $\mathcal{O}\left(2^{2n/3}\right)$-Tight Security:
($\mathcal{O}\left(2^{2n/3}\right)$-Query Attacks Exist)

Permutation-based Davies-Meyer MAC:

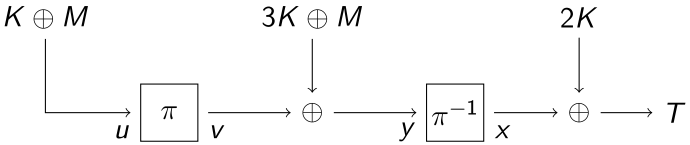


Figure: PDMMAC - A single-permutation π and single-key K based PRF.

PDM*MAC and 1K-PDM*MAC

Permutation-based Davies-Meyer MAC with Nonce:

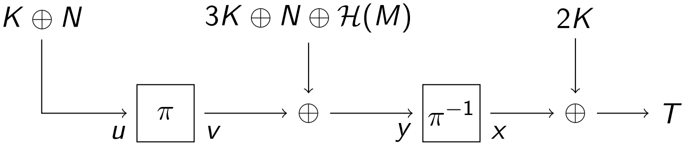


Figure: PDM*MAC - A one key K-, one RP π- and hash $\mathcal{H}$-based PRF.

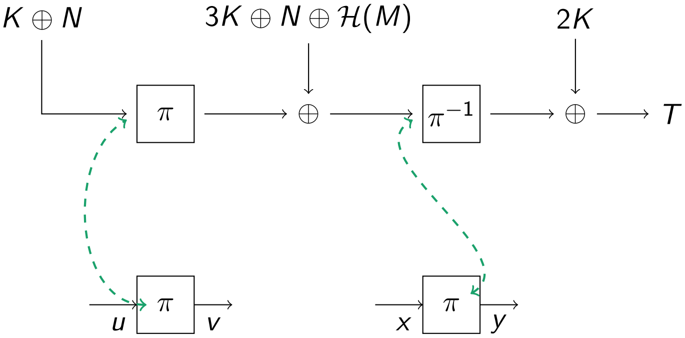
Single-Keyed Permutation-based Davies-Meyer MAC with Nonce:

The hash key H is initialized using the construction key K and primitive π as $H = \pi(K)$ in the singled-keyed **1K-PDM*MAC**.

Attack on PDM*MAC

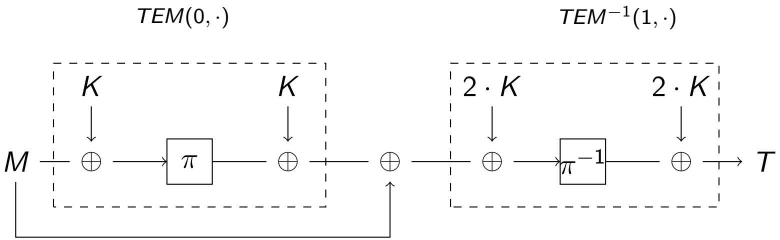
Check for each key value, whether the following equation is satisfied:

$$N \oplus v \oplus y \oplus N' \oplus v' \oplus y' = 0.$$



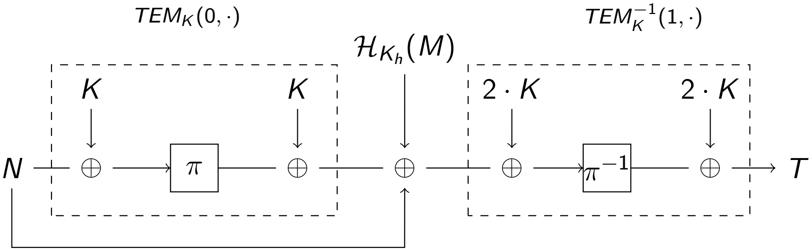
Design Rationale behind PDMMAC

DDM (Decrypted Davies-Meyer):

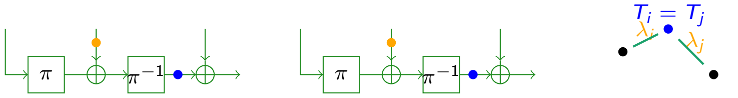


Design Rationale behind PDM*MAC

DWCDM (Decrypted Wegman-Carter with Davies-Meyer):



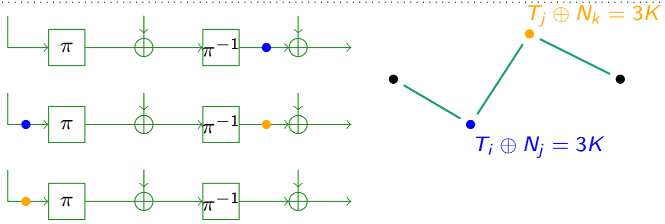
B1.



There exist $i \neq j \in [q_m]$ such that $(T_i = T_j) \wedge (N_i \oplus H_i = N_j \oplus H_j)$.

$\Pr[B1] \leq \frac{q_m^2 \epsilon}{2^n}$.

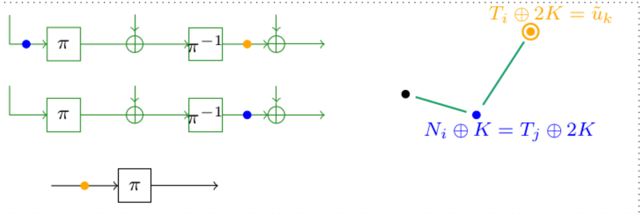
B5.



There exist $i, j, k \in [q_m]$ such that $T_i \oplus N_j = T_j \oplus N_k = 3K$.

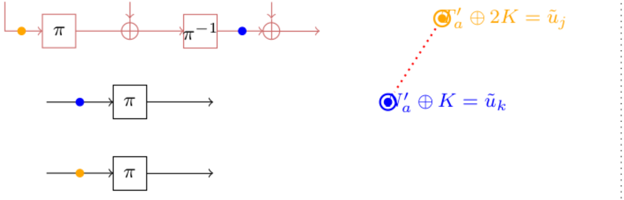
$\Pr[B5] \leq \frac{pq_m^2}{2^{2n}} + \frac{\sqrt{6npq_m}}{2^n} + \frac{2}{2^n}$.

B8.



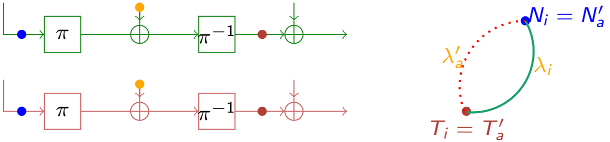
There exist $i \neq j \in [q_m], k \in [p]$ such that
$(N_i \oplus T_j = 3K) \wedge (2K \oplus T_i = \tilde{u}_k)$. $\Pr[B8] \leq \frac{pq_m^2}{2^{2n}}$.

B11.



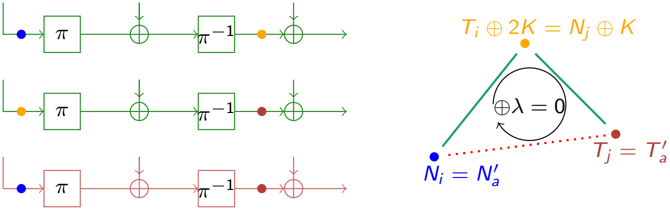
There exist $i \neq j \in [q_m], k \in [p]$ such that
$(N_i \oplus T_j = 3K) \wedge (2K \oplus T_i = \tilde{u}_k)$. $\Pr[B8] \leq \frac{pq_m^2}{2^{2n}}$

B12.



There exist $i \in [q_m], a \in [q_v]$ such that
$(N_i = N'_a) \wedge (H_i = H'_a) \wedge (T_i = T'_a)$. $\Pr[B12] \leq q_v \epsilon$.

B13.



There exist $i, j \in [q_m], a \in [q_v]$ such that
$(N'_a = N_i) \wedge (T_i \oplus N_j = 3K) \wedge (T_j = T'_a)$. $\Pr[B13] \leq \frac{q_m^2 2 q_v \epsilon}{2^n}$.

Good Transcripts – Weak Bound

Lemma

The total number of injective solutions chosen from a set $\mathcal{Z}$ of size $2^n - c$, for some $c \geq 0$, for the induced system of equations and non-equations $\mathcal{G}_{\mathrm{eq,neq}}$ is at least:

$$(2^n)_\alpha \left(1 - \sum_{i=1}^{k} \frac{6\sigma_{i-1}^2 \binom{w_i}{2}}{2^{2n}} - \frac{2(q_v + c\alpha)}{2^n}\right),$$

provided $\sigma_k w_{\max} \leq 2^n/4$, and assuming $\sigma_0 = 0$.

Results on Mirror Theory

Corollary (1)

Let $S' \subseteq \{0,1\}^n$ *be a subset of size* $(2^n - p')$ *and*

$$(X_1, X_2, \ldots, X_t, Y_1, Y_2, \ldots, Y_t, Z_1, Z_2, \ldots Z_t) \xleftarrow[wor]{\$} S'$$

be a WOR sample of size $3t$ *drawn from* $S'^{(3)}$*. Then for constants* $\lambda_1, \lambda_2, \ldots, \lambda_{2t}$ *in* $\{0,1\}^n$*,*

$$\Pr\left[(X_1 \oplus Y_1 = \lambda_1) \wedge (X_2 \oplus Y_2 = \lambda_2) \wedge \ldots \wedge (X_t \oplus Y_t = \lambda_t)\right] \geq \frac{1}{2^n}\left(1 - \frac{t \cdot p'^2}{(2^n - p')^2}\right),$$

$$\text{and } \Pr\left[\begin{pmatrix} X_1 \oplus Y_1 = \lambda_1, \\ Z_1 \oplus Y_1 = \lambda_2 \end{pmatrix} \wedge \begin{pmatrix} X_2 \oplus Y_2 = \lambda_3, \\ Z_2 \oplus Y_2 = \lambda_4 \end{pmatrix} \wedge \ldots \wedge \begin{pmatrix} X_t \oplus Y_t = \lambda_{2t-1}, \\ Z_t \oplus Y_t = \lambda_{2t} \end{pmatrix}\right] \geq \frac{1}{2^{2nt}}\left(1 - \frac{3t \cdot 2^n \cdot p'^2}{(2^n - p')^3}\right).$$

Results on Mirror Theory

Corollary (2)

Let $\mathcal{G}_{\mathrm{eq,neq}} = (\mathsf{V}, \mathsf{E}_{\mathrm{eq}} \sqcup \mathsf{E}_{\mathrm{neq}}, \mathcal{L})$ *be an equations-and-non-equations-inducing graph such that the subgraph* $\mathcal{G}_{\mathrm{eq}}$ *only has components of size* 2 *or* 3*. If* $|\mathsf{V} \setminus \mathsf{V}_{\mathrm{eq}}| = q_v$ *and* λ_i $(i \in [q_m])$ *are edge-labels of the edges in* E_{eq} *in the same order as the components, then the probability of the induced systems of equations and non-equations attaining any solution from a set* $S' \subseteq \{0,1\}^n$ *of size* $(2^n - p')$ *for all the variables represented only by the vertices in* V_{eq} *is bounded by-*

$$\frac{1}{2^{nq_m}}\left(1 - \frac{1200q_m^3 + 312(p' + 3q_v)q_m^2 + 2(p' + 3q_v)^2 q_m}{2^{2n}}\right)\left(1 - \frac{q_v}{2^n}\right).$$

- MACs and forgery games.
- BBB security.
- Permutation-based MACs.
- Even-Mansour, SoEM, SoKAC.
- PDMMAC (and variants).
- Transcript-inducing graph (for use in security proof by extended Mirror Theory).
- Final bound of $2n/3$.