Syntax: An AEAD scheme is a 3-tuple $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ where

- $\mathcal{K}$ is a probabilistic algorithm that returns a string;
- $\mathcal{E}$ is a deterministic algorithm that maps a tuple (K, N, A, M) to a ciphertext $C = \mathcal{E}(K, N, A, M)$ of length $|M|+\tau$; and
- $\mathcal{D}$ is a deterministic algorithm that maps a tuple (K, N, A, C) to a plaintext M or the symbol $\perp$

If $C = \mathcal{E}(K, N, A, M) \neq \perp$ then $\mathcal{D}(K, N, A, C) = M$

All-in-one definition

$$\mathbf{Adv}^{\mathrm{aead}}_{\Pi}(A) = \Pr[A^{\mathcal{E}(K,\,\cdots),\,\mathcal{D}(K,\,\cdots)} \Rightarrow 1] - \Pr[A^{\$(\cdots),\,\perp(\cdots)} \Rightarrow 1]$$

A may not repeat any N query to its Enc oracle.
It may not ask Dec(N, A, C) after an Enc(N, A, M) returned C.

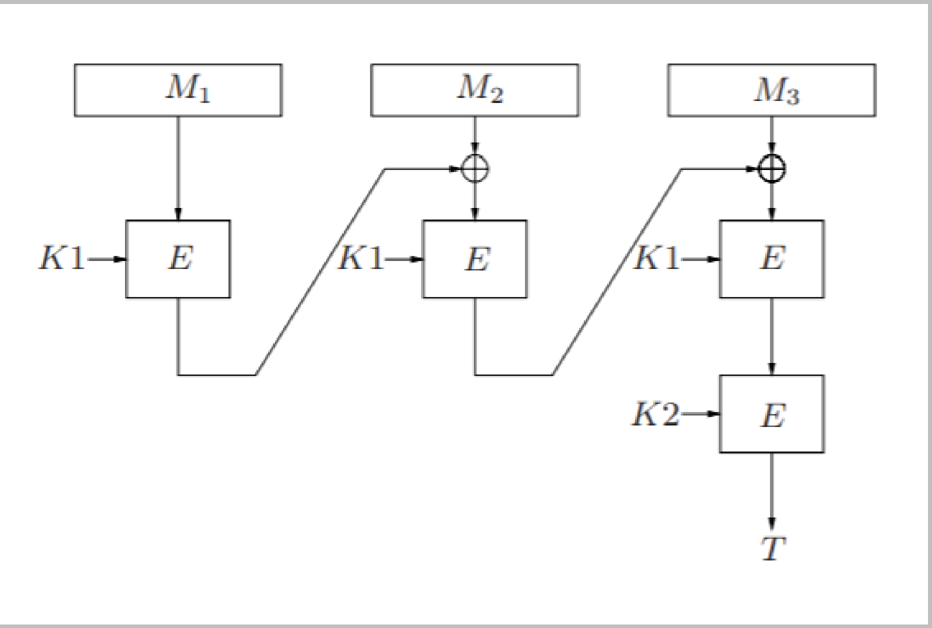
Two-part definition

$$\mathbf{Adv}^{\mathrm{priv}}_{\Pi}(A) = \Pr[A^{\mathcal{E}(K,\,\cdots)} \Rightarrow 1] - \Pr[A^{\$(\cdots)} \Rightarrow 1]$$

A may not repeat any N query.

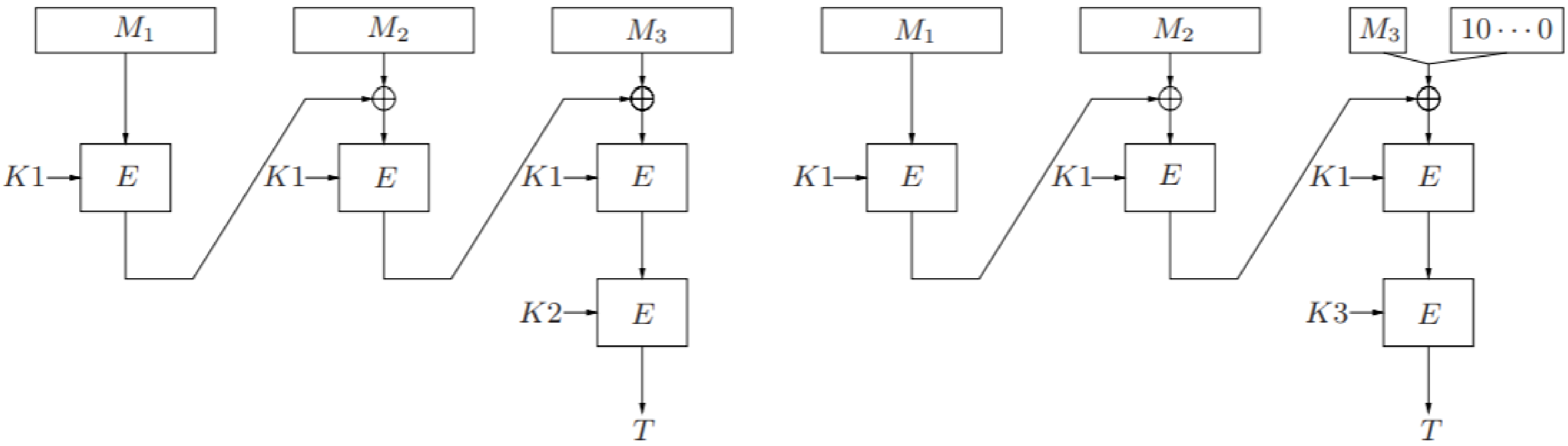
$$\mathbf{Adv}^{\mathrm{auth}}_{\Pi}(A) = \Pr[A^{\mathcal{E}(K,\,\cdots)} \text{ forges}]$$

It outputs an (N, A, C) where $\mathcal{D}(K, N, A, C) \neq \perp$ and no prior oracle query of (N, A, M) returned C

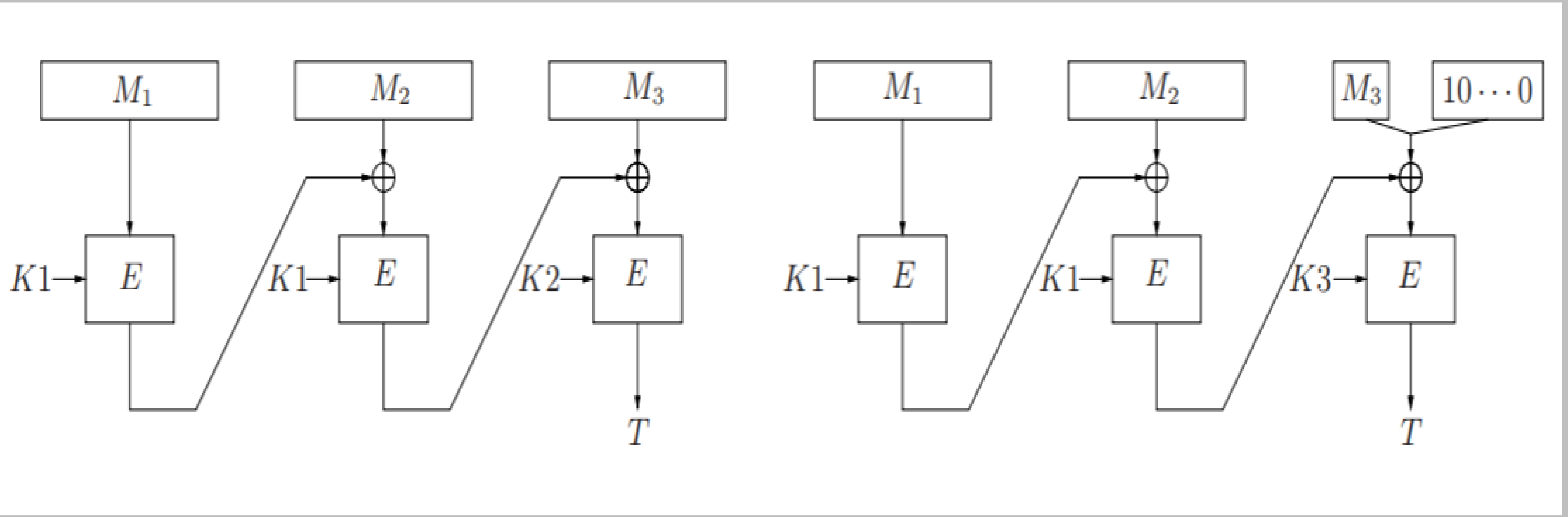


En route to CMAC

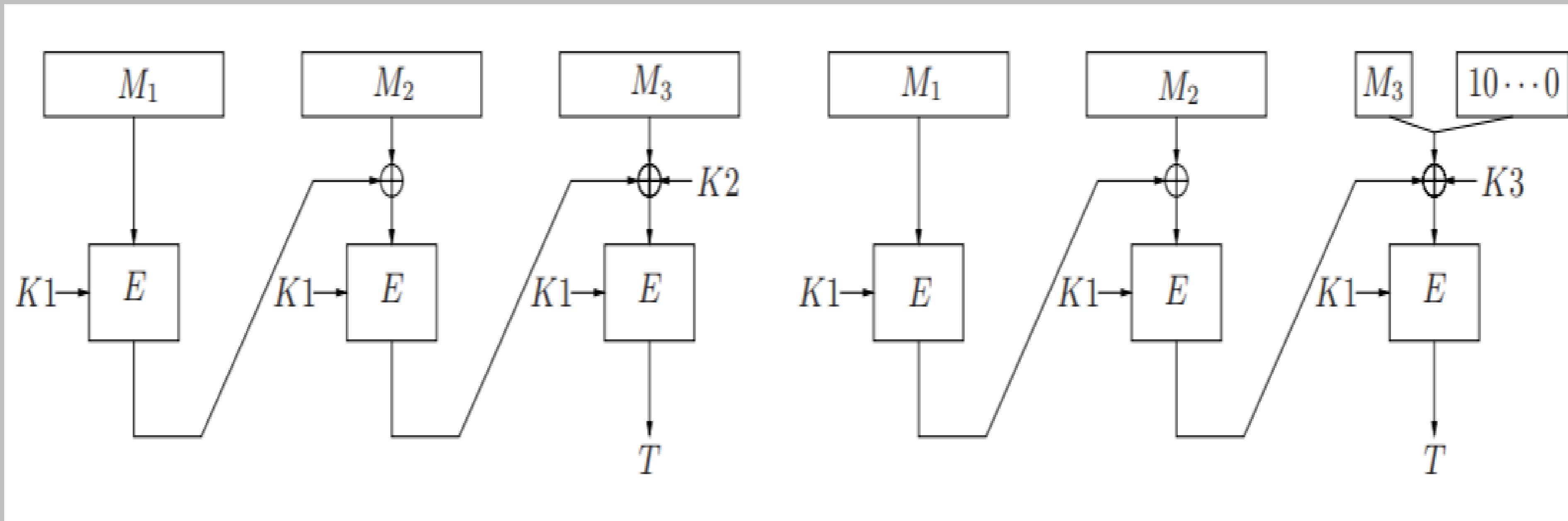
[Black, Rogaway 2000]
with a tweak from
[Iwata, Kurosawa 2003]



En route to CMAC
[Black, Rogaway 2000]
with a tweak from
[Iwata, Kurosawa 2003]



En route to CMAC
[Black, Rogaway 2000]
with a tweak from
[Iwata, Kurosawa 2003]



CMAC
[Black, Rogaway 2000]
with a tweak from
[Iwata, Kurosawa 2003]

$K2 = 2 \cdot E_{K1}(\mathbf{0})$
$K3 = 4 \cdot E_{K1}(\mathbf{0})$