**Syntax:** An AEAD scheme is a 3-tuple $\Pi = (K, E, D)$ where
- $K$ is a probabilistic algorithm that returns a string;
- $E$ is a deterministic algorithm that maps a tuple $(K, N, A, M)$ to a ciphertext $C = E(K, N, A, M)$ of length $|M| + \tau$; and
- $D$ is a deterministic algorithm that maps a tuple $(K, N, A, C)$ to a plaintext $M$ or the symbol $\perp$.

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

### All-in-one definition

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

- $A$ 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

$$\text{Adv}_{\Pi}^{\text{priv}}(A) = \Pr[A^{E(K, \ldots)} \Rightarrow 1] - \Pr[A^{\perp(\ldots)} \Rightarrow 1]$$

- $A$ may not repeat any $N$ query.

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

- It outputs an $(N, A, C)$ where $D(K, N, A, C) \neq \perp$ 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]

\[ K2 = 2 \cdot E_{K1}(0) \]
\[ K3 = 4 \cdot E_{K1}(0) \]