Odds and ends

Deterministic Encryption Constructions: SIV and wide PRP

Deterministic encryption

Needed for maintaining an encrypted database index

- Lookup records by encrypted index

Deterministic CPA security:

- Security if never encrypt same message twice using same key:

  the pair (key , msg) is unique

Formally: we defined deterministic CPA security game

Construction 1: Synthetic IV (SIV)

Let (E, D) be a CPA-secure encryption. $\mathbf{E(k, m \; ; \; r) \longrightarrow c}$

Let $F: K \times M \longrightarrow R$ be a secure PRF

Define: $\mathbf{E_{det}((k_1,k_2), m) =}$ $\begin{cases} r \leftarrow F(k_1, m) \\ c \leftarrow E(k_2, m \; ; \; r) \\ \text{output } r \end{cases}$

Thm: $\mathbf{E_{det}}$ is sem. sec. under det. CPA .

Proof sketch: distinct msgs. ⇒ all r's are indist. from random

Well suited for messages longer than one AES block (16 bytes)

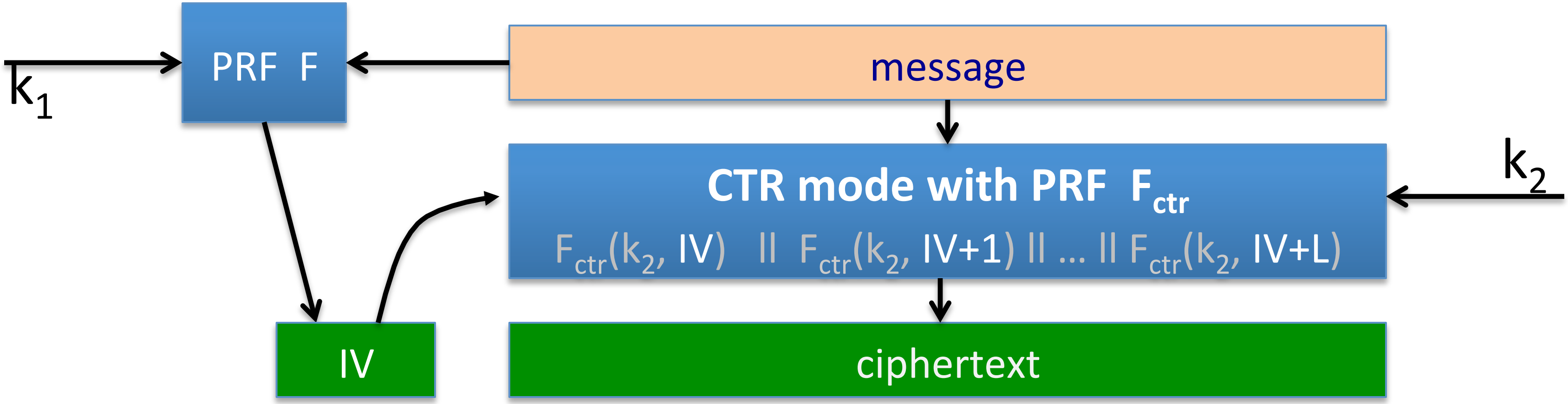
Ensuring ciphertext integrity

Goal: det. CPA security and ciphertext integrity

$\Rightarrow$ **DAE: deterministic authenticated encryption**

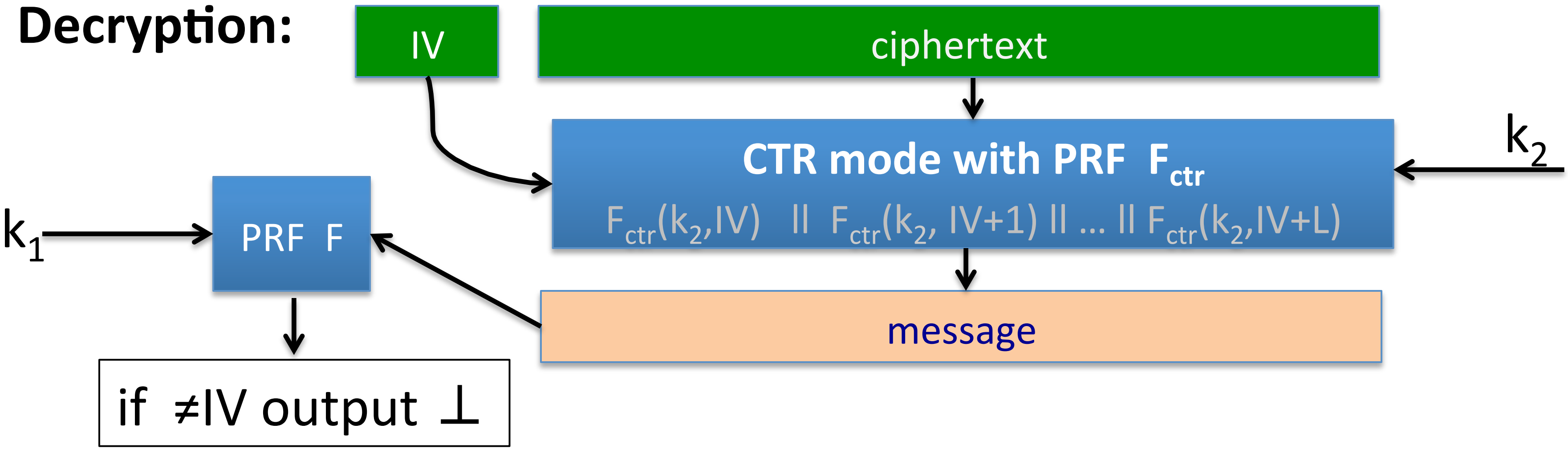
Consider a SIV special case: SIV-CTR

SIV where cipher is counter mode with rand. IV



Det. Auth. Enc. (DAE) for free

Decryption:



<u>Thm</u>: if F is a secure PRF and CTR from F_{ctr} is CPA-secure then SIV-CTR from F, F_{ctr} provides DAE

Construction 2: just use a PRP

Let (E, D) be a secure PRP. $E: K \times X \longrightarrow X$

Thm: (E,D) is sem. sec. under det. CPA .

Proof sketch: let $f: X \longrightarrow X$ be a truly random invertible func.

in EXP(0) adv. sees: $\mathbf{f(m_{1,0}), \ldots, f(m_{q,0})}$

q random values in X

in EXP(1) adv. sees: $\mathbf{f(m_{1,1}), \ldots, f(m_{q,1})}$

Using AES: Det. CPA secure encryption for 16 byte messages.

Longer messages?? Need PRPs on larger msg spaces …

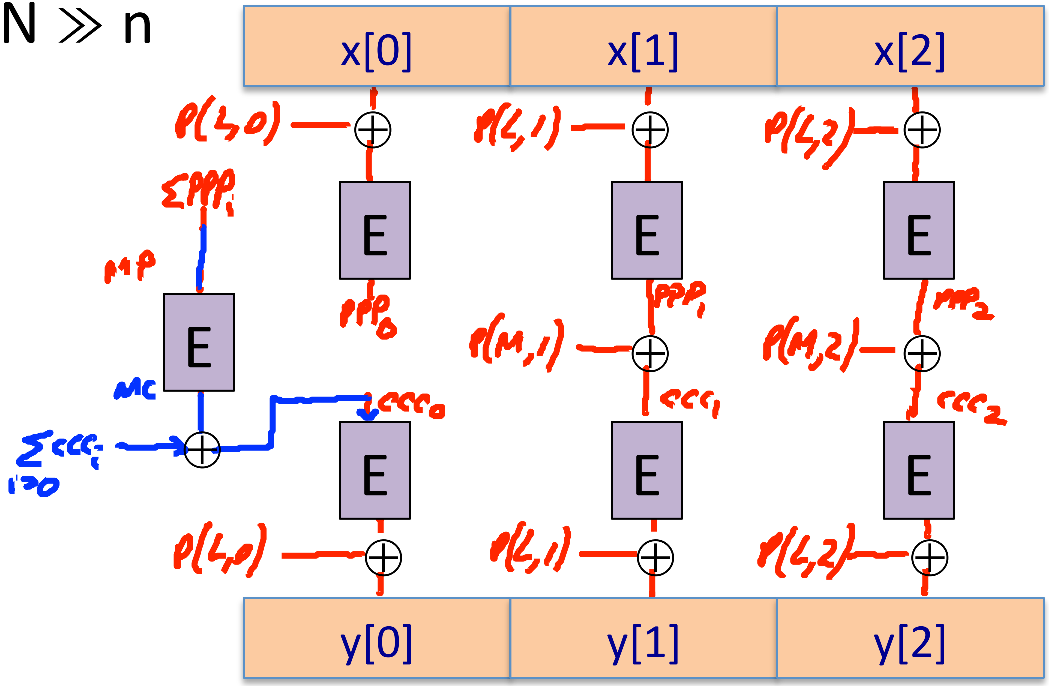
EME: constructing a wide block PRP

Let (E, D) be a secure PRP. $E: K \times \{0,1\}^n \longrightarrow \{0,1\}^n$

EME: a PRP on $\{0,1\}^N$ for $N \gg n$

Key = (K, L)

$M \longleftarrow MP \oplus MC$



Performance:

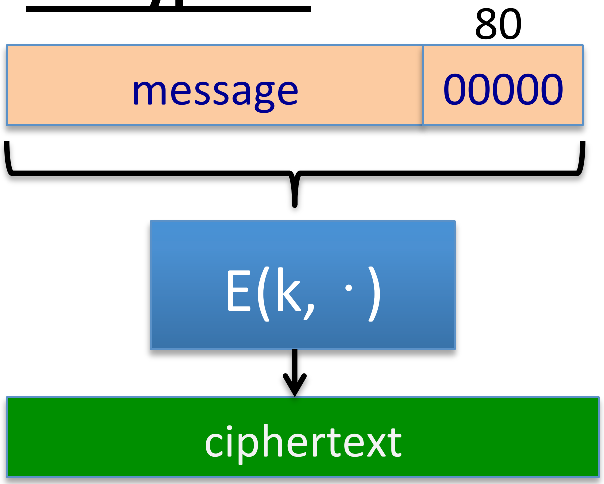
- can be 2x slower then SIV

PRP-based Det. Authenticated Enc.

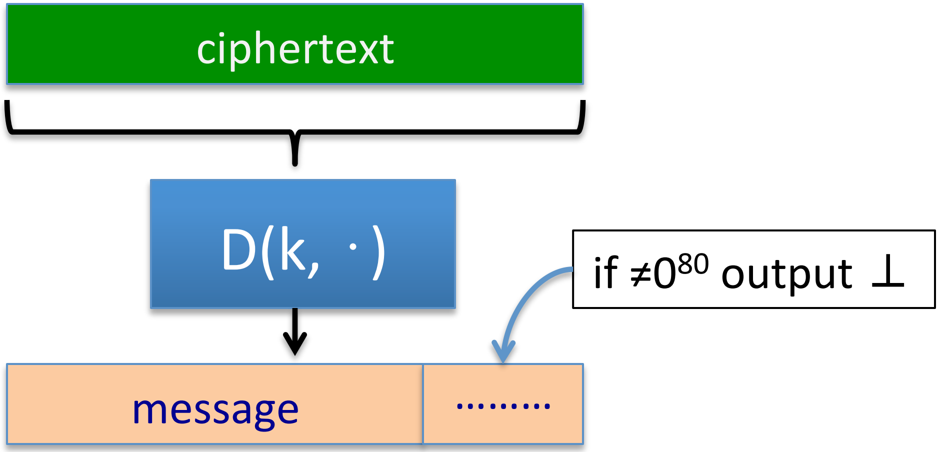
Goal: det. CPA security and ciphertext integrity

$\Rightarrow$ **DAE: deterministic authenticated encryption**

Encryption:



Decryption:



PRP-based Det. Authenticated Enc.

Let (E, D) be a secure PRP. $E: K \times (X \times \{0,1\}^n) \longrightarrow X \times \{0,1\}^n$

Thm: $1/2^n$ is negligible $\Rightarrow$ PRP-based enc. provides DAE

Proof sketch: suffices to prove ciphertext integrity

Chal.

$\pi \leftarrow \mathrm{Perms}\left[X \times \{0,1\}^n\right]$

$x_1, \ \ldots, \ x_q \in X$

$\pi(x_1\ 0^n), \ldots, \pi(x_q\ 0^n)$

$c \notin \{ \pi(x_1\ 0^n), \ldots, \pi(x_q\ 0^n) \}$

Adv.

But then $\Pr\left[\mathrm{LSB}_n(\pi^{-1}(c)) = 0^n \right] \leq$

End of Segment