

IV. Modes of operation – Counter mode

Definition 2.1 (restated) A private key encryption scheme Π consists of three probabilistic polynomial time algorithms Gen , Enc , Dec .

⋮
...

If Enc with $k \leftarrow \text{Gen}(1^n)$ works only for $m \in \{0,1\}^{l(n)}$, $l: \mathbb{N} \rightarrow \mathbb{N}$ a polynomial, then Π is called **fixed-length encryption scheme**.

Given fixed-length encryption scheme, how to encrypt long messages?

Pseudorandom functions and long messages

Construction 3.6 (restated) Let $F : \{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^*$ be a keyed, efficient, and length-preserving function. Define

$\Pi_F = (\text{Gen}_F, \text{Enc}_F, \text{Dec}_F)$ as follows:

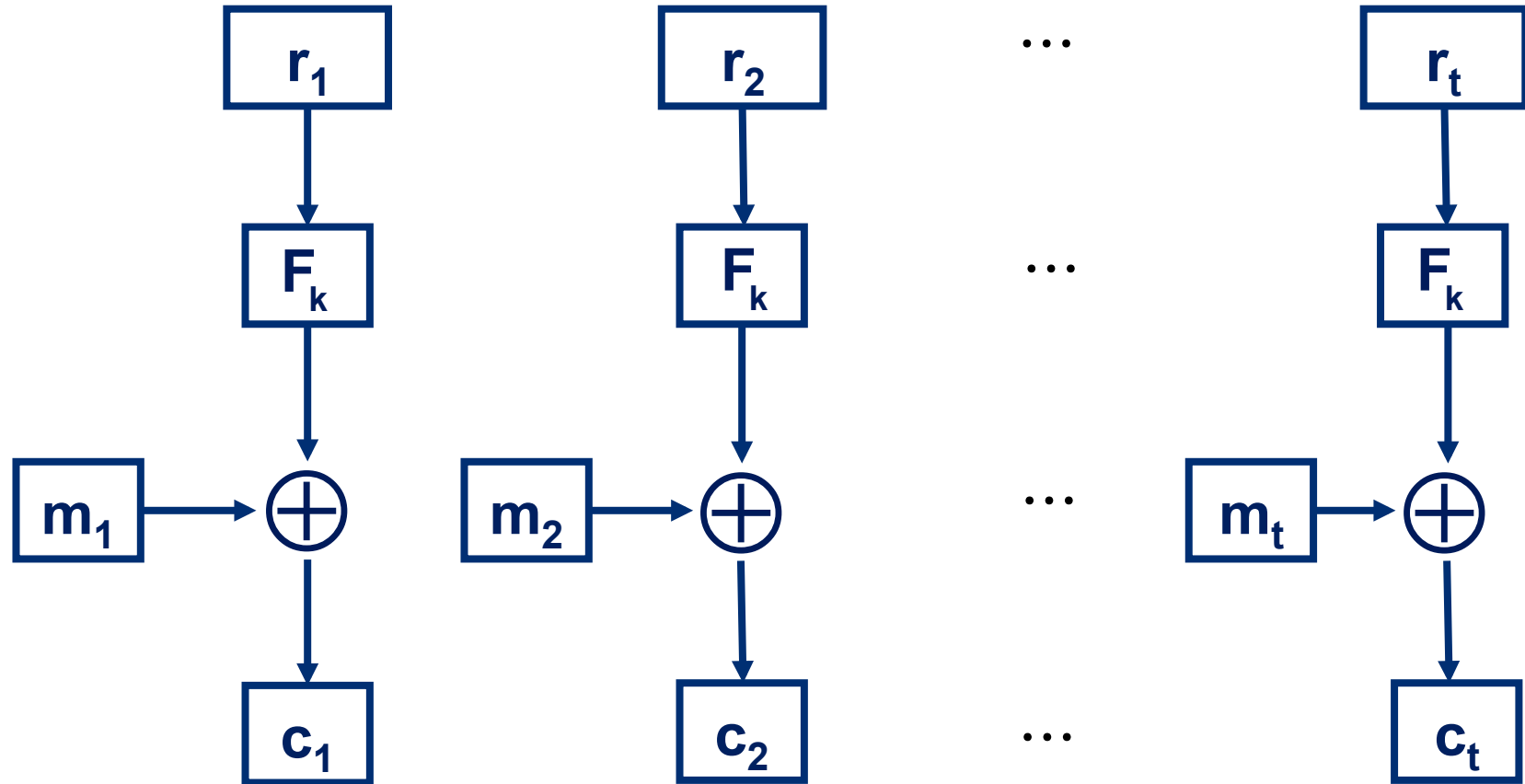
Gen_F : on input 1^n , choose $k \leftarrow \{0,1\}^n$.

Enc_F : on input $k, m \in \{0,1\}^n$, choose $r \leftarrow \{0,1\}^n$ and output $c := (r, m \oplus F_k(r))$.

Dec_F : on input $c = (r, s) \in \{0,1\}^n \times \{0,1\}^n$ and $k \in \{0,1\}^n$ output $m := s \oplus F_k(r)$.

Pseudorandom functions and long messages

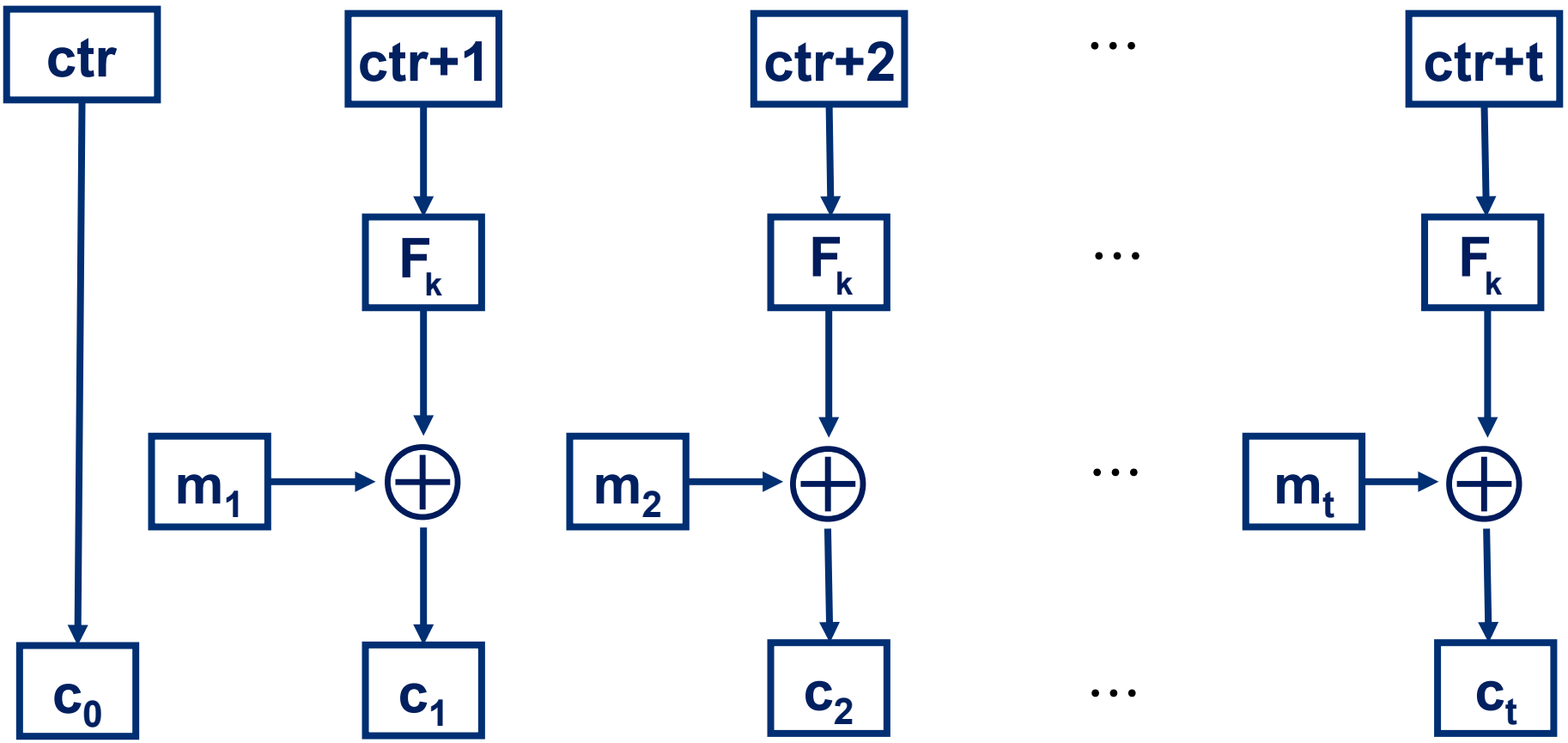
$$m = m_1 \parallel m_2 \parallel \dots \parallel m_t, m_i \in \{0,1\}^{l(n)}$$



$$\text{Enc}_F(m) = r_1 \parallel \dots \parallel r_t \parallel c_1 \parallel \dots \parallel c_t$$

Randomized counter mode - CTR

$$m = m_1 \parallel m_2 \parallel \dots \parallel m_t, m_i \in \{0,1\}^{l(n)}$$



$$Enc_F(m) = c_0 \parallel c_1 \parallel \dots \parallel c_t$$

ctr $\leftarrow \{0,1\}^n$, interpreted as n-bit number for addition

PRFs and CTR

Theorem 4.1 If F is a pseudorandom function, then randomized counter mode has indistinguishable encryptions under a chosen plaintext attack.

A conceptual scheme

Define $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ as follows:

Gen: on input 1^n , choose $f \leftarrow \text{Func}_n$.

Enc: on input $f, m \in \{0,1\}^*$, $m = m_1 \parallel \dots \parallel m_t, m_i \in \{0,1\}^n$,
choose $\text{ctr} \leftarrow \{0,1\}^n$ and output $\text{Enc}_f(m; \text{ctr})$, where
 $\text{Enc}_f(m; \text{ctr}) = \text{ctr} \parallel c_1 \parallel \dots \parallel c_t$ and $c_i := m_i \oplus f(\text{ctr} + i)$.

Dec: on input $c = c_0 \parallel c_1 \parallel \dots \parallel c_t$ and $f \in \text{Func}_n$
output $m := m_1 \parallel \dots \parallel m_t$, where $m_i := c_i \oplus f(c_0 + i)$.

Remark

- The scheme is not an encryption scheme, because it is not efficient. It is only used in the proof of Theorem 6.1.
- The CPA indistinguishability experiment can be defined for this scheme.

From adversaries to distinguishers

D on input 1^n and oracle access to $f : \{0,1\}^n \rightarrow \{0,1\}^n$

1. Simulate $A(1^n)$. When A queries for an encryption of $m \in \{0,1\}^*$, $m = m_1 \parallel \dots \parallel m_t$, $m_i \in \{0,1\}^n$ answer as follows:
 - a) $\text{ctr} \leftarrow \{0,1\}^n$ and query $f(\text{ctr} + i)$, $i = 1, \dots, t$
 - b) Compute and return $\text{Enc}_f(m; \text{ctr})$.
2. When A outputs m_0, m_1 , choose $b \leftarrow \{0,1\}$, then
 - a) $\text{ctr} \leftarrow \{0,1\}^n$ and query $f(\text{ctr} + i)$, $i = 1, \dots, t$
 - b) Compute and return $c := \text{Enc}_f(m_b; \text{ctr})$.
3. Continue to simulate A and answer encryption queries as in 1. Let A 's output be $b' \in \{0,1\}$. Output 1, if $b = b'$, otherwise output 0.

From PRF to cpa-security – two basic claims

Claim 1 For all ppts A

$$\begin{aligned} & \left| \Pr \left[\text{PrivK}_{A, \Pi_{\text{ctr}}}^{\text{cpa}}(n) = 1 \right] - \Pr \left[\text{PrivK}_{A, \Pi}^{\text{cpa}}(n) = 1 \right] \right| \\ &= \left| \Pr \left[D^{\text{F}_k(\cdot)}(1^n) = 1 \right] - \Pr \left[D^{\text{f}(\cdot)}(1^n) = 1 \right] \right|. \end{aligned}$$

Claim 2 Let A be a ppt adversary in $\text{PrivK}_{A, \Pi}^{\text{cpa}}$ and let $q(\cdot)$ be a polynomial such that on input 1^n ppt A chooses messages m_0, m_1 of length at most $q(n)$, makes at most $q(n)$ queries, and each query has length at most $q(n)$. Then

$$\left| \Pr \left[\text{Priv}_{A, \Pi}^{\text{cpa}}(n) = 1 \right] \right| \leq \frac{1}{2} + \frac{2q(n)^2}{2^n}.$$