VI. 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.

$\vdots$

$\ldots$

If Enc with $k \leftarrow \mathrm{Gen}\left(1^n\right)$ works only for $m \in \{0,1\}^{l(n)}$, $l : \mathbb{N} \to \mathbb{N}$ 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 $F : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ be a keyed, efficient, and length-preserving function. Define $\Pi_F = (\mathrm{Gen}_F, \mathrm{Enc}_F, \mathrm{Dec}_F)$ as follows:

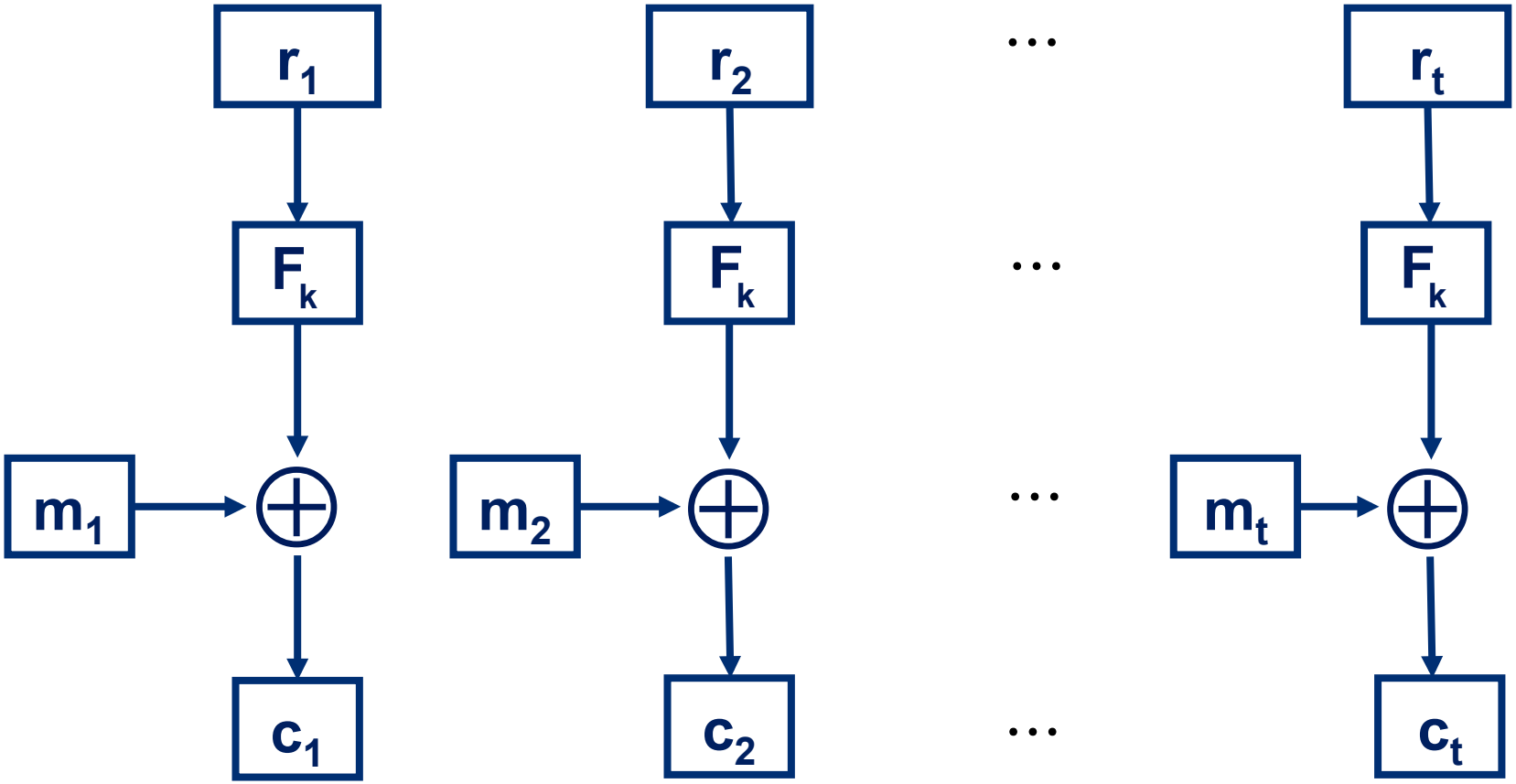
Gen_F : on input 1^n, choose $k \leftarrow \{0,1\}^n$.

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

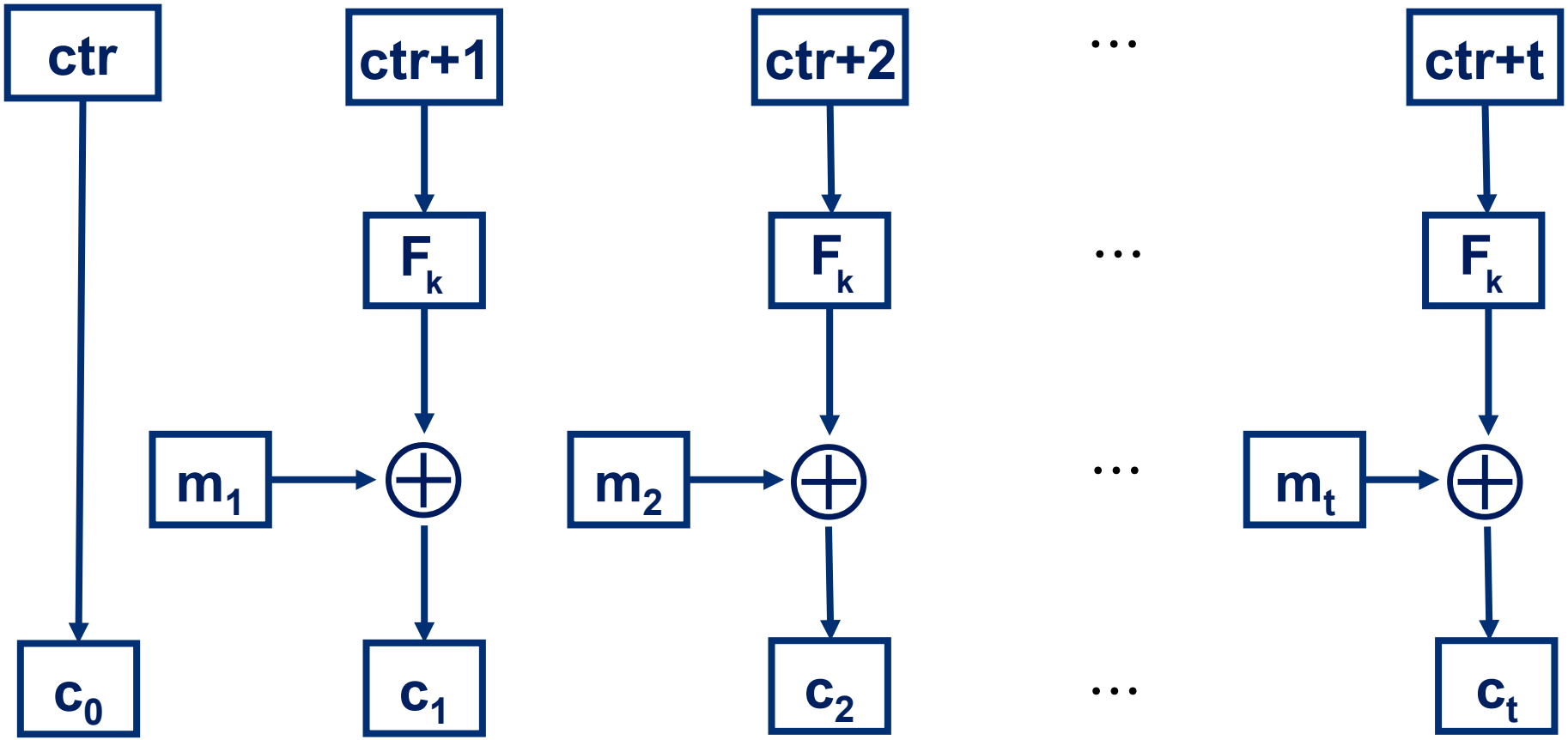
$m = m_1 \| m_2 \| \ldots \| m_t, m_i \in \{0,1\}^{l(n)}$



$Enc_F(m) = r_1 \| \ldots \| r_t \| c_1 \| \ldots \| c_t$

Randomized counter mode - CTR

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



$Enc_F(m) = c_0 \| c_1 \| \ldots \| c_t$

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

PRFs and CTR

Theorem 6.1 **If F ist a pseudorandom function, then randomized counter mode has indistinguishable encryptions under a chosen plaintext attack.**

A conceptual scheme

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

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

Enc: on input $f, m \in \{0,1\}^*, m = m_1 \| \ldots \| m_t, m_i \in \{0,1\}^n$,

choose $\mathrm{ctr} \leftarrow \{0,1\}^n$ and output $\mathrm{Enc}_f(m; \mathrm{ctr})$, where

$\mathrm{Enc}_f(m; \mathrm{ctr}) = \mathrm{ctr} \| c_1 \| \ldots \| c_t$ and $c_i := m_i \oplus f(\mathrm{ctr} + i)$.

Dec: on input $c = c_0 \| c_1 \| \ldots \| c_t$ and $f \in \mathrm{Func}_n$

output $m := m_1 \| \ldots \| m_t$, 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 indistiguishability experiment can be defined for this scheme.

From adversaries to distinguishers

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

1. Simulate $A(1^n)$. When A queries for an encryption of $m \in \{0,1\}^*, m = m_1 \| \ldots, \| m_t, m_i \in \{0,1\}^n$ answer as follows:
   a) $ctr \leftarrow \{0,1\}^n$ and query $f(ctr + i), i = 1, \ldots, t$
   b) Compute and return $Enc_f(m; ctr)$.
2. When A outputs m_0, m_1, choose $b \leftarrow \{0,1\}$, then
   a) $ctr \leftarrow \{0,1\}^n$ and query $f(ctr + i), i = 1, \ldots, t$
   b) Compute and return $c := Enc_f(m_b; ctr)$.
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

$$\left|\Pr\left[\mathrm{PrivK}^{\mathrm{cpa}}_{A,\Pi_F}(n)=1\right]-\Pr\left[\mathrm{PrivK}^{\mathrm{cpa}}_{A,\Pi}(n)=1\right]\right|$$

$$=\left|\Pr\left[D^{F_k(\cdot)}\left(1^n\right)=1\right]-\Pr\left[D^{f(\cdot)}\left(1^n\right)=1\right]\right|.$$

Claim 2 Let A be a ppt adversary in $\mathrm{PrivK}^{\mathrm{cpa}}_{A,\Pi}$ 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

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

The CCA indistinguishability game

CCA indistinguishability game $\mathrm{PrivK}^{cca}_{A,\Pi}(n)$

1. $k \leftarrow \mathrm{Gen}(1^n)$
2. A on input 1^n has access to encryption algorithm $\mathrm{Enc}_k(\cdot)$ and to decryption algorithm $\mathrm{Dec}_k(\cdot)$. A outputs 2 messages $m_0, m_1 \in \{0,1\}^*$ of equal length.
3. $b \leftarrow \{0,1\}$, $c \leftarrow \mathrm{Enc}_k(m_b)$. c is given to A.
4. $b' \leftarrow A(1^n, c)$, here A has access to encryption algorithm $\mathrm{Enc}_k(\cdot)$ and to decryption algorithm $\mathrm{Dec}_k(\cdot)$, but query $\mathrm{Dec}_k(c)$ is forbidden.
5. Output of experiment is 1, if $b = b'$. Otherwise output is 0.

CCA-security

Definition 3.8 $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ **has indistinguishable encryptions under chosen ciphertext attacks (is cca-secure) if for every probabilistic polynomial time algorithm A there is a negligible function** $\mu : \mathbb{N} \to \mathbb{R}^+$ **such that**

$$\Pr\left[\mathrm{PrivK}^{\mathrm{cca}}_{A,\Pi}(n) = 1\right] \leq 1/2 + \mu(n).$$

Observation cpa-security does not imply cca-security.