Modern Cryptography

Construction of CPA-secure sechemes

Sep 11, 2025

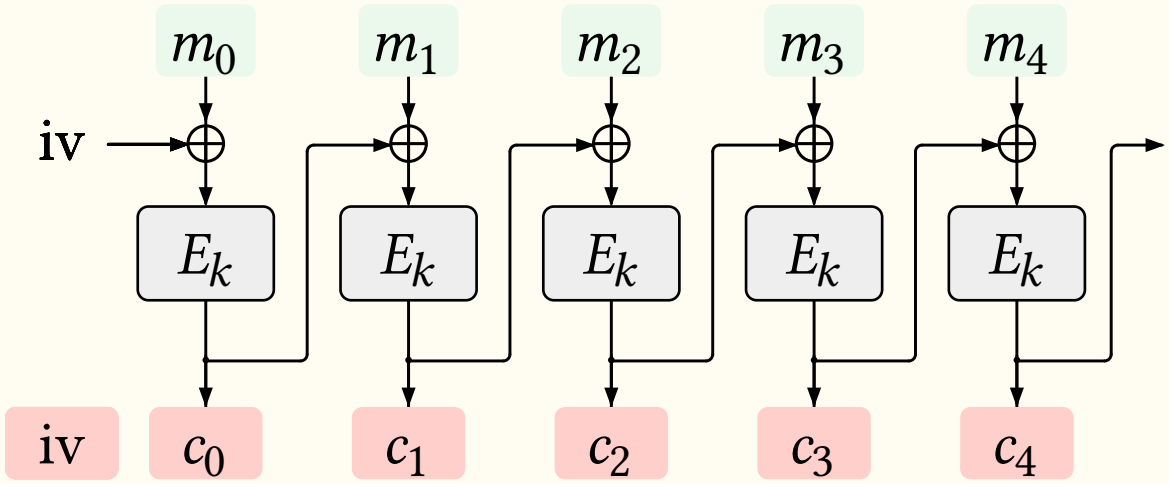
Dr Shashank Singh

Table of Contents

Modes of Operation of Block Ciphers

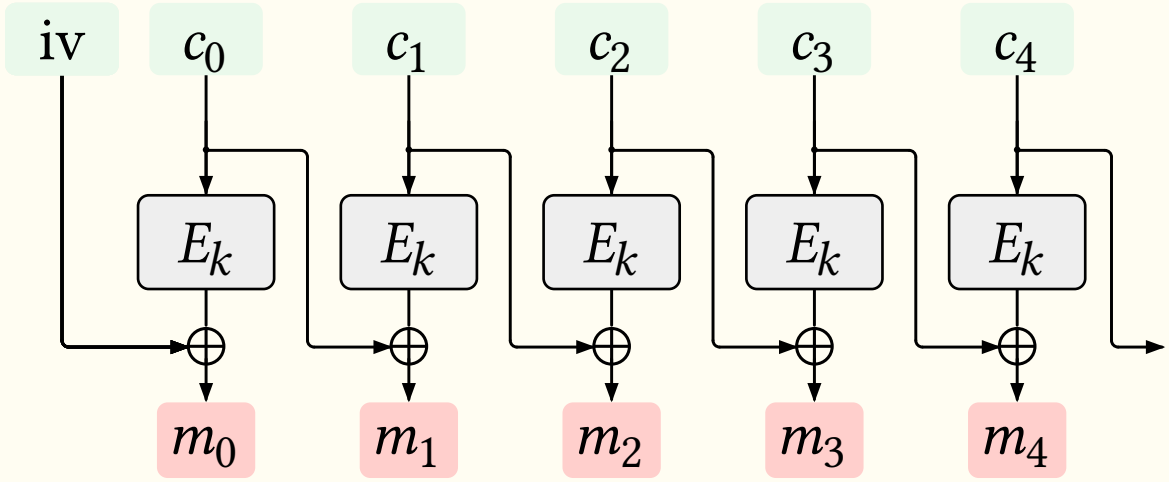
Cipher Block Chaining (CBC) MOP

Encryption:



- iv is the first cipher block of length n (the block size), randomly chosen.

Decryption:



Cipher Block Chaining (CBC) MOP..

- A random iv is required for each encryption.
- This scheme cannot be parallelised.
- Is it CPA secure? (Yes! The proof is left as an exercise.)
- **Stateful CBC**: In the stateful CBC mode of operation, for the first encryption, the iv is randomly chosen, and then onward, it is taken to be the last cipher block. (chained CBC mode used in SSL 3.0)

Theorem 1

Stateful CBC mode of operation is not CPA-secure. ♡

Proof. Proof by a counterexample. Construct an adversary $\mathcal{A}$, for which the experiment $\text{PrivK}^{\text{cpa}}_{\mathcal{A},\Pi}$ outputs 1, with probability better than half. □

Stateful CBC mode of operation is not CPA-secure

Recall, in the Stateful CBC mode of operation

$$\mathrm{ENC}_k(x_0 \mid x_1) = \left(\mathrm{iv} \mid \underbrace{F_k(x_0 \oplus \mathrm{iv})}_{c_0} \mid \underbrace{F_k(x_1 \oplus c_0)}_{c_1} \right), \quad \mathrm{ENC}_k(x_2) = F_k(x_2 \oplus c_1).$$

Stateful CBC mode of operation is not CPA-secure

Recall, in the Stateful CBC mode of operation

$$\mathrm{ENC}_k(x_0 \mid x_1) = \Big(\mathrm{iv} \mid \underbrace{F_k(x_0 \oplus \mathrm{iv})}_{c_0} \mid \underbrace{F_k(x_1 \oplus c_0)}_{c_1}\Big), \quad \mathrm{ENC}_k(x_2) = F_k(x_2 \oplus c_1).$$

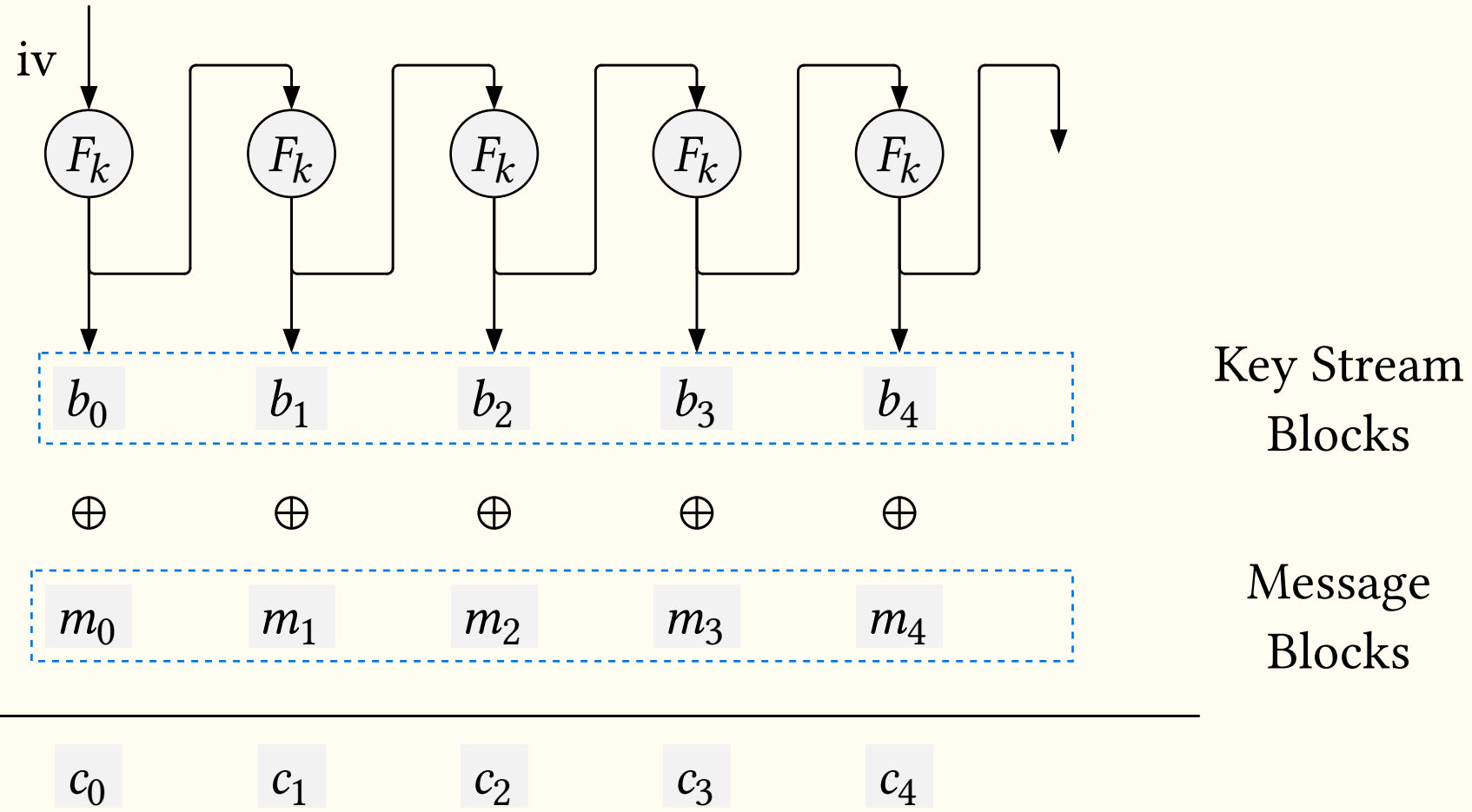
Indistinguishability Exp:

- $\mathscr{A}$ produces two-block messages: $m_0 = m_{0,0}|m_{0,1}$ and $m_1 = m_{1,0} \mid m_{1,1}$
- $\mathscr{A}$ recieves $(\mathrm{iv} \mid c_0 \mid c_1)$.
- Note that, $c_1 = F_k\big(c_0 \oplus m_{b,1}\big)$.
- $\mathscr{A}$ returns $b' = 1$ provided $c'' = c_1$, 0 otherwise.

Oracle Access:

- $\mathscr{A}$ has access to $\mathrm{ENC}_k(\cdot)$, the Stateful CBC.
- $\mathscr{A}$ picks a one block msg r.
- $(\mathrm{iv}' \mid c') \leftarrow \mathrm{ENC}_k(r)$
- $c'' \leftarrow \mathrm{ENC}_k\big(c' \oplus c_0 \oplus m_{1,1}\big)$

Output Feedback Mode (OFB)

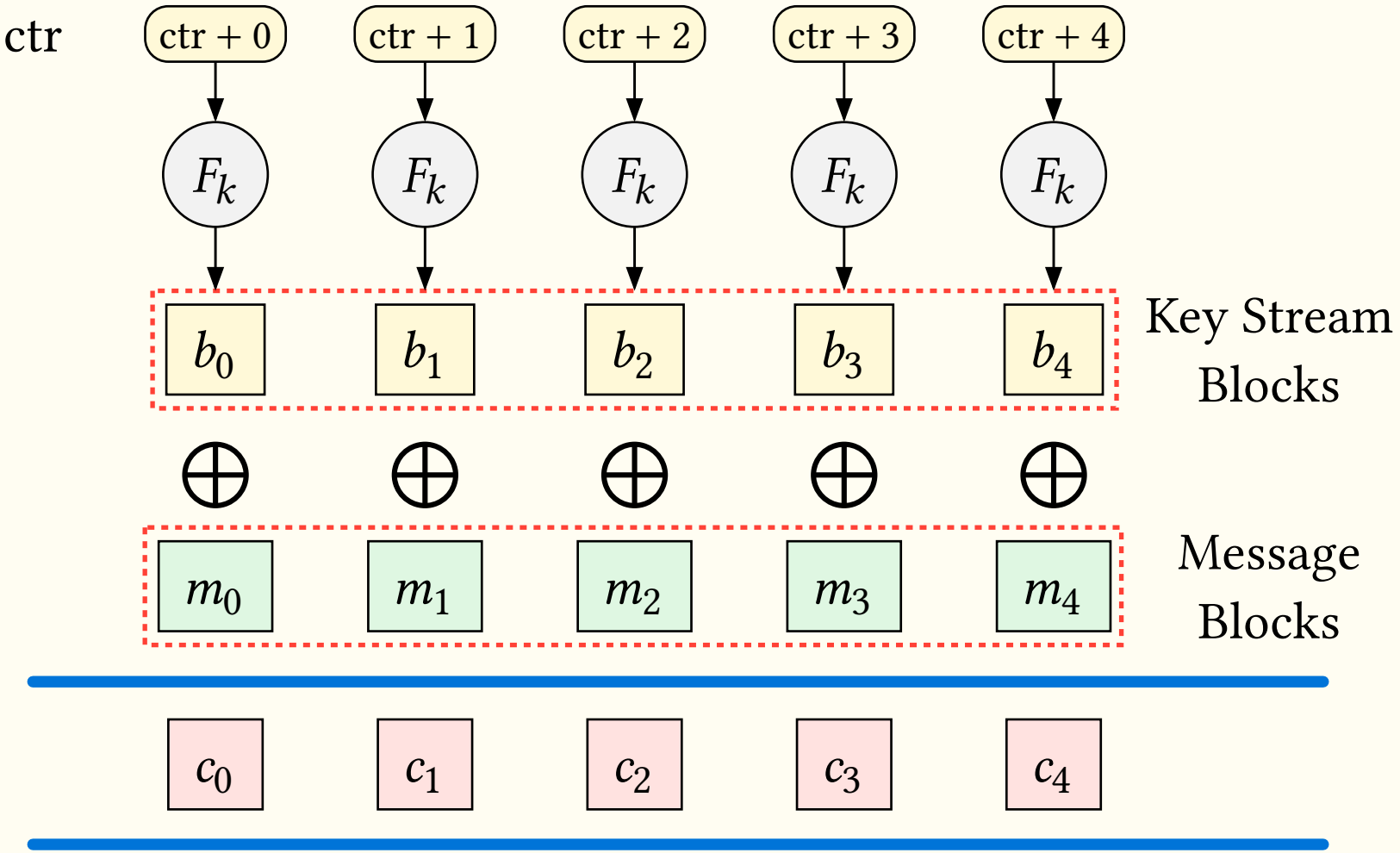


- Encryption and decryption algorithms are the same.

Output Feedback Mode (OFB)

- In output feedback mode, we do not require F_k to be invertible (PRP); any pseudorandom function (PRF) will suffice.
- No padding is necessary. It cannot be parallelised, but the key stream blocks can be generated in advance.
- The OFB mode and its stateful version are CPA-secure if the function F_k is a pseudorandom function.

The Counter Mode (CTR) of operation



- It has the same properties as the OFB, and it can be further parallelised. If F is PRF, CTR mode is CPA-secure. (Exercise)