

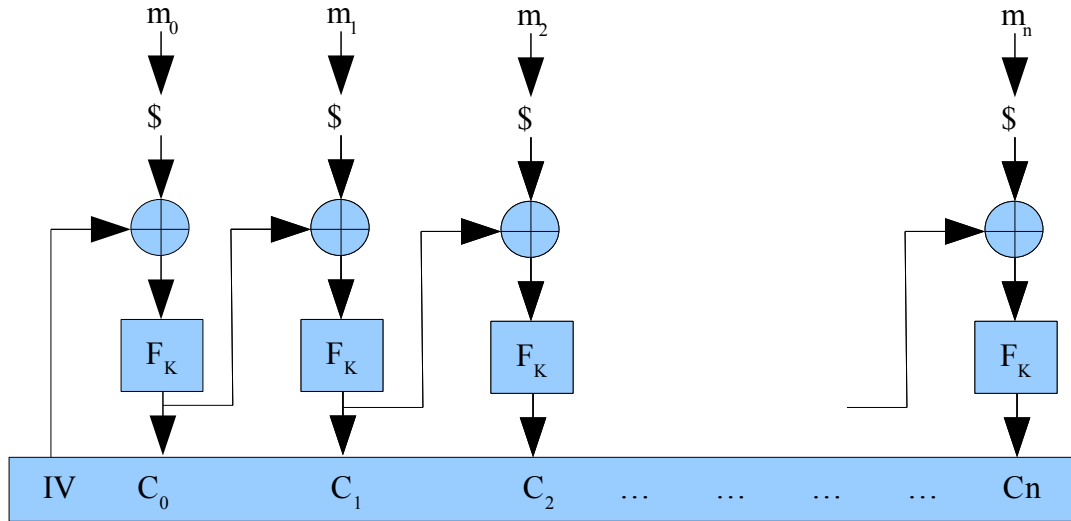
**Theorem:**

$CBC\$^F$  is  $(t - O(q), q, \epsilon + (q^2 / 2^{n+1}))$  RoR Secure if  $F$  is a  $(t, q, \epsilon)$  PRP, where  $n$  is the length of the IV.

**Proof:**

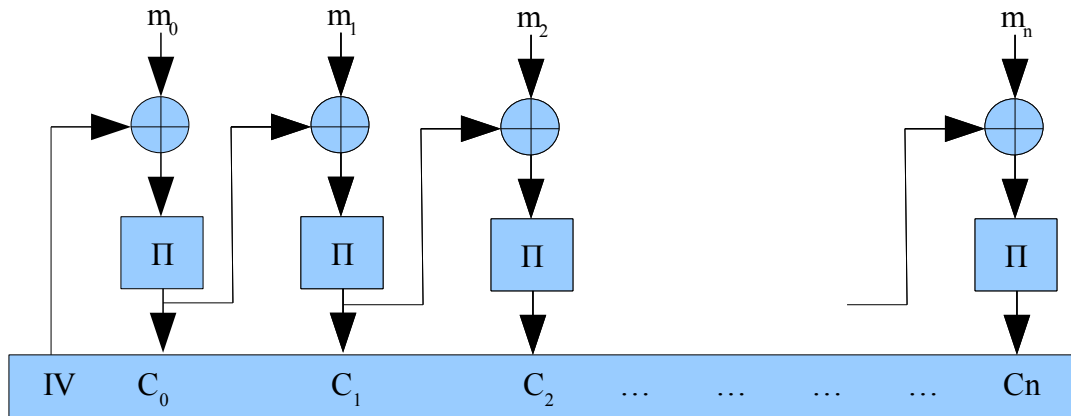
To prove the theorem we have to prove the indistinguishability of the construction from ideal world.

**Ideal World:**



**Real World:**

The real world uses  $F_K$  on message directly. As the PRP  $F_K$  is indistinguishable from a really random permutation  $\Pi$ , if we can prove the ideal world indistinguishable from the model of real world that uses the random permutation  $\Pi$  instead of  $F_K$ , we can prove the real and random worlds indistinguishable.



Our first target is to prove the ideal world indistinguishable from the above model that uses the random permutation  $\Pi$  instead of  $F_K$ . We see that the input to  $\Pi$  is an XOR of the plaintext of the current block ( $m_i$ ) and the ciphertext of the last block ( $C_{i-1}$ ). Let's call it  $X_i$ . Because  $\Pi$  is deterministic, if there is ever a repetition of this  $X$ , the two ciphertexts will be the same. In the ideal world however, the two outputs will still be different as the input to the PRP is not  $X$  but the XOR of  $\$(m_i)$  and  $C_{i-1}$ . In this case the attacker can distinguish between the real and ideal worlds. In all other cases, the two worlds are indistinguishable. Lets call the repetition of  $X$  our BAD event. This BAD event puts a limit on the indistinguishability of the Ideal world and our construction in the sense that the probability of distinguishing the two world is the same as the probability of the BAD event.

Lets quantify the probability that the previous construction is distinguishable from the Ideal World.

$$= \text{CBC}^{\Pi} \sim \text{CBC}^{\text{Fo}} \\ = |\Pr[A^{\text{CBC}^{\Pi}} = 1] - \Pr[A^{\text{CBC}^{\text{Fo}}} = 1]|$$

Now we calculate the probabilities as conditional on probability of BAD

$$= |\Pr[A^{\text{CBC}^{\Pi}} = 1 | \text{BAD}] \Pr[\text{BAD}] + \Pr[A^{\text{CBC}^{\Pi}} = 1 | \neg\text{BAD}] \Pr[\neg\text{BAD}] \\ - \Pr[A^{\text{CBC}^{\text{Fo}}} = 1 | \text{BAD}] \Pr[\text{BAD}] - \Pr[A^{\text{CBC}^{\text{Fo}}} = 1 | \neg\text{BAD}] \Pr[\neg\text{BAD}]| \\ \leq |\Pr[A^{\text{CBC}^{\Pi}} = 1 | \text{BAD}] \Pr[\text{BAD}] - \Pr[A^{\text{CBC}^{\text{Fo}}} = 1 | \text{BAD}] \Pr[\text{BAD}]| \\ + |\Pr[A^{\text{CBC}^{\Pi}} = 1 | \neg\text{BAD}] \Pr[\neg\text{BAD}] - \Pr[A^{\text{CBC}^{\text{Fo}}} = 1 | \neg\text{BAD}] \Pr[\neg\text{BAD}]|$$

The second part of the sum will be zero because if the BAD event does not happen the two cases are indistinguishable. The first part will be one because if the BAD event does happen, the attacker can immediately know that the two worlds are different. Though it is possible that even in the case BAD does happen, the adversary cannot differentiate the worlds but we are considering the worst case here. It also makes our scheme stronger.

$$= 1 * \Pr[\text{BAD}] + 0 * \Pr[\neg\text{BAD}] \\ = \Pr[\text{BAD}] \text{ (probability of finding a collision when } q, n \text{ bit values are chosen at random)} \\ \leq q^2/2^{n+1}$$

Now we have:

$$\text{CBC}^{\text{F}} \stackrel{t, q}{\approx} \text{CBC}^{\Pi} \quad \dots \text{ (I)}$$

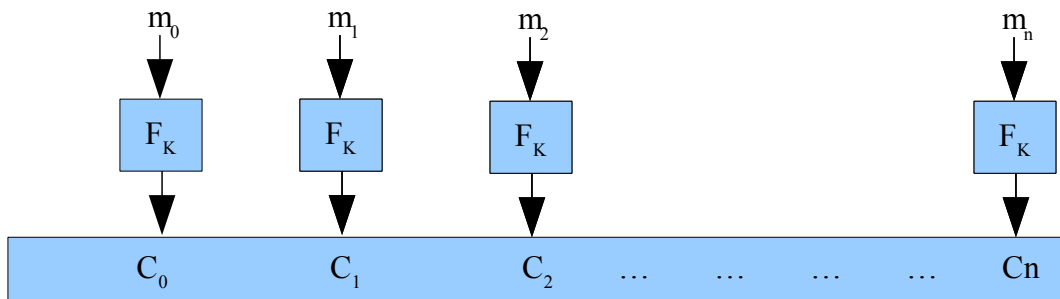
$$\text{CBC}^{\Pi} \stackrel{\infty, q}{\approx} \text{CBC}^{\text{Fo}} \quad \dots \text{ (II)}$$

From (I) and (II) and using data processing inequality and transitivity, we can derive:

$\text{CBC}^{\text{F}}$  is  $(t - O(q), q, \epsilon + (q^2 / 2^{n+1}))$  RoR Secure if F is a  $(t, q, \epsilon)$  PRP, where n is the length of the IV.

CBC mode is secure and efficient and is widely used for encryption. CTR mode has better theoretical security than CBC because the collision only depend on the IV and IV is in control of the system designer. In CBC mode the collisions depend on the value of X and it is more difficult to control it. On the other hand, in CTR mode, it is possible to selectively change bits in the plaintext by changing corresponding bits in the ciphertext while in the CBC mode, changing few bits in the ciphertext will also affect bits in the future plaintext and hence it is more difficult to selectively change bits and launch a successful attack. The CTR mode can be used with message integrity constructs in order to thwart such selective bit altering attacks.

**ECB Mode using PRP:**



ECB mode is insecure because it is deterministic and whenever plaintext is repeated, the ciphertext will be repeated as well.

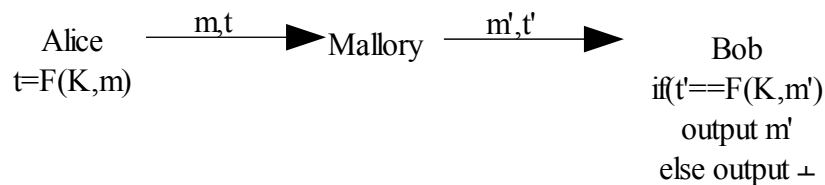
**Message Integrity:**

Even if the communication between Alice and Bob is encrypted, Mallory can flip the bits of the ciphertext and in some cases can actually change the content of the message by selectively flipping ciphertext bits.

Standard way to achieve Message Integrity is Message Integrity Code/ Message Authentication Code.

**Properties:**

- Alice and Bob share a key, this key is not used for encryption but for Message Authentication
- Alice computes a tag  $t = F(K, m)$  and sends it along with the message.
- Bob receives message  $m'$  and tag  $t'$  and computes  $F(K, m')$ . If  $t' = F(K, m')$ , the message is authentic otherwise not.



In the real world it looks more like:

