Lecture 2

Thursday, 17 November 2022 10:41

proofs allow quick development of protocols

focus cryptanalytic research on fewer targets

enforce the use of formal security statements

today: are proofs and their assumptions correct?

- are the assumptions true?
- are the assumptions used correctly?
- does the proof really say what you think it does?
- is the proof itself correct?

block cipher

message $\in \mathbb{B}^n$ ↓

key $\in \mathbb{B}^\lambda$ ⟶ blockcipher

↓ ciphertext $\in \mathbb{B}^n$

keyed permutation / pseudorandom permutation

if k is unknown, output is indistinguishable from random permutation

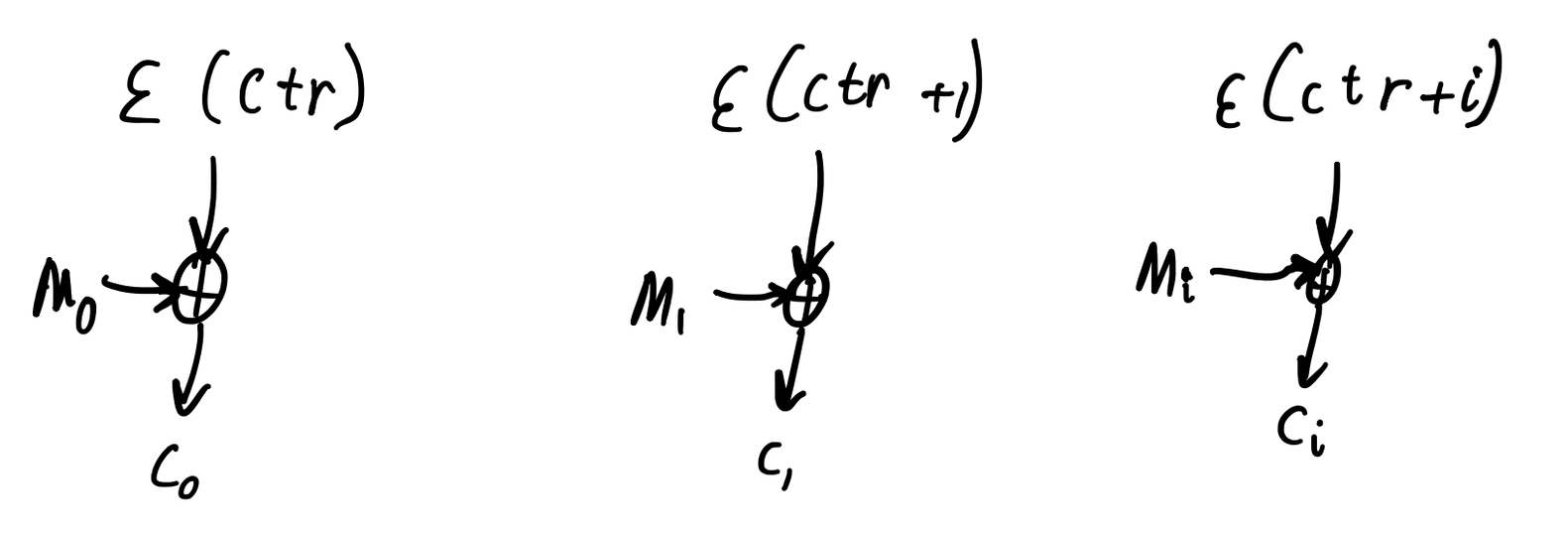
PRP-security in CPA setting: difference between probability of output having come from encryption oracle or truly random permutation is negligible

PRP-security in CCA setting: same, but inverse (i.e. decryption or inverse permutation) is also made available

this is not an encryption scheme

counter mode (CTR)

$ctr \leftarrow \mathbb{Z}_{2^N}$



block ciphers are not encryption schemes

secure modes are important and non-trivial

confidentiality alone is usually not enough!

AE (AD)

→ authenticated encryption (with associated data)

ciphertext does not reveal information about the plaintext → except for its length

even with an encryption (and a decryption) oracle
even if the adversary chooses the nonces

it is impossible to create a valid ciphertext without knowledge of the key
even with an encryption and a decryption oracle

essentially IND\$-CPA + EU-CMA (with adversarially chosen nonces)

together imply CCA-security

OCB 2

offset codebook method 2

tweakable blockcipher

similar to regular blockciphers, but takes an additional tweak (e.g. public randomness)

indistinguishable from a random permutation per tweak and per key

XEX (xor, encrypt, xor), XE (xor, encrypt)

example

$k = 2$

$\alpha_1 = x \rightarrow 2$ $\quad\quad$ $\alpha_2 = x+1 \rightarrow 3$

$\mathbb{I}_1 \subset \{0, 2^{big}\}$ $\quad\quad$ $\mathbb{I}_2 \subset \{0, 1\}$

$\mathbb{I} = \mathbb{I}_1 \times \mathbb{I}_2$

$2^3 \cdot 3^0 \neq 2^7 \cdot 3^1$

game hopping

$C[1] = 2 \cdot L \cdot Enc(2L \oplus fl)$ (L = Enc(N), N = nonce; fl = length encoding of full length block)

$C[2] = M[2] \oplus Enc(fl \oplus 2^2 \cdot L)$

$C' = C[1] \oplus fl \longrightarrow M' = C' \oplus pad = C' \oplus Enc(2L \oplus fl)$

$= C[1] \oplus fl \oplus Enc(2L \oplus fl)$

$= 2L \cdot Enc(2L \oplus fl) \oplus fl \oplus Enc(2L \oplus fl)$

$= 2L \oplus fl$

$T' = M[2] \oplus C[2]$

$2 \cdot 3 = (x)(x+1) + x = x^2 + x + x = x^2$

$T^* = Enc(2^1 \cdot 3^1 \cdot L \oplus 2L \oplus fl)$

$= Enc(2^2 \cdot L \oplus fl)$

$= pad$

$= M[2] \oplus C[2]$

$= T'$

→ valid forgery