IACR Forums: (Published after 2015)

- Eurocrypt
- Asiacrypt
- Crypto (UCSB)
- TCC

(Crypto)

- STOC
- FOCS

(Theoretical CS)

- QCrypt (Quantum Crypto)

Choose 5 papers (that haven't been extended) from these conferences

Report should have:

Adv model, network model, key problem, Structure, identify crypto primitives (Ex: PRG, PRF, One Way fns) & their overviews

Cover Intro. & Technical Overview

(No need mathematical proofs & results)

Watch the presentation for the paper

Look for ZKP in Succinctness track + Succinctness in ZKP track

Make Contributions section in report

Review: Probabilistic Encryption

PRF $F_k(\cdot)$

$c := \langle r, F_k(r) \oplus m \rangle$

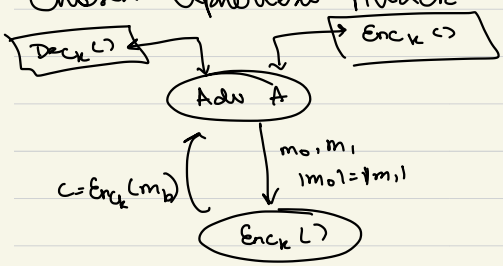
Other modes of operations for PRFs)

Block Ciphers: CBC (Cipher Block Chaining) $c_i := F_k(c_{i-1} \oplus m_i)$

Output Feedback (OFB): $r_i = F_k^{(i)}(r_0)$

Randomized Counter $r_i := F_k(r_0 + i)$

Chosen Ciphertext Attack:

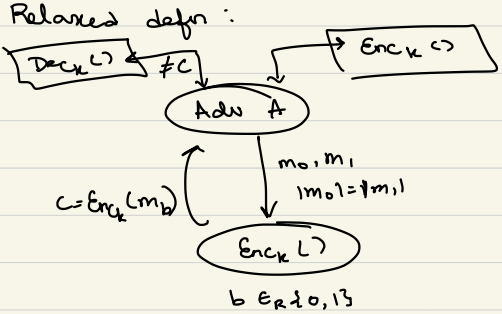


$P_R[b' = b] \leq \frac{1}{2} + negl(n)$ $\forall$ PPTM A

scheme is CCA secure.

No scheme can be CCA secure by this definition since the adversary can decrypt the challenge ciphertext & decide b with probability 1.

Relaxed defn:



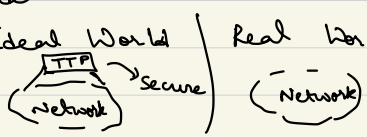
Adv. A cannot decrypt challenge ciphertext c.

Indistinguishability based defns. are harder to define but easier to work with

then simulation based defns.

Simulation based Defn.:

Assume a trusted third party (TTP) accessible from anywhere in the network in an ideal world.



$\forall$ PPTM adv A $\in$ Real World, $\exists$ adv S $\in$ Ideal World $\ni$

View (S) $\equiv$ View (A)

(View can be i.i.d or computationally ind. or statistically ind.)

Encryption scheme is secure if real world simulates the ideal world.

Showing that the old prob. scheme is not CCA secure

Let $m_0 = 0^{n-1}1$, $m_1 = 1^{n-1}0$

$c = \langle r, F_k(r) \oplus m \rangle$

$c' = \langle r, \text{LSB flipped } (F_k(r) \oplus m) \rangle$

Decrypt c' to get the flipped LSB of m.

If 0, then m_0 else m_1

This is a malleable encryption scheme, we know what change can be made in ciphertext to change plaintext without knowing the plaintext → message can be modified without knowing the message.

Message Authentication Codes (MAC)

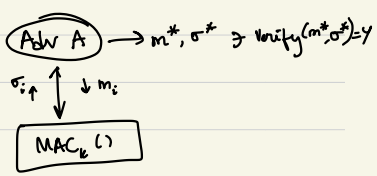
$MAC_k : \{0,1\}^n \rightarrow \{0,1\}^n \times \{0,1\}^n$

$MAC_k(m) = \langle m, \sigma \rangle$ ↳ Tag

The goal is not encryption but to ensure message isn't changed.

$Verify_k(m, \sigma) \rightarrow$ Yes / No

Secure $MAC_k()$:



$Q = \{m \mid \text{Adv queried } m \text{ to MAC}\}$

$P[m^* \notin Q, Vrfy(m^*, \sigma^*) = Y] \leq negl(n)$

Adv. should not be able to produce a valid tag for a new message.

CCA Security using MAC:

Encrypt-Then-Authenticate

$c = \langle c_i = CPA\text{-}Sec\text{-}Enc_{k_1}(m), MAC_{k_2}(c_i) \rangle$

CPA Security + Secure MAC = CCA Security

MAC & Transport Layer Security does not handle replay attack (sending same $\langle m, \sigma \rangle$ to verify). Applications should use timestamps.