Message Authentication Code (MAC) & Chosen-Ciphertext Attack

$CCAExp_A^{\mathcal{E}}(n)$

$K \leftarrow G(1^n)$

$(m_0, m_1) \leftarrow A(1^n)^{E(K,\cdot), D(K,\cdot)}$

$b \leftarrow \{0,1\}$

$c = E(K, m_b)$

$\hat{b} \leftarrow A(1^n)^{E(K,\cdot), D(K,\cdot)}$

if $b = \hat{b}$ return 1

else return 0

$\mathcal{E} = (G, E, D)$ is a private-key encryption scheme

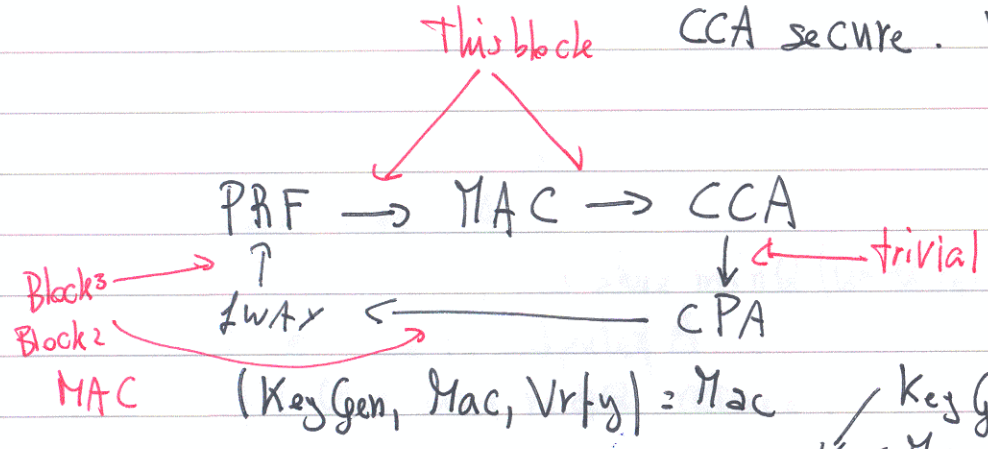
A is a PPT adversary

$\mathcal{E}$ is CCA-secure if $\forall$ PPT

$$Prob[CCAExp_A^{\mathcal{E}}(n) = 1] \leq \frac{1}{2} + \nu(n)$$

cannot ask for decryption of c

Obs. The CPA-secure encryption scheme based on PRF obtained in Block 3 is not CCA secure. Why? Exercise for students



MAC $(KeyGen, Mac, Vrfy) : Mac$

PPT: $KeyGen \rightarrow Key$

$Mac : Message + Key \rightarrow Tag$

$Vrfy : Message + Key + Tag \rightarrow 0/1$

$MACExp_A^{Mac}(n)$

$k \leftarrow KeyGen(1^n)$

$(m, t) \leftarrow A^{Mac(\cdot,k)}$ (set of queries)

If $Vrfy(m, k, t) = 1 \wedge (m \notin Q)$

then return 1

Mac unforgeable if

$\forall$ PPT A

$$Prob[MacExp_A^{Mac}(n) = 1] \leq \nu(n)$$

PRF → MAC

$|m| = n$

Let F be a family of PRF

Mac for messages of length n

KeyGen (1^n)
$k \leftarrow \{0,1\}^n$
return k

$Mac(m,k)$
return $t = f_k(m)$

$Vrfy(m,k,t)$
1 iff $t = f_k(m)$

Thm If F is a PRF then Mac is unforgeable

Pf.

Consider $RMacExp$ that is the experiment in which A's queries are answered not by running $Mac(m,k)$ but by running modified Mac in which we use a truly random function instead of f_k.

$Prob[RMacExp(1^n)=1] \leq 2^{-n}$. If $\exists A$ s.t. $Prob[MacExp(1^n)=1] \geq \frac{1}{poly(n)}$ then we can construct D that distinguishes PRF from RF

$D^O(1^n)$
- run $A(1^n)$ with $Q = \emptyset$
  query m from A
  return $O(m)$ and store $\min Q\ (Q \leftarrow Q \cup \{m\})$
- let (m,t) be the output of A
- if $t = O(m)$ and $m \notin Q$ return 1
  else return 0

If O is a PRF then A's view is like in $MacExp \Rightarrow$
$Prob[D^{f_k}=1] = Prob[MacExp(1^n)=1] \geq \frac{1}{poly(n)}$

If O is a RF then A's view is like in $RMacExp \Rightarrow$
$Prob[D^f=1] = Prob[RMacExp(1^n)=1] = 2^{-n}$

$\Rightarrow$ D break the pseudorandomness of F. ∎