SOLUTION OF EXERCISESHEET 8

Exercise 8-1

Given Π_{MAC} = (Gen, Enc, Ver)

To prove by reduction as in Figure 1

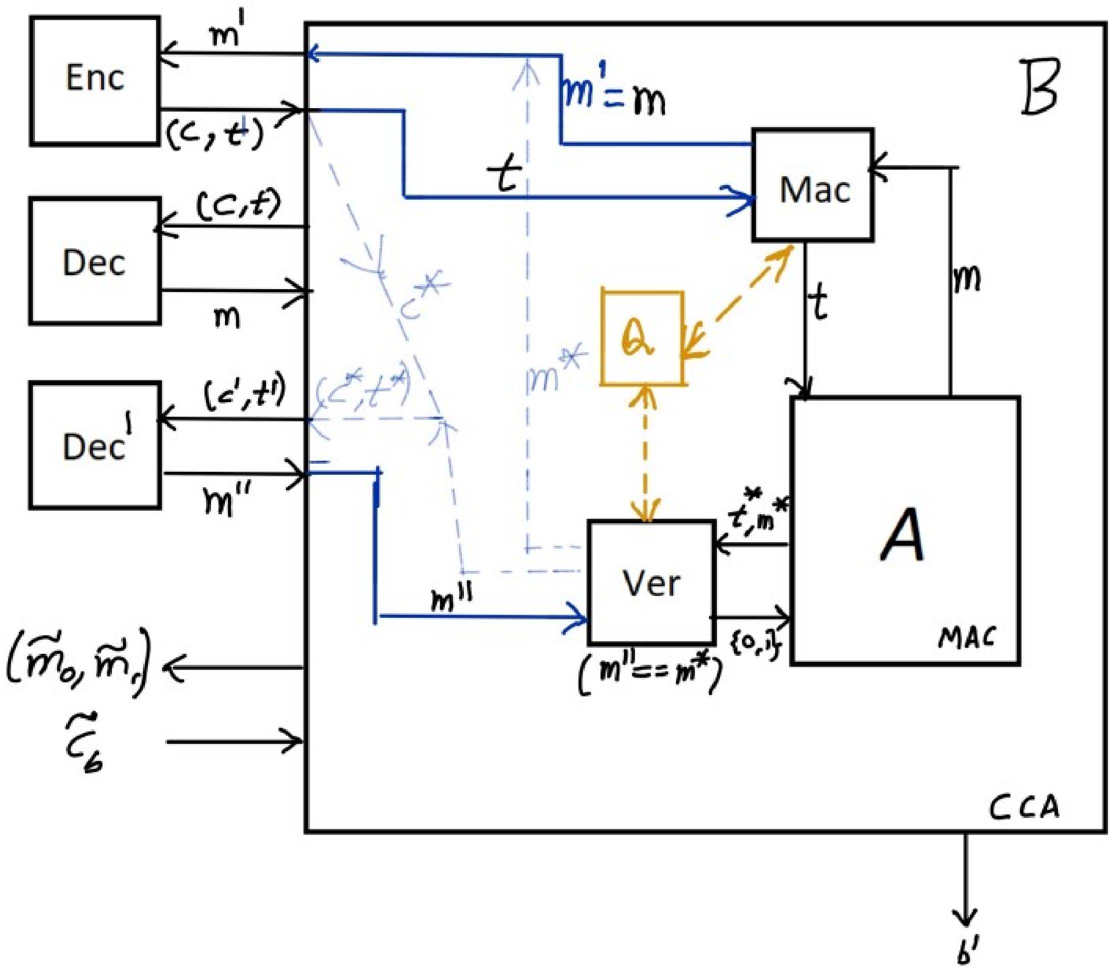

Figure 1: Proof by Reduction

Lets assume contradiction i.e., the MAC construction is not secure $\Rightarrow$ Probablity of forging this construction Π_{MAC} is a non negligible function. i.e.,

$$Pr[MacForge_{A,\Pi_{MAC}} = 1] \leq \epsilon(\lambda)$$

where $\epsilon(\lambda)$ is a non negligible function.

That implies there exists an adversary, A, able to generate a new message and tag pair (m^*, t^*) such that $m^* \notin Q$, and $Ver_k(m^*, t^*) == 1$ with a probablity $\epsilon(\lambda)$.

SOLUTION OF EXERCISESHEET 8

We now consider B attacking the MAC i.e., B runs A as subroutine. B choose two messages, lets say $\widetilde{m_0}$ and $\widetilde{m_1}$ as m^* and any other random message respectively. If B gets the tag a t^*, it corresponds to m^* otherwise it correponds to random message. So here the success probablity of B is,

$$Pr[PrivK^{CCA}_{B,\Pi'}(\lambda) = 1] \leq |1 - (\epsilon(\lambda)/2)| \tag{1}$$

But given that Π is a CCA secure enryption scheme. So for CCA secure Adversary A',

$$Pr[PrivK^{CCA}_{A',\Pi}(\lambda) = 1] \leq 1/2 + neg(\lambda) \tag{2}$$

where $neg(\lambda)$ is a negligible function.

Both equations (1) and (2) are valid only when unless $\epsilon(\lambda)$ is a negligible function which is contradiction to our assumption. Hence our assumption that such an Adversary exists is false. And the construction is secure.

Exercise 8-2

Exercise 8-3

Exercise 8-4

To show: $H(m) : \{0,1\}^{2k} \to \{0,1\}^{k+n}, H(m) := m_0||H'(m_1)$ is still a collision-resistant hash function when $m = m_0||m_1, |m_0| = |m_1| = k$ and $k > n$. $H'(m) : \{0,1\}^* \to \{0,1\}^n$ is a collision-resistant hash function.

Proof by contradiction. We assume there is an adversary $\mathcal{A}$, who can break the collision-resistance of $H(m)$ with non-negligible probability. We now build an adversary $\mathcal{B}$ against the collision-resistance of $H'(m)$ who invokes $\mathcal{A}$. When $\mathcal{B}$ gets the hash value $s' = H'(m_1)$ he prepends m_0, which he samples randomly. So he can give $s = m_0||s' = m_0||H'(m_1)$ to the adversary $\mathcal{A}$. $\mathcal{A}$ then outputs two messages x_1, x_2. $\mathcal{B}$ computes his output by truncating the first half of x_1 and x_2.

How does he knows $|m_1| = k$

$\mathcal{B}$ is an efficient adversary because $\mathcal{A}$ is efficient, so the message length is poly and the call to $\mathcal{A}$ needs only poly time and sampling and prepend m_0 and truncating bit from x_1 and x_2 can also be done in polynomial time.

To analyse the success, we know, that with non-negligible probability $\mathcal{A}$ outputs two messages x_1, x_2 with $x_1 \neq x_2$ and $H^s(x_1) = H^s(x_2)$. $\mathcal{B}$ outputs only the second half of x_1 and x_2 which results in x_1', x_2'. The probability that these are equal is $\left(\frac{1}{2}\right)^k$, because for each position the probability that the bits are equal is $\frac{1}{2}$. Therefore it holds that

$$Pr[HashColl_{\mathcal{B}}(\lambda) = 1] = Pr[HashColl_{\mathcal{A}}(\lambda) = 1] - Pr[x_1' == x_2'] = \texttt{non-negl.} - \left(\frac{1}{2}\right)^k = \texttt{non-negl.}$$

Because this is a contradiction to the collision-resistance of $H'(m)$ such an adversary $\mathcal{A}$ cannot exist.

It follows that $H(m)$ is a collision-resistant hash function.