

## Page 1 of 2

## SOLUTION OF EXERCISESHEET 8

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

That implies

$$Pr[PrivK_{A,\Pi}(\lambda) = 1 \wedge \overline{ValidQuery}] \leq \epsilon(\lambda) \quad (1)$$

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

But given that  $\Pi$  is a CCA secure encryption scheme. And for CCA,

$$Pr[PrivK_{A,\Pi}^{CCA}(\lambda) = 1 \wedge \overline{ValidQuery}] \leq 1/2 + neg(\lambda) \quad (2)$$

Equation (1) and (2) are contradicting to each other. Thus our assumption is false and this construction is secure.

### Exercise 8-2

### Exercise 8-3

### Exercise 8-4

**To show:**  $H(m) : \{0, 1\}^{2k} \rightarrow \{0, 1\}^{k+n}$ ,  $H(m) := m_0 || H'(m_1)$  is still a collision-resistant hash function when  $m = m_0 || m_1$ ,  $|m_0| = |m_1| = k$  and  $k > n$ .  $H'(m) : \{0, 1\}^* \rightarrow \{0, 1\}^n$  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  $x_2$ .

$\mathcal{B}$  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

$$Pr[HashColl_{\mathcal{B}}(\lambda) = 1] = Pr[HashColl_{\mathcal{A}}(\lambda) = 1] - Pr[x'_1 = x'_2] = \text{non-negl.} - \left(\frac{1}{2}\right)^k = \text{non-negl.}$$

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.

How does he know  $|m_1| = k$ ?