

SOLUTION OF EXERCISESHEET 8

Exercise 8-1

Given $\Pi_{MAC} = (Gen, Enc, Ver)$

$$t \leftarrow c = Enc(k, m)$$

To prove if this construction is secure or not, the reduction is as in Figure 1

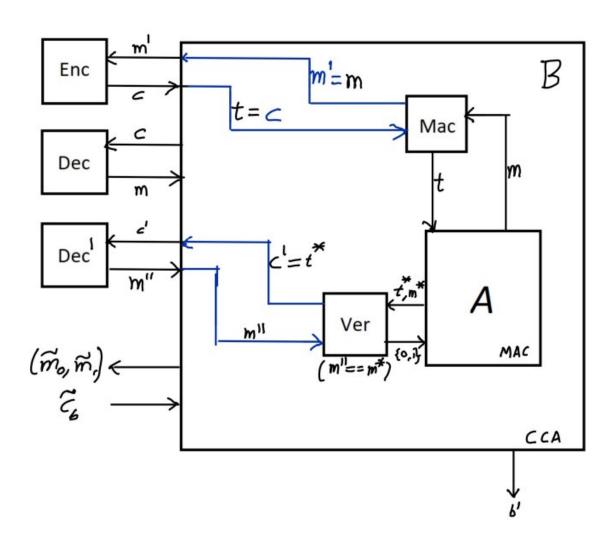


Figure 1: Proof by Reduction

First lets assume the contradiction that the construction is not secure MAC. That is probablity of forging this construction Π_{MAC} is a non negligible function. i.e.,

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

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

Theresa, Celine, Prisca, Saibaba December 12, 2022





SOLUTION OF EXERCISESHEET 8

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 $\epsilon(\lambda)$.

That implies

$$Pr[PrivK_{A,\Pi}(\lambda) = 1 \land \overline{ValidQuery}] \le \epsilon(\lambda)$$
 (1)

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

But given that Π is a CCA secure enryption scheme. And for CCA,

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

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

Exercise 8-2

Exercise 8-3

Exercise 8-4

To show: $H(m): \{0,1\}^{2k} \to \{0,1\}^{k+n}, H(m):=m_0||H'(m_1)$ 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 .

 $\mathcal B$ 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.