Solution of Exercisesheet 8

Exercise 8-1

Given Π_{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

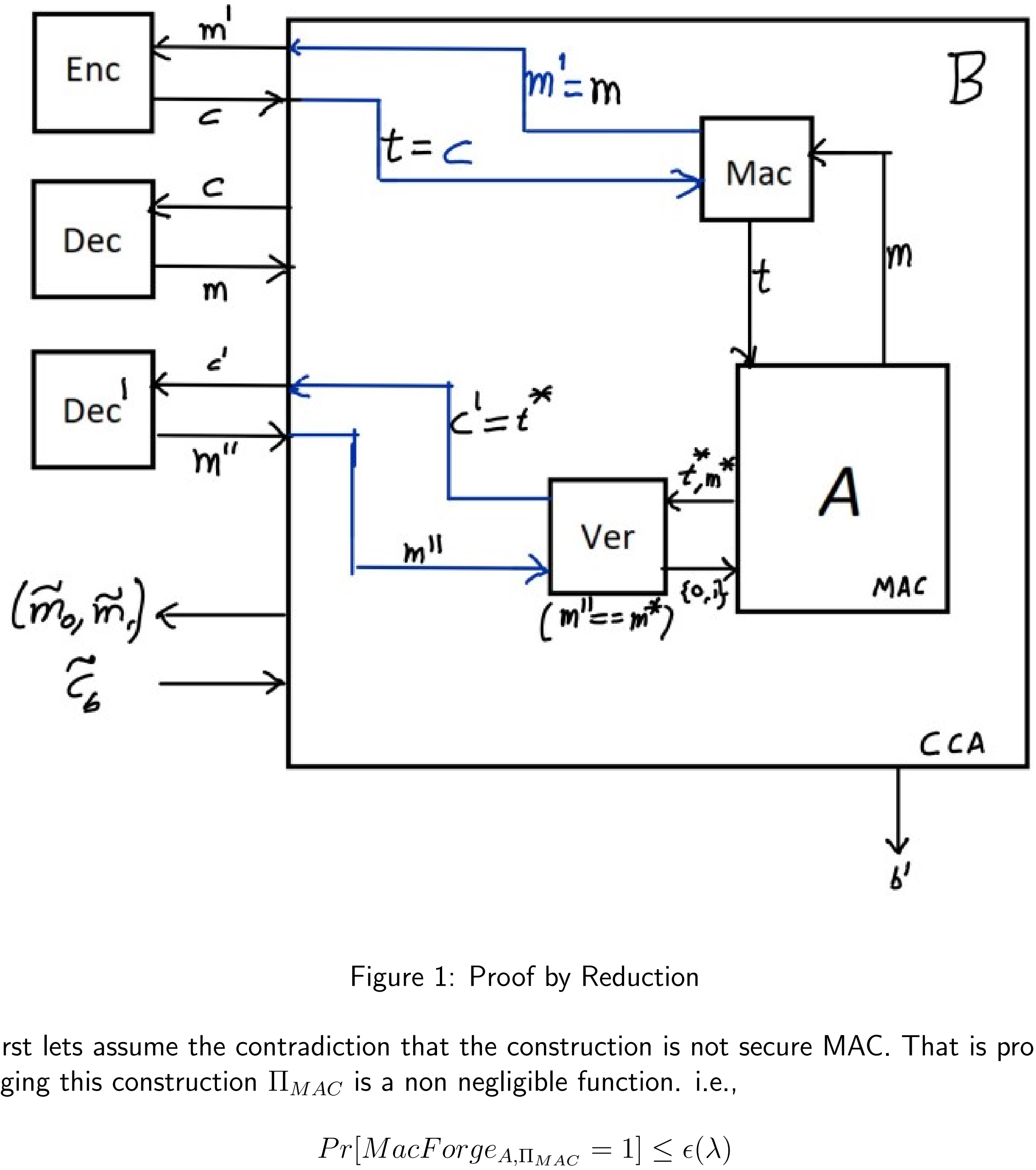

Figure 1: Proof by Reduction

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.,

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

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 $\epsilon(\lambda)$.

That implies

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

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

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

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

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