CS 202 - Introduction to Applied Cryptography **Fall 2016**

HomeWork 5

November 29, 2016 *Liangjian Chen*

Problem 1 **Solution:**

(a) No. Because a MAC scheme does not care about whether it leak the information of original to eavesdropper. Textbook raise a secure MAC where the first bit of the tag is always equal to the first bit of the message as an example. In this case whether MAC scheme has unique tags, it is always insecure.

(b) CCA-security means that even adversary can decrypt any cipher-text he want, it still can not get information about original message. Thus we can see CCA-security acquiesced that adversary has the access to the cipher-text set. So creating valid cipher-text does not make adversary stronger and it won't do harm to CCA-security.

Actually, here is a instance I found in wiki-pedia which is CCA-security but not authenticated encryption.

Optimal asymmetric encryption padding(RSA-OAEP)

https://en.wikipedia.org/wiki/Optimal˙asymmetric˙encryption˙padding

Problem 2 **Solution:**

Yes it is. Proof it by contradiction.

Assume Π' is not CPA-security, and there is a PPT adversary $\mathcal{A}'$ which is able to successfully attack Π'. Construct $\mathcal{A}$ as follow:

$\mathcal{A}$ receive the pk and $Enc(m)$, and construct $pk' = (pk, pk)$ and $Enc'(m) = (Enc(m), Enc(m))$ and send it to the $\mathcal{A}'$. $\mathcal{A}$ return the result of $\mathcal{A}'$ as its own result.

Since $\mathcal{A}'$ successfully attacking Π',$Pr[PubK^{eav}_{\mathcal{A},\Pi}] = Pr[PubK^{eav}_{\mathcal{A}',\Pi'}] > \frac{1}{2} + negl(n)$, which contradict with the assumption that Π is secure.

Thus original statement holds.