Applied Cryptography: Assignment 1

Group number 57

Elwin Tamminga
s1013846

Lucas van der Laan
s1047485

1

(a) Given an adversary $\mathcal{A}$ with query complexity q_m to the MAC function and q_v forgery attempts, a random oracle $\mathcal{RO}$ and a random key K. There is an adversary $\mathcal{A}'$ that has access to either F_K or $\mathcal{RO}$. If $\mathcal{A}$ makes a MAC query $\text{MAC}_K(M)$, then $\mathcal{A}'$ will query F or $\mathcal{RO}$ on input M and return the resulting tag T. At the end $\mathcal{A}$ outputs a forgery (M', T'). Adversary $\mathcal{A}'$ queries its oracle on input M' and verifies whether the outcome equals T'. It outputs 1 if this is the case, and outputs 0 if this is not the case.

The distinguishing advantage of $\mathcal{A}'$ is defined as:

$$\begin{aligned}
\mathbf{Adv}_{\text{F}}^{\text{prf}}(A') &= \mathbf{Pr}(A'^{\text{F}_K} = 1) - \mathbf{Pr}(A'^{\mathcal{RO}} = 1) \\
\mathbf{Adv}_{\text{F}}^{\text{prf}}(A') &= \mathbf{Pr}(A'^{\text{F}_K} = 1) - \frac{q_v}{2^n}
\end{aligned}$$

We know that:

$$\mathbf{Adv}_{\text{MAC}}^{\text{unf}}(A) = \mathbf{Pr}(A^{\text{MAC}_K} = 1)$$

Using the triangle triangle inequality with

$$\begin{aligned}
A &= \mathbf{Pr}(A^{\text{MAC}_K} = 1) \\
B &= \frac{q_v}{2^n} \\
C &= \mathbf{Pr}(A'^{\text{F}_K} = 1)
\end{aligned}$$

We get for the upperbound:

$$\begin{aligned}
|\mathbf{Pr}(A^{\text{MAC}_K} = 1) - \frac{q_v}{2^n}| &\leq |\mathbf{Pr}(A^{\text{MAC}_K} = 1) - \mathbf{Pr}(A'^{\text{F}_K} = 1)| + |\mathbf{Pr}(A'^{\text{F}_K} = 1) - \frac{q_v}{2^n}| \\
|\mathbf{Adv}_{\text{MAC}}^{\text{unf}}(A) - \frac{q_v}{2^n}| &\leq 0 + \mathbf{Adv}_{\text{F}}^{\text{prf}}(A') \\
\mathbf{Adv}_{\text{MAC}}^{\text{unf}}(A) &\leq \frac{q_v}{2^n} + \mathbf{Adv}_{\text{F}}^{\text{prf}}(A')
\end{aligned}$$

(b) For $\text{MAC}_K(M) = T_1||T_2$, the probability that T_1 and T_2 are the same if $\mathcal{D}$ is talking to RO = $1/(2^n \cdot 2^n) = 1/2^{2n}$. This means that there is a $1/2^{2n}$ chance of $\mathcal{D}$ talking to the RO while they think that they are talking to the MAC function. Any message M queried to MAC_K will result in a tag with the left and right half being equal. This leads to a PRF-advantage of:

$$\begin{aligned}\textbf{Adv}^{\text{prf}}_{\text{MAC}}(\mathcal{D}) &= Pr(\mathcal{D}^{\text{MAC}_K} = 1) - Pr(\mathcal{D}^{RO} = 1) \\ &= 1 - 1/2^{2n}\end{aligned}$$

2

(a)

$$\begin{aligned}Pr(H_L(M) \oplus H_L(M') = T) &= Pr(L \otimes M \oplus L \otimes M' = T) \\ &= Pr(L \otimes (M \oplus M') = T) \\ &= Pr(L = T \otimes (M \oplus M')^{-1}) \\ &= 1/2^n\end{aligned}$$

(b)

3

(a) The function first checks if the tag T is correct, if this is not correct it returns $\perp$ instead of the decrypted message M. Otherwise it is the inverse of the authentication function AE_K to decrypt the message.

(b) $\Delta_{\mathcal{D}}(AE_K, AE_K^{-1}; AE[p], AE[p]^{-1}) = |Pr(D^{AE_K^{\pm}} = 1) - Pr(D^{AE[p]^{\pm}} = 1)|$
This makes it so that we lose the difference of probability difference between AE_K and $AE[p]$ as now we use $AE[p]$ instead of AE_K. So now the advantage will be less, simply because of the replacement.

(c)

4

5

(a)

(b)

(c)

(d)

6

(a)

(b)