MTAT.07.003 Cryptology II
Spring 2012 / Exercise session ?? / Example Solution

Exercise (Security of user-aided key agreement). *Consider the following simple user-aided key agreement protocol. The public key* pk *of a server* $\mathcal{P}_1$ *is known to all participants. If a participant* $\mathcal{P}_2$ *wants to connect to* $\mathcal{P}_1$ *it generates a random session key* $k \xleftarrow{u} \mathcal{K}$ *and a short authentication nonce* $r \xleftarrow{u} \{0, \ldots, 9999\}$ *and sends* $\mathsf{Enc}_{\mathsf{pk}}(k\|r)$ *to* $\mathcal{P}_1$*. Next* $\mathcal{P}_1$ *recovers* k *and* r *and sends* r *as an SMS back to* $\mathcal{P}_2$*. The client* $\mathcal{P}_2$ *halts if the SMS does not correspond to his or her authentication nonce. Prove that a* t*-time adversary can alter the ciphertext without being detected with probability at most* $10^{-4} + \varepsilon$ *provided that the cryptosystem is* (t, ε)*-NM-CPA secure and no adversary cannot alter the SMS message.*

Solution. For brevity, let $\mathcal{R} = \{0000, \ldots, 9999\}$ denote the nonce space. Then we can formalise the security goal through the following game:

$\mathcal{G}_0$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}$
$k \xleftarrow{u} \mathcal{K}, r \xleftarrow{u} \mathcal{R}$
$c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(k||r)$
$\hat{c} \leftarrow \mathcal{A}(c)$
$\hat{k}||\hat{r} \leftarrow \mathsf{Dec}_{\mathsf{sk}}(\hat{c})$
if $r \neq \hat{r}$ **return** 0
return $\neg[k \stackrel{?}{=} \hat{k}]$.

Note that if the adversary return $\hat{c} = c$, he or she is guaranteed to lose the game. Hence, we can consider only adversaries that always return $\hat{c} \neq c$. More formally, it is straightforward to modify any adversary to output a different encryption if $\hat{c} = c$. This would only increase the adversaries success probability with the cost of constant overhead in running time.

Now consider a small change in the game, where instead of getting an encryption of $(k||r)$, the adversary gets an encryption of a random message $(\bar{k}||\bar{r})$. To emphasise the change, let us incorporate the generation of this encryption into the original game without no further use of it. This leads to the game pair

$\mathcal{G}_0$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}$
$k \xleftarrow{u} \mathcal{K}, r \xleftarrow{u} \mathcal{R}$
$\bar{k} \xleftarrow{u} \mathcal{K}, \bar{r} \xleftarrow{u} \mathcal{R}$
$c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(k||r)$
$\overline{c} \leftarrow \mathsf{Enc}_{\mathsf{pk}}(\bar{k}||\bar{r})$
$\hat{c} \leftarrow \mathcal{A}(c)$
$\hat{k}||\hat{r} \leftarrow \mathsf{Dec}_{\mathsf{sk}}(\hat{c})$
if $r \neq \hat{r}$ **return** 0
return $\neg[k \stackrel{?}{=} \hat{k}]$

$\mathcal{G}_1$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}$
$k \xleftarrow{u} \mathcal{K}, r \xleftarrow{u} \mathcal{R}$
$\bar{k} \xleftarrow{u} \mathcal{K}, \bar{r} \xleftarrow{u} \mathcal{R}$
$c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(k||r)$
$\overline{c} \leftarrow \mathsf{Enc}_{\mathsf{pk}}(\bar{k}||\bar{r})$
$\hat{c} \leftarrow \mathcal{A}(c_1)$
$\hat{k}||\hat{r} \leftarrow \mathsf{Dec}_{\mathsf{sk}}(\hat{c})$
if $r \neq \hat{r}$ **return** 0
return $\neg[k \stackrel{?}{=} \hat{k}]$.

Note that it is straightforward to rewrite the end-game correctness check as a relation between plaintexts

$$\pi(k||r, \hat{k}||\hat{r}) = [r \stackrel{?}{=} \hat{r}] \wedge [k \neq \hat{k}] \ . \tag{1}$$

Hence, we can directly reduce these games to the non-malleability games

$\mathcal{Q}_0$

$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}$
$\mathcal{M}_0 \leftarrow \mathcal{B}(\mathsf{pk})$
$m \leftarrow \mathcal{M}_0, \overline{m} \leftarrow \mathcal{M}_0$
$c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m)$
$\overline{c} \leftarrow \mathsf{Enc}_{\mathsf{pk}}(\overline{m})$
$\pi, \hat{c}_1, \ldots, \hat{c}_n \leftarrow \mathcal{B}(c)$
if $c \in \{\hat{c}_1, \ldots, \hat{c}_n\}$ then **return** 0
$\hat{m}_i \leftarrow \mathsf{Dec}_{\mathsf{sk}}(\hat{m}_i)$ for $i \in \{1, \ldots, n\}$
return $\pi(m, \hat{m}_1, \ldots, \hat{m}_n)$

$\mathcal{Q}_1$

$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}$
$\mathcal{M}_0 \leftarrow \mathcal{B}(\mathsf{pk})$
$m \leftarrow \mathcal{M}_0, \overline{m} \leftarrow \mathcal{M}_0$
$c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m)$
$\overline{c} \leftarrow \mathsf{Enc}_{\mathsf{pk}}(\overline{m})$
$\pi, \hat{c}_1, \ldots, \hat{c}_n \leftarrow \mathcal{B}(\overline{c})$
if $c \in \{\hat{c}_1, \ldots, \hat{c}_n\}$ then **return** 0
$\hat{m}_i \leftarrow \mathsf{Dec}_{\mathsf{sk}}(\hat{m}_i)$ for $i \in \{1, \ldots, n\}$
return $\pi(m, \hat{m}_1, \ldots, \hat{m}_n)$

The corresponding reduction is following. First, $\mathcal{B}(\mathsf{pk})$ returns an algorithm $\mathcal{M}_0$ that return a uniformly chosen element form $\mathcal{K} \times \mathcal{R}$. Second, $\mathcal{B}(c)$ runs $\mathcal{A}(c)$ and returns the description of the relation given as the equation (1). Since $\mathcal{A}$ is guaranteed never to return $\hat{c} = c$, the direct substitutions gives $\mathcal{Q}_0^{\mathcal{B}} \equiv \mathcal{G}_0^{\mathcal{A}}$ and $\mathcal{Q}_1^{\mathcal{B}} \equiv \mathcal{G}_1^{\mathcal{A}}$. The latter implies

$$\left|\Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1\right] - \Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1\right]\right| \leq \mathsf{Adv}_{\mathfrak{C}}^{\mathsf{nm\text{-}cpa}}(\mathcal{B}) \ .$$

Let us now concentrate on the simplification of the game $\mathcal{G}_1$. Since the adversaries reply does not depend on c, r and k, we can simplify the game by delaying these random choices:

$\mathcal{G}_2$

$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}$
$\bar{k} \xleftarrow{u} \mathcal{K}, \bar{r} \xleftarrow{u} \mathcal{R}$
$\overline{c} \leftarrow \mathsf{Enc}_{\mathsf{pk}}(\bar{k} || \bar{r})$
$\hat{c} \leftarrow \mathcal{A}(c_1)$
$\hat{k} || \hat{r} \leftarrow \mathsf{Dec}_{\mathsf{sk}}(\hat{c})$
$k \xleftarrow{u} \mathcal{K}, r \xleftarrow{u} \mathcal{R}$
if $r \neq \hat{r}$ **return** 0
return $\neg[k \stackrel{?}{=} \hat{k}]$.

Since r is chosen uniformly after $\hat{r}$ is fixed, we get

$$\Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1\right] = \Pr\left[\mathcal{G}_2^{\mathcal{A}} = 1\right] \leq \frac{1}{|\mathcal{R}|}$$

where the last inequality follows from the fact that we must pass the $\hat{r} \stackrel{?}{=} r$ test in order to end the game with one. Consequently, we have proven that for t-time adversaries $\mathcal{A}$, the success is bounded by

$$\Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1\right] \leq \frac{1}{|\mathcal{R}|} + \varepsilon$$

provided that the cryptosystem is $(t + \mathrm{O}(1), \varepsilon)$-NM-CPA secure.