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

Exercise (Security of simple liveness proof). *Entity authentication protocols are often used to prove liveness of a device or a person. For instance, ATM machines normally ask PIN codes several times during long transactions to assure that the person is still present. Such liveness proofs can be implemented with one-way functions. Let $f : \mathcal{X} \to \mathcal{Y}$ be a one-way function and let n be the maximal number of protocol invocations. Then a secret key sk can be chosen as a tuple of random values $x_1, \dots x_n \xleftarrow{u} \mathcal{X}$ and the corresponding public key pk as a tuple of hash values $f(x_1), \dots, f(x_n)$. Each time when a party wants to prove liveness he or she will release non-published sub-key x_i. The proof is successful if $f(x_i) = y_i$ where y_i is the ith component of the public key pk. Prove that if f is (t, ε_1)-secure one-way function and protocols are executed sequentially, then the probability that a t-time adversary succeeds in the ith authentication without seeing x_i is at most ε.*

Solution. Recall that one-wayness of a function f is defined through the following security game:

$$\begin{array}{l}\mathcal{Q}\\ \left[\begin{array}{l} x \xleftarrow{u} \mathcal{X}\\ y \leftarrow f(x)\\ \hat{x} \leftarrow \mathcal{B}(y)\\ \textbf{return } [y \stackrel{?}{=} f(\hat{x})] \end{array}\right. \end{array} \ .$$

The function f is (t, ε)-secure one-way function if for any t-time adversary $\mathcal{B}$ the corresponding advantage is bounded:

$$\mathsf{Adv}^{\mathsf{ow}}_f(\mathcal{B}) = \Pr\left[\mathcal{Q}^{\mathcal{B}} = 1\right] \leq \varepsilon \ .$$

Now the scenario of guessing an ith subkey $\hat{x}_i$ such that $f(\hat{x}_i) = f(x_i)$ can be modelled in the following game:

$$\begin{array}{l}\mathcal{G}^{\mathcal{A}}_i\\ \left[\begin{array}{l} x_1 \xleftarrow{u} \mathcal{X}\\ y_1 \leftarrow f(x_1)\\ \dots\\ x_n \xleftarrow{u} \mathcal{X}\\ y_n \leftarrow f(x_n)\\ \hat{x}_i \leftarrow \mathcal{A}(y_1, \dots, y_n, x_1, \dots, x_{i-1})\\ \textbf{return } [y_i \stackrel{?}{=} f(\hat{x}_i)] \end{array}\right. \end{array}$$

where the inputs $y_1, \dots, y_n$ for $\mathcal{A}$ correspond to the public key used in the liveness proof and inputs $x_1, \dots, x_{i-1}$ correspond to secrets leaked during previous protocol instances. Recall that in each liveness proof the honest prover reveals the corresponding sub-secret x_j. Since the communication between the prover and verifier is not secured a malicious adversary can snatch corresponding values. Moreover, the verifier itself might become malicious at some time-point. Hence, we cannot assume that the adversary does not know $x_1, \dots, x_{i-1}$ during the attack even if communication channels are indeed secure.

To bound the success of an adversary $\mathcal{A}$ in the game $\mathcal{G}_i$, note that we can use a simple wrapper:

$$\begin{array}{l}\mathcal{B}(y)\\ \left[\begin{array}{l} x_1 \xleftarrow{u} \mathcal{X}\\ y_1 \leftarrow f(x_1)\\ \dots\\ x_n \xleftarrow{u} \mathcal{X}\\ y_n \leftarrow f(x_n)\\ \hat{x}_i \leftarrow \mathcal{A}(y_1, \dots, y_{i-1}, y, y_{i+1}, \dots, y_n, x_1, \dots, x_{i-1})\\ \textbf{return } \hat{x}_i \end{array}\right. \end{array}$$

to convert the adversary against the game $\mathcal{G}_i$ to the adversary against the game $\mathcal{Q}$. Simple inlining of the adversary construction $\mathcal{B}$ into the game $\mathcal{Q}$ yields:

$$
\begin{array}{l}
\mathcal{Q} \\
\left[\begin{array}{l}
x \xleftarrow[u]{} \mathcal{X} \\
y \leftarrow f(x) \\
x_1 \xleftarrow[u]{} \mathcal{X} \\
y_1 \leftarrow f(x_1) \\
\ldots \\
x_n \xleftarrow[u]{} \mathcal{X} \\
y_n \leftarrow f(x_n) \\
\hat{x}_i \leftarrow \mathcal{A}(y_1, \ldots, y_{i-1}, y, y_{i+1}, \ldots, y_n, x_1, \ldots, x_{i-1}) \\
\textbf{return } [y \stackrel{?}{=} f(\hat{x})]
\end{array}\right. \ ,
\end{array}
$$

which is completely equivalent to the game $\mathcal{G}_i^{\mathcal{A}}$. Indeed, instead of x_i and y_i the game $\mathcal{Q}^{\mathcal{A}}$ uses x and y. However, these have exactly the same distribution. Thus, we have established that

$$
\Pr\left[\mathcal{G}_i^{\mathcal{A}} = 1\right] = \Pr\left[\mathcal{Q}^{\mathcal{B}} = 1\right] \leq \varepsilon
$$

as long as the running-time of $\mathcal{B}$ is smaller or equal to t. As the overhead of $\mathcal{B}$ compared to the running-time of $\mathcal{A}$ is $\Theta(n)$, we get the desired security claim. Note that the extra penalty $\Theta(n)$ is small but still worth noting – the bound on the running-time of $\mathcal{A}$ decreases linearly if we increase the number sub-secrets n.

Finally, note that the overall probability that an adversary manages to succeed in any of the liveness proofs is bounded by $n\varepsilon$. Although the adversary might adaptively choose which liveness proofs it tries to attack, we can still consider probabilities that it succeeds against the ith liveness proof. As success means that the adversary succeeds against some proof, union bound gives the desired result:

$$
\Pr\left[\mathcal{A} \text{ succeeds in some protocol}\right] \leq \sum_{i=1}^{n} \Pr\left[\mathcal{G}_i^{\mathcal{A}} = 1\right] \leq n\varepsilon \ .
$$