Symmetric primitives, winter 2014/15

MICHAEL NÜSKEN

5. Exercise sheet
Hand in solutions until Monday, 24 November 2014, 13:59

Exercise 5.1 (Never AKE). (6 points)

In the authenticated key exchange (AKE) model a key exchange is considered $\boxed{6}$
and the attacker's challenge is to tell whether a given key is the exchanged key or random. Assume that a key exchange produces a key k which is indistinguishable from random. But then this key is used in an authenticated encryption scheme. (Game!?) Show that the key in that combination is distinguishable from random.

Exercise 5.2 (Functions and permutations). (8+4 points)

Consider the two experiments:

Experiment. $\mathrm{Exp}_F^{\mathrm{PRF}-b}$.

Data: A bit $b \in \{0,1\}$, input size $\ell \in \mathbb{N}$, output size $L \in \mathbb{N}$, a set F of functions $\{0,1\}^\ell \to \{0,1\}^L$.

Distinguisher: An (attacking) distinguisher $\mathcal{A}$ obtaining access to an oracle with input $\{0,1\}^\ell$ and output $\{0,1\}^L$ that outputs a guess $b' \in \{0,1\}$.

1. Let the oracle $\mathcal{O}_0$ be a uniformly randomly chosen function. (Think of a stateful algorithm. When it is called with a previously seen input it returns the remembered answer. Otherwise it picks a new value, remembers it and returns it.)
2. Pick the oracle $\mathcal{O}_1 \xleftarrow{\$} F$ uniformly.
3. Let $b' \leftarrow \mathcal{A}^{\mathcal{O}_b}$.
4. Return b'.

Experiment. $\mathrm{Exp}_P^{\mathrm{PRP}-b}$.

Data: A bit $b \in \{0,1\}$, input/output size $\ell \in \mathbb{N}$, a set P of permutations $\{0,1\}^\ell \to \{0,1\}^\ell$.

Distinguisher: An (attacking) distinguisher $\mathcal{A}$ obtaining access to an oracle with input $\{0,1\}^\ell$ and output $\{0,1\}^\ell$ that outputs a guess $b' \in \{0,1\}$.

1. Let the oracle $\mathcal{O}_0$ be a uniformly randomly chosen permutation. (Think of a stateful algorithm. When it is called with a previously seen input it returns the remembered answer. Otherwise it picks a new value different from all remembered answers, remembers it and returns it.)
2. Pick the oracle $\mathcal{O}_1 \xleftarrow{\$} P$ uniformly.
3. Let $b' \leftarrow \mathcal{A}^{\mathcal{O}_b}$.
4. Return b'.

We define the advantages

$$\begin{aligned}
\operatorname{adv}_F^{\mathrm{PRF}}(\mathcal{A}) &:= \operatorname{prob}\left(\operatorname{Exp}_F^{\mathrm{PRF}-1}(\mathcal{A}) = 1\right) - \operatorname{prob}\left(\operatorname{Exp}_F^{\mathrm{PRF}-0}(\mathcal{A}) = 1\right), \\
\operatorname{adv}_P^{\mathrm{PRP}}(\mathcal{A}) &:= \operatorname{prob}\left(\operatorname{Exp}_P^{\mathrm{PRP}-1}(\mathcal{A}) = 1\right) - \operatorname{prob}\left(\operatorname{Exp}_P^{\mathrm{PRP}-0}(\mathcal{A}) = 1\right), \\
\operatorname{adv}_{\mathrm{FAM}}^{\mathrm{NOTION}}(t, q) &:= \max\left\{ \operatorname{adv}_{\mathrm{FAM}}^{\mathrm{NOTION}}(\mathcal{A}) \,\middle|\, \begin{array}{l} \mathcal{A} \text{ uses at most time } t \\ \text{and } q \text{ oracle calls} \end{array} \right\}.
\end{aligned}$$

Now the task is to proof

Theorem. *For any permutation family P with length ℓ, ie. a set of permutations $\{0,1\}^\ell \to \{0,1\}^\ell$, we have*

$\boxed{+4}$ *(i)* $\operatorname{prob}\left(\operatorname{Exp}_F^{\mathrm{PRP}-0}(\mathcal{A}) = 1\right) - \operatorname{prob}\left(\operatorname{Exp}_F^{\mathrm{PRF}-0}(\mathcal{A}) = 1\right) \le \frac{q^2}{2^{\ell+1}}$.

$\boxed{4}$ *(ii)* $\operatorname{adv}_P^{PRP}(t, q) \le \operatorname{adv}_P^{PRF}(t, q)$.

$\boxed{4}$ *(iii)* $\operatorname{adv}_P^{PRF}(t, q) \le \operatorname{adv}_P^{PRP}(t, q) + \frac{q^2}{2^{\ell+1}}$.

Hint: As an intuition, notice that a birthday attack is always possible to distinguish a permutation from P from a random function, since the latter is not a permutation with probability close to 1[1].

Hint for (i): The previous intution has to be turned into a proof of (i) which only talks about the behaviour of $\mathcal{A}$ given either a random permutation ($\mathrm{PRP}-0$) or a random function ($\mathrm{PRF}-0$). To that end consider the event D that all q oracle queries of $\mathcal{A}$ produce different answers. Then prove that $\operatorname{prob}(\neg D) \le \binom{q}{2} \cdot \frac{1}{2^\ell}$. To finish up notice that $\operatorname{prob}\left(\operatorname{Exp}_F^{\mathrm{PRP}-0}(\mathcal{A}) = 1\right) = \operatorname{prob}\left(\operatorname{Exp}_F^{\mathrm{PRF}-0}(\mathcal{A}) = 1 \,\middle|\, D\right)$.

Hint for (iii): Notice that $\operatorname{Exp}_F^{\mathrm{PRF}-1}(\mathcal{A}) = \operatorname{Exp}_F^{\mathrm{PRP}-1}(\mathcal{A})$!

[1] Namely, with probability $1 - \frac{(2^\ell)!}{2^{\ell 2^\ell}} = 1 - 2^{\delta - \frac{2^\ell}{\ln(2)} - \frac{\ell}{2} - \frac{\ln\pi}{2\ln 2} - \frac{1}{2}}$ with $\delta = \frac{\ln 2}{12\cdot 2^\ell + \theta} \in \left]0, \frac{\ln 2}{12}\right[=]0, 0.06[$ since $\theta \in]0,1[$ [see https://de.wikipedia.org/wiki/Stirlingformel for the approximation of the factorial], which is very close to 1.[2]

[2] Side remark: to indicate how a real number was rounded we append a special symbol. Examples: $\pi = 3.14 = 3.142 = 3.1416 = 3.14159$. The height of the platform shows the size of the left-out part and the direction of the antenna indicates whether actual value is larger or smaller than displayed. We write, say, $e = 2.72 = 2.71$ as if the shorthand were exact.