Symmetric primitives, winter 2014/15
Michael Nüsken

6. Exercise sheet
Hand in solutions until Monday, 1 December 2014, 13:59

Exercise 6.1 (PRF+Hash). (10+4 points)
Assume that you have a function family \( F \subseteq \{0, 1\}^\ell \rightarrow \{0, 1\}^L \) and a hash function \( H : \{0, 1\}^* \rightarrow \{0, 1\}^\ell \). Consider the family
\[
G = \{ g : \{0, 1\}^\ell \rightarrow \{0, 1\}^L \mid \exists f \in F : \forall k, x : g(k, x) = f(k, H(x)) \}.
\]
Prove or disprove:

(i) Formulate a suitable definition for an attacker on the collision-resistance and the advantage \( \text{adv}_{H}^{\text{CR}}(C) \) of such an attacker.

(ii) Given a PRF attacker \( A \) on \( G \). Then we can construct algorithms \( B \) and \( C \) using essentially the same time and oracle calls as \( A \) with
\[
\text{adv}_{G}^{\text{PRF}}(A) \leq \text{adv}_{F}^{\text{PRF}}(B) + \text{adv}_{H}^{\text{CR}}(C).
\]

(iii) Given an attacker \( C \) that finds a collision for \( H \). Then we can construct an attacker \( A \) using essentially the same time and oracle calls as \( C \) with
\[
\text{adv}_{H}^{\text{CR}}(C) \leq \text{adv}_{G}^{\text{PRF}}(A).
\]

(iv) Given a PRF attacker \( B \) on \( F \). Then we can construct an attacker \( A \) using essentially the same time and oracle calls as \( B \) with
\[
\text{adv}_{F}^{\text{PRF}}(B) \leq \text{adv}_{G}^{\text{PRF}}(A).
\]