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 $F \subset \left\{\{0,1\}^\ell \to \{0,1\}^L\right\}$ and a hash function $H\colon \{0,1\}^* \to \{0,1\}^\ell$. Consider the family

$$G = \left\{ g\colon \{0,1\}^\ell \longrightarrow \{0,1\}^L \;\middle|\; \exists f \in F\colon \forall k,x\colon g(k,x) = f(k,H(x)) \right\}.$$

Prove or disprove:

(i) Formulate a suitable definition for an attacker on the collision-resistance and the advantage $\mathrm{adv}^{\mathrm{CR}}_H(\mathcal{C})$ of such an attacker. [4]

(ii) Given a PRF attacker $\mathcal{A}$ on G. Then we can construct algorithms $\mathcal{B}$ and $\mathcal{C}$ using essentially the same time and oracle calls as $\mathcal{A}$ with [4]

$$\mathrm{adv}^{\mathrm{PRF}}_G(\mathcal{A}) \leq \mathrm{adv}^{\mathrm{PRF}}_F(\mathcal{B}) + \mathrm{adv}^{\mathrm{CR}}_H(\mathcal{C}).$$

(iii) Given an attacker $\mathcal{C}$ that finds a collision for H. Then we can construct an attacker $\mathcal{A}$ using essentially the same time and oracle calls as $\mathcal{C}$ with [2]

$$\mathrm{adv}^{\mathrm{CR}}_H(\mathcal{C}) \leq \mathrm{adv}^{\mathrm{PRF}}_G(\mathcal{A}).$$

(iv) Given a PRF attacker $\mathcal{B}$ on F. Then we can construct an attacker $\mathcal{A}$ using essentially the same time and oracle calls as $\mathcal{B}$ with [+4]

$$\mathrm{adv}^{\mathrm{PRF}}_F(\mathcal{B}) \leq \mathrm{adv}^{\mathrm{PRF}}_G(\mathcal{A}).$$