ECS 227 — Modern Cryptography — Winter 99
Problems 5–6

Phillip Rogaway

Out: 14 January 1999. Due: 28 January 1999.

5. Two ways of expressing advantage. Let $g : \{0,1\}^\ell \to \{0,1\}^L$ be a function. Let D be an adversary. Let

$$\mathrm{Adv}_g^{\mathrm{prg}}(D) \;=\; \Pr[r \leftarrow \{0,1\}^\ell :\; D(g(r)) = 1] - \Pr[y \leftarrow \{0,1\}^L :\; D(y) = 1]$$

and let

$$\begin{aligned}\mathrm{Adv}_g^{\mathrm{prg2}}(D) \;=\; & 2\Pr[b \leftarrow \{0,1\}\;;\; \texttt{if}\;\; b=0 \;\;\texttt{then}\;\; y \leftarrow \{0,1\}^L \\ & \qquad\qquad \texttt{else}\;\; \{r \leftarrow \{0,1\}^\ell\;;\; y \leftarrow g(r)\} :\; D(y) = b] - 1\,.\end{aligned}$$

Show that these two measures of advantage exactly coincide: $\mathrm{Adv}_g^{\mathrm{prg}}(D) = \mathrm{Adv}_g^{\mathrm{prg2}}(D)$ for any adversary D.

Remark: This is a much stronger sort of equivalence than we need to regard two security measures as equivalent: it would have been enough that for every adversary D there exists an adversary D' of similar resources to D such that $\mathrm{Adv}_g^{\mathrm{prg}}(D) \approx \mathrm{Adv}_g^{\mathrm{prg2}}(D')$; and for every adversary D' there exists an adversary D of similar resources to D' such that $\mathrm{Adv}_g^{\mathrm{prg}}(D) \approx \mathrm{Adv}_g^{\mathrm{prg2}}(D')$.

6. Telephone poker. In class we described how Alice and Bob can come to possess a shared random bit b (just so long as one of them is honest, and assuming that parties do not "hang up"). Building on this, develop a protocol for how Alice and Bob can play poker on the phone. Alice and Bob need to deal five cards to each of them, and possibly deal a few more cards to one or both of them as they play.

Hint: make a solution which deals the cards but fails with some constant probability. (The failure probability shouldn't be terribly large—less than 0.5, say.) Alice and Bob must know when the deal fails. When it does, they will play the game again.