Problem Set 4 – Dew Thur, 25 Apr 2024

Problem 9. In class we defined the multiquery PRG advantage for a PRG $G\colon \{0,1\}^\ell \to \{0,1\}^L$ by way of

$$\mathbf{Adv}_G^{\text{prg}*}(\mathcal{A}) = \Pr[\mathcal{A}^{\text{G}} \Rightarrow 1] - \Pr[\mathcal{A}^{\$} \Rightarrow 1]$$

where the first oracle answers any query by $G(S)$, for a freshly chosen $S \twoheadleftarrow \{0,1\}^\ell$, and the second oracle answers any query by returning a freshly chosen $R \twoheadleftarrow \{0,1\}^L$. Consider $G = \text{RC4}$, thought of as a map from 16 bytes to two (or more) bytes.

Assume, as your experiments for Prob. 8 suggested, that the second byte of RC4 output is zero with probability 1/128. Design an adversary that breaks the security of RC4 with prg$*$ advantage at least 0.99. For your analysis, you can use the following tool:

Hoeffding's inequality. (See the Wikipedia entry with this name for more information.)
Let $X_1, \ldots, X_n$ be independent and identically distributed random variables, each in $\{0,1\}$ and each taking on the value 1 with probability p. Let $\overline{X} = \frac{1}{n}\sum X_i$ be the "empirical mean" of the observations, which has the expected value of $\mathrm{E}[\overline{X}] = p$. Then for all real numbers $t \geq 0$,

$$\Pr[\left|\overline{X} - p\right| \geq t] \leq 2e^{-2nt^2} \ .$$

Problem 10. For this problem you will prove that PRG-security (the adversary is given one sample) is essentially equivalent to PRG*-security (where the adversary is given as many samples as it likes). More specifically:

(a) Let adversary $\mathcal{A}$ have advantage $\delta = \mathbf{Adv}_G^{\text{prg}}(\mathcal{A})$ in attacking $G\colon \{0,1\}^\ell \to \{0,1\}^L$. Exhibit an adversary $\mathcal{B}$ of comparable efficiency that has "good" $\mathbf{Adv}_G^{\text{prg}*}(\mathcal{B})$ advantage.

(b) Let adversary $\mathcal{B}$ have advantage $\delta^* = \mathbf{Adv}_G^{\text{prg}*}(\mathcal{B})$ in attacking $G: \{0,1\}^\ell \to \{0,1\}^L$. Exhibit an adversary $\mathcal{A}$ of comparable efficiency that has "good" $\mathbf{Adv}_G^{\text{prg}}(\mathcal{A})$ advantage.

Problem 11. On March 28 colleague Ross Anderson `https://www.cl.cam.ac.uk/~rja14/` died at his home in Cambridge, England. Read one or more papers by Anderson, and write a couple of pages in summary or analysis.