MTAT.07.003 Cryptology II
Spring 2012 / Exercise session ?? / Example Solution

Exercise (Analysis of combiner constructions). *Let $\mathbb{G}$ be a finite q-element group such that all elements $y \in \mathbb{G}$ can be expressed as powers of $g \in \mathbb{G}$. Let $\mathcal{B}$ be a discrete logarithm finder that uses algorithm $\mathcal{A}$ five times to get inputs for aggregating algorithm $\mathcal{C}$*

$$\begin{array}{l} \mathcal{B}(y) \\ \left[\begin{array}{l} x_1 \leftarrow \mathcal{A}(y), \ldots, x_5 \leftarrow \mathcal{A}(y) \\ \textbf{\textit{return}}\ \mathcal{C}(x_1, \ldots, x_5) \end{array}\right. \end{array}$$

The construction guarantees that $\mathcal{C}$ succeeds in finding the discrete logarithm of y if all x_i are correct. Find the lower bound of $\mathsf{Adv}^{\mathsf{dl}}_{\mathbb{G}}(\mathcal{B})$ if $\Pr[y \leftarrow \mathbb{G} : \text{the output of } \mathcal{A}(y) \text{ is correct}] = \varepsilon$.

Solution. Let X the random variable that indicates the success of $\mathcal{A}$, i.e.,

$$X(y;\omega) = \begin{cases} 1, & \text{if } \mathcal{A}(y;\omega) \text{ returns correct answer } , \\ 0, & \text{if } \mathcal{A}(y;\omega) \text{ returns in correct answer } , \end{cases}$$

where $\omega \leftarrow \Omega$ is the randomness used by the adversary $\mathcal{A}$ during the computations. By the assumptions,

$$\mathop{\mathbf{E}}_{\substack{y\in\mathbb{G}\\ \omega\in\Omega}}[X(y;\omega)] = \Pr[y \leftarrow \mathbb{G}, \omega \leftarrow \Omega : \text{ the output of } \mathcal{A}(y;\omega) \text{ is correct}] = \varepsilon \ .$$

As $\mathcal{B}$ succeeds only if all five instances must return correct, the exhaustive decomposition of events leads to the following equation:

$$\mathsf{Adv}^{\mathsf{dl}}_{\mathbb{G}}(\mathcal{B}) = \sum_{y_0\in\mathbb{G}} \Pr[y \leftarrow \mathbb{G} : y = y_0] \cdot \Pr[\omega \leftarrow \Omega : \text{ the output of } \mathcal{A}(y_0;\omega) \text{ is correct}]^5 \ .$$

Let $\varepsilon(y) = \Pr[\omega \leftarrow \Omega : \text{ the output of } \mathcal{A}(y;\omega) \text{ is correct}]$. By definition of mathematical expectation

$$\mathsf{Adv}^{\mathsf{dl}}_{\mathbb{G}}(\mathcal{B}) = \mathop{\mathbf{E}}_{y\in\mathbb{G}}\left[\varepsilon(y)^5\right] \ .$$

As $f(x) = x^5$ is convex-cup function, we can apply Jensen's inequality

$$\mathsf{Adv}^{\mathsf{dl}}_{\mathbb{G}}(\mathcal{B}) = \mathop{\mathbf{E}}_{y\in\mathbb{G}}\left[\varepsilon(y)^5\right] \geq \left(\mathop{\mathbf{E}}_{y\in\mathbb{G}}\left[\varepsilon(y)\right]\right)^5 \ .$$

Now note that

$$\mathop{\mathbf{E}}_{\substack{y\in\mathbb{G}\\ \omega\in\Omega}}[X(y;\omega)] = \mathop{\mathbf{E}}_{y\in\mathbb{G}}\left[\varepsilon(y)\right] = \varepsilon$$

and thus

$$\mathsf{Adv}^{\mathsf{dl}}_{\mathbb{G}}(\mathcal{B}) \geq \left(\mathop{\mathbf{E}}_{y\in\mathbb{G}}\left[\varepsilon(y)\right]\right)^5 \geq \varepsilon^5 \ .$$

On the tightness. It is easy to see that Jensens inequality is not particularly tight estimate for most cases. The latter can be established through the following argument.

Fix two group elements y_0 and y_1 and let ε_0 and ε_1 denote the success probability of $\mathcal{A}(y_0)$ and $\mathcal{A}(y_1)$. Then we can study the probability that $\mathcal{B}$ succeeds on these particular points:

$$F(\varepsilon_0, \varepsilon_1) = \Pr[y \leftarrow \mathbb{G} : \mathcal{B}(y) = 1 \wedge y \in \{y_0, y_1\}] = \frac{\varepsilon_0^5 + \varepsilon_1^5}{q}$$

under the restriction that the success probability of $\mathcal{A}$ does not change on two points:

$$\Pr\left[y \leftarrow \mathbb{G} : \mathcal{A}(y) = 1 \wedge y \in \{y_0, y_1\}\right] = \frac{\varepsilon_0 + \varepsilon_1}{q} = const \ .$$

By substituting the second equality into the first expression, we quickly obtain that $F(\varepsilon_1)$ is a convex-cup function which is minimised in the point $\varepsilon_0 = \varepsilon_1$ and maximised if $\varepsilon_0 = 0$ or $\varepsilon_0 = 1$.

Hence, the success probability is minimal if for any two points y_0 or y_1 the corresponding success probabilities are equal. Otherwise, we can decrease the success probability of $\mathcal{B}$ by setting $\varepsilon_0 = \varepsilon_1$ without altering the sum $\varepsilon_0 + \varepsilon_1$. In this case, the Jensens inequality is precise and thus $\mathsf{Adv}^{\mathsf{dl}}_{\mathbb{G}}(\mathcal{B}) = \varepsilon^5$.

The similar probability shifting argument allows us to conclude that the success probability of $\mathcal{B}$ is maximised if for any two points y_0 and y_1, the corresponding probabilities are either:

$$\begin{cases} \varepsilon_0 = 0 \\ \varepsilon_1 = 0 \end{cases} \qquad \begin{cases} \varepsilon_0 = 1 \\ \varepsilon_1 = 0 \end{cases} \qquad \begin{cases} \varepsilon_0 = 0 \\ \varepsilon_1 = 1 \end{cases} \qquad \begin{cases} \varepsilon_0 = 1 \\ \varepsilon_1 = 1 \end{cases}$$

except for a single pair of points y_0 and y_1 for which there is not enough probability mass to get assignment $\varepsilon_0 = \varepsilon_1 = 1$ and thus $\varepsilon_0 \in (0, 1)$ while $\varepsilon_1 \in \{0, 1\}$.

As a result, we have shown that a deterministic algorithm $\mathcal{A}$ that either fails or succeeds on a particular input maximises the success probability of $\mathcal{B}$. Under this restriction, running the algorithm A five times could be replaced by running the algorithm $\mathcal{A}$ once and setting all x_i to $\mathcal{A}(y)$. Since the success probability of A is ε, then the success probability of $\mathcal{B}$ will be as well ε for such an algorithm $\mathcal{A}$.

To conclude, note that for any $\varepsilon \ll 1$ the difference between ε^5 and ε is huge and thus the potentially huge mismatch between the lower bound on the success and the actual success probability is unavoidable.