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 $\mathsf{Adv}^{\mathsf{dl}}_{\mathbb{G}}(\mathcal{B})$ if $\Pr[y \leftarrow \mathbb{G} :$ the output of $\mathcal{A}(y)$ is correct$] = \varepsilon$.

Solution. Denote by X the random variable, which is equal to 1 is $A(y)$ returns the correct answer, otherwise is 0. $E_y[X] = \Pr[y \leftarrow \mathbb{G} :$ the output of $\mathcal{A}(y)$ is correct$] = \varepsilon$. In order for $\mathcal{B}$ to succeed, all five instances must return correct answers, therefore

$$\mathsf{Adv}^{\mathsf{dl}}_{\mathbb{G}}(\mathcal{B}) = E_y[X^5] \leq E_y[X]^5 = \varepsilon^5$$

by Jensen's inequeality, because x^5 is convex-cup function.