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 $\mathcal{A}_1$ be a solver that finds the first bit of the discrete logarithm with probability ε_1, i.e., $\Pr\left[x \leftarrow \mathbb{Z}_q : \mathcal{A}_1(g^x) = x_1\right] \geq \varepsilon_1$. Similarly, let $\mathcal{A}_2$ be a solver that finds the second bit of the discrete logarithm with probability ε_1 and so on. Now let $\mathcal{B}$ be the combiner algorithm that combines the outputs of $\mathcal{A}_1, \ldots, \mathcal{A}_n$ for $n = \lceil \log_2 q \rceil$ to restore the entire discrete logarithm:*

$$\begin{array}{l}\mathcal{B}(y)\\ \left[\begin{array}{l} x_1 \leftarrow \mathcal{A}_1(y), \ldots, x_n \leftarrow \mathcal{A}_n(y)\\ \textbf{\textit{return}}\ x_n \ldots x_1 \end{array}\right.\end{array}$$

The construction guarantees that $\mathcal{B}$ succeeds in finding the discrete logarithm of y if all x_i are correct. Find a good lower bound on the advantage $\mathsf{Adv}^{\mathsf{dl}}_{\mathbb{G}}(\mathcal{B}) = \Pr\left[x \leftarrow \mathbb{Z}_q : \mathcal{B}(g^x) = x\right]$.

Solution.