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

Exercise (Tight amplification of CDH). *Let $\mathbb{G}$ be a finite group of prime order q such that all elements $y \in \mathbb{G}$ can be expressed as powers of $g \in \mathbb{G}$. Then the Computational Diffie-Hellman (CDH) problem is following. Given $x = g^a$ and $y = g^b$, find a group element $z = g^{ab}$. Let $\mathcal{A}$ is the algorithm designed to solve a random instance of CDH. Then we can use the following algorithm*

$$
\begin{array}{l}
\mathcal{B}(x, y) \\
\left[\begin{array}{l}
r, t \leftarrow \mathbb{Z}_q, s \leftarrow \mathbb{Z}_q^* \\
w \leftarrow \mathcal{A}(x \cdot g^r, y^s \cdot g^t) \\
z \leftarrow \left(\dfrac{w}{x^t \cdot y^{rs} \cdot g^{rt}}\right)^{-s} \\
\textbf{\textit{return}}\ z
\end{array}\right.
\end{array}
$$

to reduce an instance of CDH to a random instance of CDH. Moreover, we can amplify the success probability by majority voting

$$
\begin{array}{l}
\mathcal{B}_n(x, y) \\
\left[\begin{array}{l}
\text{For } i \in \{1, \ldots, n\} \text{ do} \\
\quad \left[\begin{array}{l}
r, t \leftarrow \mathbb{Z}_q, s \leftarrow \mathbb{Z}_q^* \\
w_i \leftarrow \mathcal{A}(x \cdot g^r, y^s \cdot g^t) \\
z_i \leftarrow \left(\dfrac{w_i}{x^t \cdot y^{rs} \cdot g^{rt}}\right)^{-s}
\end{array}\right. \\
\textbf{\textit{return}}\ \textsc{Majority}(z_1, \ldots, z_n)
\end{array}\right.
\end{array}
$$

Prove that the reduction works and define a sharp enough lower bound on the success probability. Sketch how the bound behaves as a function of n. How big must $\mathsf{Adv}^{\mathsf{cdh}}_{\mathbb{G}}(\mathcal{A})$ be for the amplification to work at all?

Solution. We divide the analysis into four distinct parts. First, we establish randomisation. Second, we establish correctness. Third, we establish properties of the output distribution z. Fourth, we use McDiarmid's inequality together with inclusion-excusion formula to estimate the success probability for majority voting.

Randomisation of inputs. Let α, β be such that $x = g^\alpha$, $y = g^\beta$. Let α_*, β_* be such that $x \cdot g^r = g^{\alpha_*}$, $y^s \cdot g^t = g^{\beta_*}$.

Correctness. Let γ, δ be such that $w = g^\gamma$ and $z = g^\delta$. Now if $\mathcal{A}$ returns a correct answer then

$$\gamma = ??$$

and thus

$$\delta = ??$$

Randomisation of outputs. Assume that $\mathcal{A}$ gives incorrect answer. Namely, let the answer of $\mathcal{A}$ is offset by the multiplicative term g^ϵ. Then the same offset propagates to the final answer in the algorithm $\mathcal{B}$ as

$$\gamma = ??$$
$$\delta = ??$$

As the order of the group is prime we get ???

Success bounds for amplification strategy. Let us now analyse the algorithm $\mathcal{B}_n$. Let u_i be the i-th element in the list of distinct incorrect outcomes and k be the number distinct incorrect outcomes. By

construction the there can be at most n incorrect but distinct outcomes. Let v_i be number of outputs z_i that are equal to u_i. Let u_* be the correct outcome and v_* be the number of correct outputs. Let $\mathsf{Fail}(i)$ denote the event that $v_i > v_*$. For obvious reasons, the failure probability is

$$\Pr[\mathsf{Fail}] = \Pr[\mathsf{Fail}(1) \vee \mathsf{Fail}(2) \ldots \vee \mathsf{Fail}(k)]$$

By the inclusion-exclusion formula

$$\Pr[\mathsf{Fail}] \leq \sum_{i=1}^{k} \Pr[\mathsf{Fail}(1)]$$
$$\Pr[\mathsf{Fail}] \geq \sum_{i=1}^{k} \Pr[\mathsf{Fail}(i)] - \sum_{i,j=1}^{k} \Pr[\mathsf{Fail}(i) \wedge \mathsf{Fail}(j)]$$

To estimate the probability of $\mathsf{Fail}(i)$ let us define a random variable

$$X_k = \begin{cases} -1, & \text{if } z_k = u_* \ , \\ 1, & \text{if } z_k = u_i, \ , \\ 0, & \text{otherwise } . \end{cases}$$

Then the probability of $\mathsf{Fail}(i)$ is determined by sign of the sum $X_1 + \cdots + X_n$. This allows us to apply McDiarmid's inequality.

Theorem. Let $X_1, \ldots, X_m$ be independent random variables in the range $[-1, 1]$. Then for any $t > 0$

$$\Pr\left[\sum_{i=1}^{n} X_i - \mathbf{E}\left[\sum_{i=1}^{n} X_i\right] \geq t\right] \leq e^{-\frac{2t^2}{4n}}$$

As a result we can establish ...