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

Exercise (Weak random self-reducibility of DDH). *Let $\mathbb{G} = \langle g \rangle$ be a finite group of a prime order q generated by the powers of an element g. Then the Decisional Diffie-Hellman (DDH) problem is the following. For any triple $x, y, z \in \mathbb{G}$, you must decide whether it is a Diffie-Hellman triple or not. Formally, the corresponding distinguishing task is specified through two games:*

$$\mathcal{Q}_0^{\mathcal{B}}\left[\begin{array}{l} a, b \xleftarrow{u} \mathbb{Z}_q \\ c \xleftarrow{u} \mathbb{Z}_q \\ \textbf{\textit{return}}\ \mathcal{B}(g^a, g^b, g^c) \end{array}\right. \qquad \mathcal{Q}_1^{\mathcal{B}}\left[\begin{array}{l} a, b \xleftarrow{u} \mathbb{Z}_q \\ c \leftarrow ab \\ \textbf{\textit{return}}\ \mathcal{B}(g^a, g^b, g^c) \end{array}\right.$$

where the advantage is computed as $\mathsf{Adv}^{\mathsf{ddh}}_{\mathbb{G}}(\mathcal{B}) = |\Pr[\mathcal{Q}_0^{\mathcal{B}} = 1] - \Pr[\mathcal{Q}_1^{\mathcal{B}} = 1]|$. Show that DDH problem is weakly random self-reducible in the following sense. For any algorithm $\mathcal{B}$ that tries to distinguish Diffie-Hellman tuples from random tuples, there exists an algorithm $\mathcal{A}$, which has roughly the same running-time than $\mathcal{B}$ and can for any pair of group elements g^a and g^b distinguish g^{ab} form a random group element g^c with roughly the same advantage as $\mathsf{Adv}^{\mathsf{ddh}}_{\mathbb{G}}(\mathcal{B})$. More precisely, let the following games

$$\mathcal{G}_0^{\mathcal{A}}\left[\begin{array}{l} c \xleftarrow{u} \mathbb{Z}_q \\ \textbf{\textit{return}}\ \mathcal{A}(g^a, g^b, g^c) \end{array}\right. \qquad \mathcal{G}_1^{\mathcal{A}}\left[\begin{array}{l} c \leftarrow ab \\ \textbf{\textit{return}}\ \mathcal{A}(g^a, g^b, g^c) \end{array}\right.$$

model the distinguishing task. Then the corresponding advantage is

$$\mathsf{Adv}^{\mathsf{sf\text{-}ddh}}_{\mathbb{G},a,b}(\mathcal{A}) = \left|\Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1\right] - \Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1\right]\right| \quad .$$

Show that for any $a, b \in \mathbb{Z}_q$, the advantage $\mathsf{Adv}^{\mathsf{sf\text{-}ddh}}_{\mathbb{G},a,b}(\mathcal{A})$ can be bounded from below by a multiple of $\mathsf{Adv}^{\mathsf{ddh}}_{\mathbb{G}}(\mathcal{B})$, while the running-time of $\mathcal{A}$ is linear wrt the running-time of $\mathcal{B}$.

Solution. Before going to the solution lets prove the following simple fact that for any element $x \in \mathbb{Z}_q$, the element $x + z$ is uniformly random if $z \in \mathbb{Z}_q$ chosen uniformly at random from $\mathbb{Z}_q$. Indeed, note that for any $a \in \mathbb{Z}_q$, we have

$$\Pr\left[z \xleftarrow{u} \mathbb{Z}_q : x + z = a | z = y\right] = \Pr\left[z \xleftarrow{u} \mathbb{Z}_q : z = a - x\right] = \frac{1}{q} \quad .$$

By knowing this fact, will show that for fixed values a, b we can define an adversary $\mathcal{A}$ such that $\mathsf{Adv}^{\mathsf{sf\text{-}ddh}}_{\mathbb{G},a,b}(\mathcal{A}) = \mathsf{Adv}^{\mathsf{ddh}}_{\mathbb{G}}(\mathcal{B})$ and the running time of $\mathcal{A}$ is the running time of $\mathcal{B}$ plus some constant. Let us define the adversary $\mathcal{A}$ as follows:

$$\mathcal{A}(g^a, g^b, g^c)\left[\begin{array}{l} x, y \xleftarrow{u} \mathbb{Z}_q \\ \textbf{return}\ \mathcal{B}(g^a \cdot g^x, g^b \cdot g^y, g^c \cdot (g^a)^y \cdot (g^b)^x \cdot g^{xy}) \end{array}\right. \quad .$$

Obviously the running time of this adversary is the same as $\mathcal{B}$ plus a constant δ, which is approximately the time it takes to do 2 samplings from $\mathbb{Z}_q$, one multiplication in $\mathbb{Z}_q$, 5 multiplications in $\mathbb{G}$ and 5 exponentiations in $\mathbb{G}$. So it remains to show that $\mathsf{Adv}^{\mathsf{sf\text{-}ddh}}_{\mathbb{G},a,b}(\mathcal{A}) = \mathsf{Adv}^{\mathsf{ddh}}_{\mathbb{G}}(\mathcal{B})$.

First note that with the adversary $\mathcal{A}$ defined above, the games can be rewritten as follows:

$$\mathcal{G}_0^{\mathcal{A}}\left[\begin{array}{l} c \xleftarrow{u} \mathbb{Z}_q \\ x, y \xleftarrow{u} \mathbb{Z}_q \\ \textbf{return}\ \mathcal{B}(g^a \cdot g^x, g^b \cdot g^y, g^c \cdot (g^a)^y \cdot (g^b)^x \cdot g^{xy}) \end{array}\right. \qquad \mathcal{G}_1^{\mathcal{A}}\left[\begin{array}{l} c \leftarrow ab \\ x, y \xleftarrow{u} \mathbb{Z}_q \\ \textbf{return}\ \mathcal{B}(g^a \cdot g^x, g^b \cdot g^y, g^c \cdot (g^a)^y \cdot (g^b)^x \cdot g^{xy}) \end{array}\right.$$

Next notice that swapping the first two steps in both games does not change anything, and after simplifying the exponents in the parameters for $\mathcal{B}$, we get the adjusted two games with the same advantage in distinguishing between them:

$$\begin{array}{ll}
\mathcal{G}_{01}^{\mathcal{A}} & \mathcal{G}_{11}^{\mathcal{A}} \\
\left[\begin{array}{l} x, y \xleftarrow{u} \mathbb{Z}_q \\ c \xleftarrow{u} \mathbb{Z}_q \\ \textbf{return } \mathcal{B}(g^{a+x}, g^{b+y}, g^{c+ay+bx+xy}) \end{array}\right. \qquad & \left[\begin{array}{l} x, y \xleftarrow{u} \mathbb{Z}_q \\ c \leftarrow ab \\ \textbf{return } \mathcal{B}(g^{a+x}, g^{b+y}, g^{(a+x)(b+y)}) \end{array}\right.
\end{array}$$

Since x and y are independently and uniformly chosen from $\mathbb{Z}_q$, the elements $\overline{x} = x + a$ and $\overline{y} = y + b$ are also independent and have uniform distribution over $\mathbb{Z}_q$. Hence, we can further simplify the games without changing the advantage:

$$\begin{array}{ll}
\mathcal{G}_{02}^{\mathcal{A}} & \mathcal{G}_{12}^{\mathcal{A}} \\
\left[\begin{array}{l} \overline{x}, \overline{y} \xleftarrow{u} \mathbb{Z}_q \\ c \xleftarrow{u} \mathbb{Z}_q \\ \textbf{return } \mathcal{B}(g^{\overline{x}}, g^{\overline{y}}, g^{\overline{c}}) \end{array}\right. \qquad & \left[\begin{array}{l} \overline{x}, \overline{y} \xleftarrow{u} \mathbb{Z}_q \\ \overline{c} \leftarrow \overline{x} \cdot \overline{y} \\ \textbf{return } \mathcal{B}(g^{\overline{x}}, g^{\overline{y}}, g^{\overline{c}}) \end{array}\right.
\end{array}$$

where $\overline{c} = c + a(\overline{y} - b) + b(\overline{x} - a) + (\overline{x} - a)(\overline{y} - b)$ in the first game. As the $\overline{c}$ value is again sum of a fixed value $(a(\overline{y} - b) + b(\overline{x} - a) + (\overline{x} - a)(\overline{y} - b))$ and a uniformly chosen c, we can further simplify the first game:

$$\begin{array}{ll}
\mathcal{G}_{03}^{\mathcal{A}} & \mathcal{G}_{13}^{\mathcal{A}} \\
\left[\begin{array}{l} \overline{x}, \overline{y} \xleftarrow{u} \mathbb{Z}_q \\ \overline{c} \xleftarrow{u} \mathbb{Z}_q \\ \textbf{return } \mathcal{B}(g^{\overline{x}}, g^{\overline{y}}, g^{\overline{c}}) \end{array}\right. \qquad & \left[\begin{array}{l} \overline{x}, \overline{y} \xleftarrow{u} \mathbb{Z}_q \\ \overline{c} \leftarrow \overline{x} \cdot \overline{y} \\ \textbf{return } \mathcal{B}(g^{\overline{x}}, g^{\overline{y}}, g^{\overline{c}}) \end{array}\right.
\end{array}$$

Since games $\mathcal{G}_{03}$ and $\mathcal{G}_{13}$ are identical to the standard Decisional Diffie-Hellman challenges games, we get

$$\begin{aligned}
\mathsf{Adv}^{\mathsf{sf\text{-}ddh}}_{\mathbb{G},a,b}(\mathcal{A}) &= \left|\Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1\right] - \Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1\right]\right| = \left|\Pr\left[\mathcal{G}_{03}^{\mathcal{A}} = 1\right] - \Pr\left[\mathcal{G}_{13}^{\mathcal{A}} = 1\right]\right| \\
&= \left|\Pr\left[\mathcal{Q}_0^{\mathcal{B}} = 1\right] - \Pr\left[\mathcal{Q}_1^{\mathcal{B}} = 1\right]\right| = \mathsf{Adv}^{\mathsf{ddh}}_{\mathbb{G}}(\mathcal{B})
\end{aligned}$$

as desired and the proof is complete.