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

Exercise (Full proof for randomised self-reducibility of DDL). *Show that for any $\mathcal{B}$ defined as above there exists an algorithm $\mathcal{A}$, which has roughly the same running-time as $\mathcal{B}$ and for any three group elements g^a, g^b, g^c, distinguish g^{ab} from g^c with roughly the same advantage as $\mathsf{Adv}^{\mathsf{ddh}}_{\mathbb{G}}(\mathcal{B})$.*

More precisely, let the following games

$$\begin{array}{ll} \mathcal{G}_0^{\mathcal{A}} & \mathcal{G}_1^{\mathcal{A}} \\ \left[\begin{array}{l} d \leftarrow c \\ \textbf{return } \mathcal{A}(g^a, g^b, g^d) \end{array}\right. & \left[\begin{array}{l} d \leftarrow ab \\ \textbf{return } \mathcal{A}(g^a, g^b, g^d) \end{array}\right. \end{array}$$

model the distinguishing task. Then the corresponding advantage is

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

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. We begin with a similar lemma similar to the previous question. The proof is similar but omitted.

Lemma 0.1 *For any element x chosen uniformly random from $\mathbb{Z}_q$, $x \cdot z$ is uniformly random for any nonzero $z \in \mathbb{Z}_q$ chosen independently from x.*

The idea is that instead of relying on the equation $(a + x)(b + y) = (ab + ay + bx) + xy$ which was not uniformly random for uniformly random x, y, we instead try the equation $(a+x)(by+z) = aby+az+bxy+xz = (bx + c)y + (a + x)z$ which is uniformly random for unifromly random x, y, z unless $bx + c = a + x = 0$ in which case we get an even bigger advantage since we know a.

Specifically, we can prove the following:

Lemma 0.2 *Let $a, b, c \in \mathbb{Z}_q$ Let x be chosen uniformly random from $\mathbb{Z}_q - (-a)$, and y, z be chosen uniformly random from $\mathbb{Z}_q$. Then $(bx + c)y + (a + x)z$ is uniformly random over $\mathbb{Z}_q$.*

Proof: If $bx + c \neq 0$, then after fixing x, z we know from Lemma 0.2 that $(bx + c)y$ is uniformly random, and hence from Lemma 0.1 that $(bx + c)y + (a + x)z$ is uniformly random. But if $(bx + c)y = 0$ then $(bx + c)y + (a + x)z = (a + x)z$ which is uniformly random from Lemma 0.2 and the fact that $a + x \neq 0$.

So combining the above ideas we define the adversary $\mathcal{A}$ as follows:

$$\begin{array}{l} \mathcal{A}(g^a, g^b, g^d) \\ \left[\begin{array}{l} x, y, z \xleftarrow{u} \mathbb{Z}_q \\ \text{if } (g^{a+x} = 1)\textbf{return } \mathcal{C}(-x, g^{a+x}, g^b, g^d) \\ \text{else } \textbf{return } \mathcal{B}(g^{a+x}, g^{by+z}, g^{dy+az+bxy+xz}) \end{array}\right. \end{array} \qquad \begin{array}{l} \mathcal{B}(g^a, g^b, g^c) \\ \left[\ldots \right. \end{array}$$

where $\mathcal{C}(a, g^b, g^d)$ is a constant-time adversary that can pefectly distinguish the DDL game when additinally given a. Notice that all parameters thrown to $\mathcal{B}$ can be calculated in constant time similar to the previous question, if $\mathcal{A}$ is given g^a, g^b, g^d. So by using the same argument, this adversary $\mathcal{A}$ has the same running time as $\mathcal{B}$ plus a constant.

Let $\mathsf{Adv}^{\mathsf{ddh}}_{\mathbb{G}}(\mathcal{B}) = \epsilon$. If $g^{a+x} = 1$ (which happens qith probability 1/q) then we get an advantage of 1 using $\mathcal{C}$. If not, then $a + x \neq 0$ and Lemma 0.3 holds, so we can do an analogous reduction to the weak RSR question above, and get an adversary with advantage ϵ. Hence we get that

$$\begin{aligned} \mathsf{Adv}^{\mathsf{sf\text{-}ddh}}_{\mathbb{G},a,b,c}(\mathcal{A}) &= \frac{1}{q} \cdot 1 + \frac{q-1}{q} \cdot \epsilon \\ &\geq \frac{1}{q} \cdot \epsilon + \frac{q-1}{q} \cdot \epsilon \\ &= \epsilon \end{aligned}$$

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

Exercise (Two bit oracle to recover DL). *Prove or disprove that the perfect ability to extract two consecutive bits of DL is sufficient for the full recovery of the DL.*

Solution. Obviously this is true for two consecutive and most significant bits. We will disprove the general case by showing that getting the two least significant bits is not known to be sufficient in the full recovery of DL. Suppose we want to find the discrete log of g^a, with an oracle

$$f(g^x) = (x \mod q) \mod 4.$$

We assume a polynomial number of queries to the oracle (the proof for a constant number of queries is trivial: replace the last 2 bits oracle with 4 guesses to the 2 bits, and DL is solved with running time is linear to the running time by using the oracle, albeit with a large constant).

It is not known what the best algorithm is here, but a typical idea would be to iteratively get bit a_i given knowledge of bits a_{i-1}, a_{i-2}. This can be done by queries of the form $f(g^{a \cdot 2^i})$. However, if for instance we query $f(g^{2a})$ we can detect whether the result was $2a \mod 4$ or $(2a - q) \mod 4$ only with probability $3/4$. Hence this algorithm succeeds with probablility approximately $c \cdot (\frac{3}{4})^{n-2}$, which is negligible.

Of course, as we can not yet know of the most efficient adversary in this setting, it is not possible to fully disprove the claim. For example, it might later be proven that DL can be performed in polynomial time without using the oracle.