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

Exercise (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 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:*

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

where the advantage is computed as $\mathsf{Adv}^{\mathsf{ddh}}_{\mathbb{G}}(\mathcal{A}) = |\Pr[\mathcal{G}_0^{\mathcal{A}} = 1] - \Pr[\mathcal{G}_1^{\mathcal{A}} = 1]|$. Show that DDH problem is random self-reducible and show how to amplify the success probability by majority voting.

Solution. For a solution, we first discuss what random self-reducibility means in the context of Decisional Diffie-Hellman problem. Then we show how to achieve random self-reducibility and what are the consequences. As a last step, show how to amplify the success probability by majority voting.

Definition of Random Self-reducibility. It is easy to formalise random self-reducibility for a discrete logarithm or Computational Diffie-Hellman problem, as the problem is formalized through a single game. For a Decisional Diffie-Hellman problem, we have two security games $\mathcal{Q}_0$ and $\mathcal{Q}_1$.

So ideally we would like to have an algorithm $\mathcal{A}^{\mathcal{B}}$ such that for any challenge tuple $g^{a_0}, g^{b_0}, g^{c_0}$ generated in the $\mathcal{G}_0$ and a challenge tuple $g^{a_1}, g^{b_1}, g^{c_1}$ generated in the $\mathcal{G}_1$, the corresponding advantage

$$\mathsf{Adv}(\mathcal{A}) = |\Pr[\mathcal{A}(g^{a_0}, g^{b_0}, g^{c_0}) = 1] - \Pr[\mathcal{A}(g^{a_1}, g^{b_1}, g^{c_1}) = 1]| = \mathsf{Adv}^{\mathsf{ddh}}_{\mathbb{G}}(\mathcal{B}) \ .$$

However, such a goal is clearly unachievable since a valid Diffie-Hellman tuple $g^{a_1}, g^{b_1}, g^{c_1}$ can is also generated in the game $\mathcal{G}_0$, as well. Consequently, we formalise the random self-reducibility of a Decisional Diffie-Hellman problem a bit differently. An instance of Decisional Diffie-Hellman problem is *randomly self-reducible* if for any algorithm $\mathcal{A}$ there exists an algorithm $\mathcal{B}$ with comparable running-time such that

$$\mathsf{Adv}(\mathcal{A}) = |\Pr[\mathcal{A}(g^{a_0}, g^{b_0}, g^{c_0}) = 1] - \Pr[\mathcal{A}(g^{a_1}, g^{b_1}, g^{c_1}) = 1]| = \mathsf{Adv}^{\mathsf{ddh}}_{\mathbb{G}}(\mathcal{B})$$

whenever $(g^{a_1}, g^{b_1}, g^{c_1})$ is a Diffie-Hellman tuple and $(g^{a_0}, g^{b_0}, g^{c_0})$ is not a Diffie-Hellman tuple.

Construction for random self-reducibility. Let $\mathbb{G}$ be a q-element group and $\mathcal{B}$ be a distinguisher for the Decisional Diffie-Hellman problem. Then the following adversary

$$\begin{array}{l} \mathcal{A}(x, y, z) \\ \left[\begin{array}{l} u, v, w \xleftarrow{u} \mathbb{Z}_q \\ \overline{x} \leftarrow x^w g^u \\ \overline{y} \leftarrow y g^v \\ \overline{z} \leftarrow z^w x^{vw} y^u g^{uv} \\ \textbf{return}\ \mathcal{B}(\overline{x}, \overline{y}, \overline{z}) \end{array}\right. \end{array}$$

achieves the desired worst case guarantees.

Analysis. Before going any further note that the challenge games can be rewritten to a bit more conveniently:

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

as c is still uniformly distributed in $\mathcal{Q}_0$. Let us now see what happens if $\mathcal{A}$ gets an input $g^{a_i}, g^{b_i}, g^{c_i}$. By using standard algebraic equalities we can simplify the algorithm

$$\begin{array}{l}\mathcal{A}(g^{a_i}, g^{b_i}, g^{c_i}) \\ \left\lceil \begin{array}{l} u, v, w \xleftarrow{u} \mathbb{Z}_q \\ \overline{x} \leftarrow g^{a_i w + u} \\ \overline{y} \leftarrow g^{b_i + v} \\ \overline{z} \leftarrow g^{c_i w + a_i v w + b_i u + uv} \\ \textbf{return } \mathcal{B}(\overline{x}, \overline{y}, \overline{z}) \end{array} \right.\end{array}$$

As the input $g^{a_1}, g^{b_1}, g^{c_1}$ is a Diffie-Hellman tuple, $c_1 = a_1 b_1$ and we can further simplify the algorithm without changing its behaviour:

$$\begin{array}{l}\mathcal{A}(g^{a_1}, g^{b_1}, g^{c_1}) \\ \left\lceil \begin{array}{l} u, v, w \xleftarrow{u} \mathbb{Z}_q \\ \overline{x} \leftarrow g^{a_1 w + u} \\ \overline{y} \leftarrow g^{b_1 + v} \\ \overline{z} \leftarrow g^{(a_1 w + u)(b_i + v)} \\ \textbf{return } \mathcal{B}(\overline{x}, \overline{y}, \overline{z}) \end{array} \right.\end{array} \quad \Longrightarrow \quad \begin{array}{l}\mathcal{A}(g^{a_1}, g^{b_1}, g^{c_1}) \\ \left\lceil \begin{array}{l} \alpha, \beta \xleftarrow{u} \mathbb{Z}_q \\ \overline{x} \leftarrow g^{\alpha} \\ \overline{y} \leftarrow g^{\beta} \\ \overline{z} \leftarrow g^{\alpha\beta} \\ \textbf{return } \mathcal{B}(\overline{x}, \overline{y}, \overline{z}) \end{array} \right. .\end{array}$$

In particular, note that variables $\alpha \leftarrow a_i w + u$ and $\beta \leftarrow b_i + v$ have uniform distribution over $\mathbb{Z}_q$ and thus the second simplification does not change the behaviour of $\mathcal{A}(g^{a_1}, g^{b_1}, g^{c_1})$. Since the final form of $\mathcal{A}(g^{a_1}, g^{b_1}, g^{c_1})$ is equivalent to the game $\mathcal{Q}_1^{\mathcal{B}}$, we have established that

$$\Pr\left[\mathcal{A}(g^{a_1}, g^{b_1}, g^{c_1}) = 1\right] = \Pr\left[\mathcal{Q}_1^{\mathcal{B}} = 1\right] .$$

Let us now analyse the case where the input $g^{a_0}, g^{b_0}, g^{c_0}$ is not a Diffie-Hellman tuple, i.e., $c_0 = a_0 b_0 + k$ for some $k \neq 0$ in $\mathbb{Z}_q$. Again, we can use this knowledge to simplify the algorithm without changing its behaviour

$$\begin{array}{l}\mathcal{A}(g^{a_0}, g^{b_0}, g^{c_0}) \\ \left\lceil \begin{array}{l} u, v, w \xleftarrow{u} \mathbb{Z}_q \\ \overline{x} \leftarrow g^{a_0 w + u} \\ \overline{y} \leftarrow g^{b_0 + v} \\ \overline{z} \leftarrow g^{(a_0 w + u)(b_i + v) + kw} \\ \textbf{return } \mathcal{B}(\overline{x}, \overline{y}, \overline{z}) \end{array} \right.\end{array} \quad \Rightarrow \quad \begin{array}{l}\mathcal{A}(g^{a_0}, g^{b_0}, g^{c_0}) \\ \left\lceil \begin{array}{l} \alpha, \beta, w \xleftarrow{u} \mathbb{Z}_q \\ \overline{x} \leftarrow g^{\alpha} \\ \overline{y} \leftarrow g^{\beta} \\ \overline{z} \leftarrow g^{\alpha\beta + kw} \\ \textbf{return } \mathcal{B}(\overline{x}, \overline{y}, \overline{z}) \end{array} \right.\end{array}$$

To go further with the analysis, we *have to* assume that q is prime. If this condition is met then kw for $w \xleftarrow{u} \mathbb{Z}_q$ has uniform distribution over $\mathbb{Z}_q$. If q is not a prime then such claim does not hold and the construction *does not provide* random self-reducibility. To continue, if q is prime then we can further simplify the algorithm without changing its behaviour:

$$\begin{array}{l}\mathcal{A}(g^{a_0}, g^{b_0}, g^{c_0}) \\ \left\lceil \begin{array}{l} \alpha, \beta, \gamma \xleftarrow{u} \mathbb{Z}_q \\ \overline{x} \leftarrow g^{\alpha} \\ \overline{y} \leftarrow g^{\beta} \\ \overline{z} \leftarrow g^{\alpha\beta + \gamma} \\ \textbf{return } \mathcal{B}(\overline{x}, \overline{y}, \overline{z}) \end{array} \right. .\end{array}$$

Since the final form of $\mathcal{A}(g^{a_0}, g^{b_0}, g^{c_0})$ is equivalent to the game $\mathcal{Q}_1^{\mathcal{B}}$, we have established that

$$\Pr\left[\mathcal{A}(g^{a_0}, g^{b_0}, g^{c_0}) = 1\right] = \Pr\left[\mathcal{Q}_0^{\mathcal{B}} = 1\right] .$$

Consequently, we have proven that if $\mathbb{G}$ contains prime number of elements then

$$\mathsf{Adv}(\mathcal{A}) = |\Pr[\mathcal{Q}_0^{\mathcal{B}} = 1] - \Pr[\mathcal{Q}_1^{\mathcal{B}} = 1]| = \mathsf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}(\mathcal{A}) \ .$$

Amplification by majority voting. For clarity, we give the simplest construction where $\mathcal{B}$ is called out trice to amplify the distinguishing advantage. As before, let $\mathcal{A}$ denote the reduction algorithm for random self-reducibility. Then the new majority voting algorithm is the following:

$$\begin{array}{l}\mathcal{C}(x,y,z)\\ \left[\begin{array}{l} b_1 \leftarrow \mathcal{A}(x,y,z)\\ b_2 \leftarrow \mathcal{A}(x,y,z)\\ b_3 \leftarrow \mathcal{A}(x,y,z)\\ \mathsf{if}\ b_1+b_2+b_3 > 1\ \mathsf{then}\ \mathbf{return}\ 1\\ \mathsf{else}\ \mathbf{return}\ 0\ . \end{array}\right.\end{array}$$

Analysis. Let us first consider the game $\mathcal{Q}_1$ where all inputs g^a, g^b, g^c for $\mathcal{C}$ are Diffie-Hellman tuples. Let $\varepsilon_1 = \Pr\left[\mathcal{Q}_1^{\mathcal{B}} = 1\right]$. Then for any fixed tuple, we know by previous analysis that

$$\Pr[b_i = 1] = \Pr[\mathcal{Q}_1^{\mathcal{B}} = 1] = \varepsilon_1 \ .$$

Consequently, we get

$$\Pr\left[\mathcal{G}_1^{\mathcal{C}} = 1\right] = \Pr[\mathcal{C}(g^a, g^b, g^c) = 1] = \varepsilon_1^3 + 3\varepsilon_1^2(1-\varepsilon_1) \ .$$

As the second step, let us estimate the success in the game $\mathcal{Q}_0$. As an input is a Diffie-Hellman tuple with probability $\frac{1}{q}$ in the game $\mathcal{Q}_0$, we get

$$\Pr\left[\mathcal{G}_1^{\mathcal{C}} = 1\right] = \tfrac{1}{q} \cdot \Pr\left[\mathcal{C}(g^a, g^b, g^c) = 1 | c = ab\right] + \tfrac{q-1}{q} \cdot \Pr\left[\mathcal{C}(g^a, g^b, g^c) = 1 | c \neq ab\right] \ .$$

As the analysis of the first conditional is already done above, we are left with the case where g^a, g^b, g^c is not a Diffie-Hellman tuple. Again, let $\varepsilon_0 = \Pr\left[\mathcal{Q}_0^{\mathcal{B}} = 1\right]$. Then analogously to the previous analysis we get

$$\Pr\left[\mathcal{C}(g^a, g^b, g^c) = 1 | c \neq ab\right] = \varepsilon_0^3 + 3\varepsilon_0^2(1-\varepsilon_0)$$

and thus

$$\Pr\left[\mathcal{Q}_0^{\mathcal{C}} = 1\right] = \tfrac{1}{q} \cdot \left(\varepsilon_1^3 + 3\varepsilon_1^2(1-\varepsilon_1)\right) + \tfrac{q-1}{q} \cdot \left(\varepsilon_0^3 + 3\varepsilon_0^2(1-\varepsilon_0)\right) \ .$$

By combining the results, we get

$$\begin{aligned}\mathsf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}(\mathcal{C}) &= \tfrac{q-1}{q} \cdot \left|\varepsilon_1^3 + 3\varepsilon_1^2(1-\varepsilon_1) - \varepsilon_0^3 - 3\varepsilon_0^2(1-\varepsilon_0)\right|\\ &= \tfrac{q-1}{q} \cdot \left|2(\varepsilon_1-\varepsilon_0)(\varepsilon_1^2+\varepsilon_1\varepsilon_0+\varepsilon_0^2) - 3(\varepsilon_1-\varepsilon_0)(\varepsilon_1+\varepsilon_0)\right|\\ &= \tfrac{q-1}{q} \cdot |\varepsilon_1-\varepsilon_0| \cdot |3\varepsilon_0 + 3\varepsilon_1 - 2\varepsilon_0^2 - 2\varepsilon_0\varepsilon_1 - 2\varepsilon_0^2|\end{aligned}$$

By the definition $\mathsf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}(\mathcal{A}) = |\varepsilon_0 - \varepsilon_1|$ and thus

$$\mathsf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}(\mathcal{C}) = \tfrac{q-1}{q} \cdot \mathsf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}(\mathcal{C}) \cdot |3\varepsilon_0 + 3\varepsilon_1 - 2\varepsilon_0^2 - 2\varepsilon_0\varepsilon_1 - 2\varepsilon_0^2|$$

where the last term can be lower bounded in the range $\mathsf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}(\mathcal{A}) \in (\frac{1}{2}, \frac{3}{4})$ further

$$\mathsf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}(\mathcal{C}) = \tfrac{q-1}{q} \cdot \mathsf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}(\mathcal{C})^2 \cdot (3 - 2 \cdot \mathsf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}(\mathcal{A})) > \mathsf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}(\mathcal{A}) \ .$$

Hence, we do get amplification of success probability. However, the gain is not so big and the derivation of the advantage is not so straightforward as it seems.

FURTHER COMMENTS. The reduction construction is not optimal for the analysis. Usually, one uses more complex construction

$$
\begin{array}{l}
\mathcal{C}(x,y,z)\\
\left\lceil
\begin{array}{l}
\overline{z} \xleftarrow{u} \mathbb{G}\\
i_1, i_1, i_3 \xleftarrow{u} \{0,1\}\\
\mathsf{if}\ i_1 = 1\ \mathsf{then}\ b_1 \leftarrow \mathcal{A}(x,y,z)\ \mathsf{else}\ b_1 \leftarrow \mathcal{A}(x,y,\overline{z})\\
\mathsf{if}\ i_2 = 1\ \mathsf{then}\ b_2 \leftarrow \mathcal{A}(x,y,z)\ \mathsf{else}\ b_2 \leftarrow \mathcal{A}(x,y,\overline{z})\\
\mathsf{if}\ i_3 = 1\ \mathsf{then}\ b_3 \leftarrow \mathcal{A}(x,y,z)\ \mathsf{else}\ b_3 \leftarrow \mathcal{A}(x,y,\overline{z})\\
\mathsf{if}\ [b_1 \stackrel{?}{=} i_1] + [b_2 \stackrel{?}{=} i_2] + [b_3 \stackrel{?}{=} i_3] > 1\ \mathsf{then}\ \mathbf{return}\ 1\\
\mathsf{else}\ \mathbf{return}\ 0
\end{array}
\right.
\end{array}
$$

ANALYSIS SKETCH. For clarity, let us assume that $\mathsf{Adv}^{\mathsf{ddh}}_{\mathbb{G}}(\mathcal{A}) = \Pr[\mathcal{Q}_1^{\mathcal{A}} = 1] - \Pr[\mathcal{Q}_0^{\mathcal{A}} = 1]$, i.e., $\mathcal{A}$ prefers $\mathcal{Q}_1$ to $\mathcal{Q}_0$. If x, y, z is not a Diffie-Hellman tuple then with probability $\frac{q-1}{q}$, the tuple $x, y, \overline{z}$ is not a Diffie-Hellman tuple and inputs are indistinguishable for $\mathcal{B}$. As a result $\Pr[b_j = i_j] \leq \frac{1}{2} + \frac{1}{q}$. If x, y, z is a Diffie-Hellman tuple then the inputs can be distinguished and thus $\Pr[b_j = i_j] \geq \mathsf{Adv}^{\mathsf{ddh}}_{\mathbb{G}}(\mathcal{A}) - \frac{1}{q}$. In other words, the expected value of the sum

$$[b_1 \stackrel{?}{=} i_1] + [b_2 \stackrel{?}{=} i_2] + [b_3 \stackrel{?}{=} i_3]$$

is higher than $\frac{3}{2}$ and we can use Chebyshev or Hoeffding bounds to estimate the success. Even the naive method where we explicitly use that $\Pr[b_j = i_j] \geq \mathsf{Adv}^{\mathsf{ddh}}_{\mathbb{G}}(\mathcal{A}) - \frac{1}{q}$ is enough to get tractable bounds on the success probability as there is no need to introduce ε_0 and ε_1.