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

Exercise (Simple reductions to DL problem). *Let $\mathbb{G} = \langle g \rangle$ be a finite group of an order q generated by the powers of an element g. Let $\mathsf{Adv}^{\mathsf{dl}}_{\mathbb{G}}(\cdot), \mathsf{Adv}^{\mathsf{cdh}}_{\mathbb{G}}(\cdot), \mathsf{Adv}^{\mathsf{ddh}}_{\mathbb{G}}(\cdot)$ denote corresponding advantages for Discrete Logarithm, Computational Diffie-Hellman, and Decisional Diffie-Hellman problems.*

1. *Show that Decisional Diffie-Hellman problem can be reduced to Computational Diffie-Hellman problem, i.e., for any algorithm $\mathcal{B}$ that achieves advantage $\mathsf{Adv}^{\mathsf{cdh}}_{\mathbb{G}}(\mathcal{B})$, there exists an oracle algorithm $\mathcal{A}^{\mathcal{B}}$ with the advantage $\mathsf{Adv}^{\mathsf{ddh}}_{\mathbb{G}}(\mathcal{A})$ that has roughly the same running time.*
2. *Show that Computational Diffie-Hellman problem can be reduced to Discrete Logarithm problem, i.e., for any algorithm $\mathcal{B}$ that achieves advantage $\mathsf{Adv}^{\mathsf{dl}}_{\mathbb{G}}(\mathcal{B})$, there exists an oracle algorithm $\mathcal{A}^{\mathcal{B}}$ with the advantage $\mathsf{Adv}^{\mathsf{cdh}}_{\mathbb{G}}(\mathcal{A})$ that has has roughly the same running time.*
3. *Show by composing previous solutions that Decisional Diffie-Hellman problem can be reduced to Discrete Logarithm problem, i.e., for any algorithm $\mathcal{B}$ that achieves advantage $\mathsf{Adv}^{\mathsf{dl}}_{\mathbb{G}}(\mathcal{B})$, there exists an oracle algorithm $\mathcal{A}^{\mathcal{B}}$ with the advantage $\mathsf{Adv}^{\mathsf{ddh}}_{\mathbb{G}}(\mathcal{A})$ that has roughly the same running time.*

Solution. DDH⇒CDH. Let $\mathcal{B}$ be a successful CDH solver. Then we can compare its output z_* to the element z in question to determine whether the triple x, y, z is a Diffie-Hellman triple or not. The corresponding formal reduction is given below:

$$\begin{array}{l} \mathcal{A}^{\mathcal{B}}(x, y, z) \\ \left[\begin{array}{l} z_* \leftarrow \mathcal{A}(x, y) \\ \textbf{return } [z_* \stackrel{?}{=} z] \end{array}\right. . \end{array}$$

Now if we substitute $\mathcal{A}$ to the DDH games

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

we get the following games after some simplifications of the code:

$$\begin{array}{ll} \mathcal{G}_0^{\mathcal{B}} & \mathcal{G}_1^{\mathcal{B}} \\ \left[\begin{array}{l} a, b, c \xleftarrow{u} \mathbb{Z}_q \\ z_* \leftarrow \mathcal{A}(g^a, g^b) \\ \textbf{return } [z_* \stackrel{?}{=} g^c] \end{array}\right. & \left[\begin{array}{l} a, b \xleftarrow{u} \mathbb{Z}_q \\ z_* \leftarrow \mathcal{A}(g^a, g^b) \\ \textbf{return } [z_* \stackrel{?}{=} g^{ab}] \end{array}\right. . \end{array}$$

which allows us to establish the following equations:

$$\begin{aligned} \Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1\right] &= \mathsf{Adv}^{\mathsf{cdh}}_{\mathbb{G}}(\mathcal{B}) \ , \\ \Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1\right] &= \frac{1}{q} \ . \end{aligned}$$

The first equation follows form As the game $\mathcal{G}_1^{\mathcal{B}}$ is identical to the game which defines $\mathsf{Adv}^{\mathsf{cdh}}_{\mathbb{G}}(\mathcal{B})$. The second equality follows from the fact that g^c is independent from g^a and g^b and thus we rewrite the game in the following way:

$$\begin{array}{l} \mathcal{G}_0^{\mathcal{B}} \\ \left[\begin{array}{l} a, b \xleftarrow{u} \mathbb{Z}_q \\ z_* \leftarrow \mathcal{A}(g^a, g^b) \\ c \leftarrow \mathbb{Z}_q \\ \textbf{return } [z_* \stackrel{?}{=} g^c] \end{array}\right. . \end{array}$$

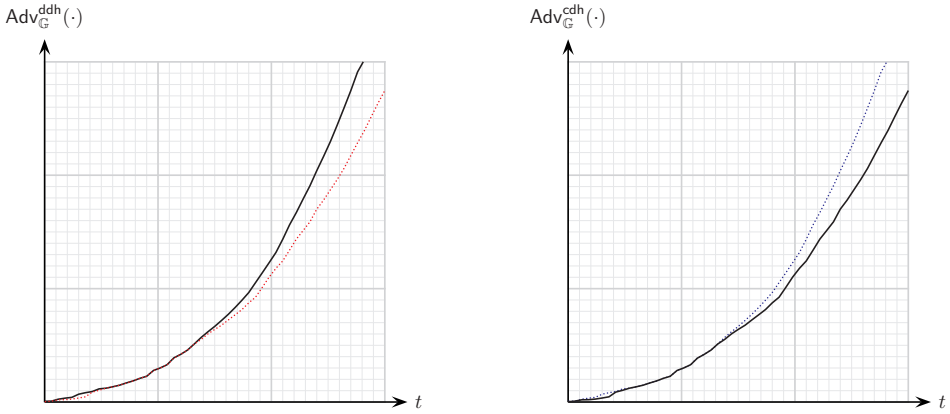

Figure 1: Upper and lower bounds induced by the DDH⇒CDH reduction. Solid black line shows the time-success profile for DDH on the left and the time-success profile for CDH for on the right. Dotted red line shows the achievable advantage if we take best CDH solvers and convert them into DDH distinguishers. Dotted blue line shows the upper bound for CDH time-success profile due to the reduction.

Since g^c is uniformly distributed over $\mathbb{G}$ after the value z_* is fixed the probability of hitting z_* is indeed $\frac{1}{q}$. As a consequence, we have proved that

$$\mathsf{Adv}^{\mathsf{ddh}}_{\mathbb{G}}(\mathcal{A}) = \mathsf{Adv}^{\mathsf{cdh}}_{\mathbb{G}}(\mathcal{B}) - \frac{1}{q} \ .$$

As the $\mathcal{A}$ does a simple comparison operation besides calling $\mathcal{B}$, running times differ only by a constant.

Remark. At first glance, asymptotic estimates do not make sense in the setting where the group is fixed as the problem instance cannot grow. However, we can also observe how the maximal advantage changes when we modify the time limit t. Consequently, we can talk about asymptotics w.r.t. and say that the difference between running times is $c = \mathrm{O}(1)$. The reduction above assures that if $\varepsilon(t)$ is the time-success profile for the CDH problem then $\varepsilon(t+c) - \frac{1}{q}$ is lower bound for the DDH time success-profile, see Figure **??**.

CDH⇒DL. Let $\mathcal{B}$ be a successful DL solver. Then it is straightforward to use it in order to compute the last element of the Diffie-Hellman triple x, y, z. If we know the discrete logarithm of x we can compute z in the same way as in the Diffie-Hellman key exchange protocol. The corresponding reduction construction is given below:

$$\begin{array}{l} \mathcal{A}^{\mathcal{B}}(x, y) \\ \left[\begin{array}{l} a_* \leftarrow \mathcal{B}(x) \\ \textbf{return } y^{a_*} \end{array}\right. \ . \end{array}$$

Now if we substitute this construction into the DL game we obtain after straightforward simplification

$$\begin{array}{l} \mathcal{G}^{\mathcal{A}} \\ \left[\begin{array}{l} a, b \xleftarrow{u} \mathbb{Z}_q \\ a_* \leftarrow \mathcal{B}(g^a) \\ \textbf{return } [g^{a_* b} \stackrel{?}{=} g^{ab}] \end{array}\right. \ . \end{array}$$

Clearly if $a_* = a$ then $g^{a_* b} = g^{ab}$ and thus

$$\mathsf{Adv}^{\mathsf{cdh}}_{\mathbb{G}}(\mathcal{B}) = \Pr\left[\mathcal{G}^{\mathcal{B}} = 1\right] \geq \Pr\left[a \xleftarrow{u} \mathbb{Z}_q : \mathcal{B}(g^a) = a\right] = \mathsf{Adv}^{\mathsf{dl}}_{\mathbb{G}}(\mathcal{B}) \ .$$

DDH⇒DL. From previous parts, we know that for any DL-finder $\mathcal{C}$ we can construct a CDH-finder $\mathcal{B}$ such that $\mathsf{Adv}^{\mathsf{dl}}_{\mathbb{G}}(\mathcal{C}) \leq \mathsf{Adv}^{\mathsf{cdh}}_{\mathbb{G}}(\mathcal{B})$ and from any CDH-finder $\mathcal{B}$ we can construct DDH-distinguisher $\mathcal{A}$ such that

$$\mathsf{Adv}^{\mathsf{cdh}}_{\mathbb{G}}(\mathcal{B}) - \frac{1}{q} \leq \mathsf{Adv}^{\mathsf{ddh}}_{\mathbb{G}}(\mathcal{A}) \ .$$

By doing both transformations, we get a new construction

$$\begin{array}{l} \mathcal{A}^{\mathcal{C}}(x, y, z) \\ \left[\begin{array}{l} a_* \leftarrow \mathcal{C}(x) \\ z_* \leftarrow y^{a_*} \\ \textbf{return } [z_* \stackrel{?}{=} z] \end{array}\right. , \end{array}$$

which is guaranteed to satisfy

$$\mathsf{Adv}^{\mathsf{dl}}_{\mathbb{G}}(\mathcal{C}) - \frac{1}{q} \leq \mathsf{Adv}^{\mathsf{ddh}}_{\mathbb{G}}(\mathcal{A}) \ .$$