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

Exercise (Random self-reducibility of CDH). *Let $\mathbb{G}$ be a finite group 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 $z = g^{ab}$.*

1. *Show that Computational Diffie-Hellman problem is random self-reducible, i.e., for any algorithm $\mathcal{B}$ that achieves advantage*

$$\mathsf{Adv}^{\mathsf{cdh}}_{\mathbb{G}}(\mathcal{B}) \doteq \Pr\left[x, y \xleftarrow{u} \mathbb{G} : \mathcal{B}(x, y) = g^{\log_g x \log_g y}\right]$$

there exists an oracle algorithm $\mathcal{A}^{\mathcal{B}}$ that for any input $x, y \in \mathbb{G}$ outputs the correct answer with the probability $\mathsf{Adv}^{\mathsf{cdh}}_{\mathbb{G}}(\mathcal{B})$ and has roughly the same running time.

2. *Given that the CDH problem is random self-reducible, show that the difficulty of CDH instances cannot wary a lot. Namely, let $\mathcal{B}$ be a t-time algorithm that achieves maximal advantage $\mathsf{Adv}^{\mathsf{cdh}}_{\mathbb{G}}(\mathcal{B})$. What can we say about worst-case advantage*

$$\min_{x,y\in\mathbb{G}} \Pr\left[\mathcal{A}(x, y) = g^{\log_g x \log_g y}\right]?$$

Can there be a large number of pairs (x, y) for which the CDH problem is easy?

3. *Show how to amplify the success rate of $\mathcal{B}$ by repetitions. Sketch the corresponding time-success profile $\varepsilon(t)$. What does this say about time-success profile of CDH problem in general?*

Solution. Random Self-reducibility. Given an original adversary $\mathcal{B}$ against computational Diffie-Hellman problem we can construct the following algorithm:

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

For the analysis, let $\alpha = \log_g x$ and $\beta = \log_g y$. Then by the definition, the tuple $x \cdot g^a, y \cdot g^b, c$ is a valid Diffie-Helmann tuple only if

$$c = g^{(\alpha+a)(\beta+b)} \quad\Longleftrightarrow\quad c = g^{\alpha\beta} \cdot g^{\alpha b} \cdot g^{ab} \cdot g^{\beta a}\ .$$

From this we can conclude

$$c = g^{(\alpha+a)(\beta+b)} \quad\Longleftrightarrow\quad g^{\alpha\beta} = c \cdot (g^{\alpha})^{-b} \cdot (g^{\beta})^{a} \cdot g^{ab}\ ,$$

which itself implies that the adversary $\mathcal{A}^{\mathcal{B}}$ succeed if and only if $\mathcal{B}$ produces a Diffie-Helmann tuple:

$$c = g^{(\alpha+a)(\beta+b)} \quad\Longleftrightarrow\quad g^{\alpha\beta} = c \cdot x^{-b} \cdot y^{-a} \cdot g^{-ab}\ .$$

Hence, the advantage of $\mathcal{A}^{\mathcal{B}}$ can be calculated as follows:

$$\Pr\left[\mathcal{A}^{\mathcal{B}}(x, y) = g^{\alpha\beta}\right] = \Pr\left[a, b \xleftarrow{u} \mathbb{Z}_{|\mathbb{G}|} : \mathcal{B}(x \cdot g^a, y \cdot g^b) = g^{(\alpha+a)\cdot(\beta+b)}\right]\ .$$

Now it is easy to see that for any $\forall\alpha, \beta \in \mathbb{Z}_{|\mathbb{G}|}$, the group elements $x \cdot g^a$ and $y \cdot g^b$ are independent and have uniform distribution. Hence, the adversary $\mathcal{B}$ inside $\mathcal{A}^{\mathcal{B}}$ gets correctly formed CDH challenges and we thus we can conclude

$$\Pr\left[a, b \xleftarrow{u} \mathbb{Z}_{|\mathbb{G}|}; \mathcal{B}(x \cdot g^a, y \cdot g^b) = g^{(\alpha+a)\cdot(\beta+b)}\right] = \mathsf{Adv}^{\mathsf{cdh}}_{\mathbb{G}}(\mathcal{B})\ .$$

If $\mathcal{B}$ runs in t-time, $\mathcal{A}^{\mathcal{B}}$ runs in $(t+\delta)$-time, where δ is a small time required to perform element sampling and multiplications.

Uniformity. Because $\mathcal{A}$ reduces each problem instance to a random one, $\Pr\left[\mathcal{A}(x,y) = g^{\log_g x \log_g y}\right]$ is equal to $\mathsf{Adv}^{\mathsf{cdh}}_{\mathbb{G}}(\mathcal{B})$ for each pair (x,y). Therefore, the worst-case advantage of $\mathcal{A}$ is the same as advantage of $\mathcal{B}$ and if there are a lot of CDH instances, which are easy for $\mathcal{B}$, the performance of $\mathcal{A}$ is good on any instance.

Amplification effects. **To be added**