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 $B$ that achieves advantage

$$\text{Adv}^{\text{cdh}}_B(x, y) = \Pr [x, y \in \mathbb{G} : B(x, y) = g^\alpha, x^\beta]$$

there exists an oracle algorithm $A^B$ that for any input $x, y \in \mathbb{G}$ outputs the correct answer with the probability $\text{Adv}^{\text{cdh}}_B(x, y)$ 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 $B$ be a $t$-time algorithm that achieves maximal advantage $\text{Adv}^{\text{cdh}}_B(x, y)$. What can we say about worst-case advantage

$$\min_{x, y \in \mathbb{G}} \Pr [A(x, y) = g^\alpha, x^\beta]?$$

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 $B$ 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 $B$ against computational Diffie-Hellman problem we can construct the following algorithm:

$$A^B(x, y) = \begin{cases} a, b \leftarrow \mathbb{Z}_{|\mathbb{G}|} \\ c \leftarrow B(x \cdot g^a, y \cdot g^b) \\ \text{return } c \cdot x^{-b} \cdot y^{-a} \cdot g^{-ab}. \end{cases}$$

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-Hellmann tuple only if

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

From this we can conclude

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

which itself implies that the adversary $A^B$ succeed if and only if $B$ produces a Diffie-Hellman tuple:

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

Hence, the advantage of $A^B$ can be calculated as follows:

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

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 $B$ inside $A^B$ gets correctly formed CDH challenges and we thus we can conclude

$$\Pr [a, b \leftarrow \mathbb{Z}_{|\mathbb{G}|} : B(x \cdot g^a, y \cdot g^b) = g^{(\alpha + a)(\beta + b)}] = \text{Adv}^{\text{cdh}}_B.$$ 

1
If $\mathcal{B}$ runs in $t$-time, $A^\mathcal{B}$ runs in $(t + \delta)$-time, where $\delta$ is a small time required to perform element sampling and multiplications.

**Uniformity.** Because $A$ reduces each problem instance to a random one, $Pr[A(x, y) = g^{\log_x x \log_y y}]$ is equal to $\text{Adv}^{\text{cdh}}_G(\mathcal{B})$ for each pair $(x, y)$. Therefore, the worst-case advantage of $A$ 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 $A$ is good on any instance.

**Amplification effects.** To be added