ETH Zürich, D-INFK
Spring 2018

Prof. Ueli Maurer
Christian Badertscher
Fabio Banfi

Cryptography Foundations
Solution Exercise 7

7.1 Search Problems

a) We have two random variables X and A, where X corresponds to the instance of the problem and is distributed according to P_X, and A is a random variable over deterministic algorithms. We denote the output of A on input x by $A(x)$ (which is a random variable over $\mathcal{W}$). Then, the success probability of A is given by

$$\Pr\big[Q(X, A(X)) = 1\big].$$

b) Since the success probability of an algorithm A is defined as the average success probability of A over all instances $x \in \mathcal{X}$, weighted according to P_X, A may perform much below its average success probability on some of the instances. Consider a computational problem with two instances x_0 and x_1 such that A always finds a witness given x_0 but never finds one given x_1. If we have $\mathsf{P}_X(x_0) = \alpha$ and $\mathsf{P}_X(x_1) = 1 - \alpha$, the success probability of A is α. In this case, the success probability of A' is also α. Obviously, the success probability of A' is at least as high as the one of A. Hence, the best lower bound on the success probability of A' is α.

c) Let $\mathbb{G} = \langle g \rangle$, $|\mathbb{G}| = q$ be the group for which A can solve the discrete logarithm problem with probability α. Algorithm A' works as follows: Let $c > 1$ be some constant. On input $h = g^x \in \mathbb{G}$, the algorithm A' chooses $r \in \mathbb{Z}_q$ uniformly at random and invokes A on $h \cdot g^r = g^{x+r}$. Given the output y of A, it computes $y' := y - r \mod q$. If $g^{y'} = h$, A' outputs y'. Otherwise, it repeats the procedure with a freshly chosen $r \in \mathbb{Z}_q$ if the number of repetitions so far (including the first iteration) is less than c. If the number of repetitions equals c, A' outputs y'.

Note that if solver A succeeds on $h \cdot g^r$, then A' outputs a correct solution y' with $g^{y'} = h$. Since $h \cdot g^r$ is a uniform random element of $\mathbb{G}$, this happens with probability α. Hence, the success probability of A' is

$$1 - (1 - \alpha)^c > \alpha$$

for $c > 1$.

d) The crucial property of algorithm A' in subtask c) is that it invokes A each time on a uniformly random instance. In general, a problem instance cannot be transformed to a random instance such that a solution to the random instance can be transformed to a solution to the original instance. Problems that allow this are called *random self-reducible*.

7.2 Reductions Related to Discrete Logarithms

Let $\mathbb{G}' := \langle \mathbb{G} \setminus \{1\}; \star \rangle$ with $g^a \star g^b := g^{ab}$. Note that $|\mathbb{G}'| = 2^k$ and $\mathbb{G}' \cong \mathbb{Z}_q^*$ via the group isomorphism $\mathbb{Z}_q^* \to \mathbb{G}', x \mapsto g^x$. Let $r \in \mathbb{Z}_q^*$ be the generator of $\mathbb{Z}_q^*$ that is assumed to be known.[1] Then, g^r generates $\mathbb{G}'$ because isomorphisms map generators to generators.

[1] One can in fact efficiently find such generator but this beyond the scope of this exercise.

We now describe the algorithm that computes the discrete logarithm of a given element $h \in \mathbb{G}$. If $h = 1$, the algorithm outputs 0. Otherwise, it computes the discrete logarithm of h in $\mathbb{G}'$ to the base g^r, i.e., an element $z \in \mathbb{Z}_q^*$ such that

$$h = \underbrace{g^r \star \ldots \star g^r}_{z \text{ times}} = g^{(r^z)}. \tag{1}$$

Since $|\mathbb{G}'| = 2^k$ and the group operation $\star$ in $\mathbb{G}'$ can be computed using the computational Diffie-Hellman oracle, the value z can be found efficiently using the algorithm from Exercise 3.3 d). Finally, our algorithm computes $x := r^z \in \mathbb{Z}_q^*$ and outputs x. Equation (1) implies that x is the discrete logarithm of h to base g and hence the algorithm is correct.

7.3 Properties of the Statistical Distance

a) Using the independence of A and X and the one of A and X', and the triangle inequality for the absolute value, we obtain

$$\begin{aligned}
\delta\big(A(X), A(Y)\big) &= \frac{1}{2}\sum_{y\in\mathcal{Y}}\left|\Pr^{AX}[A(X)=y] - \Pr^{AX'}[A(X')=y]\right| \\
&= \frac{1}{2}\sum_{y\in\mathcal{Y}}\left|\sum_{x\in\mathcal{X}}\Pr^{AX}[A(x)=y \wedge X=x] - \sum_{x\in\mathcal{X}}\Pr^{AX'}[A(x)=y \wedge X'=x]\right| \\
&\overset{\text{indep.}}{=} \frac{1}{2}\sum_{y\in\mathcal{Y}}\left|\sum_{x\in\mathcal{X}}\Pr^{A}[A(x)=y]\cdot \mathsf{P}_X(x) - \sum_{x\in\mathcal{X}}\Pr^{A}[A(x)=y]\cdot \mathsf{P}_{X'}(x)\right| \\
&= \frac{1}{2}\sum_{y\in\mathcal{Y}}\left|\sum_{x\in\mathcal{X}}\Pr^{A}[A(x)=y]\cdot \big(\mathsf{P}_X(x) - \mathsf{P}_{X'}(x)\big)\right| \\
&\le \frac{1}{2}\sum_{y\in\mathcal{Y}}\sum_{x\in\mathcal{X}}\Pr^{A}[A(x)=y]\cdot \big|\mathsf{P}_X(x) - \mathsf{P}_{X'}(x)\big| \\
&= \frac{1}{2}\sum_{x\in\mathcal{X}}\left(\big|\mathsf{P}_X(x) - \mathsf{P}_{X'}(x)\big|\cdot \underbrace{\sum_{y\in\mathcal{Y}}\Pr^{A}[A(x)=y]}_{=1}\right) \\
&= \delta\big(X, X'\big).
\end{aligned}$$

b) The claim follows from the following calculation using the definition of the statistical distance and basic properties of the uniform distribution over a finite set:

$$\begin{aligned}
\delta(X,Y) &= \frac{1}{2}\sum_{x\in I}|\mathsf{P}_X(x) - \mathsf{P}_Y(x)| \\
&= \frac{1}{2}\sum_{x\in J}|\mathsf{P}_X(x) - \mathsf{P}_Y(x)| + \frac{1}{2}\sum_{x\in I\setminus J}|\mathsf{P}_X(x) - \mathsf{P}_Y(x)| \\
&= \frac{1}{2}\sum_{x\in J}\left|\frac{1}{|I|} - \frac{1}{|J|}\right| + \frac{1}{2}\sum_{x\in I\setminus J}\left|\frac{1}{|I|} - 0\right| \\
&= \frac{1}{2}\sum_{x\in J}\left(\frac{1}{|J|} - \frac{1}{|I|}\right) + \frac{1}{2}\sum_{x\in I\setminus J}\frac{1}{|I|} \\
&= \frac{1}{2}\left(\frac{|J|}{|J|} - \frac{|J|}{|I|} + \frac{|I|-|J|}{|I|}\right) \\
&= 1 - \frac{|J|}{|I|}.
\end{aligned}$$