ETH Zürich, D-INFK
Spring 2019

Prof. Ueli Maurer
Fabio Banfi
Daniel Jost
Jiamin Zhu

Cryptography Foundations
Solution Exercise 7

7.1 The Merkle-Damgård Construction

a) An easy collision is given by $x = 0$ and $y = (0, 0)$. To see this note that $\hat{x} = \hat{y} = (0, \ldots, 0) \in \{0,1\}^m$ and thus $h(x) = f(0, \ldots, 0) = h(y)$.

b) The winner of the collision-finding game for h outputs two messages $x \neq y$ such that $h(x) = h(y)$. From this collision of h we need to compute a collision of f. Let d_x and d_y be the numbers of 0's that have to be appended to x and y, respectively, in order that we get strings that are multiples of m bits long. So, $d_x = -|x| \bmod m$ and $d_y = -|y| \bmod m$. This allows us to write

$$\hat{x} = x \parallel \underbrace{(0, \ldots, 0)}_{d_x \text{ times}} \parallel \langle d_x \rangle \quad \text{and} \quad \hat{y} = y \parallel \underbrace{(0, \ldots, 0)}_{d_y \text{ times}} \parallel \langle d_y \rangle.$$

Moreover, let h_k^x, $1 \leq k \leq s = \frac{|x|+d_x}{m} + 1$, and h_k^y, $1 \leq k \leq t = \frac{|y|+d_y}{m} + 1$, be the outputs of f in the iterative evaluation of $h(x)$ and $h(y)$. We can assume without loss of generality that $t \geq s$. Note that, by definition,

$$h_s^x = h(x) = h(y) = h_t^y.$$

If there exists a $k \in \{1, \ldots, s-1\}$ with $h_{s-k}^x \neq h_{t-k}^y$ and k is the smallest such number, then

$$f(h_{s-k}^x \parallel 1 \parallel \hat{x}_{s-(k-1)}) = h_{s-(k-1)}^x = h_{t-(k-1)}^y = f(h_{t-k}^y \parallel 1 \parallel \hat{y}_{t-(k-1)}),$$

which gives a collision of f. Therefore we can assume in the remainder of the proof that $h_{s-k}^x = h_{t-k}^y$ for all $0 \leq k \leq s-1$. We proceed by considering three cases. First suppose that $|x| \not\equiv |y| \pmod{m} \Leftrightarrow d_x \neq d_y$. Then the last compression stages in the evaluations of $h(x)$ and $h(y)$ already give a collision of f. Concretely,

$$f(\underbrace{h_{s-1}^x \parallel 1 \parallel \langle d_x \rangle}_{=x'}) = h_s^x = h(x) = h(y) = h_t^y = f(\underbrace{h_{t-1}^y \parallel 1 \parallel \langle d_y \rangle}_{=y'})$$

with $x' \neq y'$ as $d_x \neq d_y$. Next we turn to the case where $|x| \equiv |y| \pmod{m}$ but $|x| \neq |y|$. Here it follows that $t > s$ and, with $k = s-1$,

$$f((0, \ldots, 0) \parallel 0 \parallel \hat{x}_1) = h_1^x = h_{s-k}^x = h_{t-k}^y = h_{t-(s-1)}^y = f(h_{t-s}^y \parallel 1 \parallel \hat{y}_{t-(s-1)}),$$

which again gives a collision of f. Finally, suppose $|x| = |y|$. In this case there is a $1 \leq k \leq t = s$ such that $\hat{x}_k \neq \hat{y}_k$. From this we get the collision

$$f((0, \ldots, 0) \parallel \hat{x}_1) = h_1^x = h_1^y = f((0, \ldots, 0) \parallel \hat{y}_1)$$

if $k = 1$ or else the collision

$$f(h_{k-1}^x \parallel 1 \parallel \hat{x}_k) = h_k^x = h_k^y = f(h_{k-1}^y \parallel 1 \parallel \hat{y}_k).$$

7.2 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*.

7.3 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:

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