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

Exercise (Precise analysis of 2PRE $\Rightarrow$ OW). *There are several other properties that hash function families can have besides collision resistance. A hash function family $\mathcal{H}$ with the domain $\mathcal{M}$ and range $\mathcal{Y}$ is (t,ε)-secure one-way function family if for any t-time adversary $\mathcal{A}$*

$$\Pr\left[h \xleftarrow{u} \mathcal{H}, m_0 \xleftarrow{u} \mathcal{M}, m_1 \leftarrow \mathcal{A}(h, h(m_0)) : h(m_0) = h(m_1)\right] \leq \varepsilon \ .$$

A hash function family $\mathcal{H}$ is (t,ε)-secure against second preimage if for any t-time adversary $\mathcal{A}$

$$\Pr\left[\begin{array}{l} h \xleftarrow{u} \mathcal{H}, m_0 \xleftarrow{u} \mathcal{M}, m_1 \leftarrow \mathcal{A}(h, m_0) : \\ m_0 \neq m_1 \wedge h(m_0) = h(m_1) \end{array}\right] \leq \varepsilon \ .$$

Show that a compressing function that is a second-preimage resistant must be also one-way function.

Solution. We start the analysis by formalising the security games for one-way and 2nd pre-image resistance:

$$\begin{array}{ll} \mathcal{G}_0^{\mathcal{A}} & \mathcal{Q}^{\mathcal{B}} \\ \left[\begin{array}{l} h \xleftarrow{u} \mathcal{H} \\ m_0 \xleftarrow{u} \mathcal{M} \\ m_1 \leftarrow \mathcal{A}(h, h(m_0)) \\ \textbf{return } [h(m_0) \stackrel{?}{=} h(m_1)] \end{array}\right. & \left[\begin{array}{l} h \xleftarrow{u} \mathcal{H} \\ m_0 \xleftarrow{u} \mathcal{M} \\ m_1 \leftarrow \mathcal{B}(h, m_0) \\ \textbf{return } [m_0 \neq m_1] \wedge [h(m_0) \stackrel{?}{=} h(m_1)] \ . \end{array}\right. \end{array}$$

Since the hash function is compressing there are many originals and it is highly unlikely that the inversion algorithm $\mathcal{A}$ manages to restore m from $h(m)$. Thus, it makes sense to consider the following adversary:

$$\begin{array}{l} \mathcal{B}^{\mathcal{A}}(h, m_0) \\ \left[\begin{array}{l} m_1 \leftarrow \mathcal{A}(h, h(m_0)) \\ \textbf{return } m_1 \ . \end{array}\right. \end{array}$$

By substituting this definition to the second preimage game $\mathcal{Q}$ we get a game

$$\begin{array}{l} \mathcal{G}_1^{\mathcal{A}} \\ \left[\begin{array}{l} h \xleftarrow{u} \mathcal{H} \\ m_0 \xleftarrow{u} \mathcal{M} \\ m_1 \leftarrow \mathcal{A}(h, h(m_0)) \\ \textbf{return } [m_0 \neq m_1] \wedge [h(m_0) \stackrel{?}{=} h(m_1)] \ . \end{array}\right. \end{array}$$

that is more strict form the game $\mathcal{G}_0$, which is used to evaluate $\mathsf{Adv}^{\mathsf{ow}}_{\mathcal{H}}(\mathcal{A})$. Hence, we get the inequality with the wrong sign: $\mathsf{Adv}^{\mathsf{2nd\text{-}pre}}_{\mathcal{H}}(\mathcal{B}) \leq \mathsf{Adv}^{\mathsf{ow}}_{\mathcal{H}}(\mathcal{A})$. For a more useful estimate, note that

$$\Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1\right] = \Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1\right] + \Pr\left[\mathcal{G}_2^{\mathcal{A}} = 1\right]$$

where

$$\begin{array}{l} \mathcal{G}_2^{\mathcal{A}} \\ \left[\begin{array}{l} h \xleftarrow{u} \mathcal{H} \\ m_0 \xleftarrow{u} \mathcal{M} \\ m_1 \leftarrow \mathcal{A}(h, h(m_0)) \\ \textbf{return } [m_0 \stackrel{?}{=} m_1] \wedge h(m_0) \stackrel{?}{=} h(m_1) \ . \end{array}\right. \end{array}$$

The same equality can be written in terms of advantages

$$\mathsf{Adv}^{\mathsf{ow}}_{\mathcal{H}}(\mathcal{A}) = \mathsf{Adv}^{\mathsf{2nd\text{-}pre}}_{\mathcal{H}}(\mathcal{B}) + \Pr\left[\mathcal{G}_2^{\mathcal{A}} = 1\right] \ .$$

Consequently, we must upper bound the $\Pr\left[\mathcal{G}_2^{\mathcal{A}} = 1\right]$ to bound $\mathsf{Adv}^{\mathsf{ow}}_{\mathcal{H}}(\mathcal{A})$. For that, we relax the game by omitting the check $h(m_0) \stackrel{?}{=} h(m_1)$. This leads to the following game:

$$\begin{array}{l} \mathcal{G}_3^{\mathcal{A}} \\ \left[\begin{array}{l} h \xleftarrow{u} \mathcal{H} \\ m_0 \xleftarrow{u} \mathcal{M} \\ y_0 \leftarrow h(m_0) \\ m_1 \leftarrow \mathcal{A}(h, y_0) \\ \textbf{return } [m_0 \stackrel{?}{=} m_1] \ . \end{array}\right. \end{array}$$

For further analysis recall that we can use sampling idiom for restructuring the process that creates (m_0, y). Recall that the procedure $m_0 \leftarrow \mathcal{M}, y_0 \leftarrow h(m_0)$ defines a unique distribution $\mathcal{Y}_0$ of hash values y_0. Moreover, there exists a family of sets $\mathcal{M}_y = \{m : f(m) = y\}$ such that the procedure $y_0 \leftarrow \mathcal{Y}_0, m_0 \xleftarrow{u} \mathcal{M}_{y_0}$ defines the same distribution of (m_0, y_0) as the first procedure. Consequently, we can express $\mathcal{G}_3$ as follows:

$$\begin{array}{l} \mathcal{G}_4^{\mathcal{A}} \\ \left[\begin{array}{l} h \xleftarrow{u} \mathcal{H} \\ y_0 \leftarrow \mathcal{Y}_0 \\ m_0 \xleftarrow{u} \mathcal{M}_{y_0} \\ m_1 \leftarrow \mathcal{A}(h, y_0) \\ \textbf{return } [m_0 \stackrel{?}{=} m_1] \ . \end{array}\right. \end{array}$$

Since m_1 does not depend on m_0 we can simplify the game further:

$$\begin{array}{l} \mathcal{G}_5^{\mathcal{A}} \\ \left[\begin{array}{l} h \xleftarrow{u} \mathcal{H} \\ y_0 \leftarrow \mathcal{Y}_0 \\ m_1 \leftarrow \mathcal{A}(h, y_0) \\ m_0 \xleftarrow{u} \mathcal{M}_{y_0} \\ \textbf{return } [m_0 \stackrel{?}{=} m_1] \ . \end{array}\right. \end{array}$$

for which we can easily derive the success bound

$$\begin{aligned} \Pr\left[\mathcal{G}_5^{\mathcal{A}} = 1\right] &= \sum_{y_0 \in \mathcal{Y}} \Pr\left[y \leftarrow \mathcal{Y}_0 : y = y_0\right] \cdot \Pr\left[m_0 \leftarrow \mathcal{M}_{y_0} : m_0 = \mathcal{A}(h, y_0)\right] \\ &\leq \sum_{y_0 \in \mathcal{Y}} \frac{|\mathcal{M}_{y_0}|}{|\mathcal{M}|} \cdot \frac{1}{|\mathcal{M}_{y_0}|} \leq \frac{|\mathcal{Y}|}{|\mathcal{M}|} \ . \end{aligned}$$

The last inequality follows from the facts that probability of y_0 is proportional to the number of originals and the probability of collision is inversely proportional to the set of originals $\mathcal{M}_{y_0}$ if $m_1 \in \mathcal{M}_{y_0}$ and zero otherwise. As a result, we have proved that

$$\mathsf{Adv}^{\mathsf{ow}}_{\mathcal{H}}(\mathcal{A}) \leq \mathsf{Adv}^{\mathsf{2nd\text{-}pre}}_{\mathcal{H}}(\mathcal{B}) + \frac{|\mathcal{Y}|}{|\mathcal{M}|} \ .$$

Since the running time of $\mathcal{B}$ is only by o constant larger than the running time of $\mathcal{A}$, we can conclude that (t, ε)-second preimage resistant function is also $(t, \varepsilon + \frac{|\mathcal{Y}|}{|\mathcal{M}|})$-one-way function.

On the optimality. The proof given above is rather loose, since just dropped the condition $h(m_0) = h(m_1)$ from the game $\mathcal{G}_2$ to obtain an easily tractable upper bound. Maybe we more careful analysis would have

given us better result. There are two objections which nullify this argument. First, as we have made no assumptions about the function h, the analysis of our construction must hold also when h is an easily invertible permutation h. In this case, we can always assume that $h(m_1) = h(m_0)$ and thus the relaxation does not change the probabilities. For bigger domains, we can mix easily invertible singletons with hard to invert elements with large set of originals. For instance, let $f : \mathcal{M} \to \mathcal{Y}$ be (t, ε)-second preimage resistant function. Then we can define a function $h : \mathbb{Z}_2 \times \mathcal{M} \to \mathcal{Y} \cup \mathcal{M}$ as follows:

$$h(b||m) = \begin{cases} m, & \text{if } b = 0 \ , \\ f(m), & \text{if } b = 1 \ . \end{cases}$$

By the construction h is also $(t, \frac{\varepsilon}{2})$-preimage resistant function, since the necessary pair occurs only if $b = 1$. As it is straightforward to invert h with probability $\frac{1}{2}$, we the derived bound is rather close

$$\frac{1}{2} \leq \mathsf{Adv}^{\mathsf{ow}}_{\mathcal{H}}(\mathcal{B}) \leq \frac{\varepsilon}{2} + \frac{|\mathcal{Y}| + |\mathcal{M}|}{2\,|\mathcal{M}|} \leq \frac{1}{2} + \frac{\varepsilon}{2} + \frac{|\mathcal{Y}|}{2\,|\mathcal{M}|}$$

where the last two terms can be considered negligible for practical hash function families.

Analysis for regular hash functions. We can obtain more tight results when we restrict the class of hash functions. For instance, if any $y \in \mathcal{Y}$ has the same number of originals, we can directly estimate the success probability of $\mathcal{G}_2$:

$$\Pr\left[\mathcal{G}_2^{\mathcal{A}} = 1\right] = \sum_{y_0 \in \mathcal{Y}} \frac{1}{|\mathcal{Y}|} \cdot \Pr\left[m_1 \leftarrow \mathcal{A}(h, y) : h(m_1) = y\right] \cdot \frac{|\mathcal{Y}|}{|\mathcal{M}|} = \frac{|\mathcal{Y}|}{|\mathcal{M}|} \cdot \mathsf{Adv}^{\mathsf{ow}}_{\mathcal{H}}(\mathcal{A})$$

which yields much better bound without the additive term:

$$\mathsf{Adv}^{\mathsf{ow}}_{\mathcal{H}}(\mathcal{A}) = \frac{|\mathcal{M}|}{|\mathcal{M}| - |\mathcal{Y}|} \cdot \mathsf{Adv}^{\mathsf{2nd\text{-}pre}}_{\mathcal{H}}(\mathcal{B}) \approx \mathsf{Adv}^{\mathsf{2nd\text{-}pre}}_{\mathcal{H}}(\mathcal{B}) \ .$$

Thus, we can conclude that the additive term in the universal bound mostly accounts the effect of singletons.

Common fallacies. We can express the game $\mathcal{G}_2$ with the help of sampling idiom as follows:

$$\begin{array}{l} \mathcal{G}_3^{\mathcal{A}} \\ \left\lceil \begin{array}{l} h \xleftarrow{u} \mathcal{H} \\ y \leftarrow \mathcal{T} \\ m_1 \leftarrow \mathcal{A}(h, y) \\ \mathsf{if}\ h(m_1) \neq y\ \mathbf{return}\ 0 \\ m_0 \xleftarrow{u} \mathcal{M}_y \\ \mathbf{return}\ [m_0 \stackrel{?}{=} m_1] \ . \end{array} \right. \end{array}$$

And now it would be tempting to say that the probability that we pass the last test is equivalent to the probability that $\mathcal{A}$ wins the game

$$\begin{array}{l} \mathcal{G}_5^{\mathcal{A}} \\ \left\lceil \begin{array}{l} h \xleftarrow{u} \mathcal{H} \\ y \leftarrow \mathcal{T} \\ m_1 \leftarrow \mathcal{A}(h, y) \\ m_0 \xleftarrow{u} \mathcal{M}_y \\ \mathbf{return}\ [m_0 \stackrel{?}{=} m_1] \end{array} \right. \end{array}$$

fow which we know the success bound and conclude that

$$\Pr\left[\mathcal{G}_3^{\mathcal{A}} = 1\right] \leq \frac{|\mathcal{T}|}{|\mathcal{M}|} \cdot \mathsf{Adv}^{\mathsf{ow}}_{\mathcal{H}}(\mathcal{B}) \ .$$

However, this is not the case because the ability of $\mathcal{A}$ to invert elements might vary and the latter changes the distribution of hash values y and the formula, i.e., the equation

$$\Pr\left[h \xleftarrow{u} \mathcal{H}, y \leftarrow \mathcal{T}, m_1 \leftarrow \mathcal{A}(h, y) : y | h(m_1) = y\right] = \frac{|\mathcal{M}_y|}{|\mathcal{M}|}$$

does not hold in general. The easiest way to see this is to consider what are the probabilities in the counter-example discussed in the optimality section.