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

Exercise (UH + PRF = MAC). *Let $h : \mathcal{X} \times \mathcal{K} \rightarrow \mathcal{T}$ universal hash function and let $\mathcal{F}$ be a (t, ε)-pseudorandom function family with elements $f : \mathcal{T} \rightarrow \mathcal{T}$. Prove that a keyed hash function $g : \mathcal{X} \times \mathcal{K} \times \mathcal{F} \rightarrow \mathcal{T}$ defined as $g(m, k, f) = f(h(m, k))$ is weakly collision resistant.*

Solution. Recall that a keyed function g is (t, q, ε)-*weakly collision resistant* if any t-time adversary $\mathcal{A}$ that makes at most q oracle queries finds a collision with probability

$$\mathsf{Adv}_g^{\mathsf{w\text{-}cr}}(\mathcal{A}) = \Pr\left[\mathcal{G}^{\mathcal{A}} = 1\right] \leq \varepsilon$$

where the security game is defined as follows

```
$\mathcal{G}^{\mathcal{A}}$
    $k \xleftarrow[u]{} \mathcal{K}$
    $f \xleftarrow[u]{} \mathcal{F}$
    $(m_0, m_1) \leftarrow \mathcal{A}^{g(\cdot, k, f)}$
    return $[m_0 \neq m_1] \wedge [g(m_0, k, f) = g(m_1, k, f)]$ .
```

Recall that a keyed hash function h is universal if for any $x_0 \neq x_1$, the outcome pair $h(x_0, k), h(x_1, k)$ is uniformly distributed over $\mathcal{T} \times \mathcal{T}$. Recall that $\mathcal{F}$ is (t, q, ε)-pseudorandom function family if any t-time adversary $\mathcal{A}$ that makes at most q oracle queries finds . . . .

Simplified problem. Let us first consider the case where $\mathcal{A}$ makes exactly 3 calls to g to generate a pair x_0, x_1. Let $x_1, \ldots, x_3$ be the inputs to the oracle calls. Then we can simplify the security game $\mathcal{G}$ by inlining all definition. . . . As . . . we can replace $\mathcal{F}$ with the family of all functions. . . . Now it is straightforward to see that we can replace oracle answers with random replies. The latter decreases success probability at most by . . . . For the formal reasoning let us look at the sequence of games . . . . Now that $\mathcal{A}$ gets replies that are independent form queries, it cannot learn anything about the outcomes of h. Consequently, . . .

General solution. We can easily lift the simplified solution to the general case where $\mathcal{A}$ makes exactly q oracle calls. . . .

Qualitative analysis. Note that the success bound consists of two components . . .