7.1 (Using H_{poly} with power-of-2 modulus). We can adapt the definition of H_{poly} in (7.3) so that instead of working in $\mathbb{Z}_p$ we work in $\mathbb{Z}_{2^n}$ (i.e., work modulo 2^n). Show that this version of H_{poly} is not a good UHF, and in particular an attacker can find two messages m_0, m_1 each of length two blocks that are guaranteed to collide.

$$H_{poly}(K, (a_1, \cdots a_v)) = K^v + a_1 \cdot K^{v-1} + a_2 \cdot K^{v-2} + \cdots + a_{v-1} \cdot K + a_v \bmod \mathbb{Z}_p$$

(7.3)

$a_1 \cdots a_v \in \mathbb{Z}_p$. $K \in \mathbb{Z}_p$.

$\downarrow$ adapt to $\mathbb{Z}_{2^n}$, $GF(2^n)$

Proof idea: observing that calculating $K \bmod 2^n$ is essentially getting the least-n-significant bit of K.

e.g. $K = 101101_2$, $n = 3$, Then $K \bmod 2^n = 101$.

So, if one could manipute m_0, m_1 s.t. their least n bit after hashing is distinguishable, then we've broken the UHF.

Proof: let $m_0 = (1, 1)$; $m_1 = (1, 0)$

$$UHF(K, m_b) = K^2 + K \cdot a_1 + a_2 = K(K + a_1) + a_2 \bmod 2^n.$$

since $a_1 = 1$, $K(K+1) \bmod 2^n$ will definitely ends up w/ a remainder whose $LSB = 1$.

$$\begin{cases} \text{if } K \text{ is even. } & K(K+1) \text{ is odd} \\ K \text{ is odd} & \text{odd} \end{cases} \Rightarrow LSB\left[K(K+1) \bmod 2^n\right] = 1$$

So $LSB(H(K \cdot m_0)) = 0$, $LSB\left(H(K, m_1)\right) = 1$ for all $K \in \mathcal{K}$.

$\hookrightarrow$ adversary has perfect advantage of 1.

7.3 (On the alternative characterization of the ϵ-UHF property). Let H be a keyed hash function defined over $(\mathcal{K}, \mathcal{M}, \mathcal{T})$. Suppose that for some pair of distinct messages m_0 and m_1, we have $\Pr[H(k, m_0) = H(k, m_1)] > \epsilon$, where the probability is over the random choice of $k \in \mathcal{K}$. Give an adversary $\mathcal{A}$ that wins Attack Game 7.1 with probability greater than ϵ. Your adversary is not allowed to just have the values m_0 and m_1 "hardwired" into its code, but it may be *very* inefficient.

chal

$k \xleftarrow{R} \mathcal{K}$

$H(k, m_0) \stackrel{?}{=} H(k, m_1)$

adv

$\xleftarrow{m_0,\, m_1 \in \mathcal{M}}$

randomly select msg pairs?

ϵ-bounded

$\Pr[H(\cdot, m_0) = H(\cdot, m_1)] > \epsilon.$

don't know

7.27 (XOR-hash analysis). Generalize Theorem 7.6 to show that for every Q-query UHF adversary $\mathcal{A}$, there exists a PRF adversary $\mathcal{B}$, which is an elementary wrapper around $\mathcal{A}$, such that

$$\mathrm{MUHF}\mathsf{adv}[\mathcal{A}, F^{\oplus}] \leq \mathrm{PRF}\mathsf{adv}[\mathcal{B}, F] + \frac{Q^2}{2|\mathcal{Y}|}.$$

Moreover, $\mathcal{B}$ makes at most $Q\ell$ queries to F.

NOTE: $|m_i| = |(a_1, a_2 \cdots, a_v)| \leq \ell$

chal.

$b \xleftarrow{R} \{0,1\}$, $k \xleftarrow{R} \mathcal{K}$

if $b=0$, $f \leftarrow PRF$

$b=1$, $f \leftarrow \mathrm{Funs}[\mathcal{K}, \mathcal{X}^{\leq \ell}]$

$\mathcal{B}$

$\mathcal{A}$

$\xleftarrow[s \leq Q]{m_1, \cdots, m_s}$

$\leftarrow \begin{pmatrix} a_{11}, a_{12}, \cdots a_{1v} \\ \vdots \\ a_{s1}, a_{s2} \cdots a_{sv} \end{pmatrix}$ $\rightarrow (Q \cdot \ell)$ queries

$\longrightarrow$

$$t_i = \bigoplus_{m=1}^{s} a_{im} \quad (i = 1, 2, \cdots, s)$$

$\longleftarrow$

$$\hat{b} = \begin{cases} 1, & \text{if for some } i \neq j, t_i = t_j \\ 0, & \text{otherwise.} \end{cases}$$

\# Game 0: $f \leftarrow F(k, \cdot)$ $\quad \Pr[W_0] = \mathrm{UHFadv}[\mathcal{A}, F^{\oplus}]$

\# Game 1: $f \leftarrow \mathrm{Funs}[\mathcal{K}, \mathcal{X}^{\leq \ell}]$ $\quad |\Pr[W_1] - \Pr[W_0]| \leq \mathrm{PRFadv}[\mathcal{B}, F]$

$$\Pr[W_1] \leq \frac{Q(Q-1)}{2} \cdot \frac{1}{|\mathcal{Y}|}$$ (similar to proof of Theorem 7.4)

$$\rightarrow \mathrm{MUHFadv}[\mathcal{A}, F^{\oplus}] \leq \mathrm{PRFadv}[\mathcal{B}, F] + \frac{Q^2}{2|\mathcal{Y}|}$$