Problem 1: One wayness.

a. Let $f : X \rightarrow Y$ be an efficiently computable one-to-one function. Show that if $f$ has a hard core bit then $f$ is one-way.

b. Show that if $G : \{0,1\}^n \rightarrow \{0,1\}^{2n}$ is a secure PRG then $G$ is also one-way.

c. Show that if $F : K \times \{1, \ldots, n\} \rightarrow Y$ is a secure PRF then $G(s) := F(k,1)\|F(k,2)\|\cdots\|F(k,n)$ is a secure PRG.

Problem 2: Hybrid arguments. Let $G : S \rightarrow Y$ be a secure RNG. Show that $G^{(n)} : X^n \rightarrow Y^n$ defined by $G(s_1, \ldots, s_n) := (G(s_1), \ldots, G(s_n))$ is also a secure PRG.

Hint: consider $n+1$ hybrid distributions, where in distribution number $j$, for $j = 0, 1, \ldots, n$, the first $j$ components are pseudorandom and the remaining $n-j$ components are random. Observe that the two distributions $j = 0$ and $j = n$ are the ones used to define security of the PRG $G^{(n)}$.

Problem 3: Recall that the NOVY commitment scheme is perfectly hiding, but requires $n$ rounds of interaction when using a OWP $f$ on $\{0,1\}^n$. Construct an NOVY-like perfectly hiding commitment scheme that takes only $n/\log_2 n$ rounds of interaction.

Hint: Try compressing $\log_2 n$ rounds of NOVY into one. Prove that an adversary who can break binding of your scheme can invert the OWP.

Problem 4: Let $A$ be a $n \times m$ matrix in $\mathbb{Z}_2$. Define the hash function $h_A(x) := A \cdot x$ from $\mathbb{Z}_2^m$ to $\mathbb{Z}_2^n$. Now consider the set $\mathcal{H}$ of hash functions $h_A$ for all $n \times m$ matrices $A$ over $\mathbb{Z}_2$. Show that $\mathcal{H}$ is an $\epsilon$-UHF for $\epsilon = 1/2^n$.

Problem 5: Let $F$ be a PRF defined over $(K, X, X)$. Recall that the ECBC is defined as:

$$ECBC((k_1, k_2), x) := F(k_2, F_{CBC}(k_1, x))$$

and suppose we use ECBC as a MAC for fixed length messages, say messages in $X^n$ for some $n$. Show that after $O(\sqrt{|X|})$ chosen message queries an attacker can forge the MAC on some previously unqueried message, with constant probability.

Problem 6: Let $p$ be a prime and let $g \in \mathbb{Z}_p^*$ generate a subgroup of order $q$ for some $q \equiv 3 \mod 4$. Define $\text{lsb}_2(x) = 0$ if $x \mod 4$ is 0 or 1 and $\text{lsb}_2(x) = 1$ otherwise. Let $f : \{0, 1, \ldots, q-1\} \rightarrow \mathbb{Z}_p^*$ be the function $f(x) = g^x \mod p$. Show that if $\text{lsb}(x)$ is a hard core bit of $f$ then so is $\text{lsb}_2(x)$. 

1