1. **(Code-based PRG construction)** Let $\mathbb{F} = \mathbb{F}_2$. Consider the following instance of the OWF candidate $f_{\text{code}}$. The input consists of a $2k \times k$ generating matrix $C \in \mathbb{F}^{2k \times k}$, a message vector $x \in \mathbb{F}^k$, and a binary vector $\chi$ of length $\lfloor k/4 \rfloor$ representing a noise vector $e \in \mathbb{F}^{2k}$ of Hamming weight $\lfloor k/20 \rfloor$. The output is $(C, C x + e(\chi))$, where $e$ is a (deterministic) polynomial-time computable function mapping a random $\chi$ to a nearly uniform noise vector of weight $\lfloor k/20 \rfloor$.

   (a) On which input lengths $n_k$ is $f_{\text{code}}$ defined? Does it expand inputs of length $n_k$?

   (b) Suppose there is an efficient $A$ that, on inputs of length $n_k$, distinguishes between the output of $f_{\text{code}}$ on a random input and a random string of the same length with advantage $\varepsilon(n_k)$. Prove that there is an efficient $A'$ that given $f_{\text{code}}(C, x, \chi)$ and $r$ predicts $(x, r)$ with probability $1/2 + \varepsilon(n_k)/2$ (where the probability is over a uniform choice of $C, x, \chi, r$).

   Hint: Consider $A'$ that picks a random $s \in \mathbb{F}^{2k}$ and runs $A$ on an input of the form $(C', y)$ where $C' = C + s \cdot r^T$.

   (c) Prove that if $f_{\text{code}}$ is one-way on inputs of length $n_k$, then its output on these inputs is pseudo-random.

2. **(Extending the domain and range of PRFs)** Let $F : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}$ be a pseudorandom function with key length $s(n)$, where $s(n)$ is a polynomial. Recall that the first argument of $F(k, x)$ is a key and the second is the input.

   (a) Formally define a notion of a PRF with output length $m(n)$, and show how to use $F$ to construct such a PRF for every polynomial $m(n)$. Prove that your construction satisfies your definition.

   (b) Let $0 < \epsilon < 1$ be a constant. Suppose $H = (G_H, E_H)$ is a family of universal hash functions with output length $\ell(n) \geq n'$ and a uniformly random key of length $s'(n)$. Then $F'(k, k', x) = F(k, h_k(x))$ is a PRF with key length $s'(n) + s(\ell(n))$, where $k$ is a random key for $F$ and $k'$ is a random key for $H$.

   (c) Conclude that a PRF with key length $O(n)$ can be obtained by using a single invocation of $F$ (and no additional use of cryptography).

3. **(Constant-rate string commitment)** Recall that Naor’s bit-commitment scheme requires the sender to communicate $O(n)$ bits to the receiver. Consider the following efficient generalization, which supports commitment to an $n$-bit string with the same asymptotic communication:

   - Given $n$, the receiver $R$ sends to $S$ a random string $r \in \{0,1\}^{4n}$.
   - To commit to $m \in \{0,1\}^n$, the sender $S$ views $m$ as an element in the finite field $\mathbb{F} = GF(2^n)$, views $F$ as a subfield of $\mathbb{F}' = GF(2^{4n})$, picks a random seed $s \in \{0,1\}^n$ for a PRG $G : \{0,1\}^n \to \{0,1\}^{4n}$, and views $G(s)$ and $r$ as elements of $\mathbb{F}'$. The commitment sent to $R$ is $c = G(s) + mr$.

   (a) Formally define a notion of an interactive, statistically binding string commitment with message length $\ell(n)$.

   (b) Prove that the above protocol satisfies the definition for $\ell(n) = n$. 

1
4. **(Rate-1 public-key encryption)** Suppose there exist a PKE and a PRG. Prove the existence of a PKE with message length \( t(n) = n \) in which the ciphertext length is \( n + o(n) \).

5. **(From an exam)** Prove or disprove succinctly each of the following statements. If needed, you may assume that a one-way function exists or make any other (clearly stated) standard assumption among those mentioned in class.

   (a) If \( F : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n \) is a pseudorandom function with key length \( n \) and output length \( n \), then \( F'(x) = F(x,x) \) is a OWF.

   (b) If \( F : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n \) is a pseudorandom function with key length \( n \) and output length \( n \), then \( F'(x) = (F(x,0), F(x,1)) \) is a OWF, where the first argument of \( F \) is the key and the second is the input.

   (c) If \( \text{Gen, Enc, Dec} \) is a PKE for 1-bit messages, then the following algorithms \( \text{Com, Ver} \) define a bit-commitment scheme: \( \text{Com}(1^n, b) \) lets \( (pk, sk) \leftarrow \text{Gen}(1^n) \), \( c \leftarrow \text{Enc}(pk, b) \) and outputs \( \text{com, dec} \) where \( \text{com} = (pk,c) \) and \( \text{dec} = sk \); \( \text{Ver}(1^n, b, \text{com, dec}) \) accepts \( b \) if and only if \( \text{Dec}(sk,c) = b \).

   (d) There exists a PKE \( \text{Gen, Enc, Dec} \) for 1-bit messages where \( \text{Enc} \) is deterministic.

   (e) If \( \text{Gen, Eval} \) is a collision-resistant hash function then so is \( \text{Gen, Eval'} \) where \( \text{Eval'} \) is defined by \( \text{Eval'}(k,x) = \text{Eval}(k, \text{Eval}(k,x)) \).