Problem Set 5
Due at the beginning of class on May 1
Please type your solutions, preferably using latex.

1. In class you saw a single database PIR scheme based on the hardness of deciding quadratic residuosity, with communication complexity $n^{1/2}$. Show how to extend this approach to obtain communication complexity $n^\epsilon$ for any constant $\epsilon > 0$. (Hint: use recursion.) No proof is needed; just describe the construction.

2. Recall the 8-database PIR scheme from class with communication complexity $\Theta(n^{1/3})$. Recall that the user’s index $I$ is mapped to $(a,b,c)$ with $a,b,c \in \{1, \ldots, n^{1/3}\}$. Let $(S_i, T_i, U_i)$ be the query sent to database $i$. Say index $I = (a,b,c)$ is in $(S,T,U)$ if the $a$th bit of $S$ is equal to 1; the $b$th bit of $T$ is equal to 1; and the $c$th bit of $U$ is equal to 1.

(a) If the user queries the databases for index $I$, what is the probability that $I$ is in $(S_i, T_i, U_i)$ for some value of $i$?

(b) Fix any $i \in \{1, \ldots, 8\}$. If the user queries the databases for index $I$, what is the probability that $I$ is in $(S_i, T_i, U_i)$?

(c) Fix any $i \in \{1, \ldots, 8\}$ and let $I \neq I'$. If the user queries the databases for index $I$, what is the probability that $I'$ is in $(S_i, T_i, U_i)$?

(d) In class the following algorithm was suggested for attacking the user’s security: say database $i$ knows that the user’s index is either $I_0 = (a_0, b_0, c_0)$ or $I_1 = (a_1, b_1, c_1)$, each with probability $1/2$. Then the database does the following: If $I_0$ is in $(S_i, T_i, U_i)$ guess “0”; otherwise output a random guess. Compute the probability that the database correctly guesses the user’s index.

3. Prove that the existence of a one-time signature scheme for 1-bit messages implies the existence of one-way functions.

4. In class we described encoded RSA where signing a message $m$ is done by computing

$$\sigma := (\text{enc}(m))^d \mod N,$$

for some appropriate encoding function enc. Show that encoded RSA is insecure when $\text{enc}(m) \neq 0||m||0^{\ell/10}$, where $\ell$ is the bit-length of the modulus $N$.

5. A strong one-time signature scheme satisfies the following (informally): given a signature $\sigma$ on a message $m$, it is infeasible to output $(m', \sigma') \neq (m, \sigma)$ for which $\sigma'$ is a valid signature on $m'$ (note that $m = m'$ is now allowed, as long as $\sigma' \neq \sigma$).

(a) Assuming the existence of one-way functions, show a one-way function $f$ for which Lamport’s scheme is not a strong one-time signature scheme.

(b) Construct a strong one-time signature scheme using any assumption we have seen in class. (Hint: Use a particular one-way function in Lamport’s scheme.)