Applied Cryptography: Homework 13

(Deadline: 10:00am, 2020/12/23)

Justify your answers with calculations, proofs, and programs.

1. (10 points)

   Implement the 2-server covering code PIR protocol in lecture 27.

2. (20 points)

   Use the idea of the 2-server covering code PIR to design and implement a 4-server covering code PIR protocol that has communication cost $\mathcal{O}(n^{1/4})$. (Hint: Represent the database as a 4-dimension cube.)

3. (10 points, question 13.4, page 524 of the textbook)

   The purpose of this question is to perform some computations using the *Paillier Cryptosystem*. Suppose $p = 1041857$ and $q = 716809$.

   (a) Suppose $x_1 = 726095811532, r_1 = 270134931749, x_2 = 450864083576$, and $r_2 = 378141346340$. Compute $y_1 = e_K(x_1, r_1)$ and $y_2 = e_K(x_2, r_2)$.

   (b) Let $y_3 = y_1 y_2 \bmod n^2$. Compute $x_3 = d_K(y_3)$ using the decryption algorithm for the *Paillier Cryptosystem*.

   (c) Verify that $x_3 \equiv x_1 + x_2 (\text{mod } n)$.

4. (20 points)

   Implement the single-server PIR protocol in lecture 28.