Name:

Read and take notes on Section 14.3 Oblivious Transfer.

Reading Questions

1. Reread the first two paragraphs in the sectionon oblivious transfer.

   (a) Describe, in your own words, the *simple version* of oblivious transfer.

   (b) Describe, in your own words, the *more complicated version* of oblivious transfer.

2. Reread the description of a mathematical implementation of the simple version of oblivious transfer. In this case, what is the secret? Why can't Bob simply guess the secret?

3. Reread the description of a mathematical implementation of the more complicated version of oblivious transfer. In this case, what are the secrets? Why can't Bob find both of them?

4. What struck you in this reading? What is still unclear? What remaining questions do you have?