Advanced Topics in Cryptography: Homework 1

Submit in class by May 7, 2013.

Note: If you cannot solve an item which is part of a question, you can still solve other items in this question assuming that the first holds.

Prove the correctness of all your answers.

1. Let OT^m denote 1-out-of-2 oblivious transfer of m bit inputs. Let RandOT^m denote the following primitive:
    1. The sender's input consists of two m-bit strings, x_0, x_1.
    2. The receiver has no input.
    3. At the end of the protocol the receiver learns (b,x_b), for a randomly chosen $b \in \{0,1\}$, and learns nothing about x_{1-b}. The sender learns nothing. (Note that b must be chosen at random, and neither nor the server should be able to choose the value of b).

    Show the following two reductions, for the semi-honest case.

    a. It is possible to construct RandOT^1 from OT^2.
    b. It is possible to construct OT^1 from RandOT^1.

2. In Lecture 3 we studied the 1-out-of-2 OT protocol of Bellare-Micali, and the 1-out-of-2 OT protocol secure against malicious adversaries (slide 12). Show how to change each of these protocols to a 2-out-3 OT protocol. Namely a protocol in which the sender has three inputs and the receiver can ask to retrieve any two of these inputs. Try to come up with the most efficient design for the protocol. Prove that your protocol is as secure as the original protocol.

3. Following is a description of a sigma protocol for proving knowledge of an RSA decryption. The public information is n, an RSA modulus, e an RSA exponent, and a value y in Z^*_n. The prover knows x such that $x^e=y$ mod n. The protocol is the following
    1. P chooses a random r in Z^*_n and sends $a=r^e$ mod n to V.
    2. V chooses a random bit b and sends it to P.
    3. P computes $c=rx^b$ mod n and sends it to V.
    4. V accepts iff $c^e=ac^b$.

    a. Prove that this protocol satisfies the completeness property of sigma protocols.
    b. Prove that this protocol satisfies the special soundness property of sigma protocols.

c. Prove that this protocol satisfies the special honest-verifier ZK property of sigma protocols.
d. What is the probability that a prover that does not know *x* can successfully finish the protocol. How can we reduce the success probability of such a prover by repeating the protocol?