COMP-647B Advanced Cryptography

Problem set #4

due ***Tuesday April 24, 2007***

13. "Matching Games" Bit Commitment.

First, I ask you to read Section 6 (Matching Games) from reference [BBBT04]. Let *m* be a value such that the *m*-Matching Game cannot be won classically.

Build a two-prover bit commitment scheme based on this *m*-Matching Game and prove it is secure classically while being insecure quantumly.

[BBT04]
http://crypto.cs.mcgill.ca/~crepeau/COMP647/2007/QUANTIC/BBT04.pdf

14. Cloning implies no one-way permutations

Assume you have a hypothetical cloning device D such that if you input the state ρ and a fixed ancilla you produce two copies of ρ. Show that if you have an efficient quantum circuit C to compute a permutation π and the circuit D then you can construct an efficient inverter for π.

15. Non-orthogonal states

Suppose Alice is limited to sending two types of non-orthogonal qubit states $|\phi_0\rangle$ and $|\phi_1\rangle$, and suppose that Bob can only make projective measurements on the received states, qubit by qubit.

Prove as formally as possible that Alice and Bob can achieve Bit Commitment in this context.

16. Common Reference String Zero-Knowledge

[DFS04] proved that in the Common Reference String (CRS) model it is possible to construct Quantum zero-knowledge proofs that require no rewinding in the simulation. In this problem we consider the analogous classical situation.

16.A Consider an interactive proof for graph-Hamiltonicity (remember Problem Set #1 Q.3) that works as follows: the prover sends to the verifier an encrypted adjacency matrix S of a graph containing only an n-vertex cycle. The prover wishing to prove an n-vertex graph G is Hamiltonian either unveils all the entries of S and thus demonstrate it contains only a cycle or discloses a permutation π mapping the Hamiltonian cycle of G to the encrypted Hamiltonian cycle in S and unveils all the non-edges in S according to the non-edges of G through the mapping. Prove this protocol is sound and complete for graph-Hamiltonicity.

16.B Prove that the above protocol may be made computational ZK under the assumption that one-way permutations exist.

16.C The prover can use the CRS as n^2 blocks of 2n bits each. Show how he can use each block of 2n bits as a bit commitment to a single bit (the prover is assumed infinitely powerful). Show how he can use this encrypted $n \times n$ matrix as an S described above, when it so happens that the matrix describes a single Hamiltonian cycle. (unfortunately, the probability that a random matrix is a valid S is very small and thus this observation requires an improvement to yield an efficient non-interactive proof.)

***16.D** Find a trick to reduce the probability that a single edge be randomly present to $1/n^3$ and conclude that the probability of a random encrypted $n^2 \times n^2$ matrix containing a valid S is reasonable. Complete the protocol to a non-interactive ZK proof.

[DFS04]
http://crypto.cs.mcgill.ca/~crepeau/COMP647/2007/QUANTIC/DFS04.pdf