

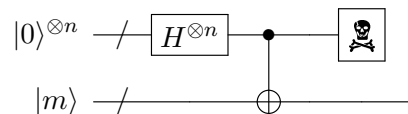
Exercise Sheet 5


Out: 2017-10-25

Due: 2017-11-01

Problem 1: Partial Trace

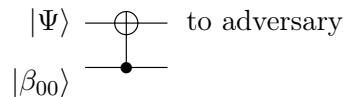
(a) Consider the following quantum circuit.



Here m is an n -bit string, the CNOT denotes bitwise CNOT (i.e., a CNOT between bit 1 of the first and the second n -qubit register, then a CNOT between bit 2 of the first and the second register, etc.). By  we mean that the corresponding register (and the information therein) is destroyed.

What is the density operator ρ of the state resulting from that circuit?

(b) Consider the following encryption circuit:



Here $|\Psi\rangle$ is a qubit (assumed to be either $|0\rangle$ or $|1\rangle$), and $|\beta_{00}\rangle$ is $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. That is, we CNOT the qubit $|\Psi\rangle$ with the first half of a Bell pair.

This is a slight variant of the one-time pad encryption. Here, we do not XOR the secret qubit $|\Psi\rangle$ with a classical bit, but with a quantum bit. (Imagine that Alice holds $|\Psi\rangle$ and the first qubit of $|\beta_{00}\rangle$, i.e., the first two wires. And Bob holds the third wire.) Then Alice sends the first wire to the adversary.

Compute the density operator describing the qubit that the adversary gets, both in the case $|\Psi\rangle = |0\rangle$ and the case $|\Psi\rangle = |1\rangle$.

Your result will show that this encryption scheme is secure for encrypting classical data. (With respect to some suitable notion of secrecy.)

Hint: First compute the quantum state of the three wires (i.e., a three-qubit state) after the CNOT. Then compute the corresponding density operator. Then use the partial trace to compute the density operator corresponding to the first wire only (i.e., after destroying the second and third wire).