Quantum Cryptography (spring 2023) Dominique Unruh

Exercise Sheet 04

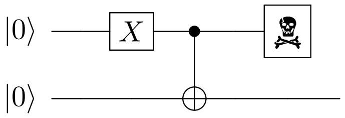
Out: 2023-03-06 Due: 2023-03-13

1 Partial trace

(a)

Knowlets:	ParTr, PauliX, CNOT ProblemID: PTraceXCNOT
Time:	
Difficulty:	

Consider the following quantum circuit.



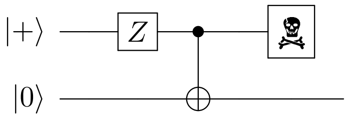
By —☠ we mean that the corresponding register (and the information therein) is destroyed. X is the X-gate (bit flip).

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

(b)

Knowlets:	ParTr, PauliZ, CNOT ProblemID: PTraceZCNOT
Time:	
Difficulty:	

Consider the following quantum circuit.



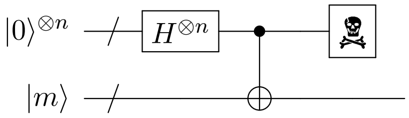
By —☠ we mean that the corresponding register (and the information therein) is destroyed. Z is the Z-gate (i.e., $Z|0\rangle = |0\rangle$, $Z|1\rangle = -|1\rangle$).

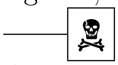
What is the density operator ρ of the state resulting from that circuit?

(c)

Knowlets:	ParTr, Hada, CNOT, ComposUni ProblemID: PTraceHnCNOT
Time:	
Difficulty:	

Consider the following quantum circuit.



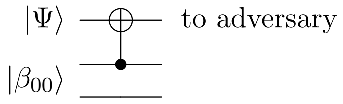
Here m is an n-bit string, the CNOT denotes bitwise CNOT (i.e., a CNOT between bit 1 of the first and the second n-qubit register, then a CNOT between bit 2 of the first and the second register, etc.). By  we mean that the corresponding register (and the information therein) is destroyed.

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

(d)

Knowlets:	ParTr, CNOT, QOTP ProblemID: PTraceQOTP
Time:	
Difficulty:	

`(Bonus problem)` 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).

2 Quantum one-time pad, with Pauli matrices

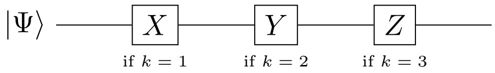
Knowlets:	QOTP, PauliX, PauliY, PauliZ ProblemID: QOTPPauli
Time:	
Difficulty:	

Consider the following variant of the quantum one-time pad:

The secret key is $k \in \{1, 2, 3, 4\}$. (Uniformly at random.)

Then, depending on k, we apply one of the four Pauli matrices X, Y, Z, I. (It is a matter of taste whether the identity I is called a Pauli-matrix.)

That is, we compute the following circuit:



Show that this variant of the quantum one-time pad is secure but computing the density operator of the final state for $|\Psi\rangle = \binom{\alpha}{\beta}$. The final state should not depend on α, β.

Note: Don't forget that there is also the case $k = 4$ in which case the circuit above applies no gate.