Quantum Cryptography (spring 2021)	Dominique Unruh

Exercise Sheet 05

Out: 2021-03-22 Due: 2021-03-30

1 Quantum one-time pad, with Pauli matrices

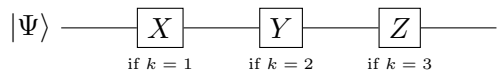
Knowlets:	QOTP, PauliX, PauliY, PauliZ ProblemID: QOTPPauli
Time:	
Difficulty:	

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.

Note: Note that α, β are complex numbers. In the lecture, we assumed for simplicity that they are real numbers, but you are not supposed to make that simplification. (At least not when full points are desired.)

2 Physical indistinguishability – the opposite direction (bonus problem)

Knowlets:	QDistr, Density, ProjMeas, DensityM ProblemID: PhysIndReverse
Time:	
Difficulty:	

Let E_1 and E_2 be quantum state probability distributions with density matrices ρ_1 and ρ_2. Assume that $\rho_1 \neq \rho_2$. Prove that E_1 and E_2 are physically distinguishable by specifying a measurement $M = \{Q_{\text{yes}}, Q_{\text{no}}\}$ with the following property: When measuring E_1 and E_2 with M, we get the outcome yes with different probabilities P_1 and P_2 (where $P_i := \Pr[\text{Outcome is yes when measuring } \rho_i]$).

Hint: Consider the matrix $\sigma := \rho_1 - \rho_2$. Show that σ is diagonalisable and that it therefore has an eigenvector $|\Psi\rangle$ with eigenvalue $\lambda \neq 0$. Set $Q_{\text{yes}} := |\Psi\rangle\langle\Psi|$. You may use without proof the fact that a density operator is always Hermitean and nonzero.