COM-440, Introduction to Quantum Cryptography, Fall 2025

Homework # 1 **due: 12:59PM, October 8th, 2019**

Ground rules:

Please format your solutions so that each problem begins on a new page, and so that your name appears at the top of each page.

You are encouraged to collaborate with your classmates on homework problems, but each person must write up the final solutions individually. You should note on your homework specifically which problems were a collaborative effort and with whom. You may not search online for solutions, but if you do use research papers or other sources in your solutions, you must cite them.

Late homework will not be accepted or graded. Extensions will not be granted, except on the recommendation of a dean. We will grade as many problems as possible, but sometimes one or two problems will not be graded. Your lowest homework grade of the semester will be dropped from your final grade.

Problems:

1. **An optimal attack**
   Let

$$N_1 = \frac{1}{\sqrt{12}}\begin{pmatrix}3 & 0\\ 0 & 1\\ 0 & 1\\ 1 & 0\end{pmatrix} \quad \text{and} \quad N_2 = \frac{1}{\sqrt{12}}\begin{pmatrix}0 & 1\\ 1 & 0\\ 1 & 0\\ 0 & 3\end{pmatrix}\ .$$

   (a) Show that (N_1, N_2) are valid Kraus operators in the definition of a quantum channel $\mathcal{N}(\rho) = N_1 \rho N_1^\dagger + N_2 \rho N_2^\dagger$ mapping one qubit to two qubits.

   (b) Show that using $\mathcal{N}$, a quantum adversary succeeds in the game for Wiesner's quantum money scheme with probability $\frac{3}{4}$.