COM-440 reading assignment #1

Due Thursday October 2nd at 23:59pm.

Wiesner

The paper on "conjugate coding" by Stephen Wiesner is usually credited as the paper where quantum information, communication, and cryptography were invented, all in one go! Even though the paper was published in 1983, it is said to have circulated since 1979. The goal of this reading is to connect physical intuition as described by Wiesner to the modern formalism of qubits, etc., used in class.

Wiesner's paper has two parts. You may skip the last part, on "Conjugate bases", starting at page 86. The following questions are meant to guide you in your reading. Provide a short answer to each of them. You may skip a question you don't like, as long as you replace it by a better question & answer. Feel free to include any additional thoughts, or observations, you may have: What do you think is the paper's main insight? The main point it got wrong? What would you have done differently?

Your complete answer should be at most 2 pages (with standard formatting).
For this assignment, ChatGPT or other AI tools are *strictly not allowed*.

Example one: message transmission

1. Wiesner presents his encoding scheme using physical language: photons, polarizations, etc. Give a description using modern language: given two messages m1 and m2, each consisting of n (classical) bits, how many qubits does the quantum state created by Wiesner's scheme contain, and what state are the qubits in? *[Hint: "photon polarized horizontally/vertically" = "|0>/|1>"; "photon polarized righ-hand/left-hand circular" = "|+>/|->".]*
2. What do you think about Wiesner's claim that "If the receiver is set up to sort the photons with respect to some elliptical polarizations intermediate between linear and circular, less information about each message is recovered than when the receiver makes the best measurement for the reception of one message alone". Is this correct? If so, can you prove it?
3. *[Optional:]* Explain, using the language from class, Wiesner's assertion that "In principle, there exist very complicated measurements that allow recovery of all the transmitted information."

Example two: quantum money

1. Wiesner's argument leading to his claim that "Thus, there is a 1/4 chance of each digit being found wrong and the probability of the whole counterfeit coin passing inspection is only (3/4) 20 < 0. 00317" has several issues. Can you find some?
2. What do you think of the last paragraph on p.85? If you were to make the claim rigorous, how would you proceed?