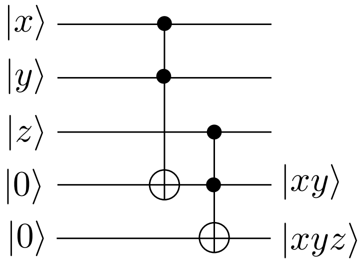
ANSWERS TO THE EXAM QUANTUM INFORMATION, 14 DECEMBER 2023

each item gives 2 points for a fully correct answer, grade = total $\times 9/24 + 1$

1. *a)* $ZX|\psi\rangle = 2^{-1/2}(|0\rangle - |1\rangle)$, $XZ|\psi\rangle = 2^{-1/2}(|1\rangle - |0\rangle)$, differs by a minus sign
   b) before the CNOT, $\rho_A = (1/2)(|0\rangle\langle 0| + |1\rangle\langle 1|)$, so a mixed state; after the CNOT, $\rho_A = (1/2)(|0\rangle + |1\rangle)(\langle 0|+\rangle 1|)$, so a pure state.
   c) The control qubit is only unchanged by the CNOT gate if it is in either the state $|0\rangle$ or the state $|1\rangle$; superpositions of these two states are changed.

2. *a)* After the Hadamard the two-qubit state is $|0\rangle(|0\rangle + |1\rangle) + |1\rangle(|0\rangle - |1\rangle)$, so after Alice's measurement the state of Bob's qubit is either $|0\rangle + |1\rangle$ or $|0\rangle - |1\rangle$ (omitting normalization constants).
   b) Both in cases 1 and 2 one has $\rho_A = (1/2)(|0\rangle\langle 0| + |1\rangle\langle 1|)$, the cross-terms in case 2 cancel.
   c) Since the state of Bob's qubit is different in cases 1 and 2, if he could measure it, he would know if Alice applied the Hadamard or not. To measure the state Bob would need to first make many copies of it, which is prevented by the no-cloning theorem.

3. *a)* $\langle\psi'|T|\psi\rangle = 0$ unless $\psi' = \psi$; because $\langle z|z \oplus xy\rangle = \langle z \oplus xy|z\rangle$ the operation T is Hermitian, $T = T^\dagger$; and since T^2 equals the identity it follows that $TT^\dagger = I$, so T is also unitary.
   b) the two-qubit operation $|x\rangle|y\rangle \mapsto |x \oplus y\rangle|xy\rangle$ is not invertible, $x, y = 0, 1$ and $1, 0$ give the same outcome, so it cannot be a unitary operation
   c)



4. *a)* Bob tells Alice the result of his coin tosses, one by one; Alice compares these results with her own coin tosses, and she tells Bob which results match; those measurements form the shared secret code. The measurement outcomes are discarded for those qubits for which the coin tosses of Alice and Bob do not match.
   b) Alice and Bob can disclose a part of their shared code and check if the bits are indeed the same. If the qubits were measured by an adversary before reaching Bob, there will be errors with high probability.
   c) If Eve a intercepts a qubit and measures it in a random basis there is a probability $1/2$ that this basis will be the same as the basis chosen by Alice, so that the measurement does not disturb the qubit. For n qubits the probability that all basis choices match is 2^{-n}, so $2^{-10} \approx 0.001$ for 10 qubits.