UNIVERSITY OF
CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Wednesday 2 June, 2004 9 to 11

PAPER 54

QUANTUM INFORMATION SCIENCE

Attempt no more than **three** *questions.*

There are **four** *questions in total.*

The questions carry equal weight.

You may not start to read the questions printed on the subsequent pages until instructed to do so by the Invigilator.

1 Show that any entangled pure state of two separated qubits violates a CHSH inequality for some set of measurements on the two qubits. [The measurements may depend on the state. You may quote the Schmidt decomposition theorem and any appropriate version of the CHSH inequality without proof.]

2 The Redundant Quantum Bank uses a primitive form of quantum authentication for its banknotes, which each contain just a single qubit known to be in one of two possible states. A forger has obtained $M \geqslant 1$ identical RQB banknotes, each of which he knows contains the same stored quantum state. He knows also that the quantum state takes one of two possible values $|\psi_0\rangle$ or $|\psi_1\rangle$, but does not know which. These states obey $0 < |\langle\psi_0|\psi_1\rangle| < 1$.

The forger attempts to create $N > M$ identical banknotes containing the same state as the original M (which may be destroyed in the process). The bank tests authenticity by measuring the projection onto the relevant qubit. Show that there is a positive number p_0 such that, whatever his strategy, the probability of at least one of the N banknotes failing the bank's authenticity test is greater than p_0.

3 Let H be a class of functions mapping a set A to a set B, where $|A| > |B|$. Explain what is meant by saying that the class H is (i) universal$_2$, (ii) strongly universal$_2$, (iii) almost strongly universal$_2$.

Describe a protocol which uses an appropriate class of almost strongly universal$_2$ hash functions, together with a shared secret sequence of random binary digits, to authenticate a message between two separated parties, using significantly fewer shared secret bits than the message length. Explain briefly why it is secure. [There is no need for a formal security proof. You should specify a suitable class of hash functions, but may quote without proof a result establishing that the specified class is almost strongly universal$_2$.]

4 Alice and Bob agree on the following bit commitment protocol. Alice will send Bob a sequence of N qubits, where N is large. If she wishes to commit to the bit value zero, she chooses the qubits randomly and independently from among the states $\{|0\rangle, \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |1\rangle\}$ with respective probabilities $\{\frac{1}{2}, \frac{1}{4}, \frac{1}{4}\}$. If she wishes to commit to the bit value one, she chooses the qubits randomly and independently from among the states $\{\sqrt{\frac{25}{26}}(|0\rangle + \frac{1}{5}|1\rangle), |1\rangle\}$ with respective probabilities $\{\frac{13}{20}, \frac{7}{20}\}$.

To unveil her bit value, she sends Bob a classical list describing the sequence of qubits previously sent. Is this protocol secure against Alice, in the sense that it genuinely forces her to commit to one bit value or the other and to unveil the bit value she originally committed? Is it secure against Bob, in the sense that he can obtain no information about the committed bit if Alice follows the protocol honestly? Justify your answers in each case, by giving either a security proof or an explicit cheating attack.