Promising the Impossible: Classical Certification in a Quantum World

Adrian Kent

Centre for Quantum Computation, Department of Applied Mathematics and Theoretical Physics, University of Cambridge, Wilberforce Road, Cambridge CB3 0WA, U.K.

(Dated: September 2004 (revised March 2005))

I give a simple proof that it is impossible to guarantee the classicality of inputs into any mistrustful quantum cryptographic protocol. The argument illuminates the impossibility of unconditionally secure quantum implementations of essentially classical tasks such as bit commitment with a certified classical committed bit, classical oblivious transfer, and secure classical multi-party computations of secret classical data. It applies to both non-relativistic and relativistic protocols.

INTRODUCTION

Wiesner's pioneering work in quantum cryptography [1], and the ensuing discoveries by Bennett and Brassard of secure quantum key distribution [2] and by Ekert of entanglement-based quantum key distribution [3], have created much interest in the possibility of secure quantum implementations of other cryptographic tasks. In particular, there has recently been a great deal of interest in exploring quantum implementations of cryptographic tasks involving mistrustful parties. This interest has been heightened by the growing realisation that, by combining quantum protocols with relativistic signalling constraints [5, 6], quite a wide variety of tasks in mistrustful cryptography can be implemented with unconditional security.

Mistrustful classical cryptography has for some time been relatively well understood. The relations between various important classical cryptographic primitives — for example, coin tossing, bit commitment, the various equivalent versions of oblivious transfer and secure multi-party computation — have mostly been established, along with some results on the composability of these primitives.

There was initially some optimism that mistrustful quantum cryptography could be understood as a straightforward generalisation of mistrustful classical cryptography. On this view, the role of the quantum cryptologist would be to investigate the possibility of secure quantum protocols which implement precisely the known classical primitives, with precisely the same composability properties. However, as Rudolph [4] and others have argued, this ambition was, with hindsight, fundamentally misguided. It is often logically inconsistent to require an unconditionally secure quantum protocol to incorporate every salient feature of an ideal classical cryptographic model: quantum information is qualitatively different from classical information, and in particular the superposition principle and the unitarity of quantum evolution imply constraints which may be inconsistent with classically motivated definitions.

Perhaps partly because of this initial confusion, even rather basic questions about the scope of mistrustful quantum cryptography remain open. This paper resolves one of them: the question of whether classical certification can be guaranteed by physical principles. That is: can a protocol guarantee that its quantum inputs belong to a fixed basis (so that the inputting parties are effectively required to input classical information)?

One might desire classical certification to ensure that the quantum protocol precisely replicates a known classical task. For example, a protocol for secure quantum multi-party computation which allows general quantum inputs clearly is not implementing precisely the same task as a protocol for secure classical multi-party computation, in which the inputs are, by definition, classical data. However, if the protocol had classical certification, the analogy would be precise.

We show here that classical certification cannot be guaranteed by quantum protocols for mistrustful cryptographic tasks. Our argument applies both to non-relativistic protocols and to protocols using relativistic signalling constraints. It is much simpler than (and supersedes) an earlier argument applying to the particular case of bit commitment [7].

CLASSICAL CERTIFICATION IS IMPOSSIBLE

We take a quantum protocol to define computable algorithms for all the participating parties, with fixed probability distributions for any random choices required. The protocol may use relativistic signalling constraints to guarantee security, requiring some or all of the parties to provide inputs from various sites within stipulated time intervals, as exemplified by the protocols of Refs. [5, 6]. The stage at which the protocol terminates may be pre-determined or may be determined by some or all of the parties’ inputs. Either way, we assume it terminates after a finite (though not necessarily pre-determined) number of inputs. The protocol may include security tests, by which some or all
of the parties can carry out prescribed measurements which check whether other parties are honestly following the protocol.

In summary, we assume that each party can pre-program a set of quantum computers (one for each separated site) to implement the protocol, using correlated states (e.g. $|0\rangle|0\rangle \ldots |0\rangle$) distributed as necessary to represent any input data or random choices that need to be replicated, either at the same site or at separated sites. As we have not stipulated a pre-determined bound on the number of inputs, and as we require that an honest party can always complete the protocol, we also assume that it is possible for the parties to program their quantum computers to make and distribute sufficient further copies of their correlated states, if and as required, during the protocol. Without loss of generality, we may take the security measurements to be projective measurements with two outcomes, 0 or 1, corresponding respectively to “fail” or “pass”, and we may suppose they are carried out after the protocol is complete. We require the protocol to be perfectly reliable: i.e. if all the parties have honestly followed the protocol, then all the security tests should always produce the outcome “pass”.

Suppose now that we have a protocol which guarantees classical certification. Consider a single classically certified bit input into a protocol by one of the parties. Without loss of generality we suppose the protocol allows either classical bit value as input (otherwise the input is trivial). If they choose to input the state $|0\rangle$, representing the classical bit 0, they prepare $|0\rangle|0\rangle \ldots |0\rangle$ input the various qubits appropriately into their quantum computers. Similarly, to input $|1\rangle$, representing the classical bit 1, they prepare $|1\rangle|1\rangle \ldots |1\rangle$ and input the various qubits appropriately.

Now suppose that they choose instead to prepare the state $a|0\rangle|0\rangle \ldots |0\rangle + b|1\rangle|1\rangle \ldots |1\rangle$. By assumption, the probability of any security measurement $P$ producing outcome “fail” is zero in the first two cases. Hence, by linearity, the probability of “fail” is zero in the third case. This contradicts the assumption that the protocol guaranteed classical certification of the bit, and shows, as claimed, that classical certification is impossible.

This argument generalises: if a party is allowed to input a length $N$ bit string with any classical bit values, they cannot be prevented from inputting a general entangled superposition of $N$ qubits. Similarly, if there are $M < 2^N$ allowed bit string values, they cannot be prevented from inputting a general superposition of the corresponding $M$ quantum states.

**WHY CLASSICAL CERTIFICATION CANNOT BE ENFORCED BY MEASUREMENT**

One might perhaps be tempted to think that (without contradicting the above proof) a property operationally equivalent to classical certification can be effectively guaranteed, since even if one party inputs a superposition of bits into a protocol, any other party can collapse the superposition by carrying out a measurement on the input in the computational basis.

This is incorrect. In general, the parties input bits into their own quantum computers, which process the quantum data, along with data received earlier in the protocol, before sending appropriate subsets to another party or parties. Consider a single input qubit, and two possible orthogonal input states, $|0\rangle$ and $|1\rangle$. Although the corresponding output states must be orthogonal, those parts of the states sent on to another party, $\rho_0$ and $\rho_1$, need not necessarily be (and even if they are, the receiving party need not necessarily be able to identify the measurement basis which distinguishes them).

For example, a bit commitment protocol in which Alice’s input commitment bits, $|0\rangle$ and $|1\rangle$, result in Bob receiving orthogonal outputs, $|\psi_0\rangle$ and $|\psi_1\rangle$, whose values are known to him, would obviously be trivially insecure. More generally, consider any protocol which includes qubits which Alice inputs and which are then sent straight to Bob, in such a way that he can, without penalty, measure them in the computational basis. While Bob can certainly effectively guarantee the classicality of these bits (even if Alice inputs a superposition, his measurement will collapse it), the corollary is that Bob can also learn the bit values: Alice might as well have generated a classical bit string and sent it unencrypted to Bob. In other words, the technique works only in those cases where cryptography plays no rôle in any case.

**DISCUSSION**

We have given a simple general argument against the possibility of physically guaranteed certificates of classicality for mistrustful cryptographic protocols.

This argument addresses a point which seems to have caused some some confusion. If we were to require that mistrustful quantum protocols should follow ideal classical definitions precisely, as has sometimes been suggested in the literature, then in particular we would have to require mistrustful quantum protocols to guarantee classical
certification of their inputs. But, as the argument shows, this would rather trivialise many of the most interesting questions in mistrustful quantum cryptology. For example, if we were to require – as a matter of definition – that any quantum bit commitment protocol must guarantee classical certification of the committed bit, we would not need Mayers’ and Lo-Chau’s celebrated and elegant demonstrations of the impossibility of non-relativistic quantum bit commitment: the one-line proof given in this paper would suffice.

In summary, we have noted a type of security which, though no doubt sometimes desirable, cannot be unconditionally guaranteed by quantum cryptographic protocols. We hope that this will help to clarify the understanding of quantum security criteria and focus attention on those which are attainable.

Acknowledgments

I thank Roger Colbeck, Hoi-Kwong Lo, Jörn Müller-Quade and Dominique Unruh for helpful comments, and acknowledge partial support from the Cambridge-MIT Institute, the project PROSECCO (IST-2001-39227) of the IST-FET programme of the EC, and the Perimeter Institute.

Electronic address: a.p.a.kent@damtp.cam.ac.uk

[1] S. Wiesner, Conjugate coding, *SIGACT News* **15**(1) 78-88 (1983).
[2] C. H. Bennett and G. Brassard, Quantum cryptography: Public-key distribution and coin tossing, *Proceedings of the International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), pp. 175-179.
[3] A. Ekert, Quantum cryptography based on Bell’s theorem, *Phys. Rev. Lett.* **67** 661-663 (1991).
[4] T. Rudolph, The Laws of Physics and Cryptographic Security, quant-ph/0202143
[5] A. Kent, Unconditionally secure bit commitment, *Phys. Rev. Lett.* **83** 1447-1450 (1999).
[6] A. Kent, Secure classical bit commitment using fixed capacity communication channels, quant-ph/9906103, to appear in J. Cryptology.
[7] A. Kent, Unconditionally Secure Commitment of a Certified Classical Bit is Impossible, *Phys. Rev. A* **61**, 042301 (2000).
[8] H.-K. Lo, Insecurity of Quantum Secure Computations, *Phys. Rev. A* **56** (1997) 1154.
[9] H.-K. Lo and H. Chau, Is quantum bit commitment really possible?, *Phys. Rev. Lett.* **78** 3410-3413 (1997).
[10] D. Mayers, Unconditionally secure quantum bit commitment is impossible, *Phys. Rev. Lett.* **78** 3414-3417 (1997).