Knowledge Concealing Evidencing of Knowledge of a Quantum State

Emily Adlam
Centre for Quantum Information and Foundations, DAMTP, Centre for Mathematical Sciences,
University of Cambridge, Wilberforce Road, Cambridge, CB3 0WA, U.K.

Adrian Kent
Centre for Quantum Information and Foundations, DAMTP, Centre for Mathematical Sciences,
University of Cambridge, Wilberforce Road, Cambridge, CB3 0WA, U.K. and
Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, ON N2L 2Y5, Canada.

(Dated: May 1, 2017)

(This submission is intended to be a self-contained abstract. Full details will be given in an arxiv paper of the same title, which we hope will be available by the time this abstract reaches referees.)

Zero-knowledge proving is a cryptographic primitive in which one agent proves a fact to another agent without giving away any information other than that the fact is true. It has a wide range of practical applications, particularly in electronic voting schemes [1] and digital signature schemes [2], and is also used for a variety of theoretical purposes, such as showing that a language is easy to prove [3]. Zero-knowledge proving of *knowledge*, where Alice is required to prove only that she knows some fact, without giving Bob any information about the fact itself, is a particularly useful version of this task which plays a key role in a number of identification protocols [4].

Horodecki et al. [5] explored the possibility of what they called a "zero knowledge convincing protocol on quantum bit". In their model, a verifier (henceforth called Bob) knows he has a single copy of a pure qubit, but has no other information about the state. A prover (henceforth called Alice) wishes to make a prediction that Bob can verify and that will hold with certainty only if she knows what the state is, without giving Bob any additional information about its identity. They showed that no non-relativistic protocol involving classical information exchanges and quantum Alice-to-Bob communications can implement this task securely [5]. They also discussed some protocols that implement very weak versions of the task, either giving Bob a great deal of information about the qubit, or giving him only weak evidence of Alice's knowledge, or both.

In this paper, we strengthen and generalize the no-go theorem of Horodecki et al to cover states of arbitrary dimension, relativistic protocols and protocols involving quantum Bob-to-Alice communications. We show in this general context that no protocol providing non-trivial evidence of Alice's knowledge about a pure quantum state of finite dimension can prevent Bob from acquiring some additional knowledge about the state. We also prove an additional no-go theorem, giving a precise quantitative characterisation of the tradeoff between Alice's ability to produce a successful proof when she does know that state of interest and Alice's ability to cheat successfully when she does not know the state, and showing how this result depends on the dimension of the state.

Having demonstrated that full proofs of knowledge of a finite-dimensional quantum state are not possible, we move to studying an approximation to this task which we refer to as *knowledge-concealing evidencing of knowledge about a quantum state* (KCEKQS). In a protocol for KCEKQS, Alice is required to give Bob evidence that she has some form of knowledge about the quantum state of a system which is in his possession whilst giving him incomplete information about the state. Ideally, a successfully completed protocol should give Bob as much evidence as possible without assuming Alice's honesty, but should also ensure as small a bound as possible on the information that Bob can obtain by honest or dishonest means. We give a formal definition of the security parameters for KCEKQS and then assess the performance of some simple protocols previously considered by Horodecki et al. [5] when applied to KCEKQS, showing that they are all relatively weak in knowledge-concealment or in evidencing knowledge.

We then propose a completely new type of protocol based on the use of relativistic quantum bit commitment. As opposed to the protocols proposed by Horodecki et al, which require that Alice gives Bob some quantum information and/or predicts the result of some measurement he makes on the system of interest, our protocol requires Bob to give Alice a collection of systems and subsequently requires Alice to identify the system of interest, using relativistic bit commitment to minimize the amount of information that Bob can gain from Alice's identification. We prove that for quantum states of large dimension, provided that Alice and Bob are able to perform and securely compose a set of relativistic bit commitment protocols, this protocol is both strongly knowledge-concealing and also provides reliable evidence of Alice's knowledge, achieving good values for the KCEKQS security parameters. Thus our protocol achieves a significant advance over previously existing protocols, and we anticipate that it could play a similar role in suitable future quantum cryptographic protocols as zero-knowledge proving plays in classical cryptography.

We also discuss a number of interesting nuances surrounding KCEKQS protocols, and knowledge of quantum states more generally, that are raised by our work. A key difference between classical zero knowledge proofs and the quantum case is that the no-cloning theorem prevents Bob from producing additional copies of the state which Alice claims to know. Alice therefore cannot provide more evidence by repeating a protocol that tests her knowledge. In contrast, classical zero-knowledge proofs usually depend on iterating protocols many times to make Alice's chances of cheating successfully arbitrarily small. We also underline the importance of distinguishing cases in which Alice has classical knowledge of or about Bob's quantum state (e.g. a classical data string describing it), from cases where she only has quantum knowledge (e.g. a box able to make only some fixed number of copies), and note that some apparently reasonable KCEKQS protocols fail to respect this distinction. Clearly, Alice can never *prove* that she knows a precise classical description of a single quantum state, even if she does not care about giving Bob information, since the classical information about the state that can be extracted by measurement is bounded, and Alice always has a chance which is bounded away from zero of guessing this information, even if she knows nothing about the state. For example, she can predict the outcome of a complete projective measurement on an unknown qubit with probability $\frac{1}{2}$. Alice will have an even higher chance of guessing the information if she has some *partial* information about the quantum state, and we provide quantitative bounds on how certain types of classical and quantum partial knowledge increase her chances of producing a successful proof in our proposed KCEKQS protocol.

[1] L. Fouard, M. Duclos, and P. Lafourcade, *Survey on electronic voting schemes*.

[2] K. Nguyen, F. Bao, Y. Mu, and V. Varadharajan, in *Information and Communication Security*, edited by V. Varadharajan and Y. Mu (Springer Berlin Heidelberg, 1999), vol. 1726 of *Lecture Notes in Computer Science*, pp. 103–118, ISBN 978-3-540-66682-0.

[3] L. Fortnow, in *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing* (ACM, New York, NY, USA, 1987), STOC '87, pp. 204–209, ISBN 0-89791-221-7, http://doi.acm.org/10.1145/28395.28418.

[4] U. Feige, A. Fiat, and A. Shamir, Journal of Cryptology **1**, 77 (1988), ISSN 0933-2790, http://dx.doi.org/10.1007/BF02351717.

[5] P. Horodecki, M. Horodecki, and R. Horodecki, eprint arXiv:quant-ph/0010048.