Simplified instantaneous non-local quantum computation with applications to position-based cryptography*

Salman Beigi and Robert König

Motivated by concerns that non-local measurements may violate causality, Vaidman [1] has shown that any non-local operation can be implemented using local operations and a single round of simultaneously passed classical communication only. His protocols are based on a highly non-trivial recursive use of teleportation. Here we give a simple proof of this fact, reducing the amount of entanglement required from a doubly exponential to an exponential amount. We also prove a linear lower bound on the amount of entanglement consumed for the implementation of a certain non-local measurement.

These results have implications for position-based cryptography: any scheme becomes insecure if the adversaries share an amount of entanglement scaling exponentially in the number of communicated qubits. Furthermore, certain schemes are secure under the assumption that the adversaries have at most a linear amount of entanglement and are required to communicate classically.

Introduction

Throughout its history, quantum mechanics has again and again seemed at odds with relativistic causality. One debate resulting from such concerns centers around the measurability of a non-local observable in a manner consistent with causality. In its most simple form, it arises from the observation that certain non-local POVMs cannot be simulated by local operations and a single round of classical communication. This seems to suggest that certain non-local observables cannot be measured at a fixed time t between spacelike separated regions and are hence unphysical.

Vaidman [1] has recently resolved this long-standing debate to a degree almost entirely satisfactory to a quantum information scientist: he showed that any measurement can be implemented with local operations and a single round of simultaneously passed communication, *if auxiliary entanglement is available*, see Fig. 1. The same is true for general non-local unitaries. Here we give a simple proof of this remarkable fact and make progress towards answering *how much entanglement is required*. The minimal amount of entanglement that allows to implement a given operation using a single round of classical communication is a natural measure of its 'entanglement content'. On a conceptual level, it can be seen as the counterpart of the entanglement of formation for a given state in the same way as the entangling capacity is a counterpart of the distillable entanglement.

Establishing bounds on the entanglement required for such an 'instantaneous' computation not only is of fundamental theoretical interest, but also has direct applications to position-based quantum cryptography. The goal of the latter is to use the position of an entity as its only credential. A fundamental cryptographic problem in this context is that of *position-verification*, where a prover tries to convince several verifiers that he is in a certain location. The no-cloning principle has motivated various proposals of quantum protocols [3–5] supposedly achieving this functionality. However, as recently shown in [6], the feasibility of instantaneous computation given entanglement directly implies that no such scheme can be unconditionally secure. Fortunately, however, it turns out that these previously known attacks require a large amount of entanglement (see below); this motivates the question of whether position-based cryptography is realizable under the assumption that the adversaries' entanglement is limited. Indeed, this is reminiscent to the story of bit commitment, where security can be established in spite of the Mayer-Lo-Chau impossibility proof [7, 8] if the adversary is assumed to have a limited [9] or noisy [10] quantum memory. A first step in this direction was made in [6, 11], where schemes were shown to be secure if the adversaries have no or only a constant amount of entanglement.

Main results

Consider a bipartite Hilbert space $\mathcal{H}_{AB}$ with n qubits on each side. For a unitary U_{AB} on $\mathcal{H}_{AB}$, let $q_\epsilon(U_{AB})$ be the amount of auxiliary entanglement required to implement U_{AB} using local operations and a single round of classical communication, see Fig. 2, with accuracy ϵ (in diamond distance on the set of CPTP maps). Clearly, product unitaries require no entanglement to implement, that is,

$$q_0(U_A \otimes U_B) = 0 \qquad \text{for all unitaries } U_A, U_B \ ,$$

while $q_\epsilon(U_{AB}) > 0$ for a generic bipartite unitary U_{AB}. It is easy to identify large classes of non-product unitaries for which $q_0(U_{AB}) < O(n)$ (see e.g., [12]). Our main result is the bound

$$q_\epsilon(U_{AB}) \leq 2^{8n+4}/\epsilon^2 \qquad \text{for every unitary } U_{AB} \ . \quad (1)$$

Indeed, given U_{AB}, we construct a protocol as on the rhs of Fig 2; the involved measurements make black-box

*A full technical version is available at [2]

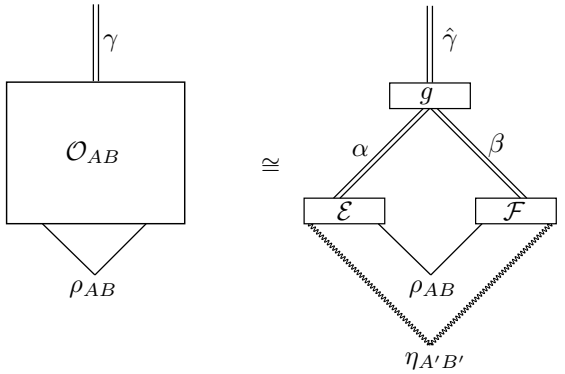

FIG. 1: Instantaneous measurement of a non-local POVM $\mathcal{O}_{AB} = \{O_{AB}^{\gamma}\}_{\gamma}$: Alice and Bob share, in addition to the state ρ_{AB} to be measured, an auxiliary entangled state $\eta_{A'B'}$ (indicated by the wiggly line). They perform local measurements $\mathcal{E} = \{E_{AA'}^{\alpha}\}_{\alpha}$ and $\mathcal{F} = \{F_{BB'}^{\beta}\}_{\beta}$, respectively. They send their results to Charlie, who is at a point in the intersection of their future lightcones. Charlie computes a function $\hat{\gamma} = g(\alpha, \beta)$ of their measurement results. The measurements and the post-processing function are chosen in such a way that this simulates the measurement of ρ_{AB} with the non-local POVM $\mathcal{O}_{AB}$.

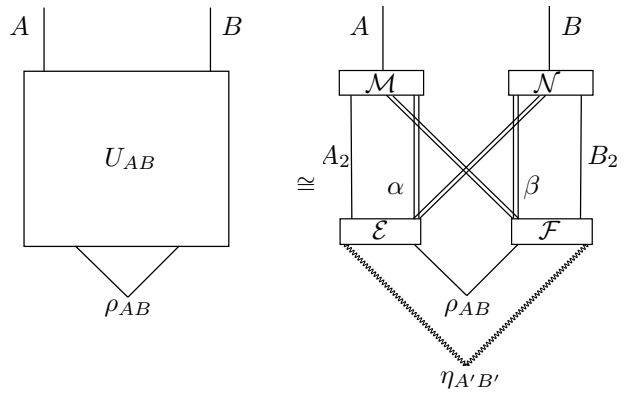

FIG. 2: Instantaneous implementation of a non-local unitary U_{AB} on a bipartite state ρ_{AB} using the shared entangled state $\eta_{A'B'}$. Alice and Bob perform local (partial) measurements $\mathcal{E} = \{E_{AA'}^{\alpha}\}_{\alpha}$ and $\mathcal{F} = \{F_{BB'}^{\beta}\}_{\beta}$. According to the (communicated) measurement results (α, β), Alice and Bob apply local post-processing operations $\mathcal{M}^{\alpha,\beta}$ and $\mathcal{N}^{\alpha,\beta}$, respectively. The measurements and postprocessing operations are chosen such that the resulting (average) state is close to the target state $U_{AB}\rho_{AB}U_{AB}^{\dagger}$.

use of U_{AB} roughly $2^{O(n)}/\epsilon^2$ times. This scaling in the number of qubits matches the complexity of doing tomography on such a general unitary, suggesting that our protocol may be optimal among those relying on a black-box use of the unitary. A similar statement holds for POVMs, and our results directly generalize to the multipartite case.

In contrast, a careful analysis (see [2]) shows that Vaidman's protocol, the only previously known general result of this kind, gives a bound of the form $q_{\epsilon}(U_{AB}) \leq 2^{O(\log(1/\epsilon)\cdot 2^{4n})}$ for a generic unitary U_{AB}. This unfavorable scaling arises from a recursive use of standard teleportation (Bell) measurements. Roughly speaking, Vaidman manages to avoid the need for communicating measurement results (i.e., necessary correction operations) to perform teleportation. Instead, his protocols use a set of teleportation measurements on ebits organized in a tree-like form, with each vertex indexed by a sequence of measurement results. As a consequence, these measurements effectively achieve postselection onto the trivial measurement outcome (which requires no correction operation), at the cost of consuming a doubly exponential amount of entanglement.

We also show that there is a POVM $\mathcal{O}_{AB}$ which cannot be implemented with less than a linear amount of entanglement, i.e.,

$$q_{\epsilon}(\mathcal{O}_{AB}) \geq \Omega(n) \qquad \text{for any } \epsilon > 0\ . \tag{2}$$

While statements (1) and (2) advance the characterization of entanglement requirements in instantaneous non-local operations, many challenging open problems remain. For example, we have been unable to establish a similar lower bound for unitaries, or prove some kind of optimality for our protocol.

Applied to position-based cryptography, (1) directly implies that an exponential amount of entanglement (in the number of communicated qubits) is sufficient to render any such scheme insecure. On the other hand, (2) gives rise to a scheme for position-verification with exponential soundness (i.e., exponentially small cheating probability) if we assume that the adversaries have fewer than $n/2$ bits of entanglement (e.g. $n/3$ ebits) and can only communicate classically during the attack. Note that the latter assumption is implicit in the sequential protocol of [6], which achieves exponential soundness only if the adversaries have no entanglement. Lifting the restriction to classical communication is yet another challenging problem which so far has only been achieved for a single-qubit protocol with constant soundness [6].

Since the position-based cryptographic scheme derived from (2) requires the manipulation of high-dimensional states by the verifiers, we analyze a different protocol based on single-qubit operations only and argue that it has identical security parameters. This is achieved by reducing the problem of designing protocols allowing entanglement to the case of no prior entanglement (the latter was previously analyzed in [6]).

Techniques

Our proof of (1) is based on 'port-based teleportation', a neat variant of teleportation by Ishizaka and Hiroshima [13, 14]. We believe that this primitive may

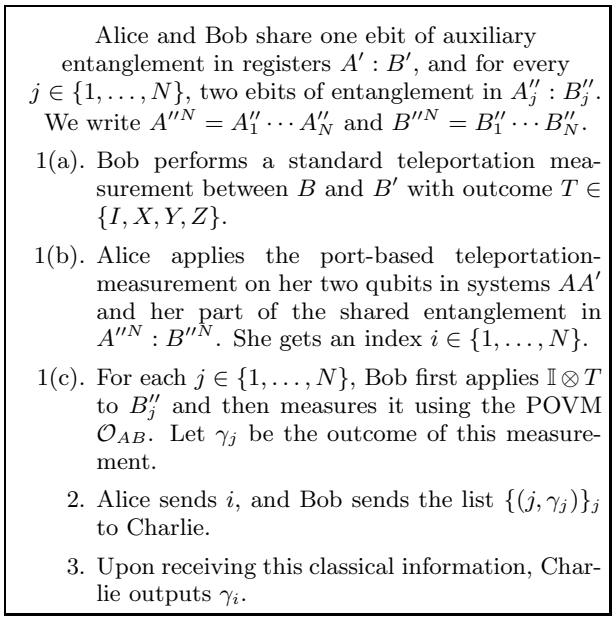

FIG. 3: Instantaneous implementation of a two-qubit POVM $\mathcal{O}_{AB} = \{O^{\gamma}_{AB}\}_{\gamma}$ on a state ρ_{AB}. Here $N = O(1/\epsilon^2)$, where ϵ is the accuracy of the simulation. Steps 1(a)–1(c) do not need to be performed in the prescribed order.

have useful applications in other areas of (theoretical) quantum information, and are excited to be able to promote its use by giving other concrete applications. Port-based teleportation is based on the idea that the complexity of teleportation measurements and correction operations can be traded off (instead of the standard Bell-measurement/Pauli correction). Ishizaka and Hiroshima show that there is a POVM $\{E_i\}_{i=1}^N$ on Alice's input qubit and half of $N := O(1/\epsilon^2)$ auxiliary shared ebits such that, given the measurement result i, Bob's i-th register contains Alice's input within its ϵ neighborhood in trace distance. Hence Bob's correction operation is trivial: it consists of tracing out all but the i-th subsystem. They also give a generalization to the teleportation of several qubits in this fashion.

Using port-based teleportation measurements, the instantaneous implementation of non-local POVMs become completely trivial; see Fig. 3 for the implementation of a two-qubit measurement. The case of a bipartite unitary is slightly involved, but still very simple: it involves an additional 'standard' teleportation measurement and correction operation. Observe that our measurements are constructed in a non-recursive fashion and are thus significantly simpler than Vaidman's approach. Details can be found in [2].

Conclusions

Vaidman's work is the culmination of a long line of research [15–20] focused on the feasibility of instantaneous measurement, a central requirement for the compatibility of quantum mechanics with relativistic causality. His solution to this fundamental problem is arguably one of the most intricate known protocols in quantum information processing. Here we have given a significantly simpler solution which also has a dramatic quantitative benefit: it reduces the entanglement consumption by an exponential amount. This is based on a little-known yet powerful form of teleportation introduced by Ishizaka and Hiroshima. We have also established a linear lower bound on the required entanglement for the instantaneous implementation of a certain non-local measurement. The recently discovered connection between instantaneous computation and position-based cryptography provides a practical motivation for such quantitative questions: indeed, our results directly give new cryptographic security proofs and impossibility results.

Further progress on quantifying the resource requirements for instantaneous computation is desirable both from a fundamental as well as a cryptographic perspective. Better bounds (or equivalently, tighter security proofs) appear to require strong entanglement monogamy relations, and many standard techniques such as resource inequalities are inapplicable in this setting because of the communication constraints. In this sense, the century-old problem of instantaneous measurements brings the limitations of our current quantum-information techniques into the limelight.

[1] L. Vaidman, Phys. Rev. Lett. **90**, 010402 (2003).
[2] S. Beigi and R. König (2011), arXiv:1101.1065.
[3] A. Kent, B. Munro, and T. Spiller, Phys. Rev. A **84**, 012326 (2011).
[4] A. Kent, *Quantum tagging with cryptographically secure tags* (2010), arXiv:1008.5380v2.
[5] R. A. Malaney, Phys. Rev. A **81**, 042319 (2010).
[6] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner, *Position-based quantum cryptography: Impossibility and constructions* (2010), arXiv:1009.2490.
[7] D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997).
[8] H.-K. Lo and H. F. Chau, Phys. Rev. Lett. **78**, 3410 (1997).
[9] I. Damgard, S. Fehr, L. Salvail, and C. Schaffner, in *FOCS* (2005), pp. 449 – 458.
[10] S. Wehner, C. Schaffner, and B. M. Terhal, Phys. Rev. Lett. **100**, 220502 (2008).
[11] H. K. Lau and H. K. Lo, Phys. Rev. A **83**, 012322 (2011).
[12] S. R. Clark, A. J. Connor, D. Jaksch, and S. Popescu, New Journal of Physics **12** (2010).
[13] S. Ishizaka and T. Hiroshima, Phys. Rev. Lett. **101**, 240501 (2008).
[14] S. Ishizaka and T. Hiroshima, Phys. Rev. A **79**, 042306

(2009).
[15] L. Landau and R. Peierls, Z. Phys. A **69**, 56 (1931).
[16] N. Bohr and L. Rosenfeld, Mat.-fys. Medd. Dansk Vid. Selsk. **12** (1933).
[17] Y. Aharonov and D. Z. Albert, Phys. Rev. D **21**, 3316 (1980).
[18] Y. Aharonov and D. Z. Albert, Phys. Rev. D **29**, 228 (1984).
[19] Y. Aharonov, D. Z. Albert, and L. Vaidman, Phys. Rev. D **34**, 1805 (1986).
[20] S. Popescu and L. Vaidman, Phys. Rev. A **49**, 4331 (1994).