Popescu-Rohrlich correlations imply efficient instantaneous nonlocal quantum computation

(extended abstract of arXiv:1512.04930 for QCRYPT 2016)

Anne Broadbent

Department of Mathematics and Statistics, University of Ottawa

1 Introduction

Outline. In instantaneous nonlocal quantum computation, two parties cooperate in order to perform a quantum computation on their joint inputs, while being restricted to a *single* round of simultaneous communication. Previous results showed that instantaneous nonlocal quantum computation is possible, at the cost of an exponential amount of prior shared entanglement (in the size of the input). Here, we show that a *linear* amount of entanglement suffices, (in the size of the computation), as long as the parties share nonlocal correlations as given by the *Popescu-Rohlich* box. This means that communication is not required for efficient instantaneous nonlocal quantum computation. Exploiting the well-known relation to position-based cryptography, our result also implies the impossibility of secure position-based cryptography against adversaries with non-signalling correlations. Furthermore, our construction establishes a quantum analogue of the classical communication complexity collapse under non-signalling correlations.

Motivation. In two-party quantum computation, Alice and Bob wish to evaluate a quantum circuit C on their joint inputs. Here, we consider that Alice and Bob are *co-operating* players that are restricted only in the way they communicate: they can agree ahead of time on a joint strategy (and possibly establish shared correlations or entanglement), but they are separated before receiving their quantum inputs, and are allowed only a *single* round of simultaneous communication (thus: Alice sending a message to Bob, and Bob sending a message to Alice, *simultaneously*). The requirement is that at the end of this round, Alice and Bob must share the output system $\rho_{\text{out}}^{AB} = C(\rho_{\text{in}}^{AB})$. This problem is known as *instantaneous nonlocal quantum computation*. Remarkably, this task is known to be achievable for any circuit as long as the parties share an exponential (in the size of the inputs) amount of an entangled resource given as copies of the two-qubit maximally entangled state, $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ [4, 10].

The motivation for the study of instantaneous nonlocal quantum computation includes the foundations of quantum physics and distributed computing; however, the original and main motivation is in the context of *position-based*

cryptography. Here, parties use their geographic location as a cryptographic credential. Protocols typically exploit the relativistic no-signalling principle: the idea being that a careful timing argument would then ascertain the location of the parties [6]. Unfortunately, a no-go result is known in the the classical context [14]. Due to the quantum no-cloning principle, it was originally believed that quantum protocols could escape this impossibility result [13, 19–22]. However, these protocols are all broken by entanglement-based attacks, as long as the colluding adversaries share a large enough (exponentially large) entangled state [4, 10] This exponential overhead in resources (in terms of entanglement and quantum memory) leads to the main open problem in this area, which is to give a protocol which can be executed efficiently by honest players, but for which any successful attack requires an exponential amount of resources (see related work [12, 28, 29]).

Popescu-Rohlich Boxes. In an apparently unrelated line of research, Popescu and Rohlich [26] defined the nonlocal box (*NLB*) as a virtual device that achieves the CHSH conditions [16] perfectly: when Alice (Bob) uses input x (y), the NLB produces output a (b) such that $a \oplus b = x \cdot y$. We note that quantum mechanics achieves this correlations with a maximum value of $\approx 85\%$ [15], but that the NLB is consistent with relativity since it does not enable communication. This device, as well as more general *non-signalling* correlations have been studied extensively, mostly in terms of understanding the power and limitations of *non-signalling* theories [3, 7–9], as well as more generally in terms of *information causality* [1, 11, 25] and *local orthogonality* [18, 27]; see also [23, 24]. One striking consequence of the NLB is that it implies the *collapse* of classical communication complexity [30], meaning that, any Boolean function can be computed in a two-party distributed context with *a single bit of communication*, as long as the parties have access to the NLB correlations[1]. This is presented as evidence against physical theories that allows the strong correlations of the NLB.

2 Summary of Contributions and Techniques

Here, we make progress towards the question of secure position-based quantum cryptography by showing an efficient attack to *any* scheme, where the participants are allowed the additional NLB resource. Our technique consists in showing that instantaneous nonlocal quantum computation is possible with a *linear* amount of pre-shared entanglement (in the size of the circuit), together with a linear amount of uses of the NLB. Furthermore, if we restrict the output to being a single qubit (say, held by Alice), the classical communication reduces to only two bits sent from Bob to Alice (in the case of quantum output), or a single bit (in the case of classical output). In both cases, this is optimal [5]. Thus our construction establishes a quantum analogue of the classical communication complexity collapse [30] under no-signalling correlations.

[1] This result was also shown by Richard Cleve (unpublished).

In order to establish this result, we make the key observation that the Pauli-X and Z corrections used in teleportation correspond precisely to the process of quantum one-time pad encryption [2]. Thus, we view the two-party computation as being evaluated on encrypted quantum data, where the classical keys are available via the teleportation corrections. More precisely, for each wire i in the computation, Alice keeps track of encryption keys $x_i^A \in \{0,1\}$ and $z_i^A\{0,1\}$ (Bob does likewise with values $x_i^B \in \{0,1\}$ and $z_i^B\{0,1\}$). At any point in the computation, the keys are *distributed*: applying the operation $\mathsf{X}^{x_i^A \oplus x_i^B}\mathsf{Z}^{z_i^A \oplus z_i^B}$ at each wire i results in the quantum state at that point in the (unencrypted) computation. Crucially, aided by the NLB correlations, the parties can evaluate the circuit on encrypted data *without any communication*: the decryption being delayed until the end of the protocol, when the parties exchange the classical keys and thus can locally decrypt (reconstruct) their outputs. We note that, inspired by a 2011 preliminary report on this work, Speelman [28] used a similar framework to achieve instantaneous nonlocal quantum computation for circuits of low T-depth; furthermore, recently, these techniques have led to the breakthrough result of *quantum fully homomorphic encryption* [17].

3 Conclusions

Our result establishes a no-go result for position-based quantum cryptography against efficient adversaries with non-signalling correlations. This implies that, if position-based quantum cryptography is indeed possible against efficient quantum adversaries, it will be thanks in part to bounds such as Tsirelson's [15], according to which quantum mechanics is not maximally non-signalling. One open question that remains is to characterize more broadly the set of physical theories that rule out position-based cryptography, for instance, in terms of non-signalling correlations that are not known to be distillable to the NLB, or other related theories.

References

1. J. Allcock, N. Brunner, M. Pawlowski, and V. Scarani. Recovering part of the boundary between quantum and nonquantum correlations from information causality. *Phys. Rev. A*, 80:040103, 2009. DOI: 10.1103/PhysRevA.80.040103.
2. A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf. Private quantum channels. In *FOCS 2000*, pages 547–553, 2000. DOI: 10.1109/SFCS.2000.892142.
3. J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts. Nonlocal correlations as an information-theoretic resource. *Phys. Rev. A*, 71(2):022101, 2005. DOI: 10.1103/PhysRevA.71.022101.
4. S. Beigi and R. König. Simplified instantaneous non-local quantum computation with applications to position-based cryptography. *N. J. Phys.*, 13(9), 2011. DOI: 10.1088/1367-2630/13/9/093036.
5. C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70(13):1895, 1993. DOI: 10.1103/PhysRevLett.70.1895.

6. S. Brands and D. Chaum. Distance-bounding protocols. In *EUROCRYPT 1993*, pages 344–359, 1993. DOI: 10.1007/3-540-48285-7_30.
7. G. Brassard, H. Buhrman, N. Linden, A. A. Méthot, A. Tapp, and F. Unger. Limit on nonlocality in any world in which communication complexity is not trivial. *Phys. Rev. Lett.*, 96:250401, 2006. DOI: 10.1103/PhysRevLett.96.250401.
8. A. Broadbent and A. A. Méthot. On the power of non-local boxes. *Theor. Comput. Sci.*, 358(1):3–14, 2006. DOI: 10.1016/j.tcs.2005.08.035.
9. N. Brunner and P. Skrzypczyk. Nonlocality distillation and postquantum theories with trivial communication complexity. *Phys. Rev. Lett.*, 102:160403, 2009. DOI: 10.1103/PhysRevLett.102.160403.
10. H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner. Position-based quantum cryptography: Impossibility and Constructions. *SIAM J. Comp.*, 43(1):150–178, 2014. DOI: 10.1137/130913687.
11. D. Cavalcanti, A. Salles, and V. Scarani. Macroscopically local correlations can violate information causality. *Nat. Comm.*, 1:136, 2010. DOI: 10.1038/ncomms1138.
12. K. Chakraborty and A. Leverrier. Practical position-based quantum cryptography. *Phys. Rev. A*, 92:052304, 2015. DOI: 10.1103/PhysRevA.92.052304.
13. N. Chandran, S. Fehr, R. Gelles, V. Goyal, and R. Ostrovsky. Position-based quantum cryptography, 2010. arXiv: 1005.1750.
14. N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky. Position based cryptography. In *CRYPTO 2009*, pages 391–407, 2009. DOI: 10.1007/978-3-642-03356-8_23.
15. B. Cirel'son. Quantum generalizations of Bell's inequality. *Lett. Math. Phys.*, 4(2):93–100, 1980. DOI: 10.1007/BF00417500.
16. J. F. Clauser, M. A. Horne., A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23(15):880–884, 1969. DOI: 10.1103/PhysRevLett.23.880.
17. Y. Dulek, C. Schaffner, and F. Speelman. Quantum homomorphic encryption for polynomial-sized circuits, 2016. arXiv: 1603.09717.
18. T. Fritz, A. B. Sainz, R. Augusiak, J. B. Brask, R. Chaves, A. Leverrier, and A. Acín. Local orthogonality as a multipartite principle for quantum correlations. *Nat. Comm.*, 4, 2013. DOI: 10.1038/ncomms3263.
19. A. Kent, W. J. Munro, and T. P. Spiller. Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints. *Phys. Rev. A*, 84(1):012326, 2011. DOI: 10.1103/PhysRevA.84.012326.
20. H.-K. Lau and H.-K. Lo. Insecurity of position-based quantum-cryptography protocols against entanglement attacks. *Phys. Rev. A*, 83(1):012322, 2011. DOI: 10.1103/PhysRevA.83.012322.
21. R. A. Malaney. Location-dependent communications using quantum entanglement. *Phys. Rev. A*, 81(4):042319, 2010. DOI: 10.1103/PhysRevA.81.042319.
22. R. A. Malaney. Quantum location verification in noisy channels. In *Proceedings of the Global Communications Conference—GLOBECOM 2010*, pages 1–6. IEEE, 2010. DOI: 10.1109/GLOCOM.2010.5684009.
23. M. Navascués, Y. Guryanova, M. J. Hoban, and A. Acín. Almost quantum correlations. *Nat. Comm.*, 6, 2015. DOI: 10.1038/ncomms7288.
24. M. Navascués and H. Wunderlich. A glance beyond the quantum model. *Proc. Roy. Soc. A*, 2009. DOI: 10.1098/rspa.2009.0453.
25. M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski. Information causality as a physical principle. *Nat.*, 461(7267):1101–1104, 2009. DOI: 10.1038/nature08400.

26. S. Popescu and D. Rohrlich. Quantum nonlocality as an axiom. *Found. Phys.*, 24(3):379–385, 1994. DOI: 10.1007/BF02058098.
27. A. B. Sainz, T. Fritz, R. Augusiak, J. B. Brask, R. Chaves, A. Leverrier, and A. Acín. Exploring the local orthogonality principle. *Phys. Rev. A*, 89:032117, 2014. DOI: 10.1103/PhysRevA.89.032117.
28. F. Speelman. Instantaneous non-local computation of low T-depth quantum circuits, 2015. arXiv: 1511.02839.
29. D. Unruh. Quantum position verification in the random oracle model. In *EUROCRYPT 2014*, pages 1–18, 2014. DOI: 10.1007/978-3-662-44381-1_1.
30. W. van Dam. Implausible consequences of superstrong nonlocality. *Nat. Comp.*, 12(1):9–12, 2013. DOI: 10.1007/s11047-012-9353-6.