Reading group on Entanglement and Cryptography

Reading list

This is a brief survey of some papers on device independence and multiparty cryptography in the quantum setting, some of which (many of which!) we may end up discussing depending on interest. I also recommend a very recent extensive survey [BCP+13] that focuses on quantum nonlocality and its information theoretic (rather than foundational) aspects. Section IV discusses device independence and applications to randomness certification, key distribution and other cryptographic tasks. It is a great starting point and Sections I, II and IV are also very much worthwhile reading.

0.1 Device independence

The idea of device independence dates back to Mayers and Yao [MY98] (read the introduction to their paper, but not the technical arguments!). Some of the tasks that have been showed achievable in this setting include:

- Randomness expansion. A good, leisurely introduction can be found in Chapter 5 of Colbeck's thesis [Col06]. (A more detailed technical argument expanding on that Chapter appeared in [CK11].) The first quantitative bounds (and experimental implementation!) were reported in [PAM+10]. See [PM11, FGS11] for expansions on these ideas, and [VV12a] for a protocol with exponential expansion.

- Free randomness amplification. Colbeck and Renner showed that a particular kind of weak source of randomness (a Santha-Vazirani source) could be ransformed into a near-perfect source of randomness [CR12]; this is well-known to be impossible classically. See also [GMdlT+12, MP13] for further developments.

- One of the main applications of device independence so far is to quantum key distribution. The first to obtain a proof of devic-independent QKD were Barrett, Hardy and Kent [BHK05]. However, their proof relied on the assumption that the devices can be re-used independently — no memory, no correlation between different uses. This assumption was recently removed in three independent works [BCK12b, VV12b, RUV12].

- Some other two-party tasks have also been considered: e.g. bit commitment and coin flipping [SCA+11]. See also [Col06] for some interesting "relativistic" protocols.

- One should be careful not to claim that device independent protocols are secure under "no assumptions". In particular, all such protocols are so far vulnerable to a series of generic attacks detailed in [BCK12a], such as the fact that the devices may remember their past input and outputs and leak them at a later time (say, if they are re-used as part of another protocol).

0.2 Secure multiparty quantum computation

Various tasks in multiparty computation have been considered in the context of quantum information. Examples include quantum secret sharing [CGS02, BOCG$^+$06], leader election [TKM05], Byzantine agreement [BOH05]. For which of these tasks is a quantum protocol truly interesting? I don't know.

0.3 Delegated quantum computation

Can a classical polynomial-time machine verify that an untrusted quantum polynomial-time machine securely executes a circuit of its choosing on a given input? In general this question is open. It has been shown achievable under two different types of assumptions:

- The classical verifier has some limited quantum ability, such as the possibility to store a constant number of qubits [ABOE10] or even simply the ability to prepare single qubits, in a limited set of states, and send them to the quantum prover [BFK09].
- The classical verifier has access to *two* isolated quantum provers [RUV12].

See also [DFPR13] for a proof of "universally composable security" of some of these protocols, which may constitute a good independent introduction to delegated computing. A related (presumably simpler) task is that of establishing quantum authentication codes; see Sections 4.1 and 4.2 in [BGS12] for more on this.

There seems to be a nice connection between *classical* protocols for delegated computation and the theory of *no-signalling* multi-prover interactive proof systems. The idea for this originates in [ABOR00], but more details are in an upcoming STOC paper by Kalai, Raz and Rothblum...unfortunately not publicly available yet; see `http://www.bu.edu/hic/2nd-charles-river-crypto-day/` for an abstract. This could be a direction worth exploring.

0.4 Rigidity and robust testing

The following papers give one reason why device independence is possible: the almost maximal violation of certain Bell inequalities (mostly, the CHSH inequality) can be used to characterize (up to a small distance) the state and measurements underlying the devices. Once such "robust testing" has been achieved the devices can be used for a variety of cryptographic tasks. See [RUV12] for recent breakthrough work in that direction (including a discussion of previous works), and [MS12] for some follow-up work.

0.5 De Finetti-type results

Very roughly, de Finetti results can be used to show that distributions on many (n) variables that are permutation-invariant have their marginals on few (k) systems that are close (depending on the setup, from $\mathrm{poly}(k/n)$ to $\exp(-k/n)$) to convex combinations of product distributions. These results can potentially be useful to establish e.g. parallel repetition results. Recent de Finetti theorems such as the one by Brandao and Harrow [BH12] may be useful in a "device-independent" scenario, and it would be interesting to have a look.

References

[ABOE10] Dorit Aharonov, Michael Ben-Or, and Elad Eban. Interactive proofs for quantum computations. In *Proc. ICS*, pages 453–469, 2010.

[ABOR00] William Aiello, Sandeep Bhatt, Rafail Ostrovsky, and S.Raj. Rajagopalan. Fast verification of any remote procedure call: Short witness-indistinguishable one-round proofs for NP. In *Automata, Languages and Programming*, volume 1853 of *Lecture Notes in Computer Science*, pages 463–474. Springer Berlin Heidelberg, 2000.

[BCK12a] Jonathan Barrett, Roger Colbeck, and Adrian Kent. Prisoners of their own device: Trojan attacks on device-independent quantum cryptography. Technical report arXiv:1201.4407, 2012.

[BCK12b] Jonathan Barrett, Roger Colbeck, and Adrian Kent. Unconditionally secure device-independent quantum key distribution with only two devices. Technical report, arXiv:1209.0435, 2012.

[BCP+13] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. Technical report, arXiv:1303.2849, 2013.

[BFK09] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. Universal blind quantum computation. In *Proc. 50th FOCS*, pages 517–526. IEEE Computer Society, 2009.

[BGS12] Anne Broadbent, Gus Gutoski, and Douglas Stebila. Quantum one-time programs. Technical report, arXiv:1211.1080, 2012.

[BH12] Fernando Brandao and Aram Harrow. Quantum de Finetti theorems under local measurements with applications. Technical report, arXiv:1210.6367, 2012.

[BHK05] J. Barrett, L. Hardy, and A. Kent. No signaling and quantum key distribution. *Phys. Rev. Lett.*, 95:010503, 2005.

[BOCG+06] Michael Ben-Or, Claude Crepeau, Daniel Gottesman, Avinathan Hassidim, and Adam Smith. Secure multiparty quantum computation with (only) a strict honest majority. In *Foundations of Computer Science, 2006. FOCS '06. 47th Annual IEEE Symposium on*, pages 249–260, 2006.

[BOH05] Michael Ben-Or and Avinatan Hassidim. Fast quantum byzantine agreement. In *Proceedings of the thirty-seventh annual ACM symposium on Theory of computing*, STOC '05, pages 481–485, New York, NY, USA, 2005. ACM.

[CGS02] Claude Crépeau, Daniel Gottesman, and Adam Smith. Secure multi-party quantum computation. In *Proceedings of the thiry-fourth annual ACM symposium on Theory of computing*, STOC '02, pages 643–652, New York, NY, USA, 2002. ACM.

[CK11] R. Colbeck and A. Kent. Private randomness expansion with untrusted devices. *Journal of Physics A: Mathematical and Theoretical*, 44(9):095305, 2011.

[Col06] Roger Colbeck. *Quantum And Relativistic Protocols For Secure Multi-Party Computation*. PhD thesis, Trinity College, University of Cambridge, November 2006.

[CR12] Roger Colbeck and Renato Renner. Free randomness can be amplified. *Nature Physics*, 8(6):1–4, 2012.

[DFPR13] Vedran Dunjko, Joseph F. Fitzsimons, Christopher Portmann, and Renato Renner. Composable security of delegated quantum computation. Technical report, arXiv:1301.3662, 2013.

[FGS11] S. Fehr, R. Gelles, and C. Schaffner. Security and composability of randomness expansion from Bell inequalities. Technical report arXiv:1111.6052, 2011.

[GMdlT$^+$12] Rodrigo Gallego, Lluis Masanes, Gonzalo de la Torre, Chirag Dhara, Leandro Aolita, and Antonio Acin. Full randomness from arbitrarily deterministic events. Technical report, arXiv:1210.6514, 2012.

[MP13] Piotr Mironowicz and Marcin Pawlowski. Amplification of arbitrarily weak randomness. Technical report, arXiv:1301.7722, 2013.

[MS12] Carl A. Miller and Yaoyun Shi. Robust self-testing quantum states and binary nonlocal xor games. Technical report, arXiv:1207.1819, 2012.

[MY98] Dominik Mayers and Anrew C.-C. Yao. Self testing quantum apparatus. *Quantum Information and Computation*, 4(4):273–286, 2004. arXiv:quant–ph/9809039, 1998.

[PAM$^+$10] S. Pironio, A. Acin, S. Massar, A. Boyer De La Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and et al. Random numbers certified by Bell's theorem. *Nature*, 464(7291):10, 2010.

[PM11] S. Pironio and S. Massar. Security of practical private randomness generation. Technical report arXiv:1111.6056, 2011.

[RUV12] Ben Reichardt, Falk Unger, and Umesh Vazirani. A classical leash for a quantum system: Command of quantum systems via rigidity of CHSH games. Technical report, arXiv:1209.0448, 2012.

[SCA$^+$11] J. Silman, A. Chailloux, N. Aharon, I. Kerenidis, S. Pironio, and S. Massar. Fully distrustful quantum bit commitment and coin flipping. *Phys. Rev. Lett.*, 106:220501, Jun 2011.

[TKM05] Seiichiro Tani, Hirotada Kobayashi, and Keiji Matsumoto. Exact quantum algorithms for the leader election problem. In Volker Diekert and Bruno Durand, editors, *STACS 2005*, volume 3404 of *Lecture Notes in Computer Science*, pages 581–592. Springer Berlin Heidelberg, 2005.

[VV12a] Umesh Vazirani and Thomas Vidick. Certifiable quantum dice: or, true random number generation secure against quantum adversaries. In *Proc. 44th STOC*, pages 61–76. ACM, 2012.

[VV12b] Umesh Vazirani and Thomas Vidick. Fully device-independent quantum key distribution. Technical report, arXiv:1210.1810, 2012.