FORUM Quantum physics

A grip on misbehaviour

Physicists have come up with a way to characterize and command untrusted quantum systems. Two experts discuss the significance of these findings for fundamental science and for practical quantum computation and cryptography. See Article p.456

THE PAPER IN BRIEF

- To reliably process information using quantum systems, it is pivotal to check whether the systems are truly quantum and behave as instructed.
- In 1969, Clauser, Horne, Shimony and Holt proposed a test, known as the CHSH test, to detect a feature of quantum mechanics called quantum non-locality.
- Building on this proposal, Reichardt *et al.*[1] (page 456) extend this test to characterize and control the dynamics of a quantum system.
- The result brings physicists closer to the dream of secure quantum cryptography even when using untrusted data-encryption and data-decryption devices.

Quantum black boxes

STEFANO PIRONIO

Characterizing the state and dynamics of an unknown system is a central problem in most scientific activities. It is a complex process that involves acquiring and interpreting data from various instruments, and often relies on a priori models and approximations that might need later validation. What can we say about a system's behaviour if we have only minimal information about it? Reichardt *et al.* consider the extreme case in which a quantum system, when viewed as a black box from the perspective of an external observer, can be probed only through a simple, digital, classical interface: the observer can ask only two questions, for example by pushing button 0 or button 1, and the system can deliver only two answers, 0 or 1, corresponding, for example, to one of two lights flashing or not (Fig. 1).

The observer does not know what the questions mean, that is, which properties are probed, and is ignorant of the process that produces the answers. The system can be queried as many times as desired, but there is no guarantee that it will behave the same way every time. The information that can be obtained is limited, whereas the system and its quantum dynamics could be arbitrarily complicated.

In this simple scenario, obtaining any useful information about the internal workings of the unknown system seems hopeless. Indeed, it is: many different processes can produce the same sequence of answers, and any such sequence could simply have been produced by a classical computer.

The situation becomes interesting when, as Reichardt *et al.* consider, instead of one there are two such systems, A and B. Then something non-trivial can be said about their joint behaviour by observing possible correlations between the two systems. Suppose, for instance, that when both systems are probed, system B always produces an answer that is correlated to the question that system A is asked: if A's question is 0, then B outputs 0, and if A's question is 1, then B outputs 1. Some kind of interaction between the two boxes is required to produce this pattern of answers. If no interaction was initially apparent, then we have learned something about the joint dynamics of the systems, although we may still be ignorant of the internal workings of each individual system.

In 1964, John Bell discovered[2] a feature of quantum theory, known as quantum non-locality, according to which certain pairs of quantum systems, although apparently separated and non-interacting, display strong correlations, almost as if they were a single entity. To demonstrate the phenomenon of quantum non-locality experimentally, Clauser, Horne, Shimony and Holt devised a statistical test, the CHSH test, that can detect non-local correlations between two systems without any assumption about their internal working[3], as in the simple example of matching 0s and 1s discussed above.

Researchers have since shown that the CHSH test can detect not only non-local correlations between two quantum black boxes but also other physical properties, such as the amount of quantum randomness produced by the boxes[4] or, in some circumstances, their joint quantum state[5]. This is possible because quantum theory imposes relationships between non-locality and those other physical features. In their study, Reichardt *et al.* push this line of reasoning further and achieve a technical breakthrough: they show that the presence of a sufficiently high amount of non-locality, as measured by the CHSH test, characterizes (almost) completely the joint state and individual dynamics of the two quantum black boxes.

Furthermore, they demonstrate that the CHSH test can be used as a tool to realize and control arbitrary quantum dynamics with two non-interacting quantum systems, without making any assumptions about their internal structure. These results are not only conceptually fascinating, but, as discussed below, they also have profound consequences for practical quantum computation and cryptography.

Stefano Pironio *is in the Laboratoire d'Infomation Quantique, Université Libre de Bruxelles, 1050 Brussels, Belgium.*
e-mail: stefano.pironio@ulb.ac.be

Trusted entanglement

DORIT AHARONOV

Schrödinger's cat is a popular image of a large quantum system. A wild tiger, however, might be more appropriate. After all, describing the quantum state of as few as 1,000 quantum spins may require $2^{1,000}$ parameters — more than the estimated number of particles in the Universe! These exponentially complex quantum states are exactly what future quantum computers will be using to achieve impressive speed-ups over classical computations. But this increase in complexity is a double-edged sword: it also means that classical systems cannot simulate complicated quantum systems in any reasonable amount of time and space, and so cannot predict their behaviour nor test whether they behave as expected[6]. And there is good reason for not trusting quantum devices: they are extremely fragile, complex and difficult to control. Can we leash the 'quantum tiger'? Can we test whether complex quantum systems behave as they should, while trusting only our good old classical devices? Reichardt and colleagues prove that, miraculously, the answer is yes.

The authors' starting point is the CHSH game[3], in which two non-communicating parties play against a referee (see Fig. 2 of the paper[1]). Classical players can win only 75% of the time, but if they share a special quantum state known as the Einstein–Podolsky–Rosen (EPR) quantum state their probability of winning becomes 85%. This result is a manifestation of what Einstein called "spooky action at a distance", also known as quantum entanglement. It provides a way of testing whether a non-communicating two-party system is in a quantum-mechanical state: play the CHSH game repeatedly, each time with the same initial state, and see whether the players win more than 75% of the games.

Now, let's reverse this logic. It turns out that if the players win 85% of the games, then their initial shared state must have been the EPR state. The main technical contribution of Reichardt *et al.* is a robust, multi-game version of this claim: if the two players play many CHSH games in sequence, starting with a shared multi-particle initial state, and win close to the optimal 85% of the games, then the entire initial state of the two players must be close to a collection of many independent EPR states. This implies much more than verifying the 'quantumness' of a system — it certifies a particular state of a large entangled quantum system, and it does so simply by posing a sequence of classical 'questions and answers' to the system being tested (Fig. 1).

Certifying entanglement of many-particle quantum systems has an important implication for high-security cryptography. Quantum-key distribution (QKD)[7], the pinnacle of quantum cryptography, is a protocol that, remarkably, allows two parties to communicate secretly even if the entire world is trying to eavesdrop. However, realizations of this protocol are not automatically secure because of imperfections in the devices. For example, the first QKD apparatus[8] emitted sounds that revealed information about the secrets being communicated, rendering it secure only against deaf eavesdroppers. Implementations of QKD have repeatedly been found to be insecure and to require corrections because of such issues. In 1998, Mayers and Yao envisioned[9] using entanglement certification to achieve 'device-independent' QKD, which is secure even if the quantum devices that are used by the two parties to communicate were manufactured by the eavesdropper herself. After 15 years of important but partial progress by other researchers, Reichardt and colleagues have finally made the missing theoretical leap towards this goal: they describe a QKD protocol and prove that it is secure even when the devices have been maliciously designed.

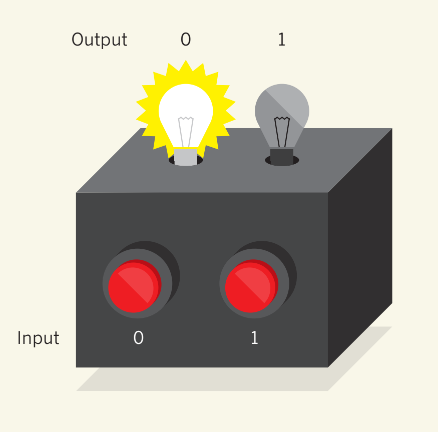

Figure 1 | Classical interaction with a quantum system. Reichardt *et al.*[1] model an arbitrarily complex quantum system as a 'black box' with simple classical inputs and outputs. An experimentalist can probe the system only by pushing button 0 or button 1, and the system outputs only two possible answers, 0 or 1, corresponding to the left or right light flashing.

But there is more to it. The authors' protocol can be extended to certify the correct time-evolution of entanglement into quantum states that are considerably more complex than a collection of independent EPR states. In other words, their extended protocol certifies that a general quantum computation was performed as claimed. How can a classical experimentalist verify that such quantum states are generated even though they are much too complex for him or her to write down? This task has previously been achieved[10] using a 'slightly quantum-mechanical' test. Reichardt *et al.* cleverly provide a completely classical test, using an approach similar to that of a policewoman interrogating two thieves about a crime she knows nothing about; she looks for inconsistencies in their answers, preventing them from coordinating. The only assumptions in the authors' work are that the quantum computer being tested can be divided into two non-interacting parts, and that the tester can communicate privately with each part.

Reichardt and colleagues' protocols are yet to be made practical, that is, fault tolerant and more efficient. However, they provide a proof of principle that hands-off testing of the inner workings of arbitrarily complex quantum systems is possible. Implementing these protocols will allow new and considerably more stringent tests of quantum-information-processing devices than previously performed. ■

Dorit Aharonov *is in the School of Computer Science & Engineering, The Hebrew University of Jerusalem, 91904 Jerusalem, Israel.*
e-mail: doria@cs.huji.ac.il

1. Reichardt, B. W., Unger, F. & Vazirani, U. *Nature* **496,** 456–460 (2013).
2. Bell, J. S. *Physics* **1,** 195–200 (1964).
3. Clauser, J. F., Horne, M. A., Shimony, A. & Holt, R. *Phys. Rev. Lett.* **23,** 880–884 (1969).
4. Pironio, S. *et al. Nature* **464,** 1021–1024 (2010).
5. McKague, M., Yang, T. H. & Scarani, V. *J. Phys. A* **45,** 455304 (2012).
6. Aharonov, D. & Vazirani, U. in *Computability: Turing, Godel, Church, and Beyond* (eds Copeland, B. J., Posy, C. J. & Shagrir, O.) (MIT press, in the press).
7. Bennett, C. H. & Brassard, G. in *Proc. IEEE Int. Conf. Computers, Systems and Signal Processing*, Bangalore, 175 (IEEE, 1984).
8. Bennett, C. H., Bessette, F., Salvail, L. & Smolin, J. *J. Cryptol.* **5,** 3–28 (1992).
9. Mayers, D. & Yao, A. *Quant. Inf. Comp.* **4,** 273–286 (2004).
10. Aharonov, D., Ben-Or, M. & Eban, E. *Proc. Innov. Comp. Sci.*, Beijing, 453–469 (Tsinghua Univ. Press, 2010).

AUTOIMMUNITY

Rubbing salt in the wound

The ability of sodium chloride to induce enzymatic activity that leads to the generation of pathogenic $\mathrm{T_H}17$ immune cells implicates salt as a possible factor that might exacerbate autoimmune disease. SEE LETTERS P.513 & P.518

JOHN J. O'SHEA & RUSSELL G. JONES

The role of the immune system is to protect our bodies from viral, bacterial, fungal and parasitic infections. But, sophisticated as this system is, it can go awry. One consequence is autoimmunity, a diverse collection of disorders in which the immune system turns against the host. Genetics and gender undoubtedly play key parts in the susceptibility to autoimmune diseases, but environmental factors are also important. In this issue, Kleinewietfeld *et al.*[1] (page 518) and Wu *et al.*[2] (page 513) provide provocative data implicating a novel component in this mix: salt*.

The stories focus on a crucial orchestrator of immune responses — the CD4$^+$, or

*This article and the papers under discussion[1,2] were published online on 6 March 2013.