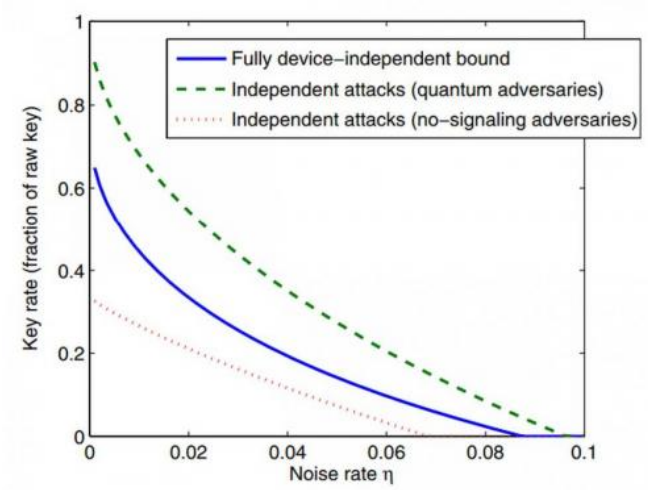
Serious security: Device-Independent Quantum Key Distribution guards against the most general attacks

20 October 2014, by Stuart Mason Dambrot



Key rate obtained in our protocol (middle curve), expressed as a fraction of the raw key (bits obtained from the key rounds). On the x axis is the noise rate ? as measured in the protocol. The top and bottom curves are the best achievable rates known for the case of quantum and no-signaling adversaries, respectively, under the additional assumption of causal independence. Credit: Umesh Vazirani and Thomas Vidick, “Fully Device-Independent Quantum Key Distribution,” *Phys. Rev. Lett*. 113, 140501 (2014).

The Holy Grail of quantum cryptography – beyond delivering security that cannot be classically achieved – is guaranteeing unconditional security when the untrusted quantum devices are involved. While this goal has been studied since the early 1990s, a robust solution has proven elusive. Although Jonathan Barrett and his co-authors published[2,3] a strong Device-Independent Quantum Key Distribution (DIQKD) security guarantee in 2005, it focused on a weaker set of constraints than those imposed by quantum mechanics – specifically, the no-signaling property dictated by special relativity – which thereby yielded stronger results. At the same time, however, it had several drawbacks, including low efficiency and, most importantly, an assumption of independence between the different occurrences when the devices are used.

Recently, scientists at University of California, Berkeley and California Institute of Technology, Pasadena have devised a strong proof of DIQKD security using a standard variation of Artur K. Ekert's entanglement-based protocol[1] targeting general, or coherent, attacks. The researchers say that their protocol is robust, and is based on a new quantitative understanding of the monogamous nature of quantum correlations in the context of a multiparty protocol. (*Quantum monogamy*, one of the most fundamental properties of entanglement, states that if two qubits are maximally correlated they cannot be correlated *at all* with a third qubit.) The authors of the current paper state that their analysis relies on a more complete picture of quantum mechanics, in particular through the use of quantum mechanics' description of post-measurement states.

Prof. Thomas Vidick discussed the paper he and Prof. Umesh Vazirani published in *Physical Review Letters*. "Our main challenge is to prove security against attackers that perform general, or correlated, attacks," Vidick tells *Phys.org*. "The kind of adversary, or eavesdropper, we're worried about is the following scenario," he illustrates. "In the morning, the adversary prepares three quantum devices – one for Alice, one for Bob, and one for himself. During the day, Alice and Bob use their devices to run the protocol. This involves pushing buttons, reading dials, and so on, they never open the device. Later in the day, Alice and Bob might also talk over the phone and exchange classical," or non-quantum, "information - which is part of the protocol. At the end of the day, Alice and Bob come

up with keys that they hope to be the same – and about which they hope no one else has any information.

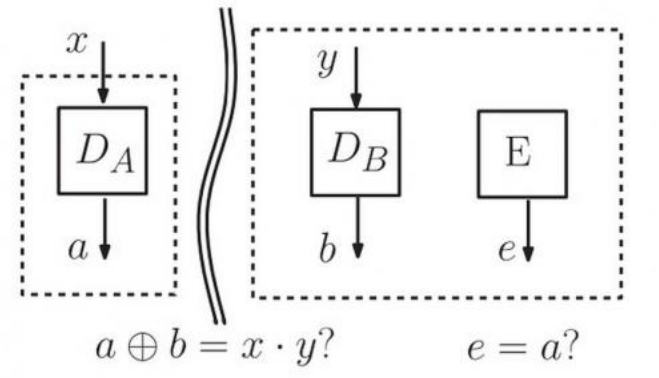
Enter the adversary, who by monitoring all of Alice and Bob's telephone communication, can also perform measurements on his device. The challenge, Vidick explains, is showing that our protocol is such that (given that Alice and Bob do not notice any anomalies) the adversary has no information about the final key.

"Prior to our work security had been established in two circumstances," Vidick notes, the first being "In the first – the *non-device-independent model* – the adversary is all-powerful, but the users trust their devices. In other words, the devices area assumed to perform exactly as expected – but there's a problem: how can this be confirmed?

Scenario #2: Users don't trust the devices, but it is guaranteed that the adversary will only try to attack the key one bit at a time. "One way to phrase this is that there is, again, an assumption that each time Alice and Bob use their device, it behaves in exactly the same way, independently of what happened in the past. Not only is this is a very strong condition, but again – since each time they use the device, we can't go back in the past and check that it's independent – how do we check?" It turns out that this simplifies analysis of these so-called *independent identical distributed (i.i.d.) states*, which is often done using *de Finetti theorems*. (An i.i.d. state is a sequence or other collection of random variables in which each random variable has the same probability distribution as the others and all are mutually independent; de Finetti-type theorems show that the analysis of permutation-invariant states can be reduced to the analysis of i.e. states – meaning that if it is assumed that the adversary treats all sequences in the same way, they can be reduced to independent attacks.

"The challenge, then, was to remove all assumptions and give a general security proof," Vidick explains. "Adversaries that can attack the whole protocol at once, instead of behaving independently across different rounds, are much harder to handle because they can use a lot of information – such as that obtained from what Alice and Bob said over the phone – and then perhaps make a global measurement that will extract information about all the bits of the key at once."

Vidick adds that their main insight had to do with the use of *quantum monogamy* – a property of entanglement stating that if strong correlations are observed between two parties, then the correlations must be weak with any third party – in this case, the adversary. "You can see this as an intuitive way to obtain security, but it's very hard to make it quantitatively precise," Vidick points out. "However, we've introduced techniques to do this. One is a technical tool – the use of pseudorandom objects studied in theoretical computer science known as *extractors*. Another technique is a conceptual tool that we call a 'guessing game' which demonstrates monogamy and shows that it makes certain tasks impossible." (Vidick notes that the scientists knew prior to their work that monogamy would be a key ingredient in any complete proof of security. "However," he says, "we've demonstrated that it's actually possible.")



The guessing game. Any devices satisfying both the CHSH condition a?b = x × y and the guessing condition a = e with high enough probability must allow signaling between DA and DB + E. Credit: Umesh Vazirani and Thomas Vidick, “Fully Device-Independent Quantum Key Distribution,” *Phys. Rev. Lett*. 113, 140501 (2014).

The idea, Vidick continues, is to show that, if the task was possible – for example, the eavesdropper could break the protocol – then the impossible

would be possible. "In the guessing game, one of the users – let's say Alice – is given a secret bit. Then Alice, Bob and the eavesdropper, each in their own corner of the world, do something with their devices. At the end, Eve manages to produce an accurate guess for Alice's secret bit. If such a task were possible, special relativity would be violated in the form of secret information being sent from Alice to the eavesdropper. What we basically show is that, if our protocol could be broken, there would be a way to devise a successful strategy in the guessing game. However, we show that this is impossible, proving that out protocol is secure."

In their paper, the scientists discuss their new quantitative understanding of the monogamous nature of quantum correlations in the context of a multiparty protocol. "This involves more technical lemmas," Vidick points out. (Lemmas, or lemmata, are propositions proved or accepted for immediate use in the proof of some other proposition) "We show a trade-off: if Alice and Bob observe sufficiently strong classical correlations when they talk over the phone and discuss the results of what they read off their respective devices, then the adversary does not even have quantum correlations with the inside of the users' devices. These correlations are measured using a quantum measure of information, the quantum conditional min entropy." (In information theory, *min entropy* corresponds to the most conservative way of measuring the unpredictability of a set of outcomes as the negative logarithm of the probability of the most likely outcome. *Conditional quantum min entropy* is a conservative analog of conditional quantum entropy.)

A key contribution of the study described in the paper is using post-measurement states to achieve a more complete analytic picture of quantum mechanics compared to the previous no-signaling approach. "Previous proof techniques work even *without* using the formalism of quantum mechanics – that is, even if nature allows actions that are beyond quantum mechanics but are still restricted by relativity, they still obtained security," Vidick says. On the one hand, this is stronger because the adversary is allowed more power – but is at the same time weaker because these approaches need to assume independent attacks. "In fact," he adds, "we know that in this framework, we could not possibly obtain general security."

Vidick points out that this creates an important question. "In order to get general security we know one has to use quantum mechanics more strongly and more deeply than previous proofs did – but which principle should we use? Our proof gives an answer to this by showing that quantum mechanics, as a theory, gives us a way to describe the state of a system after a measurement has been made, allowing predictions the outcomes of further measurements to be made. The use of such post-measurement states is essential for us – and at a simple level, lets us model what happens when the devices have memory, and repeatedly measure the same state every time they're used."

Another point discussed in the paper is the implication of the new protocol's linear key rate and toleration of constant noise rate in the quantum devices. "I'd be lying if I said the protocol was practical," Vidick quips. "However, getting linear rate and noise tolerance is an important step towards the possibility of practical implementations. These will always suffer from linear noise, and for the protocol to be efficient we want the rate to be linear." That said, Vidick notes that in terms of analysis, allowing some amount of noise equates *exactly* with allowing the adversary to surreptitiously introduce some amount of adversarial behavior. "What we see as noise could very well be malicious behavior" he explains, "so the more noise we allow, the more power we give to the adversary, the harder the proof, and therefore the stronger the result. The proof would be much simpler if we were to tolerate only zero noise, since in that setting the devices can be very well-characterized[4]. However, this is not the case if we allow a little noise, which we really ought to do if we're ever to use that protocol in the field."

Moving forward, Vidick says that he and Vazirani have several research directions planned:

- Improve the protocol's practicality – specifically, better error dependence and key rate – so that it can be implemented
- Extend analysis to other types of device-independent protocols that have been

proposed in the literature, such as *measurement-device-independent* protocols, which have weaker security guarantees but are more practical, and complete security analysis based on the tools they develop
- Apply their quantum monogamy techniques to completely different areas – the direction he finds most exciting – to quantum complexity theory, the quantum PCP conjecture, black hole theory (where there is significant discussion on the role played by monogamy but nothing quantitatively substantial), and other areas

(Quantum complexity theory – part of computational complexity theory in theoretical computer science – studies complexity classes defined using quantum computers and quantum information which are computational models based on quantum mechanics. Specifically, it studies the hardness of problems in relation to these complexity classes, and the relationship between quantum and classical complexity classes. The PCP theorem, or PCP conjecture, is the foundation of the theory of computational hardness of approximation, which investigates the inherent difficulty in designing efficient approximation algorithms for various optimization problems; PCPs, or Probabilistically Checkable Proofs, embody the idea that verification of proofs becomes nearly trivial if one is willing to use randomness.)

In addition, there are other innovations that the researchers might consider developing. "I think our proof technique has a very promising future, so I'd like to design device-independent protocols for tasks than other quantum key distribution," Vidick tells *Phys.org*. "A very different kind of scenario it can be applied to is the following questions: *Given access to some black-box machine that is supposedly a quantum computer, how do we know if it actually is? How do we gain confidence as to what is going on inside the machine if we can only have a classical interaction?* While this is a very real concern, as is evidenced by the controversy surrounding the D-Wave system, very few convincing techniques are known. We just don't know which kinds of quantum systems can be characterized outside of the inaccessible quantum black box, and how."

In addition to quantum cryptography, complexity theory and physics, Vidick notes that other areas of research that might benefit from the study include "Any area that draws heavily on the properties of entanglement requires tools like the ones that we develop," he concludes, "such as areas of condensed-matter physics and the study of many-body systems."

More information: Fully Device-Independent Quantum Key Distribution, *Physical Review Letters* **113**, 140501 (29 September 2014), doi:10.1103/PhysRevLett.113.140501

Related:

[1]Quantum cryptography based on Bell's theorem, *Physical Review Letters* **67**, 661 (5 August 1991), doi:10.1103/PhysRevLett.67.661
[2]No Signaling and Quantum Key Distribution, *Physical Review Letters* **95**, 010503 (27 June 2005), doi:10.1103/PhysRevLett.95.010503
[3]Nonlocal correlations as an information-theoretic resource, *Physical Review A* **71**, 022101 (2 February 2005), doi:10.1103/PhysRevA.71.022101
[4]Classical command of quantum systems, *Nature* **496**, 456–460 (25 April 2013), doi:10.1038/nature12035