nature

THE INTERNATIONAL WEEKLY JOURNAL OF SCIENCE

HOW TO KEEP A SECRET

Quantum cryptography, randomness and human cunning can outfox the snoopers

PAGE XXX

NEWS FEATURE

TWO LINE TEASER HEERE

Two-line explanation goes in here too

PAGE XXX

BIOMEDICINE

MAKING MICE MODELS WORK

Engineering rodents to ape human diseases

PAGE XXX

QUANTUM PHYSICS

THE NATURE OF NOW

Why the present moment is all about me

PAGE XXX

NATURE.COM/NATURE

27 March 2014 £10

Vol. 507, No. 7493

9 770028 083095 28

PERSPECTIVE

doi:10.1038/nature13132

The ultimate physical limits of privacy

Artur Ekert[1,2] & Renato Renner[3]

Among those who make a living from the science of secrecy, worry and paranoia are just signs of professionalism. Can we protect our secrets against those who wield superior technological powers? Can we trust those who provide us with tools for protection? Can we even trust ourselves, our own freedom of choice? Recent developments in quantum cryptography show that some of these questions can be addressed and discussed in precise and operational terms, suggesting that privacy is indeed possible under surprisingly weak assumptions.

Edgar Allan Poe, an American writer and an amateur cryptographer, once wrote "… it may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve …"[1]. Is it true? Are we doomed to be deprived of our privacy, no matter how hard we try to retain it? If the history of secret communication is of any guidance here, the answer is a resounding 'yes'. There is hardly a shortage of examples illustrating how the most brilliant efforts of code-makers were matched by the ingenuity of code-breakers[2]. Even today, the best that modern cryptography can offer are security reductions, telling us, for example, that breaking RSA, one of the most widely used public key cryptographic systems, is at least as hard as factoring large integers[3]. But is factoring really hard? Not with quantum technology. Indeed, RSA, and many other public key cryptosystems, will become insecure once a quantum computer is built[4]. Admittedly, that day is probably decades away, but can anyone prove, or give any reliable assurance, that it is? Confidence in the slowness of technological progress is all that the security of our best ciphers now rests on.

This said, the requirements for perfectly secure communication are well understood. When technical buzzwords are stripped away, all we need to construct a perfect cipher is shared private randomness, more precisely, a sequence of random bits known as a 'cryptographic key'. Any two parties who share the key, we call them Alice and Bob (not their real names, of course), can then use it to communicate secretly, using a simple encryption method known as the one-time pad[5]. The key is turned into a meaningful message by one party telling the other, in public, which bits of the key should be flipped. An eavesdropper, Eve, who has monitored the public communication and knows the general method of encryption but not the key will not be able to infer anything useful about the message. It is vital though that the key bits be truly random, never reused, and securely delivered to Alice and Bob, who may be miles apart. This is not easy, but it can be done, and one can only be amazed how well quantum physics lends itself to the task of key distribution.

Quantum key distribution, proposed independently by Bennett and Brassard[6] and by Ekert[7], derives its security either from the Heisenberg uncertainty principle (certain pairs of physical properties are complementary in the sense that knowing one property necessarily precludes knowledge about the other) or the monogamy of quantum entanglement (certain quantum correlations cannot be arbitrarily shared). At first, the idea of using quantum phenomena to improve secrecy was nothing more than an academic curiosity, but over time, with the progress of quantum technologies, it was embraced by experimental physicists and eventually turned into a viable commercial proposition. But even though quantum cryptography can offer the best security available at present, it is not immune to attacks exploiting botched implementations (see, for example, refs 8–11 for practical illustrations). The flaws in the design may be unintentional, the result of ignorance or negligence on the part of some honest individuals who design quantum cryptosystems; but they can also be malicious, secretly implanted by powerful adversaries. Should we not then dissect our cryptographic devices, analyse them and make sure that they do exactly what they are supposed to do? Given that some of the flaws may be unknown to us, what exactly should we be looking for? It has long been believed that here we reach the limits of privacy, and that at this point whoever is more technologically advanced, be it the NSA, GCHQ or some other agency, has the upper hand. Surprisingly, this is not the case.

Recent research shows that privacy is possible under stunningly weak assumptions. All we need are monogamous correlations and a little bit of 'free will', here defined as the ability to make choices that are independent of everything pre-existing and are hence unpredictable[12,13]. Given this, we can entertain seemingly implausible scenarios. For example, devices of unknown or dubious provenance, even those that are manufactured by our enemies, can be safely used to generate and distribute secure keys. There are caveats, of course: the devices must be placed in well-isolated locations to prevent any leaks of the registered data, and the data must be analysed by a trusted entity. Barring this, once the devices pass a certain statistical test they can be purchased without any knowledge of their internal working. This is a truly remarkable feat, also referred to as 'device-independent' cryptography[14–20]. Needless to say, proving security under such weak assumptions, with all the mathematical subtleties, is considerably more challenging than in the case of trusted devices, but the rapid progress in the past few years has been very encouraging, making device-independent cryptography one of the most active areas of quantum information science.

In fact, some of the device-independent schemes do not even rely on the validity of quantum theory[21–24], and they therefore guarantee security against adversaries who may have access to superior, 'post-quantum', technologies. The adversaries may even be given control over the choices made by Alice and Bob during the key distribution protocol[25]. As long as this control is not complete, Alice and Bob can do something about it. It turns out that 'free will' or, more specifically, the ability to make unpredictable, and, therefore, random, choices can be amplified[26]. Randomness amplification has recently triggered a flurry of research activity, culminating in a striking result: anything that is not completely deterministic can be made completely random[27,28]. This means, as we explain below, that as long as some of our choices are random and beyond control of the powers that be, we can keep our secrets secret.

The power of free choice

If there is one encryption method that comes close to a perfect cipher, it is the one-time pad. As we have already explained, its security critically

[1]Mathematical Institute, University of Oxford, Oxford OX2 9GG, UK. [2]Centre for Quantum Technologies, National University of Singapore, 117543 Singapore. [3]Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland.

relies on the randomness and secrecy of the cryptographic key. There is a snag, however, known as the 'key distribution problem'. Each key bit can be used only once, to encrypt one single message bit. To maintain their private communication, Alice and Bob must find a way to generate and distribute fresh key bits continuously. But how?

Let us put all the practicalities aside, just for a moment, and dream about something that would solve the key distribution problem. For example, imagine that Alice and Bob were given two magically linked coins, which always come out the same side up—either two heads or two tails—with equal probabilities. Alice and Bob can then toss such coins at their respective locations, writing '0' for heads and '1' for tails. The resulting binary strings will be random and identical, but will they be secret? Not necessarily. Technologically superior Eve could have manufactured an additional coin, magically linked to the coins held by Alice and Bob. The three coins always tally and Eve knows all the bits in the string.

Clearly, to achieve secrecy we must let Alice and Bob do something that is beyond Eve's control. For example, Alice and Bob may be given a choice between two different coins; Alice can toss either coin A_1 or coin A_2 and Bob, either B_1 or B_2. For each toss they must choose one of the two; tossing both A_1 and A_2 or both B_1 and B_2 is forbidden. Suppose, again, that the coins are magically linked; Alice and Bob's coins always come out the same, except when they toss A_1 and B_2, which always come out opposite. The magic can be succinctly summarized by the following four conditions[29,30] (Fig. 1):

$$A_1 = B_1,\ B_1 = A_2,\ A_2 = B_2,\ B_2 \neq A_1 \qquad (1)$$

These conditions are clearly contradictory; it is impossible to assign values to A_1, A_2, B_1 and B_2 so that all the four conditions are satisfied. But remember, Alice and Bob can toss only one coin each, and thus they can test only one of the four conditions in equation (1) at a time. Unperformed tosses do not have outcomes, and, hence, there is no contradiction here.

What if, say, Alice could break the rule and toss both of her coins, A_1 and A_2, in one go? It turns out that she would deprive Bob of his free choice. Suppose that Alice tossed first (correlations are not affected by the chronological order of the tosses) and that her outcomes are such that $A_1 = A_2$. Then Bob has no choice but to toss B_1, because this is the only choice compatible with the conditions in equation (1). Similarly, if $A_1 \neq A_2$, the only choice left to Bob is to toss B_2. This simple argument implies that the magic coins cannot be cloned. Having a clone, Z, of, say, A_1 (such that $Z = A_1$), and being able to toss it together with A_2 would lead to the same contradictions as tossing both A_1 and A_2. The existence of Z deprives Bob of his free choice. The conclusion is that if Alice and Bob have free choice then the magic correlations must be monogamous, that is, nothing else can be correlated to their coins. This turns the tables on Eve. Neither she nor anyone else can manufacture a coin that will always tally with any of the coins held by Alice or Bob. All ingredients for secure key distribution are now in place.

Key distribution

To establish a cryptographic key, Alice and Bob toss their magic coins. For each toss, Alice and Bob choose randomly, and independently of each other, which particular coin will be tossed: Alice is choosing between A_1 and A_2, and Bob, between B_1 and B_2. After the toss, they announce publicly the coins they selected, but not the outcomes they registered. The outcomes are secret, because the coins cannot be cloned, and identical, because the coins are magically linked (except when A_1 and B_2 are tossed, in which case either Bob or Alice must flip his or her bit). The net result is that Alice and Bob share one secret bit. To establish a longer key, they simply repeat this procedure as many times as required.

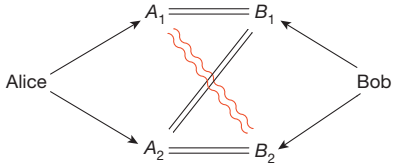

Figure 1 | Magic correlations. Alice and Bob choose and toss one coin each. Their choices are free, random and independent of each other, and the coins always come out the same way up, except when they toss A_1 and B_2, which always come out the opposite way up (represented by the red wiggly lines). Such correlations cannot be shared with a third party; for example, nobody can manufacture a coin that will always tally with any of the coins held by Alice or Bob.

We note that Alice and Bob do not need to make any assumptions about the provenance of the coins; as long as the coins comply with the conditions in equation (1), they are as good as it gets and could have been manufactured by anyone, adversaries included. But this compliance has to be checked. Alice and Bob can do it, for example, by revealing the outcomes of some randomly chosen tosses and checking if they agree with equation (1). Such publicly disclosed tosses are then discarded and the key is composed from the remaining tosses, outcomes of which have never been revealed in public. If Alice and Bob notice a deviation from the magic correlations, they abort the key distribution and try again with another set of coins.

Here we have tacitly assumed that Alice and Bob can communicate in public, but in such a way that nobody can alter their messages; for example, they might use a radio broadcast or an advert in a newspaper, or some other way that prevents impersonations. This communication is passively monitored by Eve and is the only information she gathers during the key distribution, because the coins are tossed in well-isolated locations that prevent any leaks of the registered outcomes. Given this, the secrecy of the key is based solely on the monogamy of the magic correlations and on one innocuous but essential assumption: both Alice and Bob can freely choose which coins to toss.

It seems that we have already achieved our goal. There is only one little problem with our, otherwise impeccable, solution of the key distribution problem, which is that the magic correlations do not exist. That is, we do not know of any physical process that can generate them. But all is not lost, because there are physically admissible correlations that are 'magical' enough for our purposes. Welcome to the quantum world!

The quantum of solace

Quantum theory is believed to govern all objects, large and small, but its consequences are most conspicuous in microscopic systems such as individual atoms or photons. Take, for example, polarized photons. Millions of identically polarized photons form the familiar polarized light, but at the quantum level polarization is an intrinsic property of each photon, corresponding to its spin. Although the polarization of a single photon can be measured along any direction, the outcome of the measurement has only two values, indicating whether the polarization is parallel or orthogonal to the measurement direction. For our purposes, we will label these outcomes 0 and 1.

A number of quantum optical techniques can be employed to generate pairs of polarization-entangled photons. Such photons respond to measurements, carried out on each of them separately, in a very coordinated manner. Suppose that Alice and Bob measure the polarizations of their respective photons along different directions, α and β. It turns out that, although the values 0 and 1 are equally likely to appear, Alice and Bob's outcomes tally with the probability

$$\cos^2(\alpha - \beta) \qquad (2)$$

This is just about everything you need to know about quantum physics for now.

Let us now replace the coin tosses by appropriately chosen polarization measurements: instead of tossing coin A_1, Alice simply measures her photon along $\alpha_1 = 0$; and instead of tossing A_2, she measures the photon along $\alpha_2 = 2\pi/8$. Similarly, Bob replaces his coin tosses B_1 and B_2 by measurements along directions $\beta_1 = \pi/8$ and $\beta_2 = 3\pi/8$, respectively. The resulting joint probabilities of all possible outcomes, obtained using equation (2) and the specified polarization angles, are shown in Table 1.

From a more general perspective, for any value of ε, which can be considered the probability of deviation from the magic correlations, the

Table 1 | Approximating magic correlations

	$A_1 = 0$	$A_1 = 1$	$A_2 = 0$	$A_2 = 1$
$B_1 = 0$	$\frac{1-\varepsilon}{2}$	$\frac{\varepsilon}{2}$	$\frac{1-\varepsilon}{2}$	$\frac{\varepsilon}{2}$
$B_1 = 1$	$\frac{\varepsilon}{2}$	$\frac{1-\varepsilon}{2}$	$\frac{\varepsilon}{2}$	$\frac{1-\varepsilon}{2}$
$B_2 = 0$	$\frac{\varepsilon}{2}$	$\frac{1-\varepsilon}{2}$	$\frac{1-\varepsilon}{2}$	$\frac{\varepsilon}{2}$
$B_2 = 1$	$\frac{1-\varepsilon}{2}$	$\frac{\varepsilon}{2}$	$\frac{\varepsilon}{2}$	$\frac{1-\varepsilon}{2}$

Joint probabilities of binary outcomes given the choices of A_i and B_j ($i, j = 1, 2$). The parameter ε takes the value 0 for the magic correlations (see equation (1)). The lowest physically admissible value, $\varepsilon = \sin^2(\pi/8) \approx 0.146$, can be obtained by measuring polarizations of appropriately entangled photons at some specific angles, for example 0, $\pi/8$, $2\pi/8$ and $3\pi/8$, corresponding to A_1, B_1, A_2 and B_2, respectively.

table describes 'non-signalling' correlations: Alice, by choosing between A_1 and A_2, cannot communicate any information to Bob, and vice versa Bob choosing between B_1 and B_2 cannot send any information to Alice. Neither of them can see through the statistics of the outcomes what the other one is doing. Correlations with $\varepsilon \geq 1/4$ are called 'classical', because they admit pre-assigned values of A_1, A_2, B_1 and B_2. This is no longer the case when $\varepsilon < 1/4$, because any pre-assignment is bound to violate at least one of the four conditions in equation (1). Surprisingly, as we have just seen, there are physically admissible correlations for which ε can reach $\sin^2(\pi/8) \approx 0.146$, which is the lowest value that can be achieved with quantum correlations[31]. Even though perfect magic correlations, with $\varepsilon = 0$, do not exist, there is still some magic left in quantum correlations, and it can be exploited.

Less reality, more security

The impossibility of assigning numerical values to certain physical quantities, for example the different polarizations of a photon, has been baffling physicists for almost a century[32]. After all, most of us grew up holding it self-evident that there is an objective reality in which physical objects have properties that can be quantified and whose values exist regardless of whether we measure them or not. Shocking as it may be, our world is not of this kind. Statistical inequalities, such as $\varepsilon \geq 1/4$, derived on the assumption that the values of unmeasured physical quantities do exist and commonly referred to as Bell's inequalities[33], have been violated in a number of painstaking experiments[34–44]. We shall not dwell on the philosophical implications of this experimental fact (volumes have been written on the subject), but simply point out that it should be embraced by all those who worry about secrecy because what does not exist cannot be eavesdropped, and so it is much easier to keep secrets in a non-classical world.

Indeed, given the correlations parameterized by ε, it can be shown that the probability of Eve guessing correctly any particular outcome cannot exceed $(1 + 4\varepsilon)/2$ (Box 1). Eve may know something about the outcomes (which is not good) but Alice and Bob, after running a statistical test and estimating ε, know how much she may know (which is good). If ε is low enough, this allows them to distil an almost perfect key from the outcomes, using a technique known as 'privacy amplification'.[45,46] The basic idea behind privacy amplification is quite simple. Imagine that you have two bits and that you know your adversary knows at most one of them, but that you do not know which one. Add the two bits together (modulo 2); the resulting bit will be secret. Needless to say, given more bits, there are more sophisticated ways of achieving secrecy, to mention only two-universal hash functions[47] or Trevisan's extractor[48].

In summary, whenever Alice and Bob are given any devices that generate correlated outcomes, they can run the key distribution protocol supplemented by a statistical 'honesty test' to estimate ε. If this value is small enough, say $\varepsilon = 0.15$, the end result, after privacy amplification, is a perfect cryptographic key. We obtain trusted privacy from untrusted devices, but what constitutes a device? We need to sort out one more thing before we can celebrate the arrival of the ultimate cipher. Should Alice and Bob trust the ultimate measuring and controlling devices; that is, should they trust themselves?

BOX 1

Eavesdropping quantified

Suppose that Eve wants to manufacture a device that outputs binary values, Z, designed to tally with, say, A_1. Regardless of her technological prowess, Eve has limited chances to succeed. For any two outcomes, A_i and B_j, the probabilities that they are equal to Z, that is, $\Pr(Z = A_i)$ and $\Pr(Z = B_j)$, cannot differ by more than $\Pr(A_i \neq B_j)$. This implies a sequence of inequalities:

$$\Pr(Z = A_1) - \Pr(Z = B_1) \leq \Pr(A_1 \neq B_1)$$
$$\Pr(Z = B_1) - \Pr(Z = A_2) \leq \Pr(B_1 \neq A_2)$$
$$\Pr(Z = A_2) - \Pr(Z = B_2) \leq \Pr(A_2 \neq B_2)$$
$$\Pr(Z = B_2) - \Pr(Z \neq A_1) \leq \Pr(B_2 = A_1)$$

Adding these inequalities together and taking into account that $\Pr(Z \neq A_1) = 1 - \Pr(Z = A_1)$ gives

$$\Pr(Z = A_1) \leq \frac{1}{2}(1 + I_2)$$

where the quantity $I_2 = \Pr(A_1 \neq B_1) + \Pr(B_1 \neq A_2) + \Pr(A_2 \neq B_2) + \Pr(B_2 = A_1)$ is the sum of the probabilities that any of the conditions in equation (1) is violated. The derivation presented here works for any A_i and B_j, and, it is worth stressing, does not involve quantum theory.

Although the values A_1, A_2, B_1 and B_2 do not coexist, all the probabilities used here involve only pairs of values, A_i and B_j, which can be measured simultaneously. They can be determined from the statistics of the experimental data. For the polarization measurements described in the text, we would obtain $I_2 = 4\varepsilon$ where $\varepsilon = \sin^2(\pi/8) \approx 0.146$. The bound thus asserts that $\Pr(Z = A_1) \leq 0.793$; that is, Eve's value, Z, will deviate from A_1 in more than 20% of the cases.

The notion of magic correlations can be extended to cases where Alice and Bob choose between $n \geq 2$ different measurements[67,68], with the conditions in equation (1) replaced by

$$A_1 = B_1,\ B_1 = A_2,\ \ldots,\ A_n = B_n,\ B_n \neq A_1 \qquad (3)$$

To approximate such correlations, Alice and Bob may use entangled photons and measure polarizations A_i and B_j, specified by angles α_i and β_j. These angles are chosen to be even and odd multiples of $\pi/4n$, respectively, so that the adjacent values of α_i and β_j are $\pi/4n$ radians apart. Then, according to equation (2), each of the conditions in equation (3) is satisfied, except with an error probability of $\varepsilon_n = \sin^2(\pi/4n) < 1/n^2$. It can then be shown, by the same arguments as for the $n = 2$ case, that any attempt by Eve to compute a prediction, Z, for the outcome of, say, A_1, can succeed with probability at most $(1 + I_n)/2$, where $I_n = \Pr(A_1 \neq B_1) + \Pr(B_1 \neq A_2) + \cdots + \Pr(A_n \neq B_n) + \Pr(B_n = A_1)$. For any classical correlations, $I_n \geq 1$. In contrast, quantum theory admits correlations such that $I_n = 2n\varepsilon_n < 2/n$. Consequently, in the limit of large n, the probability of Eve guessing the value of A_1 correctly becomes 1/2; that is, A_1 is uniformly random and independent of any information held by Eve. This observation is not only relevant for key distribution[21], but has been crucial for randomness amplification[26].

Should we trust ourselves?

We can hardly get more paranoid than that. Can we make free choices or are we held to the ransom of a greater force? In other words, what if we are manipulated?

We have already stressed the power of free choice. Decisions such as which coin to toss and which polarization to measure must be made freely (randomly) and independently. If referring to the experimenter's 'free will' sounds too esoteric, then think about the random number generators that in practical implementations make such choices. Where is

their randomness coming from? What if these random number generators are of dubious provenance, possibly manufactured by the same person who offered the key distribution kit? It is evident that without randomness there is no privacy: if everything is pre-determined, and all possible choices we make (with the help of tweaked random number generators or otherwise) are predictable or pre-programmed by our adversaries, then there is nothing that we can build our privacy on. Or is there?

There is if the manipulation is not complete and there is a little bit of freedom left. If someone we trust tells us that such and such a fraction of the choices made by our random number generators cannot be determined by the adversary, then privacy is still possible because local randomness can be amplified[26]. Randomness amplification can itself be done with device-independent protocols, and it works even if the fraction of initial randomness is arbitrarily small or the devices are noisy[27,28].

It all looks bizarre and too good to be true. Perfect privacy, secure against powerful adversaries who provide us with cryptographic tools and who may even manipulate us? Is such a thing possible? Yes, it is, but 'the devil is in the detail' and we need to look into some practicalities.

Practicalities

Quantum key distribution, in which security is tested by the degree of violation of Bell's inequalities, was proposed some time ago[7] and was followed shortly by a proof-of-principle experiment at what used to be called the Defence Research Agency (now Qinetiq) in Malvern, UK[49]. However, the device-independent character of this protocol has not been recognized until recently[15]. Moreover, proving the security of such a scheme in the presence of noise has not been easy. It has taken over a decade to agree on a useful definition of secrecy, even for trusted devices, and to conclude a long sequence of steadily improved security results[50–53] that eventually took into account all the quantum resources that Eve can muster[54]. Dealing with untrusted devices is even more tricky and keeps many of our colleagues busy[55–57].

Although all security proofs infer secrecy from the monogamy of the correlations, a major challenge is to make these arguments quantitative and robust to noise and imperfections, and applicable to keys of finite size[58,59]. There are other issues as well. For example, here we have taken for granted that Alice and Bob can estimate the parameter ε from a sufficiently large sample of their registered data. In the quantum domain, a statement of that kind requires a quantum version of what is known in classical statistics as de Finetti's theorem[54,60]. It guarantees that, for instance, pairs of photons can be treated as individual objects with individual properties and without any hidden correlations to other pairs. These, and many other results, addressed a number of subtleties and, finally, twenty years after its inception, the original entanglement-based key distribution protocol[7] has been shown to offer security even if the devices are not fully trusted and are exposed to noise[15–20]. This is assuming that quantum theory is all that there is, and that Eve is bound by the laws of quantum physics. However, if Alice and Bob are paranoid enough to give Eve some 'post-quantum' powers (technologies more powerful than quantum technologies which may rely on as-yet undiscovered physical phenomena that are not described by quantum physics), they can still resort to less efficient protocols that do not rely on quantum theory[21–24]. We should stress, however, that device-independent protocols and their security proofs have not yet reached the level of sophistication that is now common for the device-dependent scenario. In particular, more work is needed to improve the efficiency of the key distribution protocols or to identify conditions under which untrusted devices may be reused in multiple rounds of such protocols.

Given that violation of Bell's inequality is an experimental fact, what is it that prevents us from running the experiments that violated Bell's inequality again, but this time under the label of the device-independent key distribution? Convincing as they are, these experiments still leave some loopholes. For example, it is in principle possible that the photons detected in the experiments did not represent a fair sample of all photons emitted by the source (the 'detection loophole') or that the various parts and components of the experiment were causally connected (the 'locality loophole'). Some of these concerns were addressed in more recent experiments[43,44], but, a single experiment that closes all the loopholes at once, demonstrating the ultimate violation of Bell's inequality, is still lacking.

This is not so disturbing for physicists, because nature would have to be very malicious if it were to cheat us selectively—on locality in some experiments and in exploring detection loopholes in some other. In contrast, there is nothing to prevent an eavesdropper being malicious. In this adversarial setting, a proper experimental demonstration of device-independent cryptography requires a proper violation of Bell's inequalities. This is particularly true for the detection loophole. Imagine, for example, that Eve pre-programmed the devices assuming in advance a sequence of settings that Alice and Bob may choose for their measurements. Whenever her guess is correct, the devices will respond with pre-programmed results, and when it is not, one of the devices will simulate failure to respond. If Alice and Bob naively discard all the instances in which at least one of the devices failed to deliver a result, then they can be easily fooled by Eve. Thus, we do need the loophole-free violation of Bell's inequalities.

Closing the detection loop-hole is very challenging, because almost any optical component adds losses and imperfections to the key distribution set-up, but it is within the reach of today's technology, especially with the rapid progress in photodetection techniques. If distance is not an issue, then we can achieve near-perfect detection efficiency using entangled ions rather than photons[40], and this has been used to generate the first device-independent certified randomness[61,62]. Short of full device independence, we can also entertain intermediate scenarios, where some parts of the devices are trusted and some are not. Indeed, proposals that address issues such as untrusted detectors[63,64] offer significant improvements over the existing quantum key distribution schemes[65,66] and move secure communication in interesting new directions.

Experimental device-independent cryptography is far from easy, but technological progress so far has encouraged optimism. The days we stop worrying about untrustworthy or incompetent providers of cryptographic services may be not that far away.

Conclusion

Over the past decade or so, quantum cryptography has come of age, but the field is still an amazingly fertile source of inspiration for fundamental research. The search for the ultimate physical limits of privacy is still very much a work in progress, but we know that privacy is possible under surprisingly weak assumptions. Monogamous correlations, of whatever origin, and an arbitrarily small amount of free will are sufficient to conceal whatever we like. Free will is our most valuable asset. Come to think about it, without free will, there is no point in concealing anything anyway.

Received 12 August 2013; accepted 7 February 2014.

1. Poe, E. A. A few words on secret writing. *Graham's Mag.* **19,** 33–38 (1841).
2. Kahn, D. *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet* (Scribner, 1996).
3. Rivest, R., Shamir, A. & Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **21,** 120–126 (1978).
4. Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **26,** 1484–1509 (1997).
5. Vernam, G. S. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *J. Am. Inst. Electr. Eng.* **45,** 109–115 (1926).
6. Bennett, C. H. & Brassard, G. in *Proc. IEEE Int. Conf. Computer Syst. Signal Process.* 175–179 (IEEE, 1984).
   This work reported key distribution based on encoding information in complementary bases.
7. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67,** 661–663 (1991).
   This work reported key distribution based on quantum entanglement.
8. Fung, C.-H. F., Qi, B., Tamaki, K. & Lo, H.-K. Phase-remapping attack in practical quantum-key-distribution systems. *Phys. Rev. A* **75,** 032314 (2007).
9. Lydersen, L. *et al.* Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photon.* **4,** 686–689 (2010).
10. Weier, H. *et al.* Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors. *New J. Phys.* **13,** 073024 (2011).
11. Gerhardt, I. *et al.* Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nature Commun.* **2,** 349 (2011).
12. Bell, J. S. *Speakable and Unspeakable in Quantum Mechanics: Collected Papers on Quantum Philosophy* (Cambridge Univ. Press, 2004).
13. Colbeck, R. & Renner, R. No extension of quantum theory can have improved predictive power. *Nature Commun.* **2,** 411 (2011).

14. Mayers, D. & Yao, A. in *FOCS '98: Proc. 39th Annu. Symp. Foundations Computer Sci.* 503–509 (IEEE, 1998).
This work included a proposal for self-testing cryptographic devices.
15. Acín, A. *et al.* Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **98,** 230501 (2007).
This work included a proposal for device-independent quantum key distribution.
16. McKague, M. *Quantum Information Processing With Adversarial Devices*. PhD thesis, Univ. Waterloo (2010).
17. Hänggi, E. & Renner, R. Device-independent quantum key distribution with commuting measurements. Preprint at http://arxiv.org/abs/1009.1833 (2010).
18. Masanes, L., Pironio, S. & Acin, A. Secure device-independent quantum key distribution with causally independent measurement devices. *Nature Commun.* **2,** 238 (2011).
19. Vazirani, U. & Vidick, T. in *ITCS '14: Proc. 2014 Conf. Innovations Theor. Computer Sci.* (ed, Naor, M.) 35–36 (ACM, 2012).
20. Reichardt, B. W., Unger, F. & Vazirani, U. Classical command of quantum systems. *Nature* **496,** 456–460 (2013).
21. Barrett, J., Hardy, L. & Kent, A. No signaling and quantum key distribution. *Phys. Rev. Lett.* **95,** 010503 (2005).
This work demonstrated that the security of entanglement-based key distribution can be guaranteed without relying on the correctness of quantum theory.
22. Acín, A., Gisin, N. & Masanes, L. From Bell's theorem to secure quantum key distribution. *Phys. Rev. Lett.* **97,** 120405 (2006).
23. Masanes, L. Universally composable privacy amplification from causality constraints. *Phys. Rev. Lett.* **102,** 140501 (2009).
24. Hänggi, E., Renner, R. & Wolf, S. in *Advances in Cryptology – EUROCRYPT 2010* Vol. 6110 (ed. Gilbert, H.) 216–234 (Springer, 2010).
25. Koh, D. E. *et al.* Effects of reduced measurement independence on Bell-based randomness expansion. *Phys. Rev. Lett.* **109,** 160404 (2012).
26. Colbeck, R. & Renner, R. Free randomness can be amplified. *Nature Phys.* **8,** 450–454 (2012).
This work proved that randomness amplification is possible.
27. Gallego, R. *et al.* Full randomness from arbitrarily deterministic events. *Nature Commun.* **4,** 2654 (2013).
28. Brandao, F. *et al.* Robust device-independent randomness amplification with few devices. Preprint at http://arxiv.org/abs/1310.4544 (2013).
29. Khalfi, L. A. & Tsirelson, B. S. in *Symp. Foundations Mod. Phys.* (eds Lahti, P. & Mittelstaedt, P.) 441–460 (World Scientific, 1985).
30. Popescu, S. & Rohrlich, D. Quantum nonlocality as an axiom. *Found. Phys.* **24,** 379–385 (1994).
31. Cirel'son, B. Quantum generalizations of Bell's inequality. *Lett. Math. Phys.* **4,** 93–100 (1980).
32. Einstein, A., Podolsky, B. & Rosen, N. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.* **47,** 777–780 (1935).
33. Bell, J. S. On the Einstein-Podolsky-Rosen paradox. *Physics* **1,** 195–200 (1964).
34. Freedman, S. J. & Clauser, J. F. Experimental test of local hidden-variable theories. *Phys. Rev. Lett.* **28,** 938–941 (1972).
35. Aspect, A., Grangier, P. & Roger, G. Experimental tests of realistic local theories via Bell's theorem. *Phys. Rev. Lett.* **47,** 460–463 (1981).
36. Aspect, A., Grangier, P. & Roger, G. Experimental realization of Einstein-Podolsky-Rosen-Bohm gedankenexperiment: a new violation of Bell's inequalities. *Phys. Rev. Lett.* **49,** 91–94 (1982).
37. Aspect, A., Dalibard, J. & Roger, G. Experimental test of Bell's inequalities using time-varying analyzers. *Phys. Rev. Lett.* **49,** 1804–1807 (1982).
38. Weihs, G., Jennewein, T., Simon, C., Weinfurter, H. & Zeilinger, A. Violation of Bell's inequality under strict Einstein locality conditions. *Phys. Rev. Lett.* **81,** 5039–5043 (1998).
39. Tittel, W., Brendel, J., Zbinden, H. & Gisin, N. Violation of Bell inequalities by photons more than 10 km apart. *Phys. Rev. Lett.* **81,** 3563–3566 (1998).
40. Rowe, M. A. *et al.* Experimental violation of a Bell's inequality with efficient detection. *Nature* **409,** 791–794 (2001).
41. Pomarico, E., Bancal, J.-D., Sanguinetti, B., Rochdi, A. & Gisin, N. Various quantum nonlocality tests with a commercial two-photon entanglement source. *Phys. Rev. A* **83,** 052104 (2011).
42. Stuart, T. E., Slater, J. A., Colbeck, R., Renner, R. & Tittel, W. Experimental bound on the maximum predictive power of physical theories. *Phys. Rev. Lett.* **109,** 020402 (2012).
43. Giustina, M. *et al.* Bell violation using entangled photons without the fair-sampling assumption. *Nature* **497,** 227–230 (2013).
44. Christensen, B. G. *et al.* Detection-loophole-free test of quantum nonlocality, and applications. *Phys. Rev. Lett.* **111,** 130406 (2013).
45. Bennett, C. H., Brassard, G., Crepeau, C. & Maurer, U. M. Generalized privacy amplification. *IEEE Trans. Inf. Theory* **41,** 1915–1923 (1995).
46. Renner, R. & König, R. in *Second Theory Cryptogr. Conf.* (ed. Kilian, J.) 407–425 (Lect. Notes Computer Sci. 3378, Springer, 2005).
47. Tomamichel, M., Schaffner, C., Smith, A. & Renner, R. Leftover hashing against quantum side information. *IEEE Trans. Inf. Theory* **57,** 5524–5535 (2011).
48. De, A., Portmann, C., Vidick, T. & Renner, R. Trevisan's extractor in the presence of quantum side information. *SIAM J. Comput.* **41,** 915–940 (2012).
49. Ekert, A. K., Rarity, J. G., Tapster, P. R. & Palma, G. M. Practical quantum cryptography based on two-photon interferometry. *Phys. Rev. Lett.* **69,** 1293–1295 (1992).
50. Biham, E. & Mor, T. Security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **78,** 2256–2259 (1997).
51. Lütkenhaus, N. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A* **61,** 052304 (2000).
52. Shor, P. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85,** 441–444 (2000).
53. Mayers, D. Unconditional security in quantum cryptography. *J. ACM* **48,** 351–406 (2001).
54. Renner, R., *Security of Quantum Key Distribution*. PhD thesis, ETH Zurich (2005).
This work included a comprehensive security analysis of quantum key distribution with trusted devices that offer composable security.
55. Arnon-Friedman, R. & Ta-Shma, A. Limits of privacy amplification against non-signalling memory attacks. *Phys. Rev. A* **86,** 062333 (2012).
56. Hänggi, E., Renner, R. & Wolf, S. The impossibility of non-signaling privacy amplification. *Theor. Comput. Sci.* **486,** 27–42 (2013).
57. Barrett, J., Colbeck, R. & Kent, A. Memory attacks on device-independent quantum cryptography. *Phys. Rev. Lett.* **110,** 010503 (2013).
58. Scarani, V. & Renner, R. Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way postprocessing. *Phys. Rev. Lett.* **100,** 200501 (2008).
59. Scarani, V. *et al.* The security of practical quantum key distribution. *Rev. Mod. Phys.* **81,** 1301–1350 (2009).
60. Renner, R. Symmetry of large physical systems implies independence of subsystems. *Nature Phys.* **3,** 645–649 (2007).
61. Colbeck, R. *Quantum And Relativistic Protocols For Secure Multi-Party Computation*. PhD thesis, Univ. Cambridge (2006).
62. Pironio, S. *et al.* Random numbers certified by Bell's theorem. *Nature* **464,** 1021–1024 (2010).
63. Lim, C. C. W., Portmann, C., Tomamichel, M., Renner, R. & Gisin, N. Device-independent quantum key distribution with local Bell test. *Phys. Rev. X* **3,** 031006 (2013).
64. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108,** 130503 (2012).
65. Rubenok, A., Slater, J. A., Chan, P., Lucio-Martinez, I. & Tittel, W. Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks. *Phys. Rev. Lett.* **111,** 130501 (2013).
66. Liu, Y. *et al.* Experimental measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **111,** 130502 (2013).
67. Pearle, P. Hidden-variable example based upon data rejection. *Phys. Rev. D* **2,** 1418–1425 (1970).
68. Braunstein, S. L. & Caves, C. M. Wringing out better Bell inequalities. *Ann. Phys.* **202,** 22–56 (1990).

Author Information Reprints and permissions information is available at www.nature.com/reprints. The authors declare no competing financial interests. Readers are welcome to comment on the online version of the paper. Correspondence should be addressed to A.E. (artur.ekert@quibit.org) or R.R. (renner@phys.ethz.ch).

Author Queries

Journal: **Nature**
Paper: **nature13132**
Title: **The ultimate physical limits of privacy**

Query Reference	Query
Web summary	Developments in quantum cryptography show that it is possible to protect secrets — from those with superior technology, those who profess to provide our security and even those who manipulate us without our knowledge — under surprisingly weak assumptions.

For Nature office use only:

Layout	☐	Figures/Tables/Boxes	☐	References	☐
DOI	☐	Error bars	☐	Supp info	☐
Title	☐	Colour	☐	Acknowledgements	☐
Authors	☐	Text	☐	Author contribs	☐
Addresses	☐	Methods	☐	COI	☐
First para	☐	Received/Accepted	☐	Correspondence	☐
		AOP	☐	Author corrx	☐
		Extended Data	☐	Web summary	☐
				Accession codes link	☐