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
The ultimate physical limits of privacy

Artur Ekert1,2 & Renato Renner3

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 conceot 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-breakers2. 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 integers3. 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 built4. 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. 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 two-party protocol known as a ‘cryptographic key’5. Well understood. When technical buzzwords are stripped away, all we need to construct a perfect cipher is shared private randomness. 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 two-party protocol known as a ‘cryptographic key’5. 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. 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 two-party protocol known as a ‘cryptographic key’5. 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.

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 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 unpredictable4,21. 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, 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’ cryptography4,21–24. 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 theory22–24, 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 protocol22. 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, random, choices can be amplified25. 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 random26–28. 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.

1Mathematical Institute, University of Oxford, Oxford OX2 9GG, UK. 2Centre for Quantum Technologies, National University of Singapore, 117543 Singapore. 3Institute for Theoretical Physics, ETH Zürich, 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, and ‘1’ for tails.

The magic can be succinctly summarized by the following
correlations (Fig. 1):

\[ A_1 = B_1, \quad B_1 = A_2, \quad A_1 = B_2, \quad B_2 \neq A_1 \] (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 only test 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, \( Z_0 \), 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
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 public-
ly 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.

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 distri-
bution 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 indi-
vidual 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 coordi-
nated manner. Suppose that Alice and Bob measure the polarizations
of their respective photons along different directions, \( \alpha \) and \( \beta \). It turns
out that, although the values 0 and 1 are equally likely to appear, Alice and
Bob’s outcomes tally with the probability

\[ \cos^2(\alpha - \beta) \] (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 measure-
ments 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 \( \theta \), which can be con-
sidered the probability of deviation from the magic correlations, the
table describes ‘non-signalling’ correlations: Alice, by choosing between
A1 and A2, cannot communicate any information to Bob, and vice versa
Bob choosing between B1 and B2 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 \( \varepsilon \equiv 1/4 \) are called ‘classical’, because
they admit pre-assigned values of A1, A2, B1, and B2. 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 \( \varepsilon \) can reach
\( \sin^2(\pi/8) \approx 0.146 \), which is the lowest value that can be achieved with quantun
correlations\(^{34}\). 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 quan-
tities, for example the different polarizations of a photon, has been baffling
physicists for almost a century\(^2\). 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 \( \varepsilon \equiv 1/4 \), derived on the assumption that the values of unmeasured physical quantities do exist and commonly referred to as Bell’s inequalities\(^{35}\), have been violated in a number of painstaking experiments\(^{44-45}\). 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 eaves-
dropped, and so it is much easier to keep secrets in a non-classical world.

Indeed, given the correlations parameterized by \( \varepsilon \), 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 \( \varepsilon \), know how much she may know (which is good). If \( \varepsilon \) is low enough, this allows them to distil an almost perfect key from the out-
comes, using a technique known as ‘privacy amplification’\(^{46-47}\). 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\(^{48}\) or Trevisan’s extractor\(^{49}\).

In summary, whenever Alice and Bob are given any devices that gen-
erate correlated outcomes, they can run the key distribution protocol supplemented by a statistical ‘honesty test’ to estimate \( \varepsilon \). 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
ting before we can celebrate the arrival of the ultimate cipher. Should

### Table 1 | Approximating magic correlations

<table>
<thead>
<tr>
<th>( A_1 = 0 )</th>
<th>( A_1 = 1 )</th>
<th>( A_2 = 0 )</th>
<th>( A_2 = 1 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( B_1 = 0 )</td>
<td>( 1 - \varepsilon )</td>
<td>( \varepsilon )</td>
<td>( 1 - \varepsilon )</td>
</tr>
<tr>
<td>( B_1 = 1 )</td>
<td>( \varepsilon )</td>
<td>( 1 - \varepsilon )</td>
<td>( \varepsilon )</td>
</tr>
<tr>
<td>( B_2 = 0 )</td>
<td>( \varepsilon )</td>
<td>( 1 - \varepsilon )</td>
<td>( \varepsilon )</td>
</tr>
<tr>
<td>( B_2 = 1 )</td>
<td>( 1 - \varepsilon )</td>
<td>( \varepsilon )</td>
<td>( 1 - \varepsilon )</td>
</tr>
</tbody>
</table>

Joint probabilities of binary outcomes given the choices of A and B (j = 1, 2). The parameter \( \varepsilon \) 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, 90°, 2x90° and 3x90°, corresponding to \( A_1, B_1, A_2, \) and \( B_2 \), respectively.

### BOX I

#### 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, \( A_1 \) and \( B_1 \), the probabilities that they are equal to Z, that is, \( \text{Pr}(Z = A_1) \) and \( \text{Pr}(Z = B_1) \), cannot differ by more than \( \text{Pr}(A_1 \neq B_1) \). This implies a sequence of inequalities:

\[
\text{Pr}(Z = A_1) - \text{Pr}(Z = B_1) \leq \text{Pr}(A_1 \neq B_1)
\]
\[
\text{Pr}(Z = B_1) - \text{Pr}(Z = A_2) \leq \text{Pr}(B_1 \neq A_2)
\]
\[
\text{Pr}(Z = A_2) - \text{Pr}(Z = B_2) \leq \text{Pr}(A_2 \neq B_2)
\]
\[
\text{Pr}(Z = B_2) - \text{Pr}(Z \neq A_1) \leq \text{Pr}(B_2 \neq A_1)
\]

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

\[
\text{Pr}(Z = A_1) \leq \frac{1}{2}(1 + \varepsilon_z)
\]

where the quantity \( \varepsilon_z = \text{Pr}(A_1 \neq B_1) + \text{Pr}(B_1 \neq A_2) + \text{Pr}(A_2 \neq B_2) + \text{Pr}(B_2 \neq A_1) \) 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 \( \varepsilon_z = 4\varepsilon \), where \( \varepsilon = \sin^2(\pi/8) \approx 0.146 \). The bound thus asserts that \( \text{Pr}(Z = A_1) \leq 0.793 \); 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\(^{50,52}\), with the conditions in equation (1) replaced by

\[
A_1 = B_1, \quad A_1 = B_2, \quad \ldots, \quad A_n = B_n, \quad B_n \neq A_1
\]

To approximate such correlations, Alice and Bob may use entangled photons and measure polarizations \( A_i \) and \( B_j \) specified by angles \( x_i \) and \( y_j \). These angles are chosen to be even and odd multiples of \( \pi/4n \), respectively, so that the adjacent values of \( x_i \) and \( y_j \) 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

\[
\varepsilon_z = \sin^2(\pi/4n) < 1/n^2.
\]

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 \( (1 + \varepsilon_z)/2 \), where

\[
l_0 = \text{Pr}(A_1 = B_1) + \text{Pr}(B_1 \neq A_2) + \cdots + \text{Pr}(A_n \neq B_n) + \text{Pr}(B_n = A_1).
\]

For any classical correlations, \( l_0 \geq 1/2 \). In contrast, quantum theory
admits correlations such that \( l_0 = 2n/2^n < 2/n \). 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\(^{51}\), but has been crucial for randomness amplification\(^{52}\).

Alice and Bob trust the ultimate measuring and controlling devices; that is, should they trust themselves?

### 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? Is it 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 amplified28. 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 noisy27,28.

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 and was followed shortly by a proof-of-principle experiment at what used to be called the Defence Research Agency (now Qinetiq) in Malvern, UK46. However, the device-independent character of this protocol has not been recognized until recently29. 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 results30–53 that eventually took into account all the quantum resources that Eve can muster44. Dealing with untrusted devices is even more tricky and keeps many of our colleagues busy55–57.

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 size46,59. 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 theorem56,57. 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 has been shown to offer security even if the devices are not fully trusted and are exposed to noise45–50. This is assuming that quantum physics 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 freedom, then 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 photons46, and this has been used to generate the first device-independent certified randomness41,52. 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 detectors43,54 offer significant improvements over the existing quantum key distribution schemes45,56 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 few words on secret writing, Graham’s Mag. 19, 33–38 (1841).
This work included a proposal for self-testing cryptographic devices.

This work included a proposal for device-independent quantum key distribution.

This work demonstrated that the security of entanglement-based key distribution can be guaranteed without relying on the correctness of quantum theory.

This work proved that randomness amplification is possible.

This work proved that randomness amplification can be guaranteed without relying on the correctness of quantum theory.


This work demonstrated that the security of entanglement-based key distribution can be guaranteed without relying on the correctness of quantum theory.
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.