LESS REALITY, MORE SECURITY

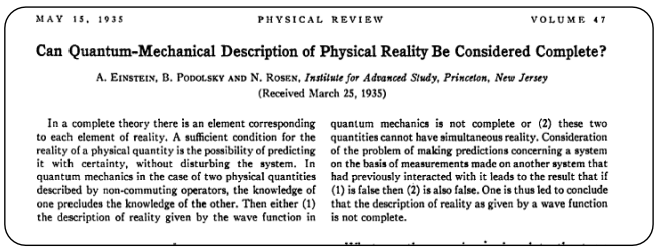
ARTUR EKERT

'No way, we will never use anything that we cannot dissect into pieces, scrutinize and certify ourselves. Even if it comes from No Such Agency across the pond. You see, cryptography is a serious business and we must be absolutely sure that the stuff is clean; no Trojan horses, no fancy quantum back-doors, nothing of that kind, nada.' Unaccustomed as he was to dealing with academia, Charlie, (not his real name, of course), to his credit, was exceptionally open minded. He poured me another glass of wine and added in a more reconciliatory tone. 'But, I would love to understand how on earth a device of unknown provenance, manufactured by enemies, you say, can be put into a good use, without even knowing how it works. This is, to say the least, bizarre.' The hour was still young and I was in no rush, the wine was good[1], so I started from the very beginning.

1. I would rather be a cobbler...

The year was 1935 and by then Albert Einstein could hardly argue with the success of quantum theory. Yet he felt very strongly that it was "not yet the real thing", not a complete theory, for its mathematics could not describe individual events. Given the most precise description possible of how things are now, the most you can do is predict the probability that things will turn out one way or another. Einstein found it very disturbing. For over a decade he had been refining his arguments against the indeterminism of quantum theory and finally he played his trump card.

On March 25, 1935, John Tate, the editor of the Physical Review, received a paper which Einstein co-authored with his younger Princeton colleagues, Boris Podolsky and Nathan Rosen. The log books of Physical Review show that the EPR paper, as it has been known since, bypassed the refereeing process and went straight to press. Four printed pages of beautifully constructed argument appeared in the May 15 issue [1]. They were heralded by a brief article in the New York Times titled "Einstein Attacks Quantum Theory". And so he did.



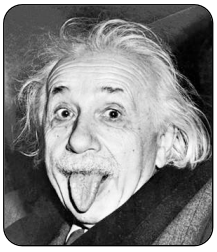
MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. Einstein, B. Podolsky and N. Rosen, *Institute for Advanced Study, Princeton, New Jersey*

(Received March 25, 1935)

In a complete theory there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system. In quantum mechanics in the case of two physical quantities described by non-commuting operators, the knowledge of one precludes the knowledge of the other. Then either (1) the description of reality given by the wave function in quantum mechanics is not complete or (2) these two quantities cannot have simultaneous reality. Consideration of the problem of making predictions concerning a system on the basis of measurements made on another system that had previously interacted with it leads to the result that if (1) is false then (2) is also false. One is thus led to conclude that the description of reality as given by a wave function is not complete.



Physics, Einstein believed, describes objective reality, not our perception of reality. Physical objects do exist, they do have physical properties, and these properties can be quantified. Take, for example, polarization. It is a physical property of a photon and when measured it can take two values ± 1, in the units of $\hbar$. In fact, there are many different types of polarizations, parameterized by all possible directions along which polarization can be measured. And each of these polarizations

[1] Anthonij Rupert Cabernet Franc 2005, one of the best things South Africa can offer.

should have an objective value, $+1$ or -1, that is revealed by an appropriate measurement. Thus there is no room for any inherent randomness here, for if the value of a given polarization does exist prior to the measurement then the measurement simply uncovers it. Conversely, if the result of the measurement is inherently unpredictable— if two identical measurements on two identically prepared photons give different results—then one may assume that there is a problem with our description of reality. We must be missing something, our description must be incomplete.

This line of argument hinges on the interpretation of phrases such as "the value does exist". The EPR paper offered a carefully worded definition:

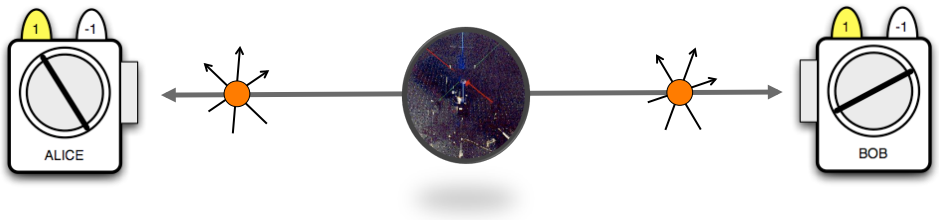
> If, without in any way disturbing a system, we can predict with certainty the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity.

The paper then went on to demonstrate that there are cases where one can establish the existence of the "element of reality" of physical quantities, such as position and momentum, so that their values exist, and yet when these quantities are measured the results are random. Here we rephrase the original argument in terms of polarizations. Think about two photons, labeled A and B. One can prepare a pair of photons in such a way that the measurement of polarization on B provides precise information about the value of a corresponding polarization of A. Moreover, because the two photons can be far apart from each other the measurement on B cannot disturb A. This is the EPR locality requirement, which, in its original form, reads: "The real factual situation of the system A is independent of what is done with the system B, which is spatially separated from the former". Thus there is an element of reality corresponding to the polarization of A. This polarization has a certain value and, it follows from the locality requirement, this value must exist even if the measurement on B is not performed. Still, the best quantum theory can do is to make statistical predictions whenever the polarization of A is measured directly.

For Einstein this exposed the provisional character of quantum theory, for things don't just happen and "God does not play dice with the universe". The world, he firmly believed, might be inordinately complicated, but at the bottom of it there should be order and predictability. If chance were to replace causality, then, as far as Einstein was concerned, the rational basis of science had been swept away and he'd "rather be a cobbler, or even an employee in a gaming house, than a physicist".

2. For whom the Bell tolls

Thirty years later the EPR argument was turned into a refutable proposition. The world evolving in a fully definite, fully predictable manner permits only certain types of correlations. The argument, originally proposed by John Bell [2], and subsequently slightly modified by John Clauser, Michael Horne, Abner Shimony, and Richard Holt [3], is deceptively simple and can be explained to anyone who knows something about probability but never came across quantum physics.



Alice and Bob, two characters with a predilection for wacky experiments, are equipped with polarization analyzers and sent to two distant locations. Somewhere in between them there is a source

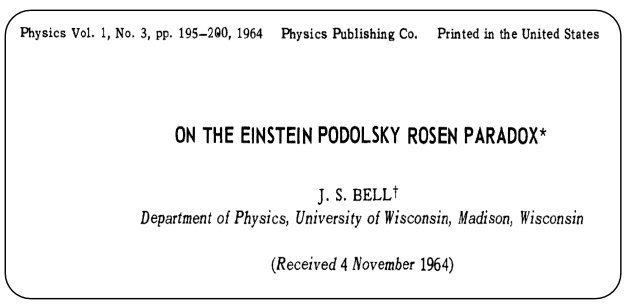
that emits pairs of photons that fly apart, one towards Alice and one towards Bob. Let us label the two photons in each pair as A and B respectively and let us assume that both A and B have well defined values of their polarizations. We ask Alice and Bob to measure one of the two pre-agreed polarizations. For each incoming photon, Alice and Bob choose randomly, and independently from each other, which particular polarization will be measured. Alice chooses between A_1 and A_2, and Bob between B_1 and B_2. Each polarization has value $+1$ or -1 thus we are allowed to think about them as random variables A_k and B_k, $k = 1, 2$, which take values ± 1. Let us define a new random variable S,

$$S = A_1(B_1 + B_2) + A_2(B_1 - B_2). \tag{1}$$

It is easy to see that one of the terms $B_1 \pm B_2$ must be equal to zero and the other to ± 2, hence $S = \pm 2$. The average value of S must lie somewhere in-between, i.e.

$$-2 \leq \langle S \rangle \leq 2. \tag{2}$$

That's it! Such a simple mathematical statement about correlations, to which we refer simply as Bell's inequality, and yet so profound. No quantum theory involved because Bell's inequality is not specific to quantum theory; it does not really matter what kind of physical process is behind the appearance of binary values of A_1, A_2, B_1 and B_2.

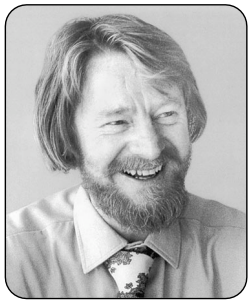

Physics Vol. 1, No. 3, pp. 195–200, 1964 Physics Publishing Co. Printed in the United States

ON THE EINSTEIN PODOLSKY ROSEN PARADOX*

J. S. BELL†

Department of Physics, University of Wisconsin, Madison, Wisconsin

(*Received* 4 *November* 1964)



In fact, instead of photons and polarization analyzers Alice and Bob may be given sealed, impregnable boxes each. The inner working of the boxes is unknown but the exterior design is simple — a big knob with two settings, a 'read' button to press, and two light bulbs labelled as $+1$ and -1. Alice and Bob can then take the boxes into their respective locations, turn the knobs between the two allowed settings, press the buttons and watch the boxes responding with flashes of light. For example, for the first reading Alice and Bob may choose settings A_1 and B_2 respectively. When they press their 'read' buttons the boxes generate outcomes, say, Alice's box flashes $+1$ and Bob's -1. They record the settings and the results, and repeat the process until they accumulate a sufficiently large amount of data to evaluate relative frequencies of different outcomes. The boxes may respond in a correlated manner, the correlations can be estimated, and Bell's inequality can be checked. Technical details of the hardware are irrelevant. The focus is on correlations alone and, surprisingly enough, there are correlations that violate Bell's inequality.

3. Hello world, are you there ?

So, what does it take to violate Bell's inequality? We know that violation of Bell's inequality is inconsistent with assigning numerical values to A and B prior to these values being actually

registered. This said, we still may be able to assign numerical values to correlations $\langle AB\rangle$. If we take this unorthodox approach then the expression

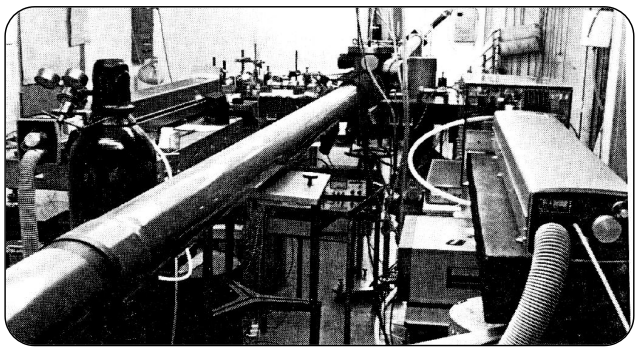
$$\langle S\rangle = \langle A_1B_1\rangle + \langle A_1B_2\rangle + \langle A_2B_1\rangle - \langle A_2B_2\rangle. \tag{3}$$

admits ± 4 as its two extreme values. This happens, for example, when the first three correlations on the right hand side take value $+1$ and the last one -1 (or vice versa). However, generating correlations of this kind involves either instant communication between distant objects or inherent randomness, or both.

Instant communication is hard to swallow. It means that, say, Alice by making a choice between A_1 and A_2 affects Bob's results. Bob can immediately 'see' what Alice 'does'. For example, Bell's inequality is maximally violated when A_1, A_2 and B_1 are fixed at $+1$ and B_2 takes value $+1$ when measured together with A_1 and -1 when measured together with A_2. Thus, unlike the other three variables, B_2 does not have any pre-determined numerical value of its own. The registered value is contextual as it depends on what was chosen to be measured by Alice. Indirectly, it implies that in order to avoid a logical contradiction Alice must not be able to measure both A_1 and A_2. Moreover, Alice, choosing between A_1 and A_2, can signal one bit of information to Bob in no time. It gets even more weird when one realizes that numerical values B_1 or B_2 depend on Alice's choices even if the choices are made after the values B_1 or B_2 are registered! Any physical theory that allows such instant influences creates more problems than it was meant to solve. We let it rest and try randomness instead.

In order to rule out any instant signaling we must let the results registered by Alice and Bob to be completely random and unpredictable. They may be correlated though. For example, they may register values A and B, such as $(+1,+1)$ or $(-1,-1)$, with equal probability. We can easily show that correlations of this kind can offer the maximal violation of Bell's inequality without any instant communication. For example, let the values of A_2 and B_2 be random but always different from each other, $A_2B_2 = -1$, and let all the remaining variables be random but always identical, $A_1B_1 = A_1B_2 = A_2B_1 = 1$. This gives $\langle S\rangle = 4$. But this inherent randomness is equally mind-boggling. If things just happen and numerical values appear out of the blue then they did not "exist" prior to being recorded. Would nature support such correlations?

Nature, it seems, embraces randomness and permits correlations that violate Bell's inequality but the violation is a modest one, far short of $\langle S\rangle = 4$. And this, to be sure, has been observed in a number of painstaking experiments [4–7]. The early efforts were truly heroic, and the experiments had many layers of complexity (below Alain Aspect and his laboratory in Orsay, near Paris).



Today, however, such experiments are routine. For example, in a process called "parametric down conversion" a photon from a laser beam enters a beta-barium-borate crystal and gets absorbed

while it excites an atom in the crystal. The atom subsequently decays, emitting two "polarization-entangled" photons, so that if the polarization analysers A and B are set θ degrees apart then the results agree ($AB = 1$) with probability $\sin^2\theta$ and hence differ ($AB = -1$) with probability $\cos^2\theta$. This experimental fact is consistent with quantum mechanical predictions, assuming the photons are prepared in the so-called singlet state. This gives the correlation coefficient $\langle AB\rangle = \sin^2\theta - \cos^2\theta = -\cos 2\theta$. Correlations of this kind cannot be used to send instantaneous messages but they do violate Bell's inequality. Choose angles 0, $\pi/4$, $\pi/8$ and $3\pi/8$ for A_1, A_2, B_1 and B_2 respectively and you obtain $\langle S\rangle = -2\sqrt{2}$. This, by the way, is the maximal violation that quantum correlations can offer.

Thus if we accept the EPR definitions of reality and locality then we have no choice but to admit that God is an inveterate gambler who throws the dice on every possible occasion. In spite of this, we may find some consolation in harnessing this randomness and putting it into a good use. And this, finally, brings us to cryptography.

4. Less reality, more security

The first practical application of Bell's inequality was in the spooky art of secret communication [8]. With a benefit of hindsight it is not very surprising. Information is always represented by measurable physical properties and if such properties exist then, following the EPR definition of the element of reality, their value can be predicted with certainty "...without in any way disturbing a system..." This is just a description of a perfect eavesdropping. Conversely, if such properties do not exist prior to measurements, then there is nothing to eavesdrop on. This was the basic idea that led me to the development of a new tool for detecting eavesdropping.

The most secure methods of communication rely on pre-distributed, random and secret sequences of bits, known as cryptographic keys. Once Alice and Bob, the same who like wacky experiments, share a secret key they can use it to encrypt messages and communicate secretly over any public, unprotected, channel. For example, given the key (1100101) Alice can encrypt her binary message, say (1011100), by combining each bit of the message with the respective bit of the key, according to the rules of addition in base 2, that is, $1 + 1 = 0$.

$$\begin{array}{cccccccc} & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ + & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ \hline & 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{array}$$

The resulting cryptogram (0111001), can be then publicly transmitted to Bob, who can recover the message by adding (in base 2 again) the cryptogram and the key. The key is a random sequence of 0's and 1's, and therefore the resulting cryptogram—the plaintext plus the key—is also random and completely scrambled unless one knows the key. Both Alice and Bob must have exact copies of the key beforehand; Alice needs the key to encrypt the plaintext, Bob needs the key to recover the plaintext from the cryptogram. Eve, an eavesdropper, who has intercepted the cryptogram and knows the general method of encryption but not the key, will not be able to infer anything useful about the original message. The secrecy of communication depends entirely on the secrecy of the key. Indeed, one can prove that if the key is secret, the same length as the message, truly random, and never reused, then this method of encryption, known as the one time pad, is unbreakable. However, this implies that new keys must be repeatedly generated and distributed. The problem of getting the key from Alice to Bob without Eve intercepting it had become an expensive logistical issue for banks, governments and the military. Can Alice and Bob distribute the keys and detect eavesdropping? Yes, they can. They can do it with *any* set-up that produces binary data and violates Bell's inequality. For example, with the sealed boxes of unknown provenance, that were described before.

The key distribution protocol is basically equivalent to taking the boxes into their respective locations and running the test of Bell's inequality, but then the test is run only on some portion of the recorded data; the remaining part is used to distill a secret key [8, 9]. Thus Alice and Bob repeatedly choose one of the settings of their knobs and press 'read' button to register the result. They keep a detailed record of the settings and the corresponding results. Then they communicate in public and agree on a random sample of the recorded data that is subsequently revealed to estimate the correlations and the degree of the violation of Bell's inequality. If the violation of Bell's inequality is observed then the remaining results, which were recorded but not communicated in public, remain secret. They were never read by anyone, because, before they were registered they did not exist. They can be turned into a secret key.

Eve may have manufactured the boxes and pre-programed their responses but she could not predetermine the results registered by Alice and Bob. We know this, because if the results had existed in the program in any form, be it directly or as a computational procedure, then Bell's inequality would have been satisfied. So how come Eve, who has control upon just about everything, cannot learn the key? Surely there must be something upon which she has no control, something that is essential for the security of the whole scheme? Indeed, there is, and this something is called "free will". Each binary outcome registered by Alice is obtained for a randomly chosen setting of the knob; her choice is free and independent from that of Bob. The same holds for Bob. This fact is absolutely crucial. If Alice's and Bob's choices were known in advance then Eve can easily pre-program the results of the pre-determined measurements, so that Bell's inequality would be violated and Alice and Bob would foolishly believe that they generated a secret key. However, as long as Alice's and Bob's choices are their own, unknown and unpredictable, then the most mind-boggling cryptographic scheme ever proposed works just fine.

5. Yes, we can

The fact that the conclusions drawn from Bell's inequality are independent from how exactly the recorded results were generated takes cryptography to an entirely different level, even when compared with the quantum "prepare and measure" cryptography [10]. Although the key distribution protocol is basically the same as the one I proposed some time ago [8] more recent work by Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio and Valerio Scarani [9] gives it an entirely new twist. It shows that the original protocol is in fact much more powerful than originally anticipated. It makes seemingly insane scenario possible — devices of unknown or dubious provenance, even those that are manufactured by our enemies, can be safely used for secure key distribution. This is a truly remarkable feat, also referred to as the "device independent" key distribution. Can we implement it? Yes, we can! But there are several questions of practical nature that must be addressed before we can push cryptography to the "device independent" limit.

Does any violation of Bell's inequality guarantee secrecy? If quantum theory is all that there is, then the maximal violation allowed, $|\langle S\rangle| = 2\sqrt{2}$, implies both perfect randomness and perfect security. Anything less than that may contain corrupted correlations, in which some bits may be known to an adversary. Still, as long as we can estimate how many bits are compromised we can use a number of cryptographic techniques, such as error correction combined with hashing, to distill a secret key. As it happens, the amount of information available to the adversary is related directly to the degree of violation of Bell's inequality [9]. Thus the key distillation is possible with the usual price to pay, namely, the length of the key. After error correction and hashing it will be much shorter than the number of registered outcomes.

We have already mentioned that violation of Bell's inequality is an experimental fact. What is it then, that prevents us from running the experiments that violated Bell's inequality again, but this time under the label of 'device-independent' key distribution? Convincing that they were, these experiments still left 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 so-called 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 [11, 12], however, truth to be told, the ultimate violation of Bells inequality, that is a single experiment that closes all the loopholes at once, is still missing. But nature would have to be very malicious if it were to cheat us selectively; on locality in some experiments and exploring detection loopholes in some other. In contrast, an eavesdropper has all the rights to be malicious.

Our colleagues, who set up the experiments, knew their equipments very well and exercised total control over all the components. They could hardly be duped by nature, by sources or detectors conspiring against them and producing misleading data. Alice and Bob are in a very different situation. With the two impregnable boxes they are at the mercy of Eve. In this adversarial setting a proper experimental demonstration of the "device-independent" cryptography requires a proper violation of Bell's inequalities, without any loop-holes and the like. This is in particular 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 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. This goal challenging but perfectly achievable, is currently the subject of experimental investigations in a number of quarters.

Last but not least—even if one day quantum physics is refuted and superseded by a new theory, even then, as long as the new theory does not admit any instant communication, we can use Bell's inequality as an indicator of secrecy. In a truly pioneering work, Jonathan Barrett, Lucien Hardy and Adrian Kent showed that a technologically advanced eavesdropper, limited only by the impossibility of superluminal signaling, who uses post-quantum physics to manufacture and pre-program the boxes, cannot fool Alice and Bob [13]. The security which stems from violation of Bell's inequality transcends the borders of quantum theory. New, more refined security proofs, most notably those by Lluís Masanes [14], apply to any non-classical cryptography, which includes both quantum cryptography and possibly the future post-quantum cryptography. The sheer fact that Bell's inequality allows us to make sensible statements about security of devices operating according some yet to be discovered laws of physics is amazing.

6. Epilogue

'So, Charlie, if your mortal enemy, or, for that matter, a friendly agency, offers you a pair of impregnable boxes that generate correlations which violate Bell's inequality do not hesitate, take them, you will be able to put them into a good use, without even knowing how they work.' Charlie looked down into an empty glass. 'Yeah, amazing', he mumbled. 'My head is spinning.' It was not clear whether he referred to the effect of wine or to my story. 'This reality, or rather lack of it, sounds very, very dodgy. For one thing, Einstein, such a smart guy, and yet you are telling me that when it comes to quantum theory he got it all wrong?' I did not want to leave him with this impression. 'That would be too harsh' I said. 'After all, it required Einstein's insight to point at the features of nature which are so mind-boggling that even today, seventy five years later, we have problems to understand. The notion of "reality", as understood by Einstein and his colleagues, was probably too simplistic.' Then, with some trepidation, I added. 'If the formalism of quantum theory is anything to go by then one particular interpretation, proposed by Hugh Everett in 1956, indicates that "reality" is more complex, that everything that can possibly happen actually happens, and all possible outcomes of measurements have the same status [15]. In this multiplicity of "universes", often called the multiverse, Bell's argument, which requires a predetermined single outcome of a quantum experiment, simply does not make sense. However, even then, secure key

distribution is possible, albeit, with so many copies of Alice, Bob and Eve, the notion of secrecy requires somewhat different interpretation. Would Einstein embrace the multiverse? I think so but we will never know for sure.' For a moment Charlie looked at me with bewilderment in his eyes, then, without saying a word, he arose from the table and walked out of the bar...

References

[1] A. Einstein, B. Podolsky, and N. Rosen, *Can quantum-mechanical description of physical reality be considered complete?*, Phys. Rev. **47** (1935), no. 10, 777–780.

[2] J. S. Bell, *On the Einstein Podolsky Rosen paradox*, Physics **1** (1964), no. 3, 195–200.

[3] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Proposed experiment to test local hidden-variable theories*, Phys. Rev. Lett. **23** (1969), no. 15, 880–884.

[4] S. J. Freedman and J. F. Clauser, *Experimental test of local hidden-variable theories*, Phys. Rev. Lett. **28** (1972), no. 14, 938–941.

[5] A. Aspect, P. Grangier, and G. Roger, *Experimental tests of realistic local theories via Bell's theorem*, Phys. Rev. Lett. **47** (1981), no. 7, 460–463.

[6] ———, *Experimental realization of Einstein–Podolsky–Rosen–Bohm Gedankenexperiment: A new violation of Bell's inequalities*, Phys. Rev. Lett. **49** (1982), no. 2, 91–94.

[7] A. Aspect, J. Dalibard, and G. Roger, *Experimental test of Bell's inequalities using time- varying analyzers*, Phys. Rev. Lett. **49** (1982), no. 25, 1804–1807.

[8] A. Ekert, *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett. **67** (1991), no. 6, 661–663.

[9] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, *Device-independent security of quantum cryptography against collective attacks*, Phys. Rev. Lett. **98** (2007), no. 23, 230501.

[10] C. H. Bennett and G. Brassard, *Quantum cryptography, public key distribution and coin tossing*, Proceedings of international conference on computer systems and signal processing, 1984, pp. 175–179.

[11] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, *Violation of Bell's Inequality under Strict Einstein Locality Conditions*, Phys. Rev. Lett. **81** (1998), no. 23, 5039–5043.

[12] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland, *Experimental violation of a Bell's inequality with efficient detection*, Nature **409** (2001Feb), no. 6822, 791–794.

[13] J. Barrett, L. Hardy, and A. Kent, *No Signaling and Quantum Key Distribution*, Phys. Rev. Lett. **95** (2005), no. 1, 010503.

[14] L. Masanes, *Universally-composable privacy amplification from causality constraints*, available at `arXiv:0807.2158`.

[15] H. Everett III, *"Relative State" Formulation of Quantum Mechanics*, Rev. Mod. Phys. **29** (1957), no. 3, 454–462.

Mathematical Institute, University of Oxford & Centre for Quantum Technologies, National University of Singapore.