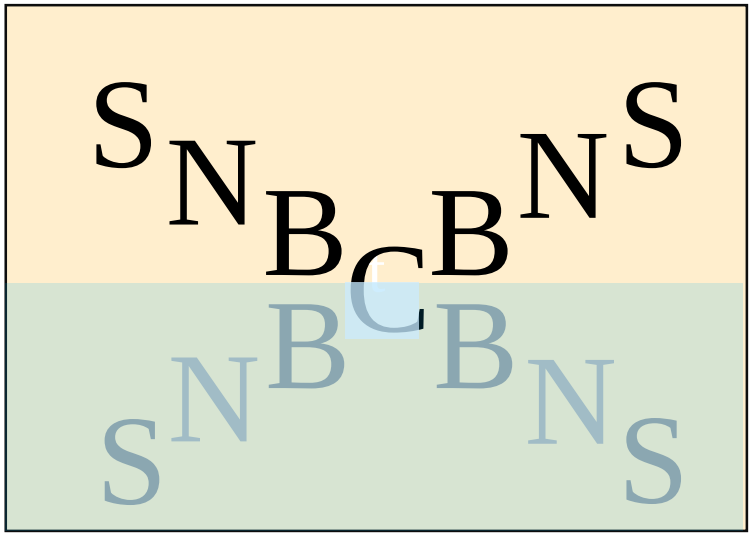
Forging the Culture of Quantum Information

Charles H. Bennett
IBM Research Division

S. N. Bose Center for
Basic Natural Sciences
2 February 2018



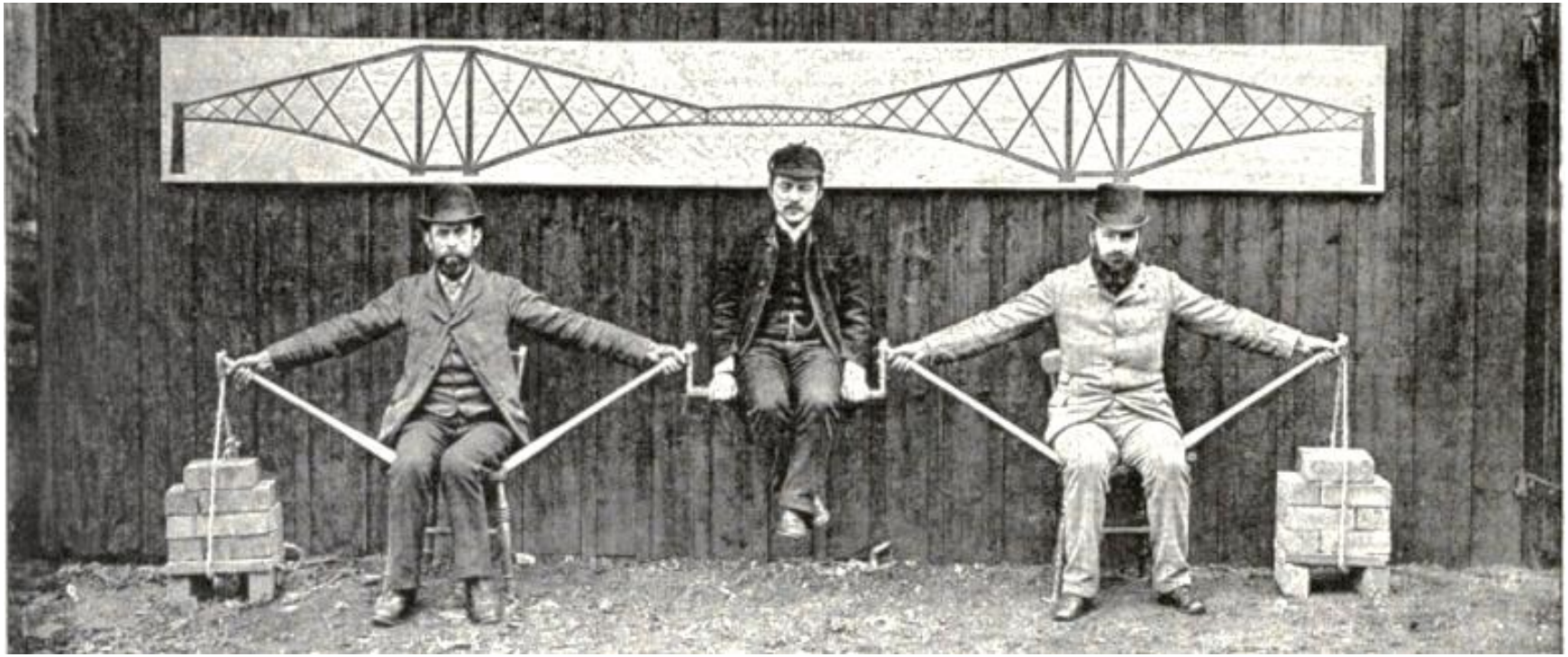
Physicists, mathematicians and engineers, guided by what has worked well in their respective disciplines, acquire different scientific tastes, different notions of what constitutes a well-posed problem or an adequate solution.

While this has led to some frustrating misunderstandings, it has invigorated the theory of communication and computation, enabling it to outgrow its brilliant but brash beginnings with Turing, Shannon and von Neumann, and develop its own mature scientific taste, adopting and domesticating ideas from thermodynamics and especially quantum mechanics that physicists had mistakenly thought belonged solely to their field.

And, speaking of Engineers...

Why smart curious people like us should browse **and edit** Wikipedia

This morning, while researching my favorite (Howrah) bridge, I happened upon this circa 1890 illustration of how such bridges work.



"The suspended span, where Kaichi Watanabe sits, is seen in the center. The need to resist compression of the lower chord is seen in the use of wooden poles while the tension of the upper chord is shown by the outstretched arms. The action of the outer foundations as anchors for the cantilever is visible in the placement of the counterweights"—Wikipedia

In more detail:

- Anyone can edit it, really. If you register and begin to make edits, your subsequent edits will be taken more seriously.
- Many of the articles are reasonably good, and many of the introductions are **very** good. One can spend hours jumping from article to article, learning amazing things, and fixing others.
- Though it takes some time and effort to learn enough about Wikipedia guidelines and etiquette to make one's larger edits stick—e.g. backing up assertions likely to be contested with reliable secondary sources—it's easy and fun to make smaller edits that correct errors and improve clarity of exposition.
- Unfortunately, there are a good many obstructionists who resist all changes, even improvements, to articles they think they own, and these amateurs have more time to argue than you. But the guidelines favor you, not them, and with tact and persistence you can win.
- Any improvement you make will benefit millions of people.

Theoretical computer scientists, like their counterparts in physics, suffer and benefit from a high level of intellectual machismo. They believe they have some of the biggest brains around, which they need to tackle some of the hardest problems.

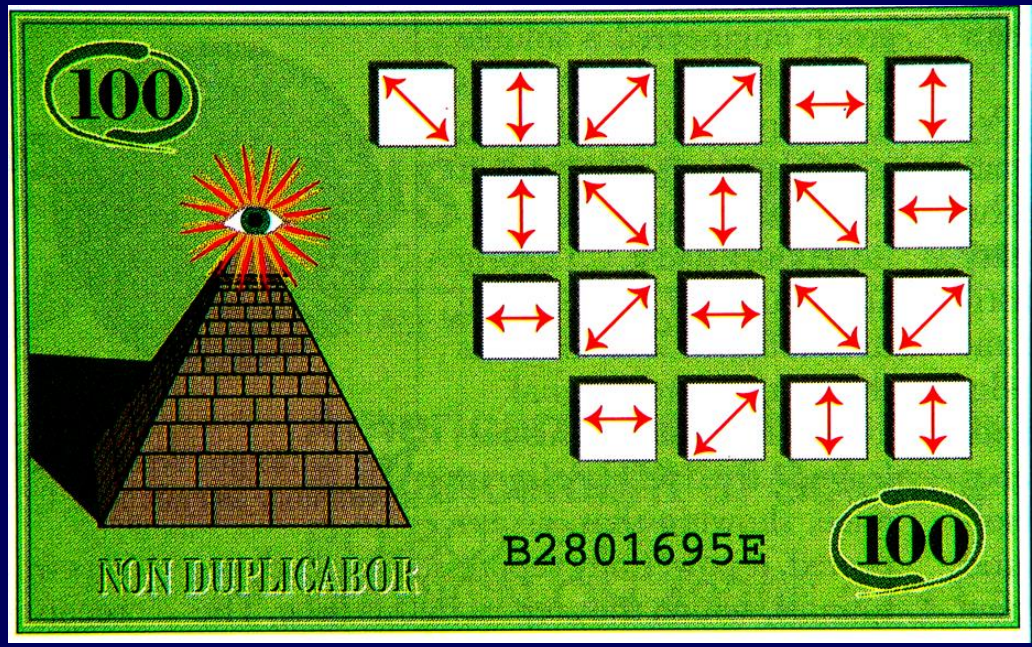
Like mathematicians, they prove theorems and doubt the seriousness of those who don't (e.g. physicists like me).

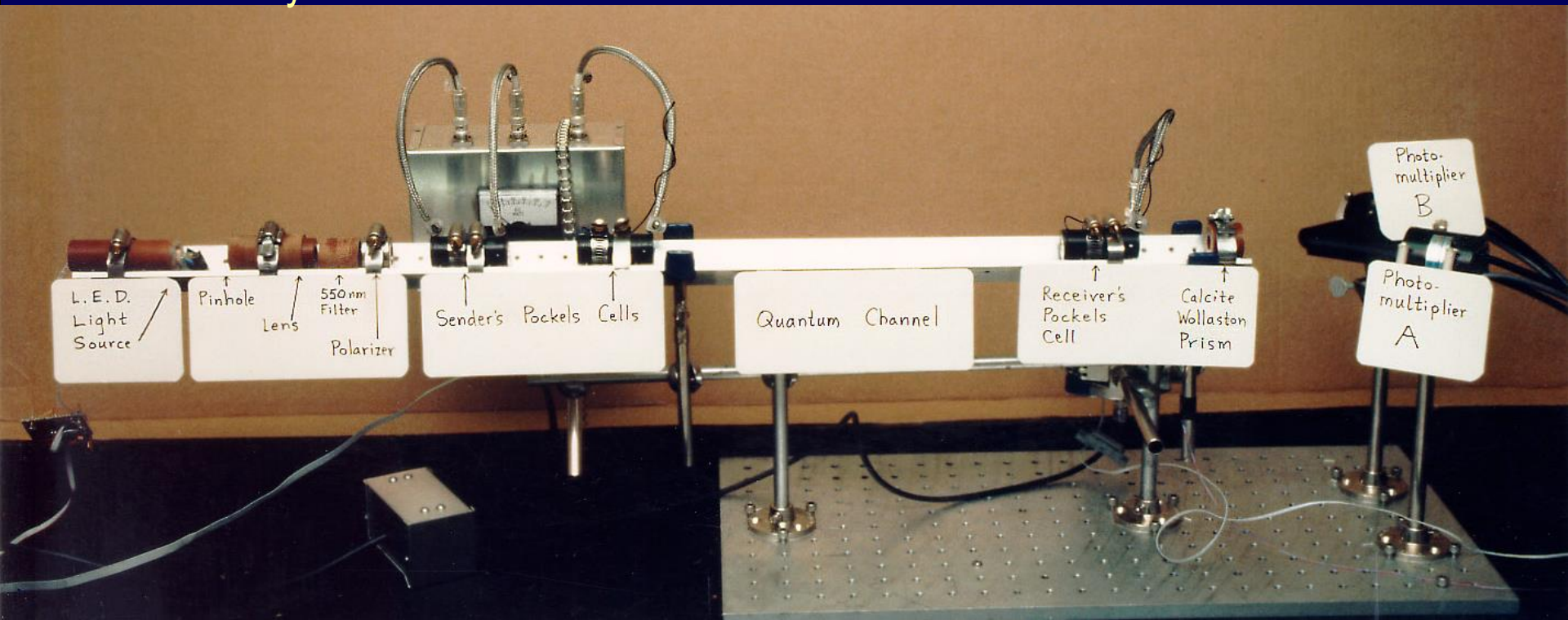
But beginning in the 1960's a few (e.g.Landauer, Wiesner, Feynman, and Deutsch) tried to bring physical ideas into informatics but were not well understood. Gilles Brassard was one of the first computer scientists to take these ideas seriously.

Since then the productive friction between the cultures of physics, mathematics and engineering has produced more complete informatics, extending the old theory as subtly and beautifully as complex numbers extend the reals. But cultural adjustments are still being made.

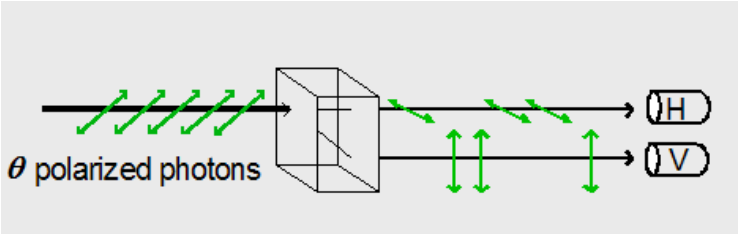
Quantum money (Wiesner ’70, ’83) cannot be copied by a counterfeiter, but can be checked by the bank, which knows the secret sequence of polarized photons it should contain.

Quantum cryptography uses polarized photons to generate shared secret information between parties who share no secret initially.





Bill Wootters' pedagogic analog for quantum measurement



Like a pupil confronting a strict teacher, a quantum system being measured is forced to choose among a set of distinguishable states (here 2) characteristic of the measuring apparatus.

Teacher: Is your polarization vertical or horizontal?

Pupil: Uh, I am polarized at about a 55 degree angle from horizontal.

Teacher: **I believe I asked you a question.** Are you vertical or horizontal?

Pupil: Horizontal, sir.

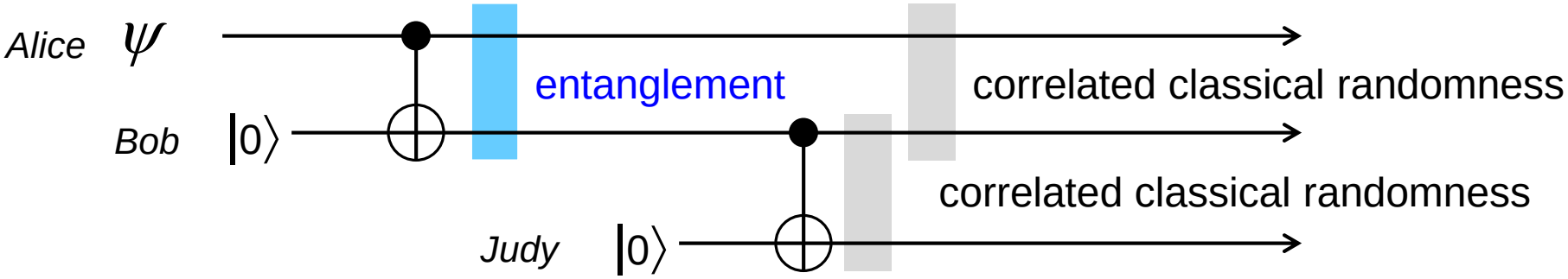
Teacher: Have you ever had any other polarization?

Pupil: No, sir. I was always horizontal.

The Monogamy of Entanglement

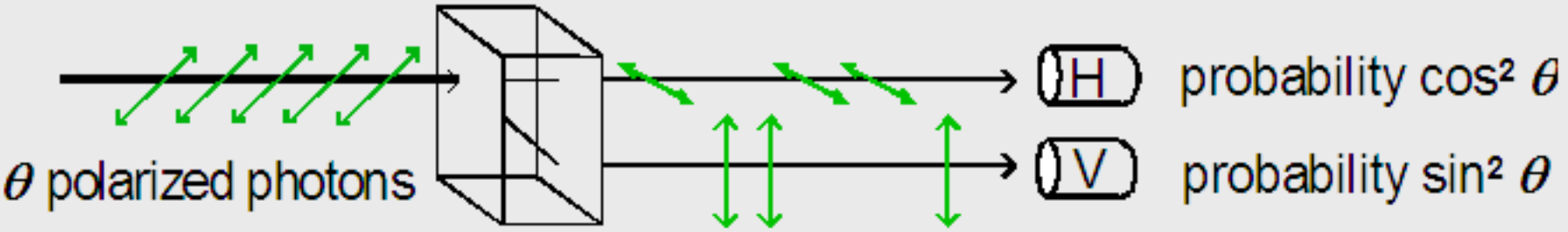
- If A and B are maximally entangled with each other, they can't they be entangled with anyone else.
- Indeed classical correlation typically arises from vain attempts to clone entanglement. If one member of an entangled pair tries to share the entanglement with a third party, each pairwise relation is reduced to mere correlated randomness.

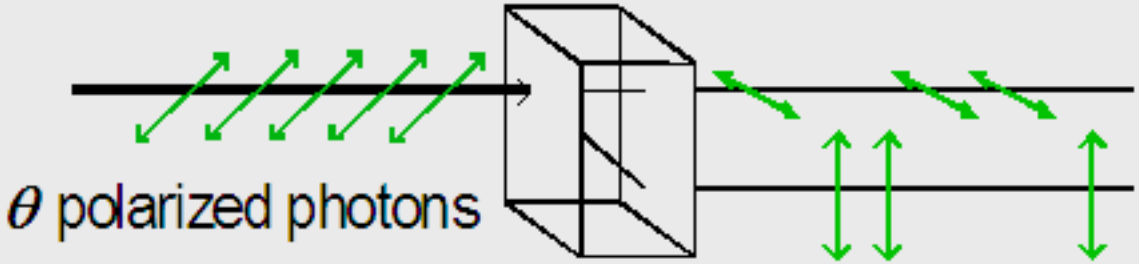
"Two is a couple, three is a crowd."



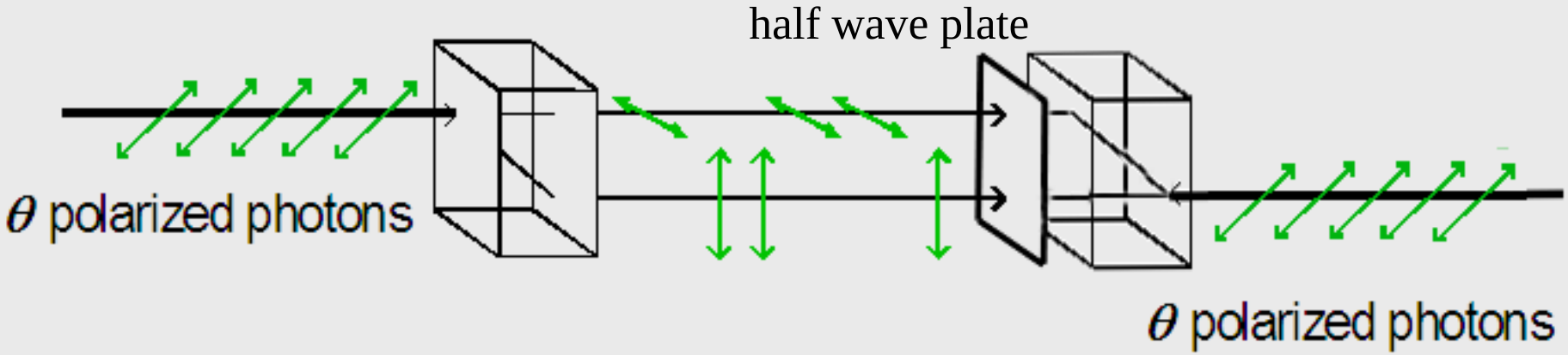
Bob ends up perfectly entangled, not with Alice or Judy, but with the now nontrivial *relationship* between them, an appropriate punishment.

Entanglement and the origin of Quantum Randomness





If no one observes the photons, their random "behavior" can be undone.



Metaphorically speaking, it is the **public embarrassment** of the pupil, in front of the whole class, that makes him forget his original polarization.

Entanglement is ubiquitous: almost every interaction between two systems creates entanglement between them.

Then why wasn't it discovered before the 20th century?

Because of its monogamy.

Most systems in nature, other than tiny ones like photons, interact so strongly with their environment as to become entangled with it almost immediately .

This destroys any previous entanglement that may have existed between internal parts of the system, changing it into mere correlated randomness.

The Einstein -Bohr debate: an early phase of the cultural adjustment that gave birth to quantum information theory

When the weird behavior of subatomic particles became evident in the early 20th century, Niels Bohr argued that physicists must learn to accept it. There were two kinds of weird behavior: indeterminacy, and entanglement. Einstein was deeply troubled by both disparaging indeterminacy as "God playing dice," and entanglement as "spooky action at a distance." He spent his remaining years searching unsuccessfully for a more naturalistic theory, where every effect would have a nearby cause. Newton's mechanics, Maxwell's electromagnetism, and his own relativity share this common-sense property, without which, Einstein thought, science could no longer aspire to be an orderly explanation of nature.

Meanwhile the rest of the physics community, including greats like Schrödinger, Heisenberg, and Dirac, followed Bohr's advice and accepted these disturbing phenomena, and the mathematics that explained them, as the new normal.

Einstein disliked quantum mechanics, and his distaste for it, together with his fame (being the only 20th century scientist whose name is a household word) which helped people grasp relativity, retarded their grasp of quantum mechanics and especially entanglement. Even in the 21st century most science journalists are clueless about it.

Einstein thought entanglement was spooky (*spukhafte Fernwirkung*), but his wrong take on it, as action at a distance, refuses to die. That's *spukhafte Spätwirkung.*

Mistakenly believing entanglement could be used for long-range communication, Nick Herbert published a paper in 1982 and Jack Sarfatti tried to patent this imagined application of it. The swift refutation of these proposals, by Dieks, Wootters and Zurek, is part of what led to modern quantum information theory. But this wrong idea, like perpetual motion, is so appealing that it is perpetually being "rediscovered".

The long-delayed understanding of entanglement, by scientists as well as lay people, is also manifest in the difficulty some otherwise accomplished scientists have in accepting proofs based on it, notably the No-Go theorem for quantum bit commitment.

Though Gilles and I had shown how to defeat a special case of bit commitment in 1984, for years we thought some other form of bit commitment might be possible, opening up what would have been exciting possibilities for other information-theoretically secure 2-party protocols. These hopes were dashed by the No-Go theorem of 1997, still being ineffectually contested as late as a month ago, based on "entanglement destruction by forced measurements".

Sarfatti's and Herbert's ideas about entanglement were so wrong that they facilitated the acceptance of the no-cloning theorem as a central fact about quantum information. The theorem had actually been proved in 1970, by J. L. Park, [Foundations of Physics, 1, 23-33, (1970)], but his paper went unnoticed until the theorem was rediscovered by Dieks and by Wootters and Zurek at a time more ripe for its importance to be appreciated.

Moral:
Bad ideas sometimes stimulate scientific progress.

Conversely, good ideas—indeed quantum mechanics itself—sometimes retard scientific progress.

My IBM mentor Rolf Landauer is known for discovering the thermodynamic cost of information erasure, thereby helping launch the theory of reversible computation, many of whose methods proved useful in quantum computation.

With an engineering and physics background, he became concerned with the problem of energy consumption and waste heat removal from computers. The 1981 Endicott conference, which he co-organized with Ed Fredkin and Tom Toffoli of MIT, got the Physics of Computation started as respectable discipline.

Physics of Computation Conference Endicott House MIT May 6-8, 1981

1 Freeman Dyson
2 Gregory Chaitin
3 James Crutchfield
4 Norman Packard
5 Panos Ligomenides
6 Jerome Rothstein
7 Carl Hewitt
8 Norman Hardy
9 Edward Fredkin
10 Tom Toffoli
11 Rolf Landauer
12 John Wheeler
13 Frederick Kantor
14 David Leinweber
15 Konrad Zuse
16 Bernard Zeigler
17 Carl Adam Petri
18 Anatol Holt
19 Roland Vollmar
20 Hans Bremerman
21 Donald Greenspan
22 Markus Buettiker
23 Otto Floberth
24 Robert Lewis
25 Robert Suaya
26 Stan Kugell
27 Bill Gosper
28 Lutz Priese
39 Madhu Gupta
30 Paul Benioff
31 Hans Moravec
32 Ian Richards
33 Marian Pour-El
34 Danny Hillis
35 Arthur Burks
36 John Cocke
37 George Michaels
38 Richard Feynman
39 Laurie Lingham
40 Thiagarajan
41 ?
42 Gerard Vichniac
43 Leonid Levin
44 Lev Levitin
45 Peter Gacs
46 Dan Greenberger

But Landauer had some ideas about mathematics which I think were as unproductive as Einstein's ideas about entanglement.

In blunt opposition to Wheeler's enigmatic and mystical "It from Bit", Landauer's favorite slogan was "Information is Physical." He took this to mean that mathematical concepts incapable of direct physical embodiment, such as the 2^{1000}th digit of pi, when there are not that many atoms in the universe, were of dubious reality and probably not worth thinking about.

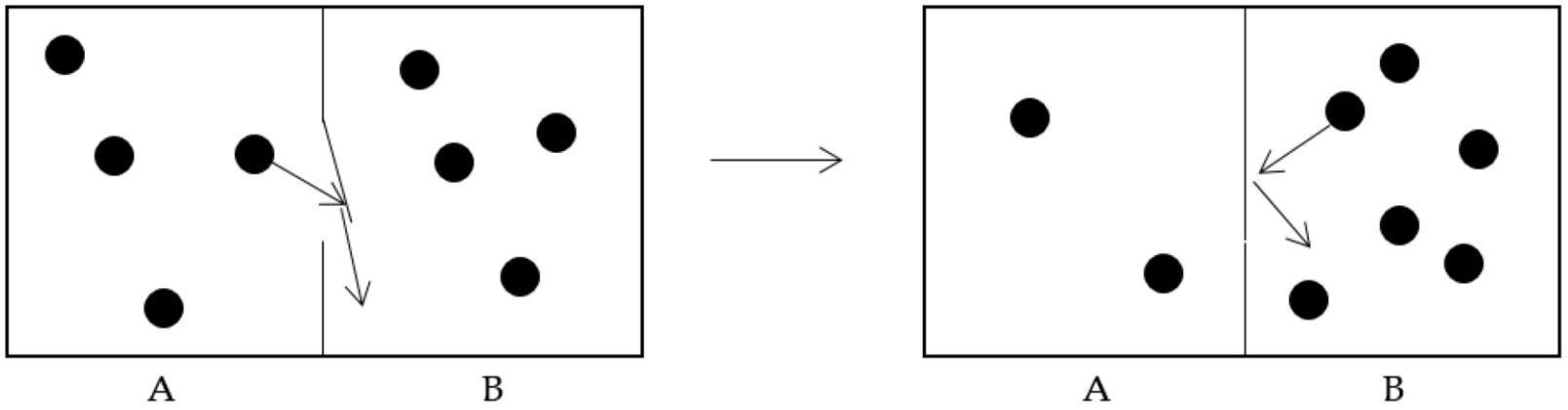
I told him this reminded me of the ancient Greeks' discomfort with infinity and irrational numbers, both concepts that later proved a very fruitful both theoretically and practically.

The analogy between computation and physical dynamics is very old. For example Galileo's "The book of nature is written in the language of mathematics" and Laplace's elegant description of a universe governed by Newtonian mechanics,

"We may regard the present state of the universe as the effect of its past and the cause of its future. An intellect which at a certain moment would know all forces that set nature in motion, and all positions of all items of which nature is composed, if this intellect were also vast enough to submit these data to analysis, it would embrace in a single formula the movements of the greatest bodies of the universe and those of the tiniest atom; for such an intellect nothing would be uncertain and the future just like the past would be present before its eyes."
Pierre Simon Laplace 1814

Note that this computation is deterministic and reversible, a feature seemingly lost with quantum indeterminism, but then recovered in a more inclusive form with unitary quantum evolution.

Smoluchowski's valve or ratchet version of Maxwell's Demon and his successful 1912 exorcism of it. A spring-loaded trap door, light enough to be pushed open by molecular impacts, would seem to violate the Second Law, effortlessly collecting molecules on the right in a pressure version of Maxwell's temperature demon.

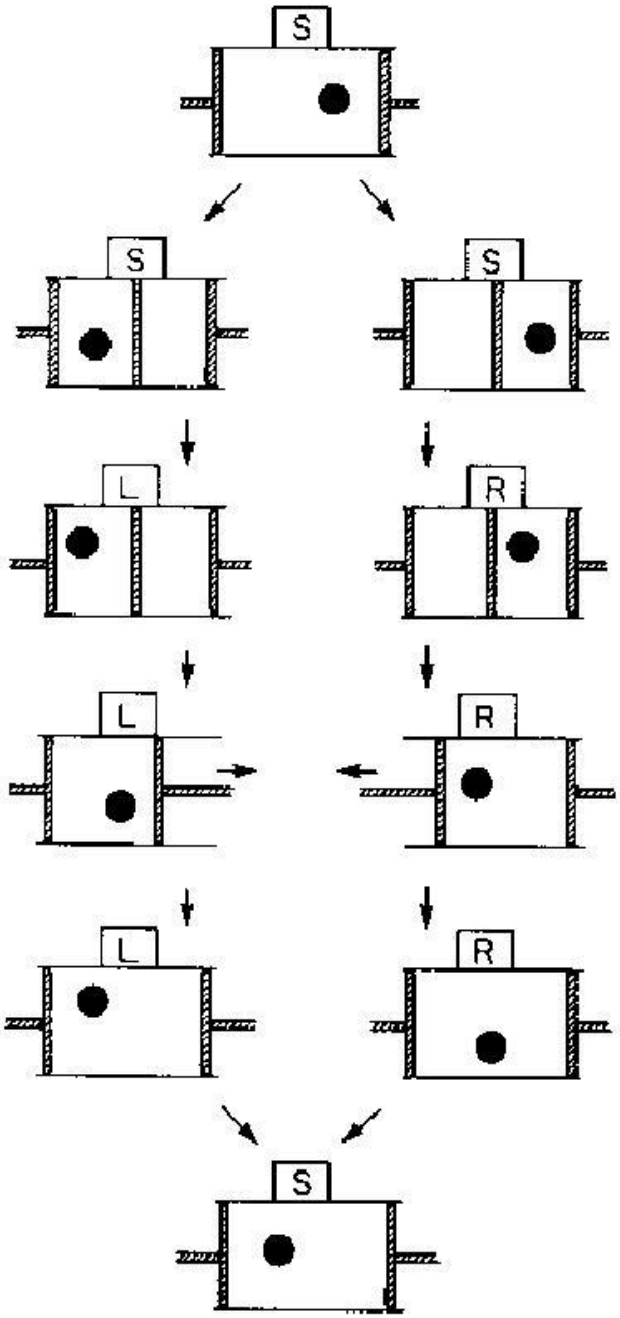


But, Smoluchowski argued, if the door were that light and the spring that weak, the door would soon heat up to the same temperature as the gas and undergo random motion of its own, swinging open and shut. It would then swing shut against a molecule that had wandered in front of it, pushing it to the left, just as often as it would be pushed open by a molecule striking it from the left, and there would be no net flow.

Despite Laplace's deterministic universe, whose vast mechanism presumably included the brains of all its inhabitants, early 20th century physicists became strangely reluctant to think of ***thought*** itself as a mechanistic process, causing Smoluchowski's correct exorcisim of the demon to unravel somewhat in subsequent decades. The title of Leo Szilard's 1929 paper, exemplifies this timidity

"On the decrease of entropy in a thermodynamic system by the intervention of intelligent beings."

The situation was further muddied by the discovery of quantum mechanics, which problematized the previously uncontroversial act of measurement. This tempted physicists to look for an irreducible cost of *information acquisition, transmission* or *processing*, when they would have done better to think like Smoluchowski. Even von Neumann incorrectly asserted in 1949 that each elementary act of information processing must have a thermodynamic cost of order kT ln 2. In 1961 Rolf Landauer correctly identified ***information destruction*** as the fundamentally costly act.



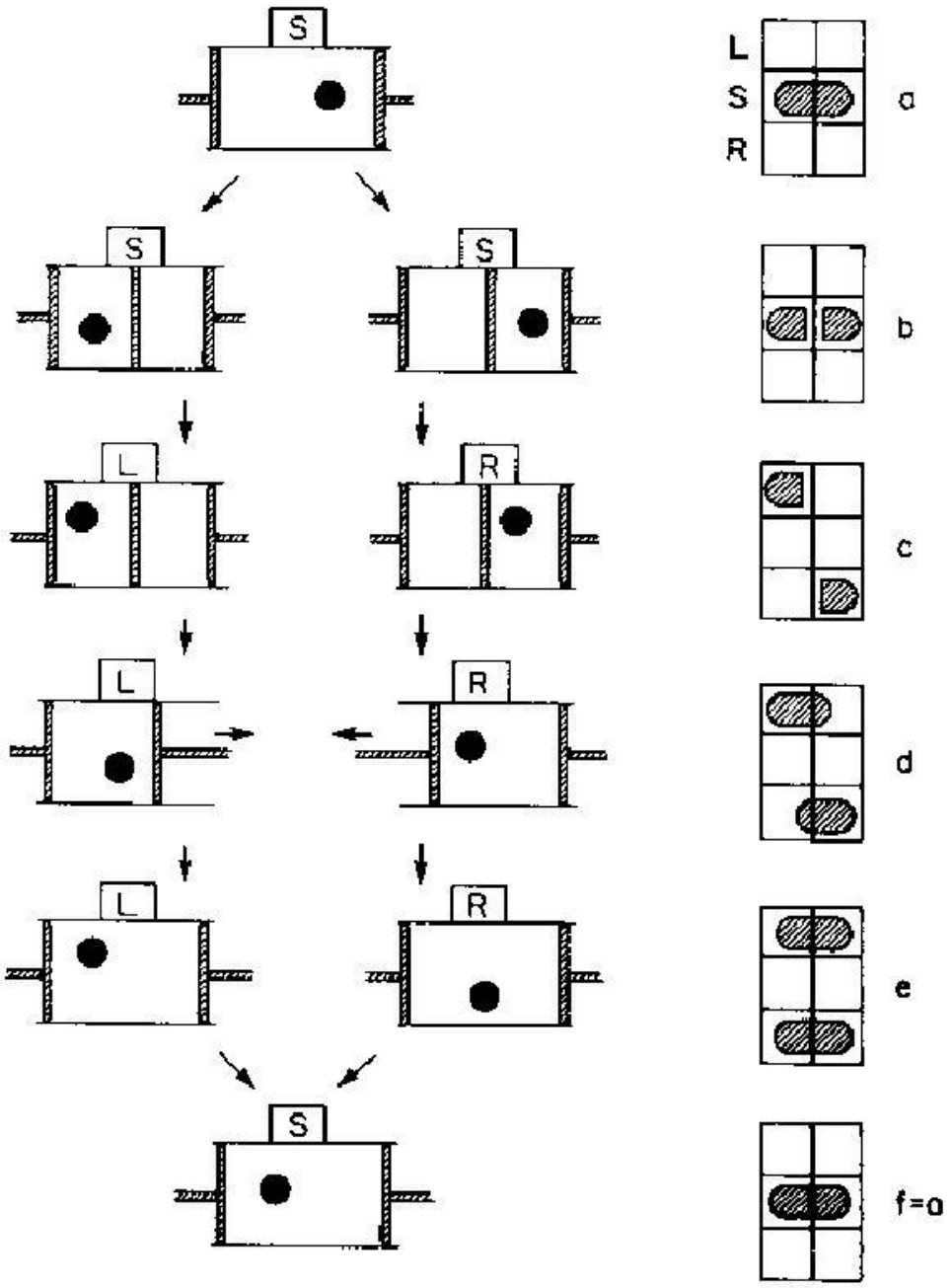
Sziliard's 1929 Engine, attempting to repeatedly extract isothermal work from a molecule.

Demon inserts partition in middle, trapping the molecule on one side or the other.

Measures and remembers which side molecule is on.

Inserts piston on opposite side, removes partition, then lets molecule do kT ln 2 of isothermal work pushing piston back to its original position.

Finally demon resets its memory and repeats the cycle



Joint phase space diagram of molecule and memory register shows how, if the register is initially in a standard blank state S, the measurement can be done reversibly, but the final step (f) of resetting the memory entails a compression of phase space that must pay back all the work gained step (d).

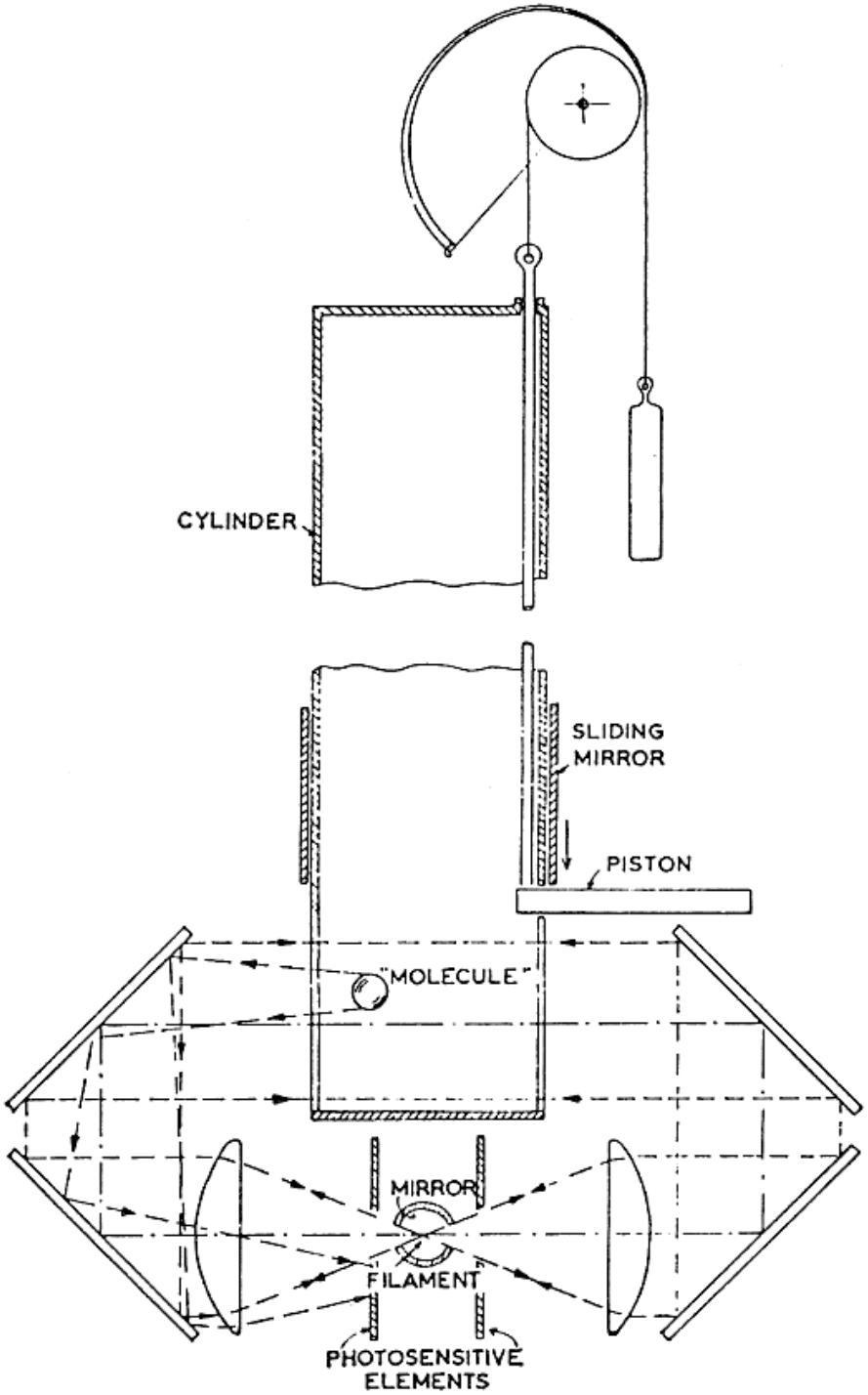
Szilard's 1929 paper made this clear in its equations, but unfortunately not its prose, so the notion that measurement is intrinsically irreversible persisted.

The Second Law of Thermodynamics has many avatars, manifestations that seem unrelated but in fact are equivalent

- Heat cannot, of itself, pass from one body to a hotter body. (Kelvin / Flanders & Swann)
- No physical process has as its sole result the conversion of heat into work. (Clausius)
- You can't see anything inside a uniformly hot furnace by the light of its own glow. (Kirchoff)
- No physical process has as its sole result the erasure of information. (Landauer / Schumacher)

Examples of that sloppy thinking due to misapplication of quantum mechanics to Maxwell's demon include Leon Brillouin's 1956 argument that to even see a molecule, against the background of quantum black body radiation at temperature T, a demon would need to expend at least one photon more energetic than kT.

Denis Gabor's 1961 refutation of his own high-compression version of Szilard's engine was the most intricately unnecessary invocation of quantum optics to prove what Smoluchowski had already proved.



Denis Gabor's high-compression Szilard engine (1961).

- Light beam circulates losslessly across one end of a long cylinder
- Photosensors detect when molecule wanders into the beam, and insert a piston to trap it there.
- Piston extracts $kT \ln (V/V_0)$ work by a very long isothermal power stroke.
- Some of the work is used to reset piston & recreate the light beam.
- Since it takes only a fixed amount of work **w** to do that, one can break the Second Law by making V so large that $kT \ln(V/V_0) > \mathbf{w}$.

What keeps it from breaking the 2nd Law?

Can you guess Gabor's answer? (hard)

Can you guess the correct answer? (easy)

*Answers to questions about Gabor's high-compression Szilard engine.

Correct answer: No trapping mechanism, whether mechanical (e.g. a mouse trap) or optical (Gabor's engine), can be completely irreversible. By the principle of Smoluchowski's trap door and Feynman's ratchet, the work **w** of resetting a trap, rather than being constant, must increase logarithmically with the compression ratio **V/Vo**, to keep the trap from running in the reverse of its intended direction.

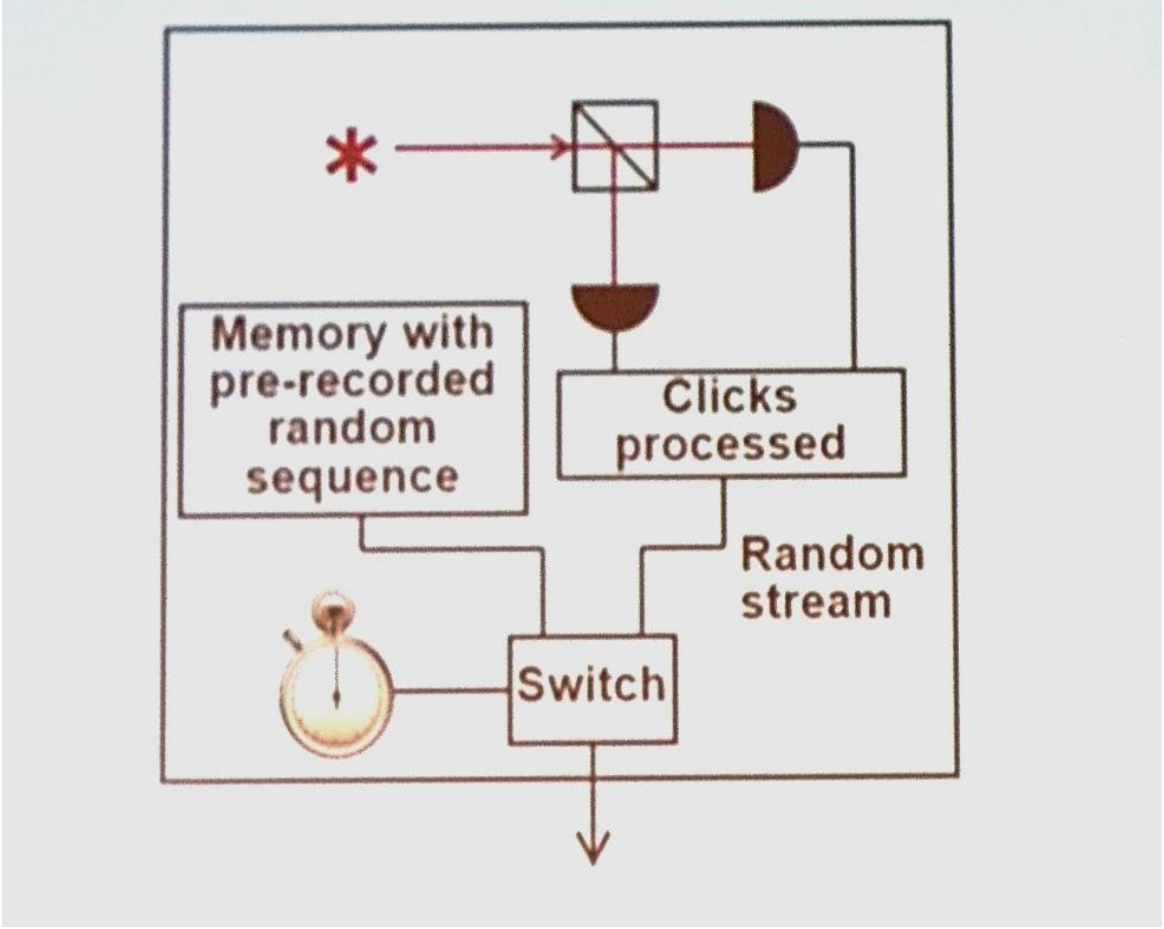
Gabor's 1961 answer instead invoked quantum optics, saying the longer the cylinder the more optical modes it has, and the more energy would be required to confine a light beam to one end of it. Though true, this implied that that quantum effects were necessary to save the second law, whereas simple considerations of reversibility suffice.

Though computer scientists and physicists communicate pretty well about quantum information and computation theory, there are still cultural problems in practical areas like cryptography. The undeserved popularity of device-independent (DI) protocols illustrates this. These are widely considered the gold standard for generating:

- *Private* random numbers known only to the person generating them, e.g. for passwords and crypto keys.
- *Shared* randomness certified to be known to Alice and Bob but no one else, as in QKD.
- *Public* randomness, as in the US NIST randomness beacon, random numbers which are unknown to anyone before generation, but become public information immediately afterward.

I will argue that DIY (do-it-yourself) randomness is better than DI randomness for most of these purposes.

Vadim Makarov with his sketch of a Trojan-horsed random number generator



This generator cannot be distinguished from an honest one by any test of its output, and would be hard to distinguish by opening and examining it, X-raying it, etc. It would be worthless for public or private use.

Trusting nature vs. trusting people.

Bell violations prove to whoever witnesses them that the randomness being generated is fresh and real, but, like a zero-knowledge proof, they do not enable that person to convince anyone else. A dishonest RNG manufacturer or beacon operator may have generated the data last year and sold them to an accomplice, who would use them to break a code or buy a "lucky" lottery ticket.

How can one build public trust?

For **private randomness**, build your own DIY RNG, and optionally XOR it with one or more commercial RNGs.

For **public randomness**, use several geographically and administratively independent local beacons.

- Each would follow a standard, like existing NIST beacon
- Several would be XORed or hashed together to generate a result unpredictable if even one component is honest.

DIY randomness sources made from commodity components (e.g. resistors, diodes, standard IC's) have a trust advantage over ones bought from an untrusted vendor. We need a **Public Standard** for DIY-RNGs that would include specifications for several kinds of DIY source, e.g. beamsplitter/APD, electronic shot noise, digitized acoustic noise from aerodynamic turbulence.

But how do we know these physical process are random enough?

It suffices to make conservative estimate of the source's min entropy, based on known physics, then use a randomness extractor to compress the raw digitized stream sufficiently, keeping in mind the dictum that nature is subtle but not malicious.

By contrast, in cryptology, one's adversaries are wlog both subtle and malicious.

The tension between Device Independence and privacy

The DI scenario involves the proverbially unwise act of bringing objects designed by a clever adversary into one's home. In the DI case the Bell-violating boxes are supposed to be unable to covertly signal each other or an outside accomplice, or engage other hostile activity like the original Trojan horse.

A more recent example is the seemingly harmless wooden plaque, a gift from Soviet children to the US Ambassador, that functioned for years as a passive eavesdropping microphone. It worked by modulating a radio frequency carrier beamed in at it from outside the Ambassador's residence. The listening device was devised by Leon Theremin, inventor of the eponymous electronic musical instrument.

Granddaughter playing Theremin at family music school

Device Independence Continued

Getting back to Device Independence, the Bell-violating boxes can of course be prevented from signaling each other in real time by operating them at a **spacelike separation**, but there is no practical way of blocking all covert channels (e.g. electromagnetic, ultrasonic, or neutron emissions, or modulations of outside carriers), as would be needed to prevent the boxes from eventually sending everything they know, including all their inputs (e.g. detector settings) and outputs (detector results) to an outside accomplice, who could then distill the same random numbers as the legitimate users had.

In conclusion, while device independent protocols are good for assuring oneself that the generated numbers are fresh and random, this assurance is not transferable to others, nor is there any guarantee that the untrusted devices have not leaked the numbers to an adversary.

What about measurement device independence?

Measurement device independent QKD sounds weaker (less secure) than device independent QKD, but in fact it is stronger because

- photon counters are easier to hack than lasers
- Light sources (coherent ones at least) are easier to make from commodity components in a DIY fashion.

In DI-QKD one must hope that the untrusted devices do not communicate with an adversary.

In MDI-QKD with DIY light sources, one must trust only one's competence in constructing the sources without inadvertently introducing covert channels. By contrast in fully DI QKD, one must trust that one's adversary has not deliberately equipped the untrusted boxes with hard-to-discover covert signaling abilities.

Physical Randomness examples

-Photons or coherent state incident on a beamsplitter
-Bell-violating measurements on entangled states
-Radioactive decay
-Shot noise (e.g. arrival times of electrons emitted by a hot filament)
-Chaotic dynamics, e.g. turbulence, Lava lamp, wind noise.

Since the world is fundamentally quantum, such macroscopic and seemingly classical noises are also quantum, originating as amplified quantum fluctuations

Common features of such processes

- A dynamical process that is reversible in principle but infeasible to undo in practice
- (Often) escape of some subsystem involved in the dynamics to an inaccessible place, thereby rendering the undoing impossible, not just infeasible.

In more detail,

-Photons incident on a beamsplitter remain in a superposition until they are detected. This complex amplification, and escape of some subsystems, (e.g. phonons from clicks) fixes the random outcome, preventing it from being coherently undone as in a quantum eraser experiment.

-Radioactive decay: the alpha particle is in a superposition of places (including still inside the nucleus) until it is detected and thereby amplified and the decay made irreversible.

-Shot noise (e.g. arrival times of electrons emitted by a hot filament) similarly a superposition collapsed by detection.

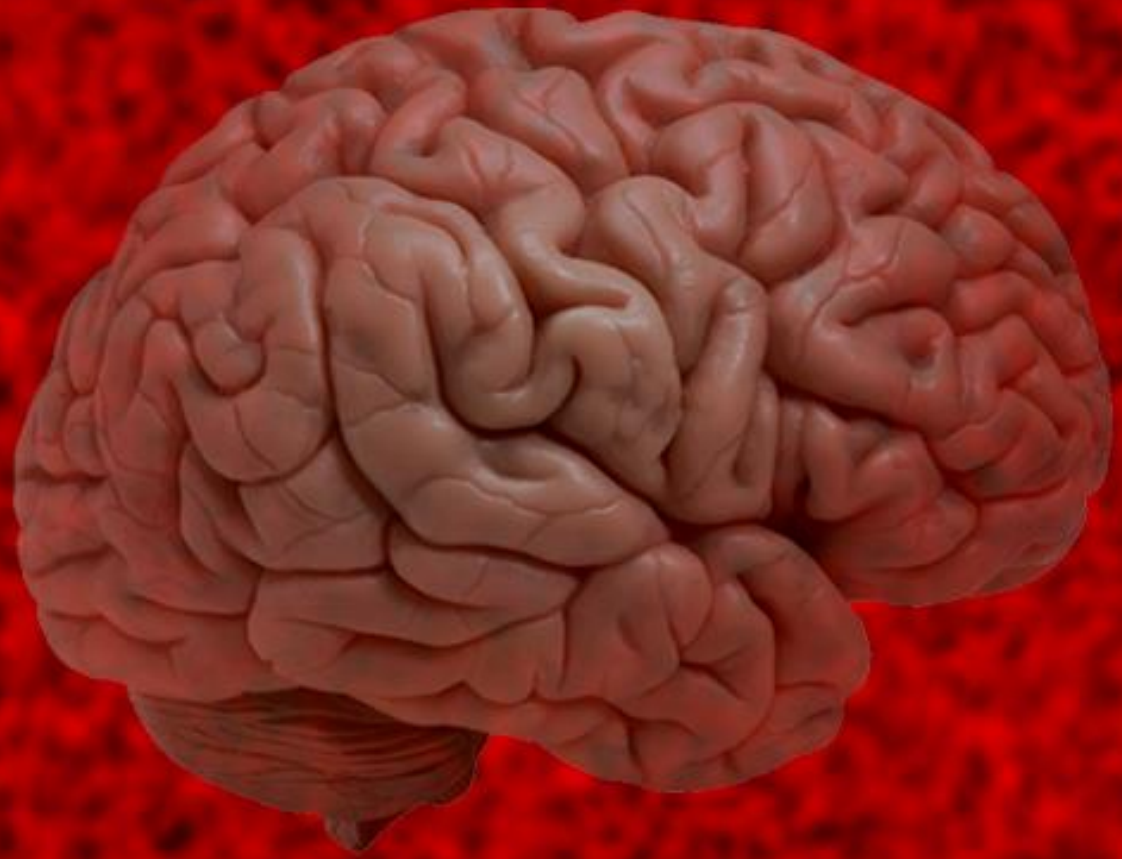
By contrast to cryptography, 21st century **cosmology** is a very **impractical** field that offers new challenges and opportunities for intercultural sensitivity and synthesis.

Observational astronomy strongly supports the ΛCDM "standard model", which predicts that the expansion of our universe is accelerating, which, by an Unruh-like effect, will cause the resulting empty space to be filled with thermal radiation at a low but positive temperature. This so-called asymptotic de Sitter state raises two fundamental questions:

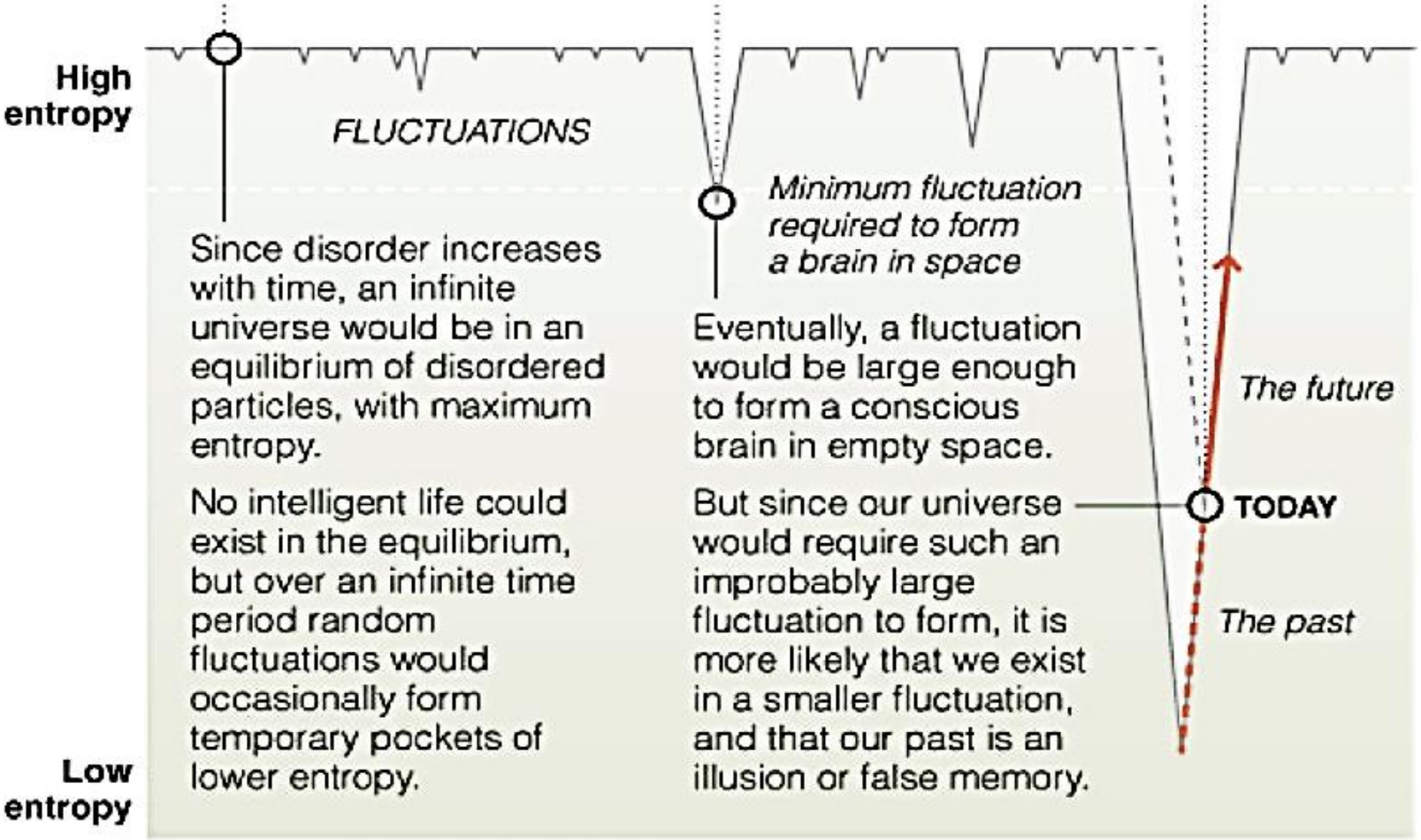
- The Boltzmann brain problem—how do we know we are inhabitants of a young live universe rather than fluctuations in an old dead one? $\infty / 2^N = \infty$ even when $N = 10^{24}$.

- The Wigner's friend problem—what does it feel like to be inside a quantum superposition? In particular, does the de Sitter state even have fluctuations, if there is no measuring apparatus present to observe them? *"If a tree falls and no one is there to hear it, does it make a noise?"*

A friend of Boltzmann proposed that the low-entropy world we see may be merely a thermal fluctuation in a much larger universe. "Boltzmann Brain" has come to mean a fluctuation just large enough to produce a momentarily functioning human brain, complete with false memories of a past that didn't happen, and perceptions of an outside world that doesn't exist. Soon the BB itself will cease to exist.



A diabolical conundrum: Boltzmann fluctuations nicely explain the low entropy state of our world, and the arrow of time, but they undermine the scientific method by implying that our picture of the universe, based on observation and reason, is ***false.***



Diabolical Conundrum continued: People began worrying about equilibration in the 19th Century, calling it the "heat death of the universe", but thought of it as a problem for the far future.

Boltzmann showed us that it is already a problem in the present, undermining our ability to make inferences make about conditions in the past or elsewhere, based on those here and now. The inhabitants of any universe with local interactions that will ultimately come to thermodynamic equilibrium, must make the additional postulate, unsupported by observation, that they are situated ***atypically early*** in its history. Otherwise, their "scientific" inferences are no better than those of the inhabitants of J.L Borges' fictional *Library of Babel*, which contained, randomly shelved, one copy of every book-length sequence of letters (Borges may have got the idea from having once worked in a library with too many mis-shelved books).

Doomsday arguments illustrate undisciplined thinking based on assumed typicality of the observer, without considering ways in which the observer may be atypical.

"I am probably not atypical; therefore it is 90% probable that between 5 and 95 per cent of all people who will ever live already have."

Carlton Caves' birthday party rebuttal the doomsday argument arxiv:0806.3538: Imagine wandering into a birthday party and learning that the celebrant is 50 years old. Then there is a 1/2 chance they will live to be 100 years old and a 1/3 chance to 150. Conversely, upon encountering a one day old baby, would it be fair to warn the parents that their child will probably only live a few weeks?

In both cases the person's body contains internal evidence of their life expectancy that invalidates the assumption of typicality.

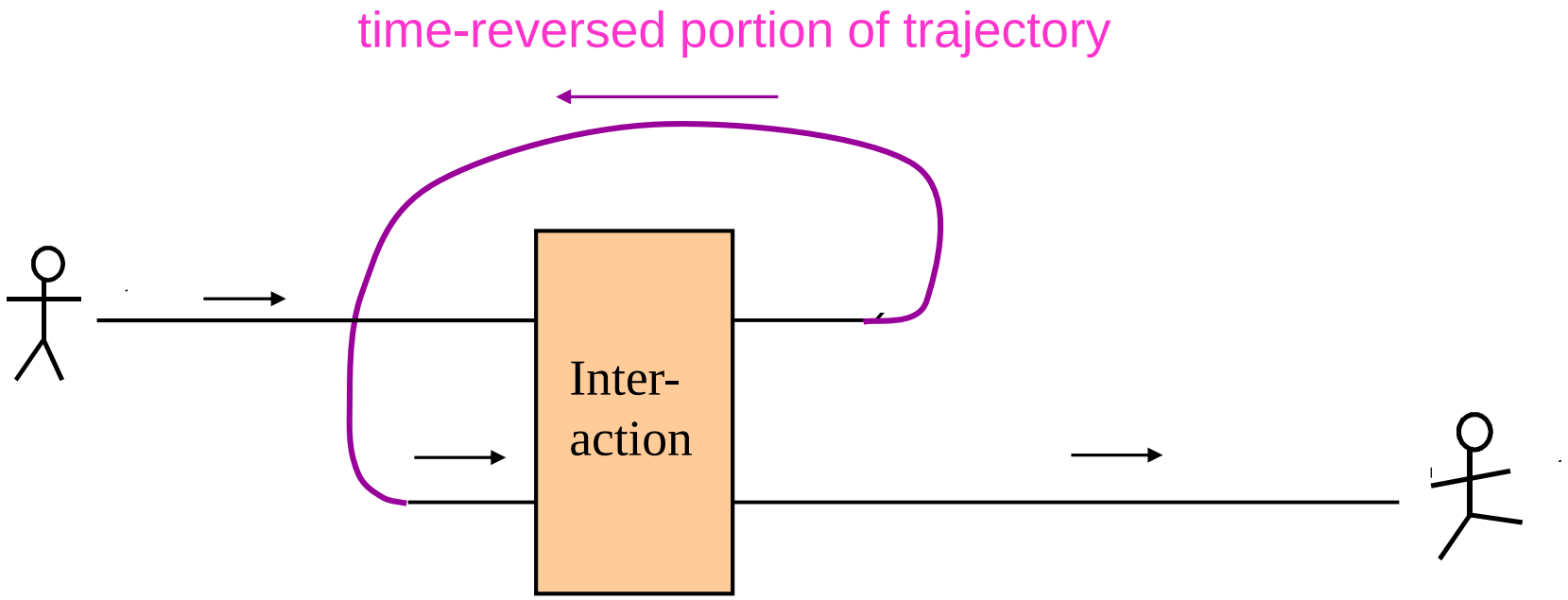
Babies are untroubled by worries of atypicality, being naturally egotistic. Adult egotists, especially dictators, rather enjoy thinking that they occupy a privileged position at the beginning of a long future.

A building dating from year VII of the Fascist Era (1922-43), more typical than Mussolini imagined it would be.

Einstein's greatest achievement, general relativity, allows the existence of severely warped spacetimes containing closed timelike curves (CTCs). If such curves are sufficiently stable, they might make some form of time travel possible. In another cultural interaction with physicists, some computer scientists have suggested that equipping a quantum computer with a CTC would enable it to distinguish non-orthogonal states, but Leung, Smith, Smolin and I (mostly physicists) are arrogant enough to think they have neglected a basic principle of their own discipline, namely that the purpose of a computer is to solve problems that its builder doesn't already know the answer to. (Bennett, Leung, Smith, and Smolin, Phys Rev Lett 103.170502(2009), arXiv:0908.3023v2)

*On Monday, Prasanta Panigrahi discussed a similar line of reasoning leading to the conclusion that CTCs would make all four Bell states LOCC-distinguishable.

Traveling into the past to interact with one's former self:

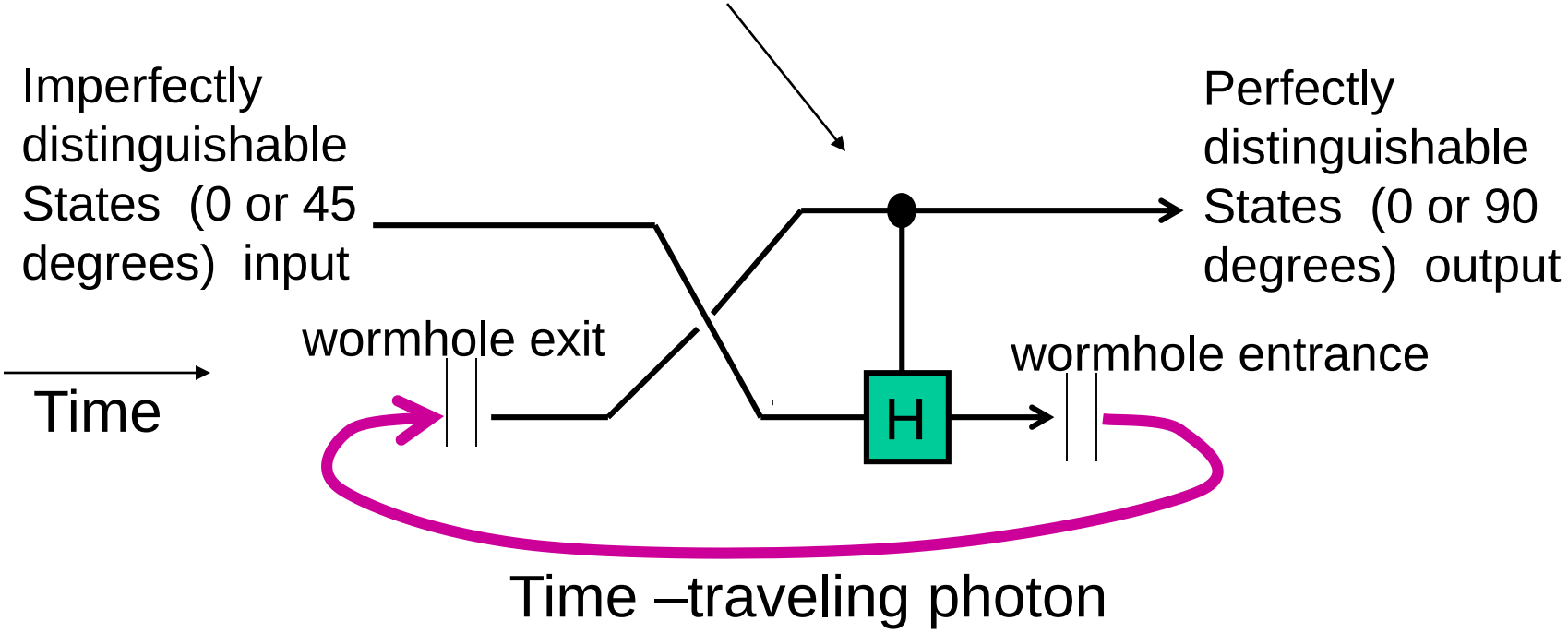


For some initial conditions, no future is possible ("grandfather paradox").

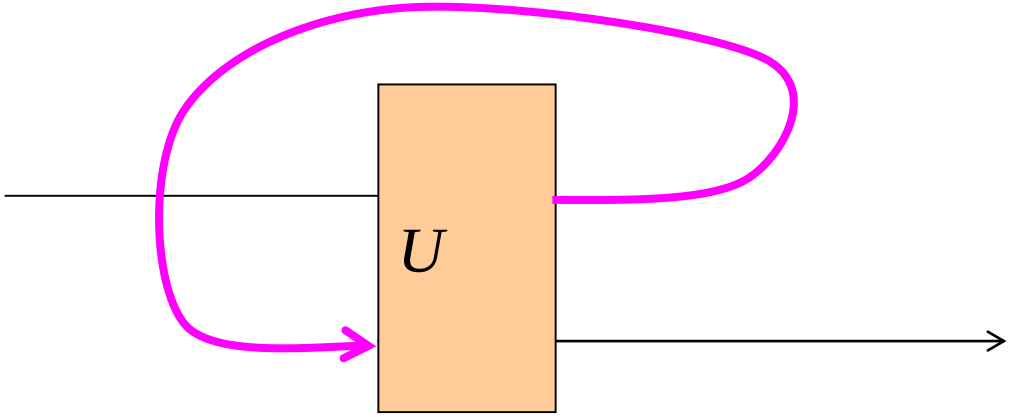
For others, multiple futures are possible.

Is this multiplicity/paucity of futures a feature or a bug?

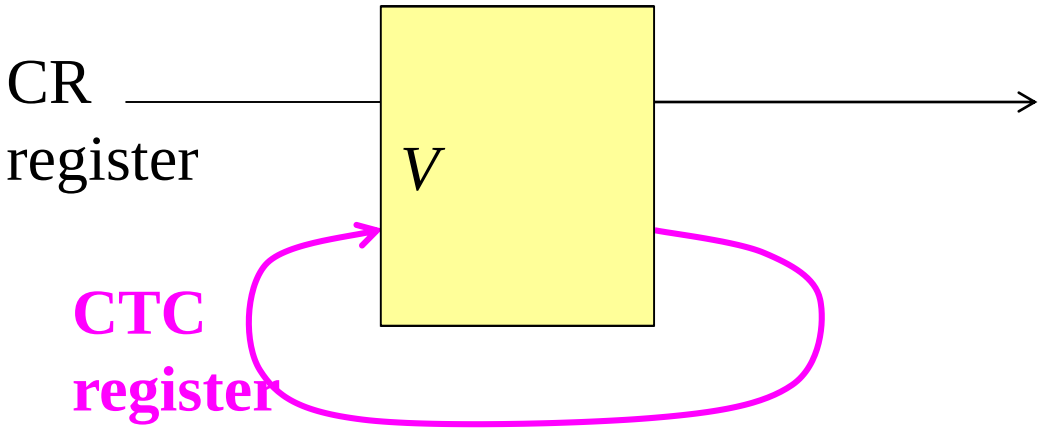
Using a CTC to reliably distinguish nonorthogonal states: If upper photon is vertical (90 degrees), rotate the lower photon by +45 degrees. If upper photon is horizontal (0 degrees), leave the lower one alone.

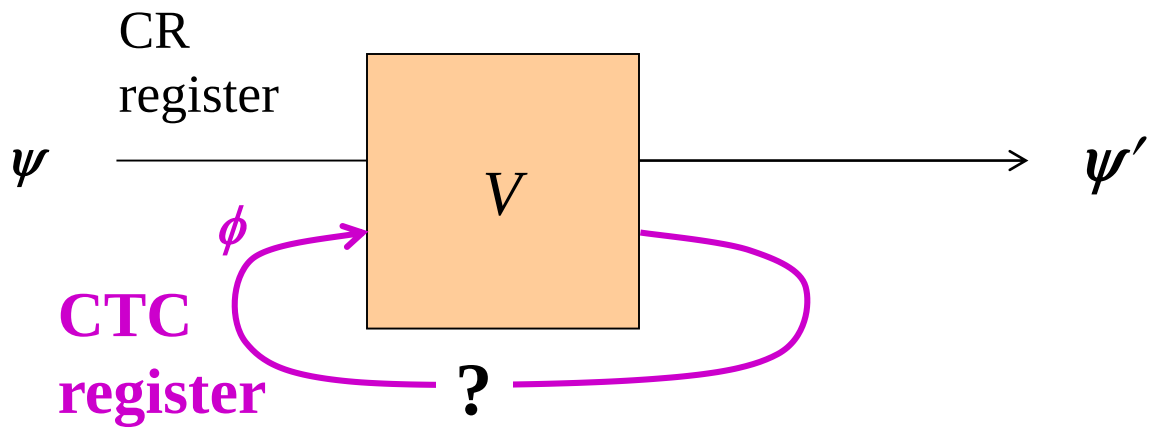


Interaction with earlier self stretches two initially non orthogonal states of the photon apart and makes them orthogonal.



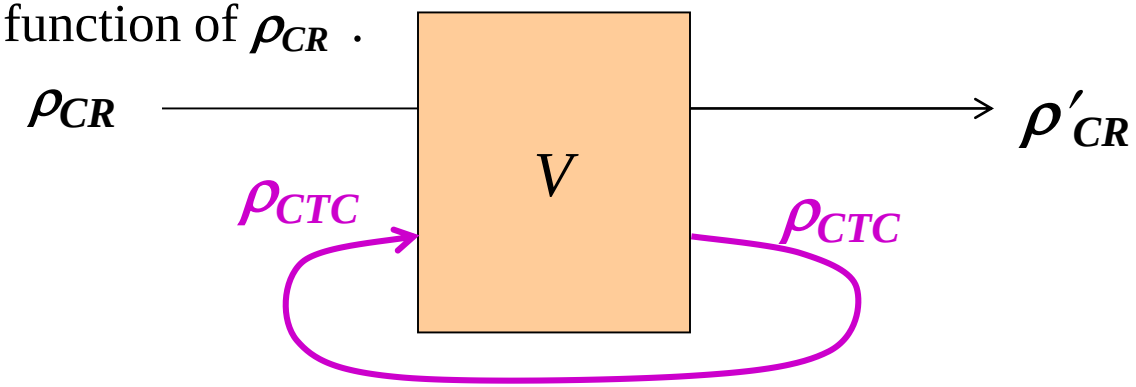
Time travel is usually discussed in terms of an equivalent untwisted diagram involving interaction of an ordinary causality-respecting register CR with a register CTC that traverses a closed timelike curve.





The grandfather paradox means that for some interactions V and initial states ψ, there is no ***pure*** fixed point for the CTC register, i.e. no state ϕ of the CTC register which emerges unchanged by its interaction with ψ. This makes ψ' hard to define.

To avoid this, Deutsch (1991), instead looked for a ***mixed*** fixed point. He postulated that for every input ρ_{CR} to the CR register, the CTC ***finds*** a mixed state ρ_{CTC} such that the same mixed state emerges after interaction with the CR register. Such a mixed state fixed point always exists. This then allows ρ'_{CR} to be defined as a nonlinear function of ρ_{CR} .



Recapitulating the Deutsch Formalism,

$$\rho'_{CR} = \mathrm{Tr}_{CTC}\left(V\left(\rho_{CR}\otimes\rho_{CTC}\right)V^{\dagger}\right),$$

where ρ_{CTC} is a fixed point defined by

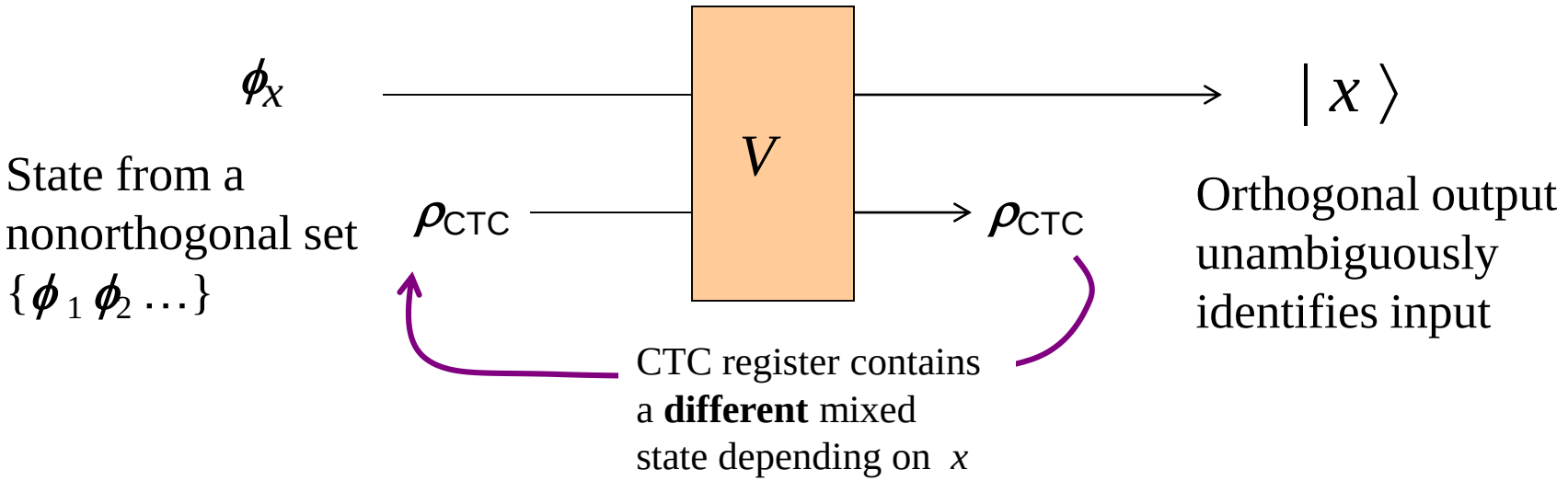
$$\rho_{CTC} = \mathrm{Tr}_{CR}\left(V\left(\rho_{CR}\otimes\rho_{CTC}\right)V^{\dagger}\right)$$

Because ρ_{CTC} depends on ρ_{CR},

the mapping $\rho_{CR} \rightarrow \rho'_{CR}$ is nonlinear.

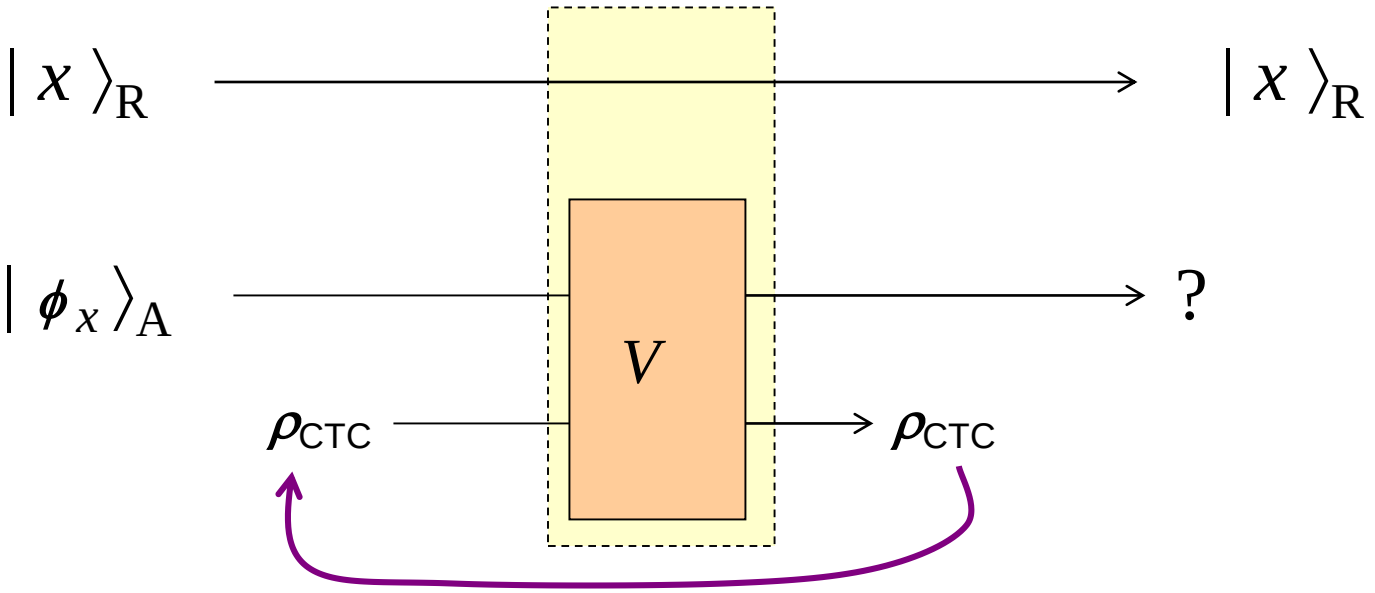
In recent years it has been noted that this nonlinearity (and even the milder nonlinearity of postselected time travel) gives rise to some dramatic consequences for cryptography and computational complexity.

BHW 0811.1209 Argument using Deutsch model



The trouble with the these arguments is that, because the fixed point is allowed to depend nonlinearly on the input state, the ability to distinguish an arbitrary pure state from the set $\{\phi_x\}$ does not mean it the circuit would still work if given a mixture of the states.

A more satisfying criterion for state discrimination would be to be able to distinguish an ***externally labeled mixture*** of states via a CTC fixed point that ***does not*** depend on the external label.



In other words, the input to the causality respecting register should rather be

$$\rho_{RA} = \sum_x p_x |x\rangle\langle x|_R \otimes |\phi_x\rangle\langle\phi_x|_A$$

where R is a noninteracting reference register keeping track of which pure state has been furnished in register A, which actually interacts with the CTC. The induced CTC state will then be the fixed point appropriate to the mixture ρ_{RA} , not its pure components.

Proper state discrimination on a labeled mixture should work like this. On a labeled mixture of inputs,

$$\rho_{RA} = \sum_{x=0}^{1} p_x |x\rangle\langle x|_R \otimes |\phi_x\rangle\langle\phi_x|_A$$

the output should be

$$\rho'_{RA} = \sum_{x=0}^{1} p_x |x\rangle\langle x|_R \otimes |x\rangle\langle x|_A$$

But the actual output is

$$\boldsymbol{\rho'_{RA} = (\Sigma_x\, p_x |x\rangle\langle x|_R) \otimes \rho'_A}$$

where ρ'_A depends the ensemble $\{p_x, \phi_x\}$ but not on the index x. In other words, the CTC-equipped computer outputs a mixture of all the answers, not the one requested.