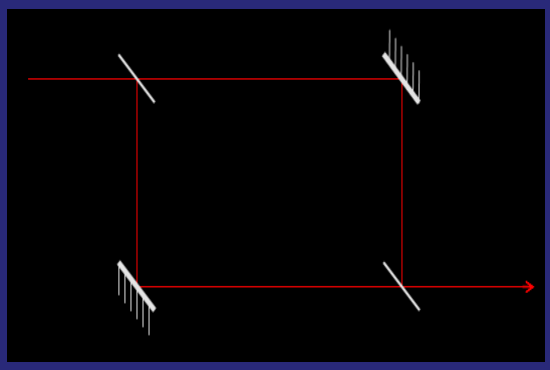
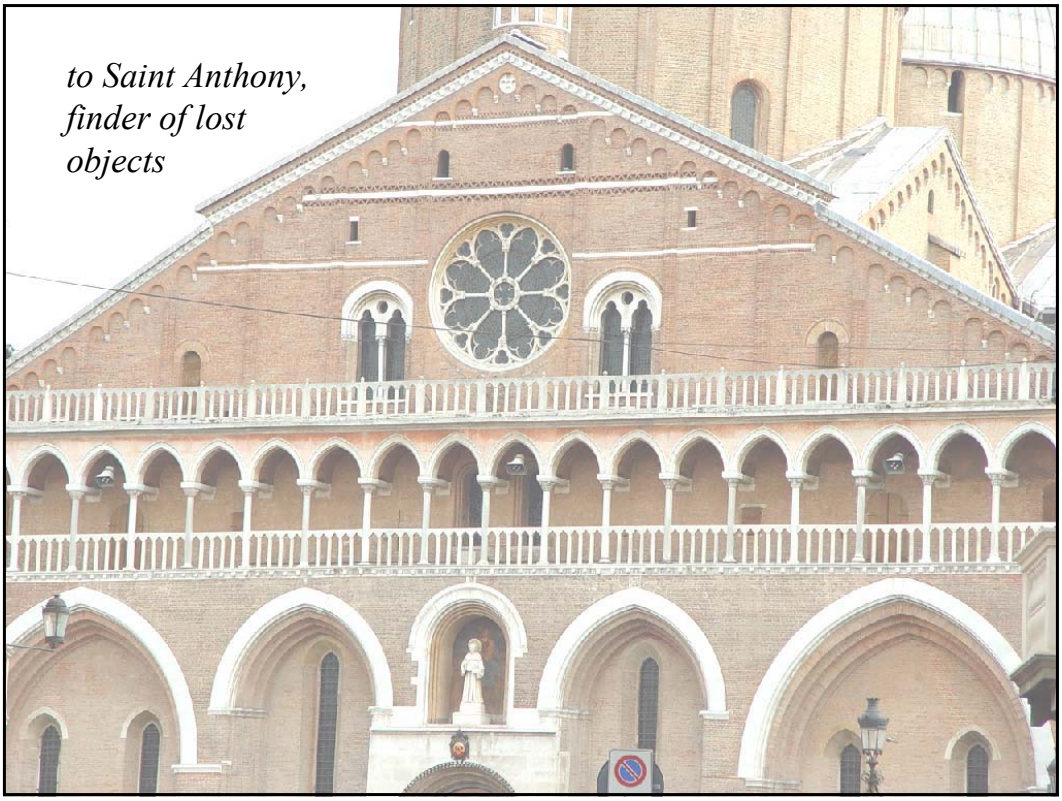
Quantum Information and the Forgetfulness of Nature



Charles H. Bennett
IBM Research Yorktown

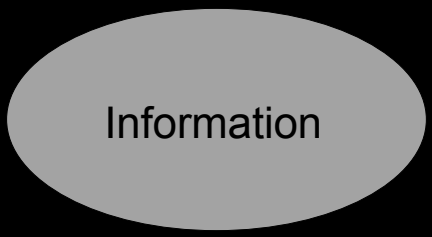
Univ. de Padova
22 October 2007



- The nature of information, and its quantum generalization.
- The perfect privacy of quantum information
- Levels of privacy, publicity, and permanence of information

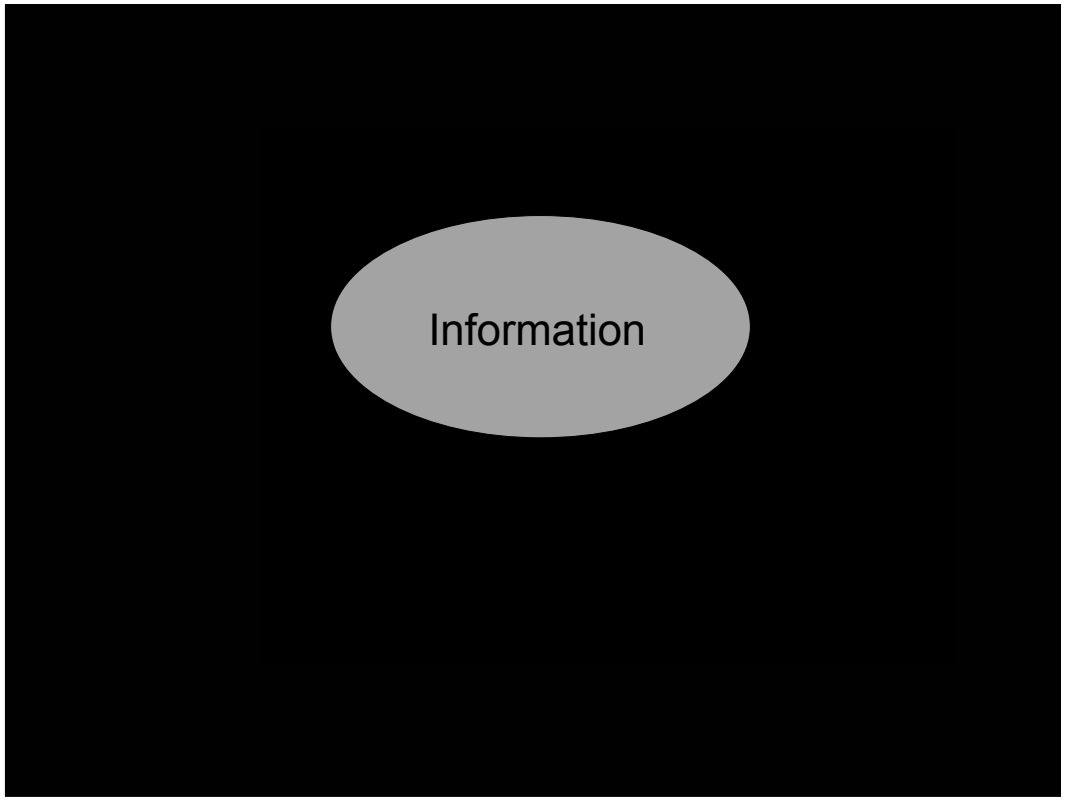
- Lost information in the ancient world, e.g. Sappho's lost poems
- The post-Gutenberg and post-Internet information glut.
- What happens to all this information? Is it saved or lost?
- Surveillance, loss of privacy, and information policy

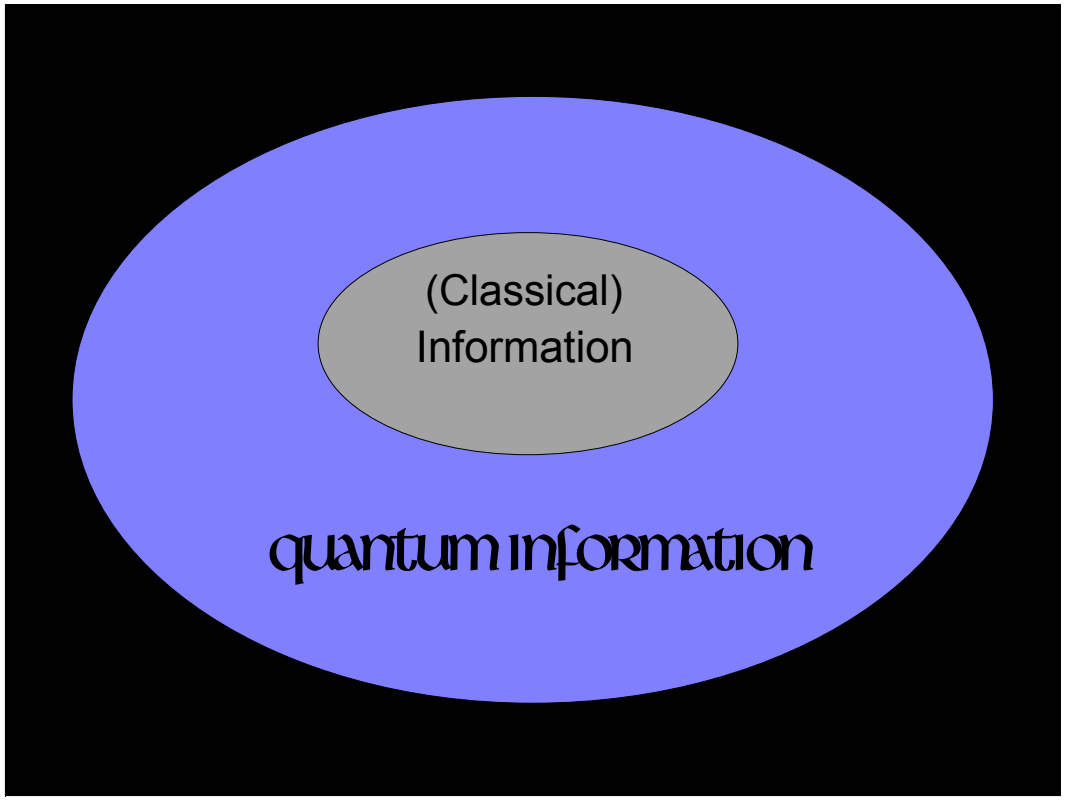
- Estimates of information production, storage, and loss to space
- The fate of a typical piece of information in the world.
- How to commit a perfect crime.

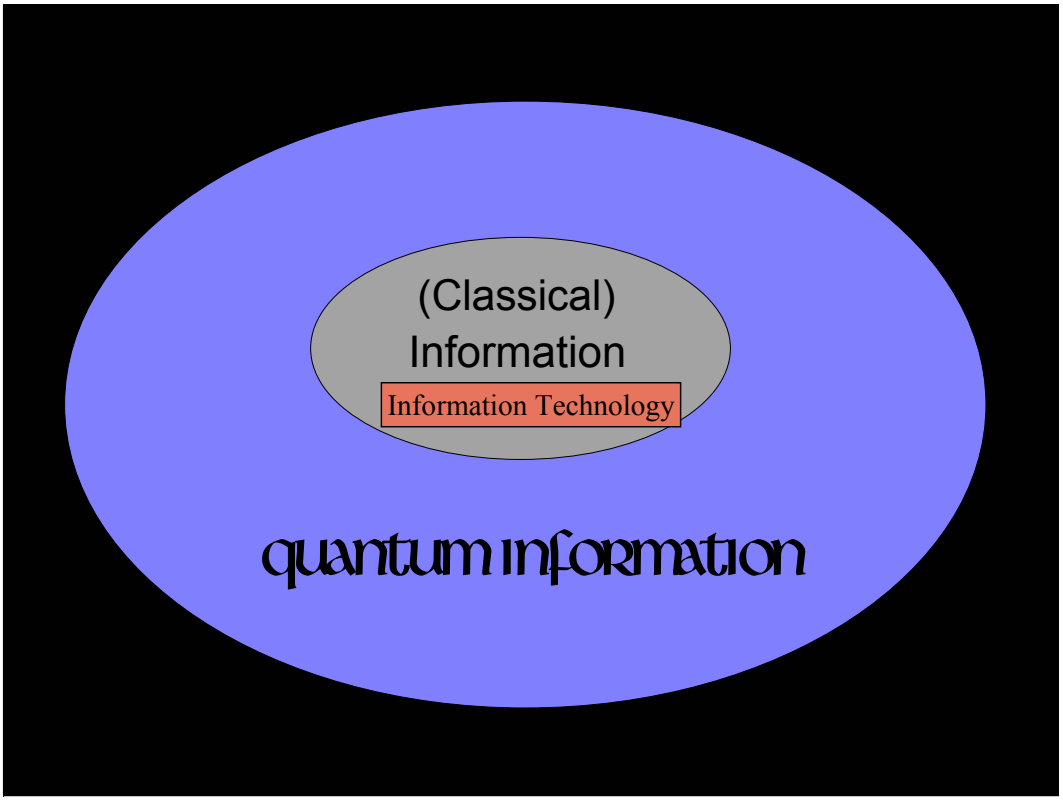


What is information?

Our society is the midst of an information revolution. As a result, nowadays, even non-technical people are familiar with the basics of information storage, transmission and processing.


Information


(Classical)
Information
quantum information



Information = Distinguishability, considered abstractly, separate from any physical medium.
(Using a pencil, a piece of paper can be put into various states distinguishable by eye. Using one's voice, the air can be put into various states distinguishable by ear, etc...)

- Information is reducible to bits (**0** ,**1**)
- Information processing, to reveal implicit truths, can be reduced to logic gates (**NOT**3**AND**)
- bits and gates are *fungible*, independent of their physical embodiment, making possible Moore's law (As bits become ever smaller and cheaper they become ever more useful, unlike shoes or cars)

Even though we have tried to abstract all the physics out of the notion of information, some physics is left. We take for granted that information

- **cannot travel faster than light** (relativity)
- **can be erased when no longer wanted** (thermodynamics)
- **can be copied without disturbing it** (quantum mechanics)

Indeed chemists and physicists have long known that

Information in microsopic bodies such as photons or nuclear spins obeys quantum laws. Such information

- cannot be read or copied without disturbance.

- can connect two spacelike separated observers by a correlation too strong to be explained by classical communication. However, this "entanglement" cannot be used to send a message faster than light or backward in time.

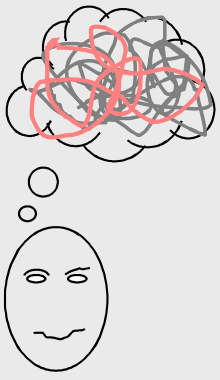
Quantum information is reducible to **qubits** i.e. two-state quantum systems such as a photon's polarization or a spin-1/2 atom.

Quantum information processing is reducible to one- and two-qubit gate operations.

Qubits and quantum gates are fungible among different quantum systems

Ordinary classical information, such as one finds in a book, can be copied at will and is not disturbed by reading it.

Quantum information is more like the information in a dream



• Trying to describe your dream changes your memory of it, so eventually you forget the dream and remember only what you've said about it.

• You cannot prove to someone else what you dreamed.

• You can lie about your dream and not get caught.

But unlike dreams, quantum information obeys well-known laws.

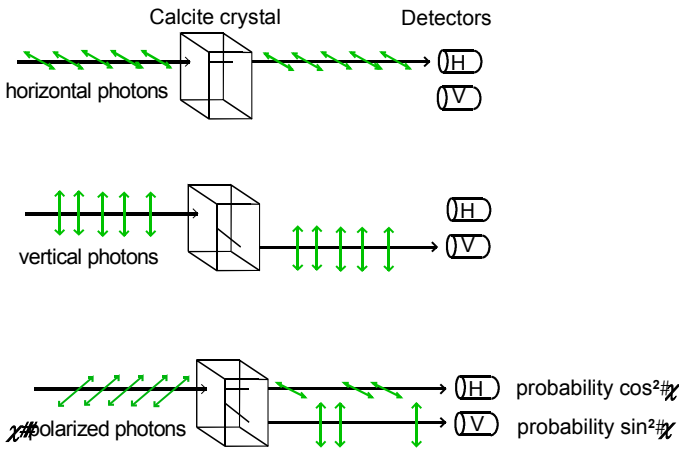
superposition principle

Between any two reliably distinguishable states of a quantum system

(for example horizontally and vertically polarized single photons)

there exists a continuum of intermediate states (representable as complex linear combinations of the original states) that in principle cannot be reliably distinguished from either original state.

(for example diagonal polarizations)



(Mathematically, a superposition is a weighted sum or difference, and can be pictured as an intermediate *direction* in space)

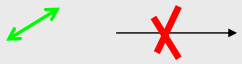
$$\nearrow = \frac{\leftrightarrow 2\#}{\sqrt{9}}$$

$$\searrow = \frac{\leftrightarrow 4\#}{\sqrt{9}}$$

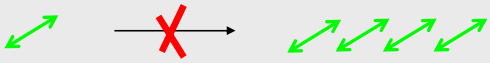
Non-orthogonal states like ↔ and ↗ are in principle imperfectly distinguishable.

↔ always behaves somewhat like ↗ and vice versa.

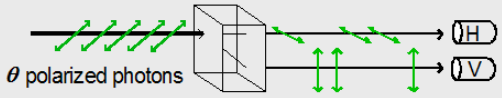
Measuring an unknown photon's polarization exactly is impossible (no measurement can yield more than 1 bit about it).



Cloning an unknown photon is impossible. (If either cloning or measuring were possible the other would be also).



If you try to amplify an unknown photon by sending it into an ideal laser, the output will be polluted by just enough noise (due to spontaneous emission) to be no more useful than the input in figuring out what the original photon's polarization was.



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?

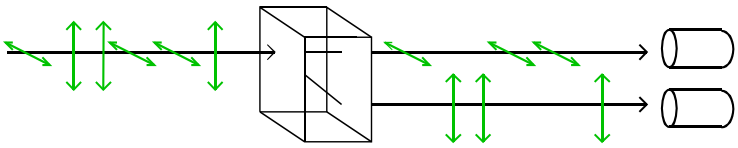
Pupil: Uh, I am polarized at about a 55 degree angle from horizontal.

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

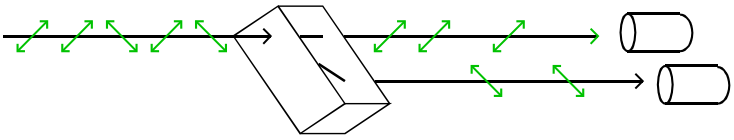
Pupil: Horizontal, sir.

Teacher: Have you ever had any other polarization?

Pupil: No, sir. I was always horizontal.



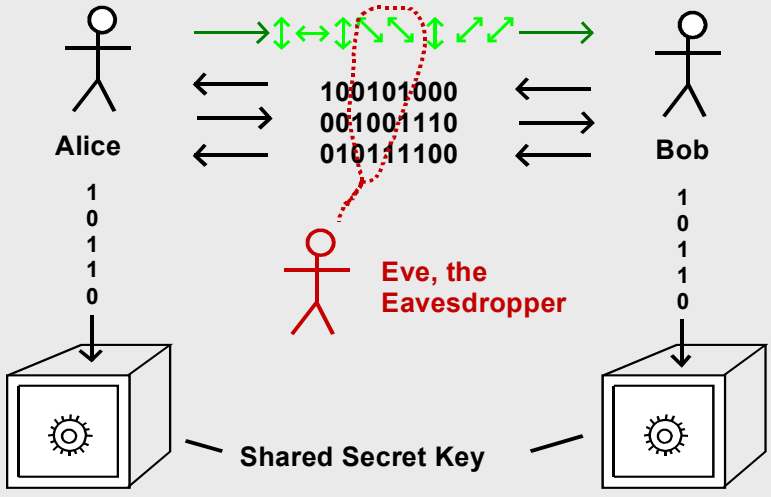
Vertical and horizontal photons can be distinguished by one kind of measurement, but this measurement causes diagonal photons to behave randomly.



45 and 135 degree diagonal photons can be distinguished by another kind of measurement, but this measurement causes vertical and horizontal photons to behave randomly.

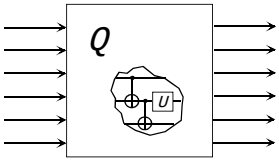
The impossibility of distinguishing all four kinds of photons is used in quantum cryptography

Quantum Cryptographic Key Distribution



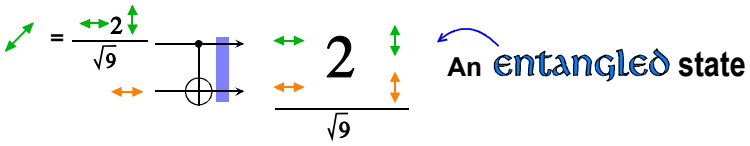
In the end, Alice and Bob will either agree on a shared secret key, or else they will detect that there has been too much eavesdropping to do so safely. They will not, except with exponentially low probability, agree on a key that is not secret.

Any quantum data processing can be done by 1- and 2-qubit gates acting on qubits.

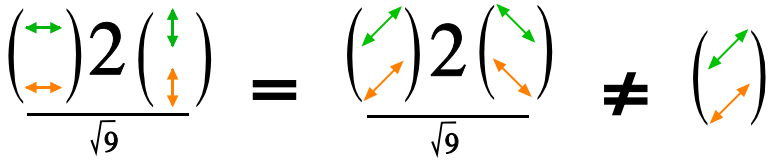


The 2-qubit XOR or "controlled-NOT" gate flips its 2nd input if its first input is 1, otherwise does nothing.

A superposition of inputs gives a superposition of outputs.



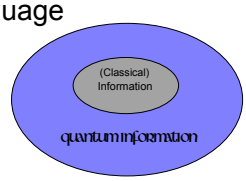
An entangled state is a state of the whole system that cannot be described by attributing states to its parts.



The two entangled photons can be said to be in a definite state of ***sameness*** even though neither has a state of its own.

Like two hippies in Woodstock or Haight-Ashbury, who sense that their spirits are in perfect agreement, even though neither has an opinion about anything.

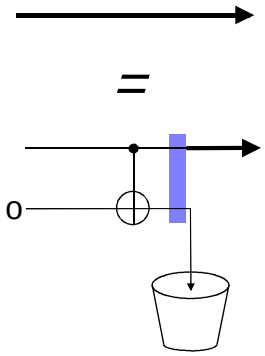
Re-expressing classical information in quantum language



A classical bit is just a qubit with one of the Boolean values **0** or **1**.

A classical wire is a quantum channel that conducts **0** and **1** faithfully, but randomizes superpositions of **0** and **1**.

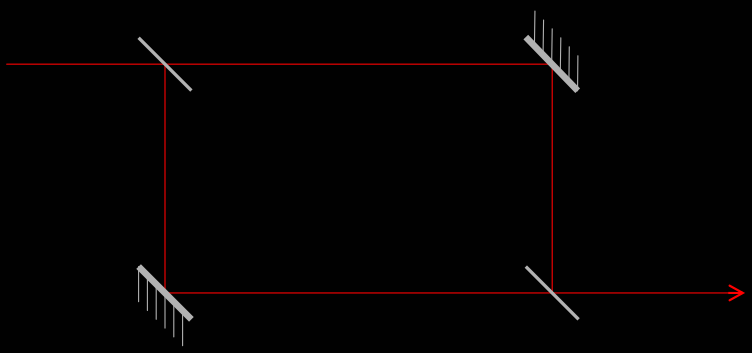
(This occurs because the data passing through the wire interacts with its environment, causing the environment to learn the value of the data, if it was **0** or **1**, and otherwise become entangled with it.)



A classical channel is a quantum channel with an eavesdropper.

A classical computer is a quantum computer handicapped by having eavesdroppers on all its wires.

Quantum information is famously evanescent



If no record is made of which path a photon follows through an interferometer, or if a record is made but then unmade, the photon will have followed a superposition of both paths. After the experiment is over, even God doesn't remember.

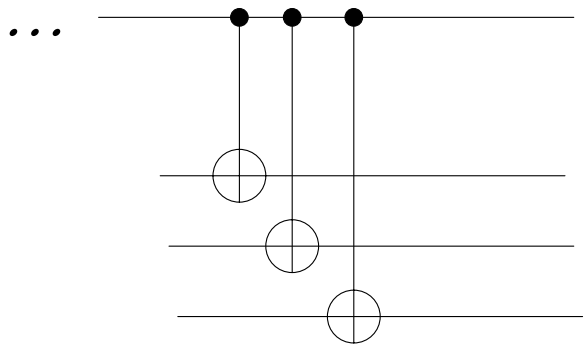
Thus there are 3 levels of privacy.

• **Quantum:** Information like the path taken in an interferometer, that exists only temporarily, and afterward can best be thought of as never having existed.

• **Classically Private:** Information that has been amplified to the point of becoming classical, but is not widely distributed in easily recoverable form. Humans can erase it, then lie about it with impunity, although perhaps not without guilt.

• **Public:** Information that is so widely distributed that it is infeasible to conceal. Lying about it only makes you look foolish.

What does it mean for information to be "classical?"



Information becomes classical by being replicated redundantly throughout the environment.

"Quantum Darwinism" Blume-Kohout, Zurek quant-ph/0505031 etc.

In the practical tradeoff between Publicity and Privacy, digital technology has created a problem and an opportunity

Cheap, easy-to-use video cameras and cheap data storage leads to the temptation to record everything happening in public or even private places and save it forever, with ensuing loss of privacy, and potential loss of liberty if despotic rulers get hold of the data.

But these recordings are sometimes good, protecting human rights and promoting the rule of law. In many situations the bad guys want privacy for their misdeeds, while the good guys want publicity, with authenticity.

A popular viewpoint in the US is that it is good for society for everyone to have the right to carry a gun.

Perhaps a better idea would be for everyone to carry a camera.

Public policy would then encourage amateurs to make audiovisual recordings, but restrict how the recordings could legally be used. (Yes for exposing crime and corruption; No for blackmail).

CNN billboard in Delhi, India:

If you see it, shoot it—
Every citizen a photojournalist.

Nowadays, it is tempting to believe that once information has become public, it can never be destroyed.

The modern world appears very different in this regard from the ancient pre-Gutenberg era, when major literary works were written down, performed, and widely known, but then then lost.

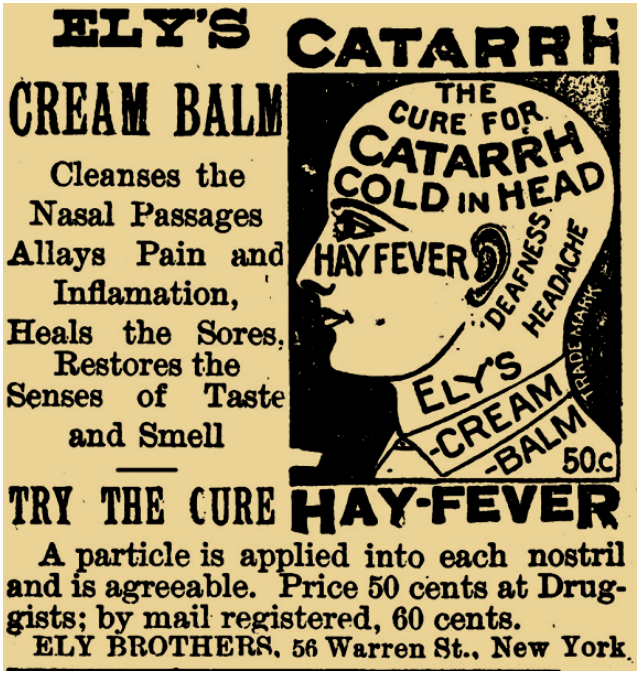
Sappho, ca 620-525 BC, by Gustav Klimmt

"Since classical times, Sappho has been a source of fascination and romantic construction. The ancients, who had nine books of her poems at their disposal, were unstinting in their admiration…. It is difficult to judge her for ourselves when so little of her work remains. What we have consists on the one hand of quotations and more general references in ancient authors, and on the other hand of torn scraps from ancient papyrus and parchment copies…. Only twenty-one contain any complete stanzas; and only three – till now – gave us poems near enough complete to appreciate as literary structures.

"A recent find enables us to raise this number to four… This text, recovered from Egyptian mummy cartonnage, is the earliest manuscript of her work so far known. It was copied early in the third century bc, not much more than 300 years after she wrote."

[Martin West, Times Literary Supplement 24 June 2005]

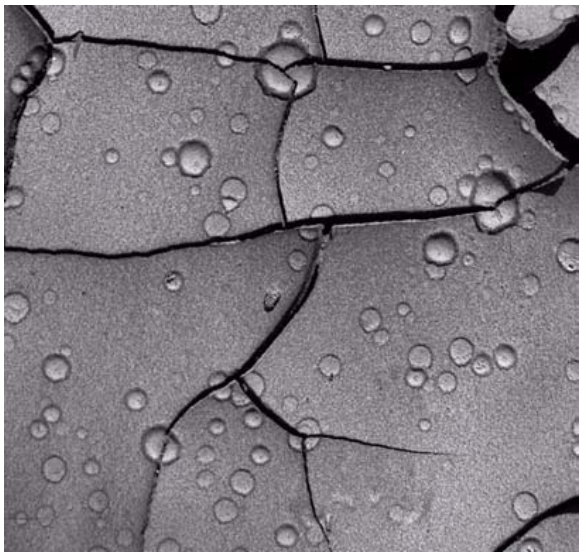
Papyrus fragments from Egyptian mummy cartonnage which, in conjunction with another fragmentary manuscript found decades earlier, allowed Sappho's latest poem to be reconstructed



Advertisement from an 1891 newspaper used as a drawer liner in a piece of antique furniture.

A modern example of fossilization not so different from the re-purposing of Sappho's poems as mummy cartonnage .

But even in today's world, much macroscopic, publicly accessible information is lost because no person, nor any natural process, happens to record it in a durable medium.



Dried mud with cracks and raindrop craters in a river bed in Las Vegas, USA in 1965. A few days later these details were washed away by a subsequent rain.

If no one had photographed them, would all record of them have been lost?

It is tempting to believe that such macroscopic information is not lost, just that it becomes so diffusely and complexly spread out as to be irrecoverable in practice while being still recoverable in principle (just as when a book is burned its contents are in principle recoverable from the exact state of the smoke, ashes, and heat it generated).

Could it be that every major past phenomenon, say Sappho's other poems, or the fate of mysteriously disappeared persons like the physicist Ettore Majorana or U.S. labor leader Jimmy Hoffa, can be recovered from physical evidence in principle, if not in practice?

To believe otherwise is venturing dangerously close to the postmodernist view, abhorred by most scientists as arrogantly anthropocentric, that the past (or maybe even the present) has no objective reality independent of our beliefs about it, and therefore that it is pointless to inquire what "actually" happened.

But I think some information is really lost, not from the universe but from the world (i.e. the planet Earth). Why? –because most information we might care about is washed away by much larger entropy flows into and out of the Earth.

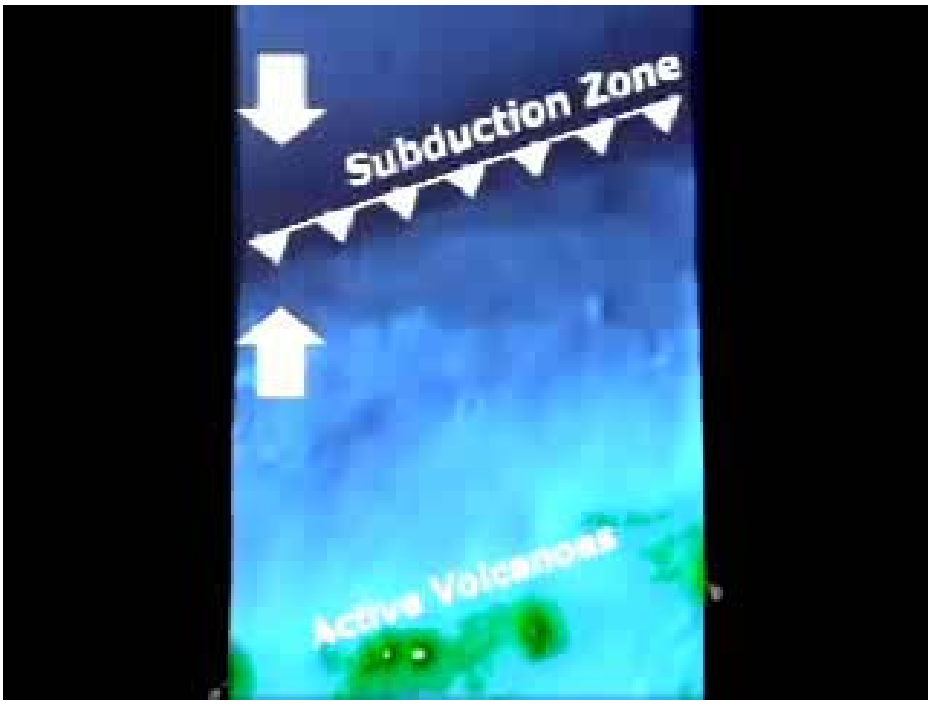
The Earth has finite information storage capacity, but it exports a lot of randomness (generates a lot of entanglement with its environment, in the quantum way of speaking) in the form of thermal radiation into the sky.

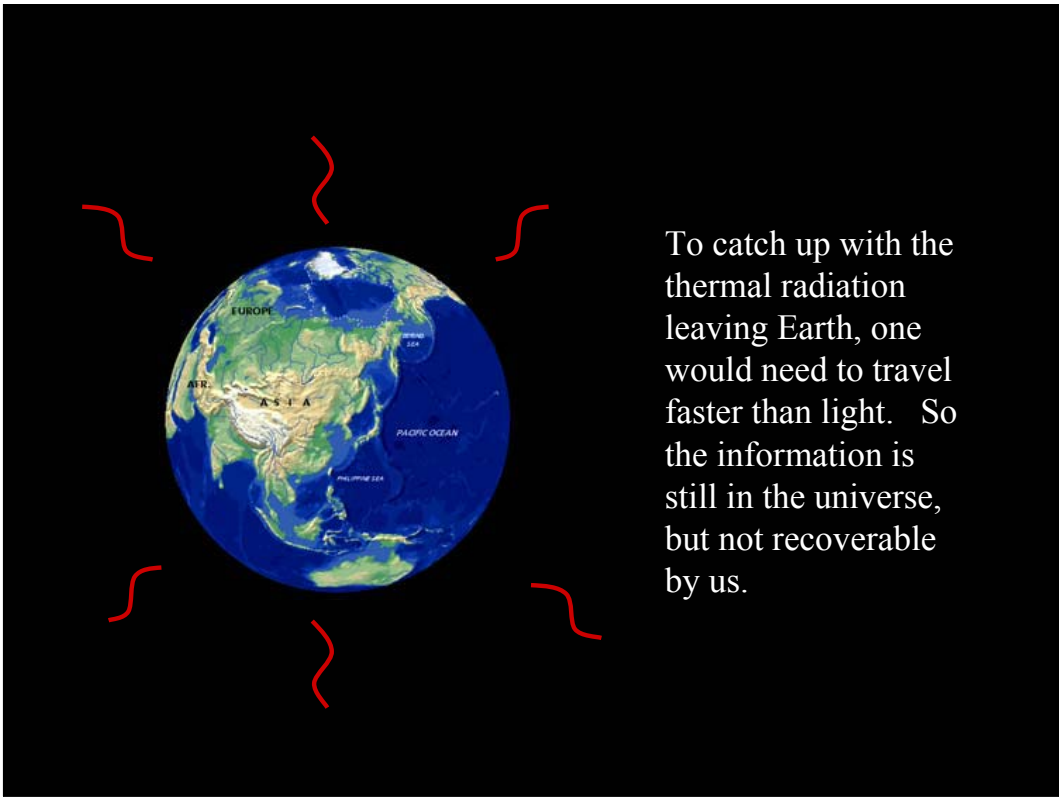
Thermal entropy export rate $\approx$ 200 watts/sq meter at 300K
$\approx 10^{30}$ bits per square meter per year.

Geological information capture rate in "hard" degrees of freedom, stable for geological times against thermal motion (e.g. atomic substitutional disorder and crystal lattice defects in solid rock of earth's crust) = crust thickness ($\approx$10 km) $\times$ rock information density ($\approx$1 bit/cubic nm) / rock lifetime ($\approx 10^8$ yr)
$\approx 10^{22}$ bits / per square meter per year.

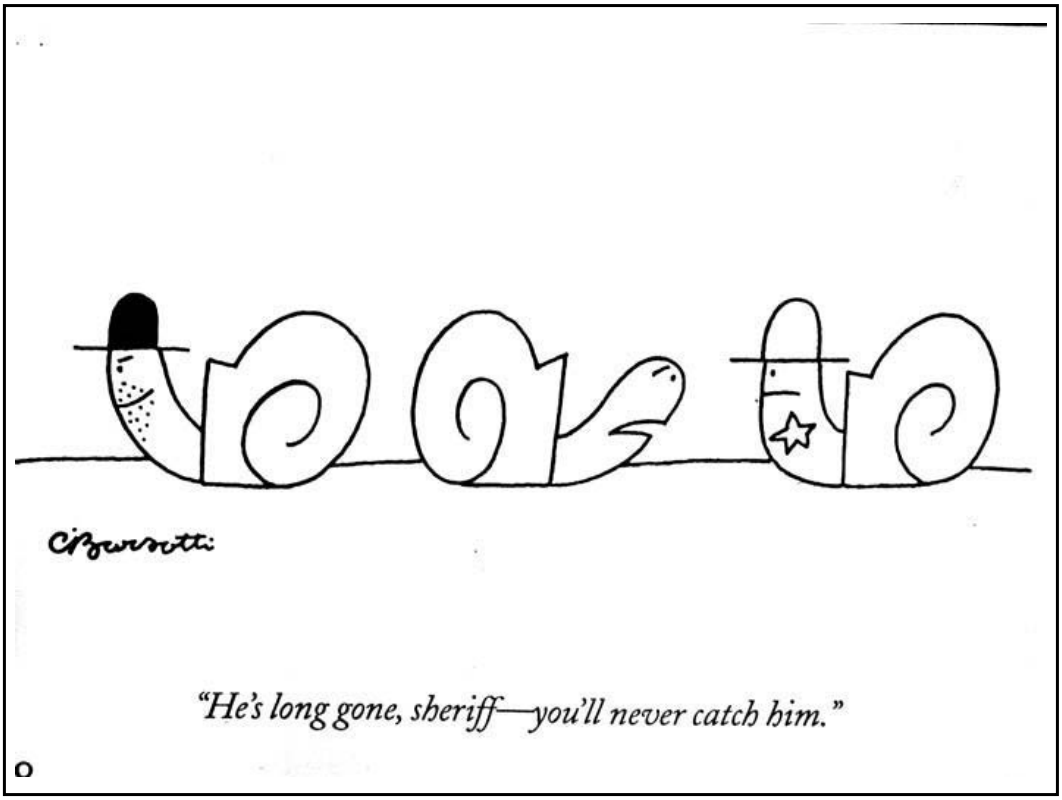
Human digital information capture rate 100GB/person x 10^9 people who are heavy information users $\approx 10^{21}$ bits per year

(that's for the whole world, not per sq meter)





To catch up with the thermal radiation leaving Earth, one would need to travel faster than light. So the information is still in the universe, but not recoverable by us.



So now we add a new level of privacy.

- **Quantum:** Information like the path taken in an interferometer, that exists only temporarily, and afterward can best be thought of as never having existed.

- **Classical but Escaped:** Information that has been amplified to the point of becoming classical, but has escaped from Earth in thermal radiation. Humans have no way of recovering it.

- **Classically Private:** Information that has been amplified to the point of becoming classical, and still resides on earth in a few places recoverable in principle.

- **Public and Permanent** Information that is so widely distributed that it is infeasible to erase all the copies.

Mysteries of the Past:

Still recorded on earth, though unknown to any human and inaccessible with current technology:

- Locations of gold rings, dropped in an annual ceremony into the Venice Lagoon over a period of several centuries, to symbolize Venice's marriage to the Sea.

Maybe still recorded on earth, maybe escaped: Fates of mysteriously disappeared persons such as

- Physicist Ettore Majorana disappeared 1938
- Labor leader Jimmy Hoffa disappeared 1975
- Computer Scientist Jim Gray disappeared 2007

Escaped:

- Unrecorded raindrops from past rain storms.
- Pattern of foam on my yesterday morning's cappuccino.

What can we do to make a particular chosen body of information long-lasting (say until the sun turns into a red giant)?

Why would we want to?
- To preserve important works of literature
- To preserve evidence of a crime until it is safe to publicize, thereby discouraging crime even in times of despotism and corruption
- Because we hate postmodernism and want to make even unimportant details of the past uncontestable.

Record the information in a durable digital medium, and bury many copies in geologically stable rock formations in various parts of the world, as if it were nuclear waste.

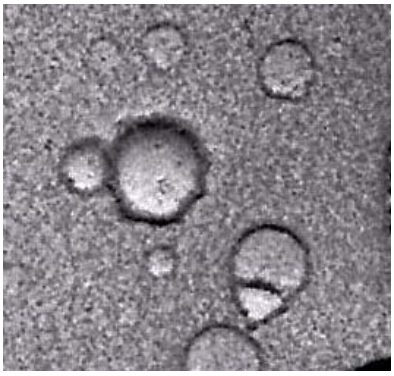
But suppose we wanted to store not all or most, but a lot of information, say a real-time video surveillance of entire earth surface at millimeter-millisecond resolution.

This works out to about 10^{16} bits/sq m year, well within geological capture rate.

Is this scary thing perhaps happening already, automatically, without deliberate human effort, just because frozen accidents in newly formed rock in a sense provide a hash of the current state of the earth?

Probably not, due to randomizing effect of dynamics.

Randomizing dynamics in a representative case.



Though the raindrop originates in quantum and thermal fluctuations, it does not fall in a superposition of places. Independent observers would agree where it fell, and as long as the drop or its crater exists, reflected light will generate a torrent of replicas of the information, fulfilling the classicality criterion of quantum Darwinism. However, unless the crater is lucky enough to get fossilized, it will be washed away, and its former location will then lose any stable earthly embodiment. The torrent of optical replicas will cease, and the old optical replicas will escape into space. So the classical information of where it was remains in the universe, but not the Earth.

How to obliterate earthly evidence of Jimmy Hoffa's demise? (Former US labor leader disappeared in 1975, presumed murdered by the New York City Mafia, but body was never found. Police are still searching.)

• Cremate his body and let the smoke and heat escape

• Dissolve the ashes to make a clear liquid, with no solid fragments, then pour the liquid into the ocean

• Don't tell anyone you did it, even on your deathbed

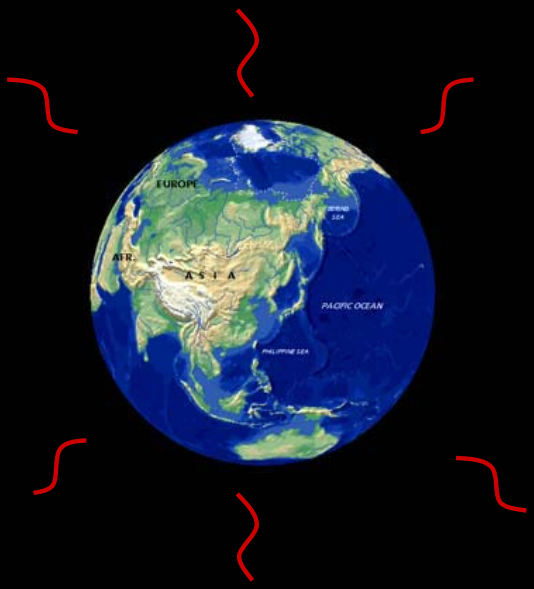
• For good measure, have yourself cremated and your ashes dissolved to make sure physical traces of your memory are thoroughly gone.

• Is it really impossible to recapture the escaped radiation?

• What is the ontological status of escaped information? Does God remember where the raindrops fell, even after all terrestrial evidence is gone?

• Even if classical information is lost from "hard" geological storage, might it still be retained in the earth's far more numerous "soft" degrees of freedom such as phonons in the earth's core and mantle?

• Can we outrun the radiation?



For example, one might hope to outrun the thermal radiation, because the refractive index of interstellar space is slightly >1.

But this hope is probably dashed by the accelerating expansion of the universe (a.k.a. cosmological constant, dark energy) which causes remote objects now visible (e.g. other galaxies) to eventually become inaccessible.

Ontological Status of Escaped Information

Consider a raindrop that may fall in one of 2 locations **L** or **R**.
Suppose that it forms, falls, and finally evaporates, so that all earthly record of where it fell is lost as radiation into the sky.

(**LLLL**+**RRRR**) /√2 Drop forms, falls and begins to emit radiative replicas into space. All observers, terrestrial and celestial, will see the drop as having fallen in one of two places. God sees a cat state-like superposition in which both outcomes happen.

(**LLLLL**+**RRRRR**) /√2 Drop begins to evaporate, emitting further radiative replicas.

(**LLLLL**+**RRRRR**) /√2 Drop has entirely evaporated. No terrestrial information remains about where it fell.

• Conclusion: Escape of last classical information from earth restores terrestrial observers to God's Olympian viewpoint in which both outcomes happened. Escaped information not so different, after all, from which-path information. Wheeler: "The past exists only insofar as it is recorded in the present."

The Evolving Human Viewpoint

• Before raindrop forms: Humans know it's about to rain, but they don't know where the drops will fall.

• (**LLLL**+**RRRR**) /√2 Humans agree where drop has fallen. Depending on how it affects their plans, they may or may not care, but they all agree that one of the outcomes R or L is real while the other is merely an unrealized possibility.

• (**LLLLL**+**RRRRR**) /√2 Drop has entirely evaporated. People may remember that it fell but no one remembers where. No other terrestrial memory remains about which of the possibilities, L or R, "happened" and which did not.

In the end, humans will come to accept what God knew all along, that the distinction between what happened and what might have happened is transient and illusory.
God, in His infinite modesty and tact, will not say "I told you so."

Most classical information, such as the pattern of snow flakes on the ground last winter, or rice grains on my dinner plate last night, is impermanent, eventually losing its durable embodiment and escaping from the earth in outgoing radiation.

Occasionally information is lucky enough to get fossilized by natural processes or recorded by humans in a durable medium. Such information can last billions of years.

Escaped information still exists in the universe, but it is inaccessible on earth.
Humans have little justification for continuing to think that one alternative actually happened and the other didn't.