Quantum Information Theory

Renato Renner
ETH Zurich

Do quantum computers exist?

Geordie Rose and his D-Wave quantum computer

Commercial devices

Quantum cryptography device by *id Quantique*, in operation at the FIFA World Cup competition in Durban

Commercial devices

Quantis Random Number Generator (4 Mbits/s)

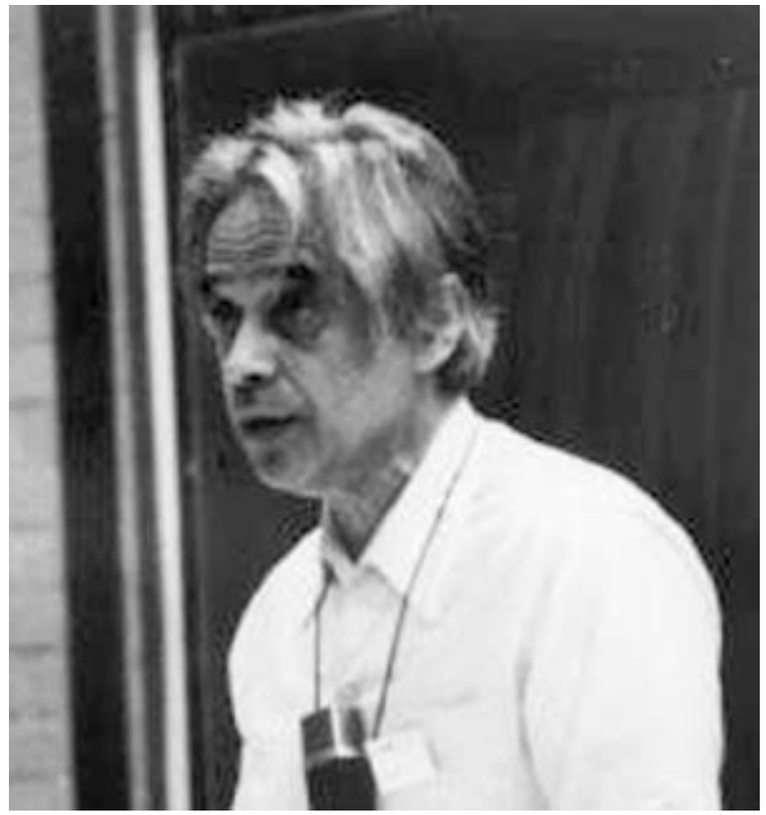
Is the world deterministic?

„Jedenfalls bin ich überzeugt, daß der nicht würfelt.“

Albert Einstein, in a letter to Max Born

It took several decades until the inherent non-deterministic nature of quantum theory was accepted as a “physical” fact.

„Mein Ziel war zu beweisen, dass niemand, nicht mal Gott, den Verlauf der Welt voraussagen kann.“

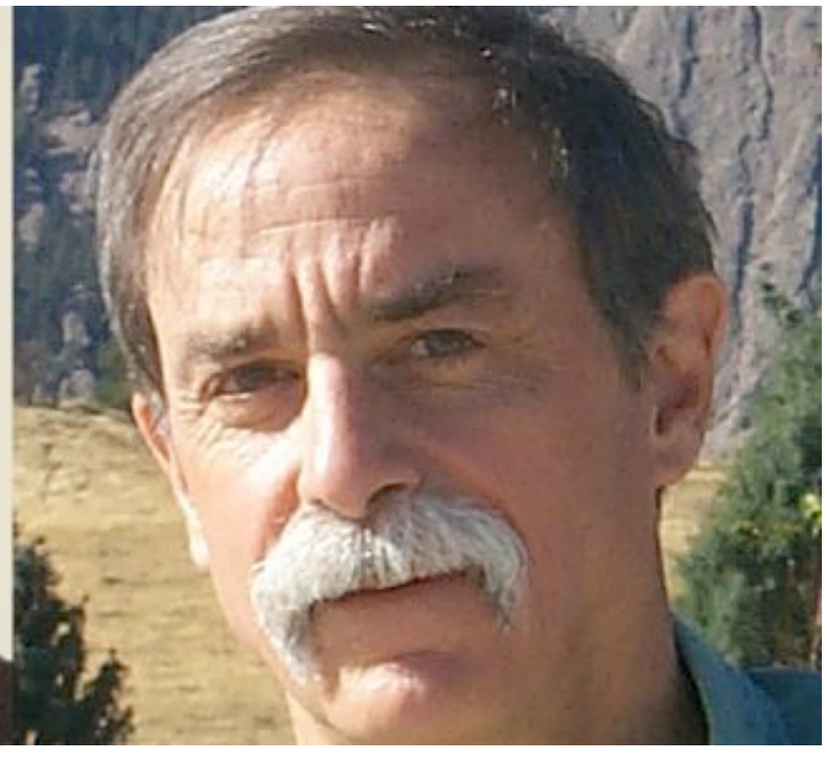


Ernst Specker (mathematician, ETH Zurich)

Research in quantum information

Nobel prize
2012

Serge Haroche



David Wineland

Research in quantum information

Research groups in quantum information science (from http://www.quantiki.org)

Research in quantum information

QSIT Quantum Science and Technology
National Centre of Competence in Research

Swiss network consisting of more than 300 scientists

YouTube™ → QSIT

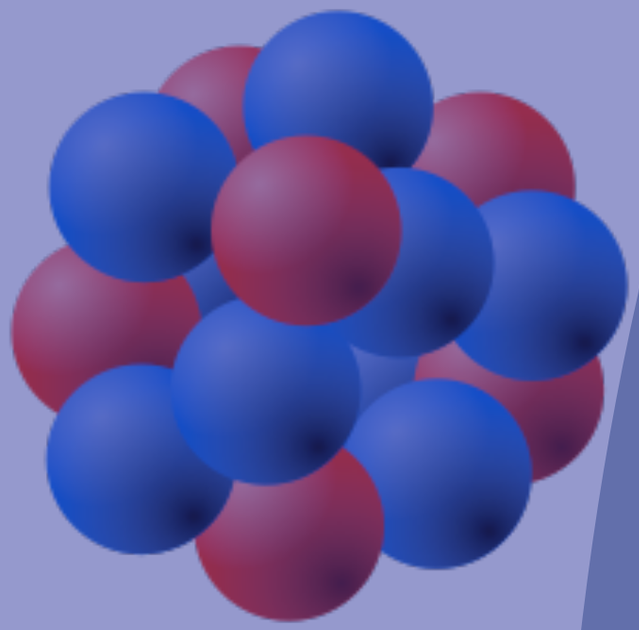
Quantum
Information Theory

What is “quantum”?

quantum physics

classical physics

general relativity

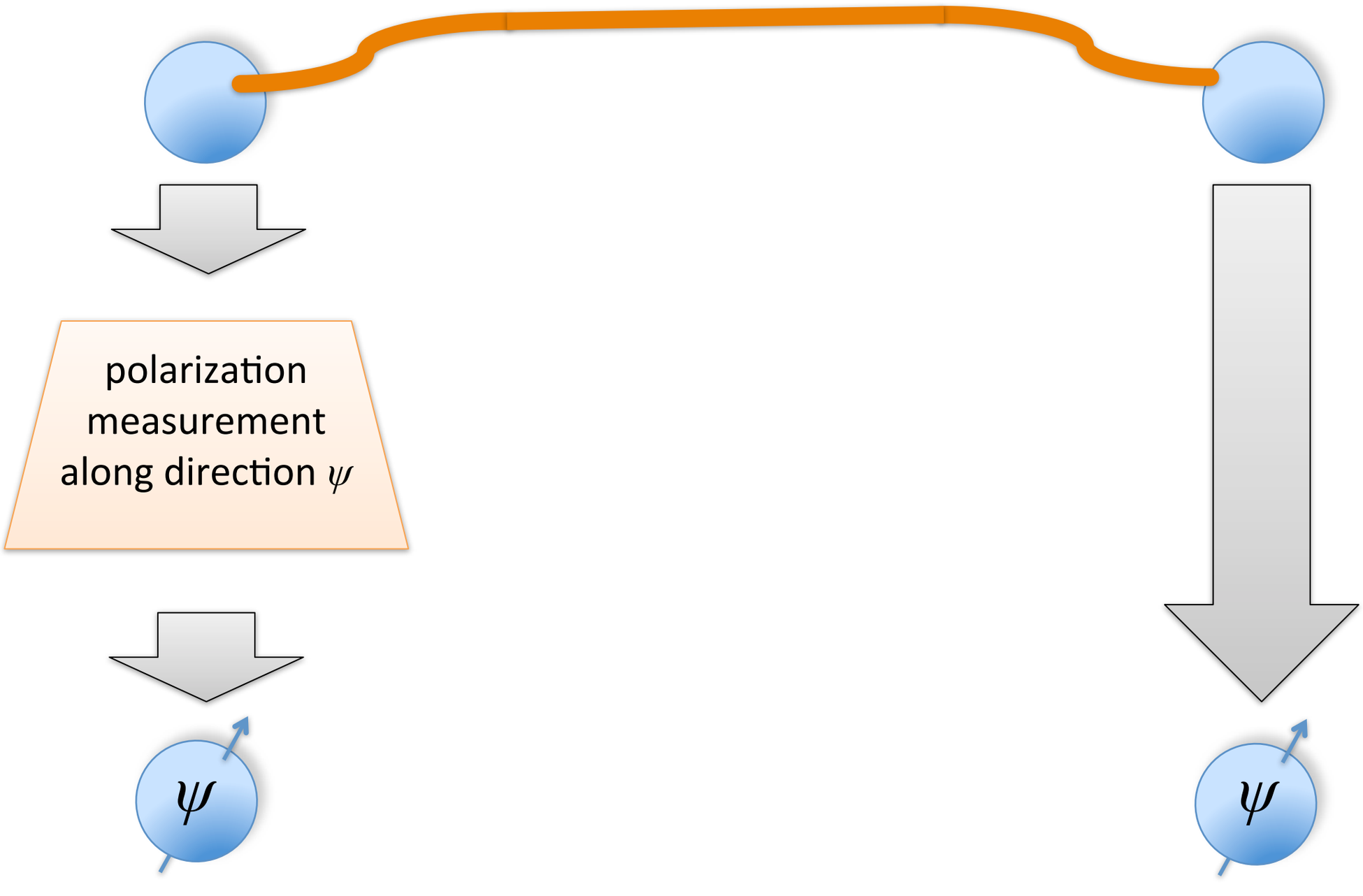


10^{-15} m 10^{-9} m 10^{-3} m 10^{3} m 10^{9} m 10^{15} m 10^{21} m

1 fm 1 pm 1 nm 1 µm 1 mm 1 m 1 km 1 Mm 1 Gm 1 Tm 1 Pm 1 Em 1 Zm

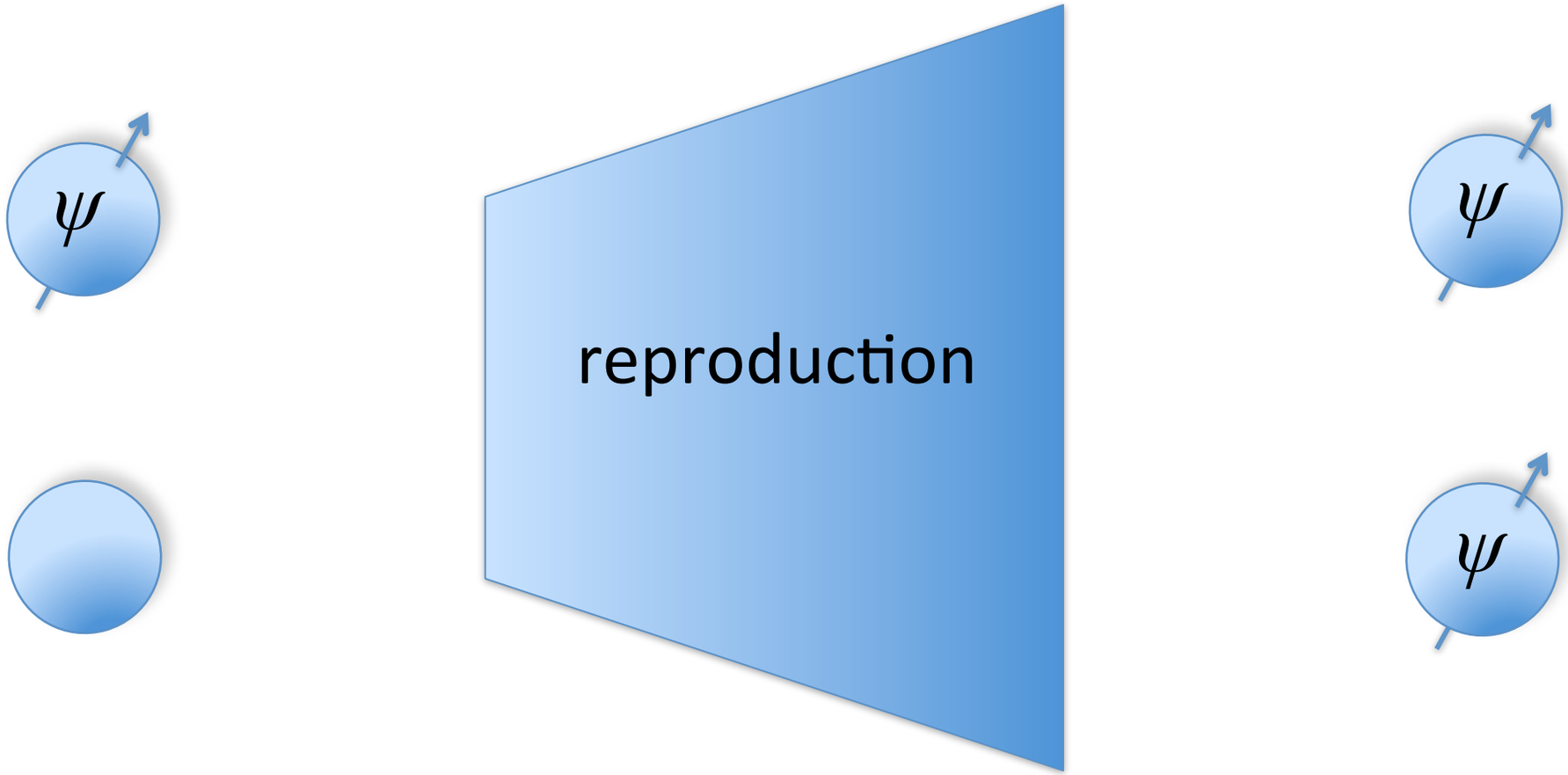
Quantum physics deviates from our day-to-day experience about the world around us

Example 1: Entanglement



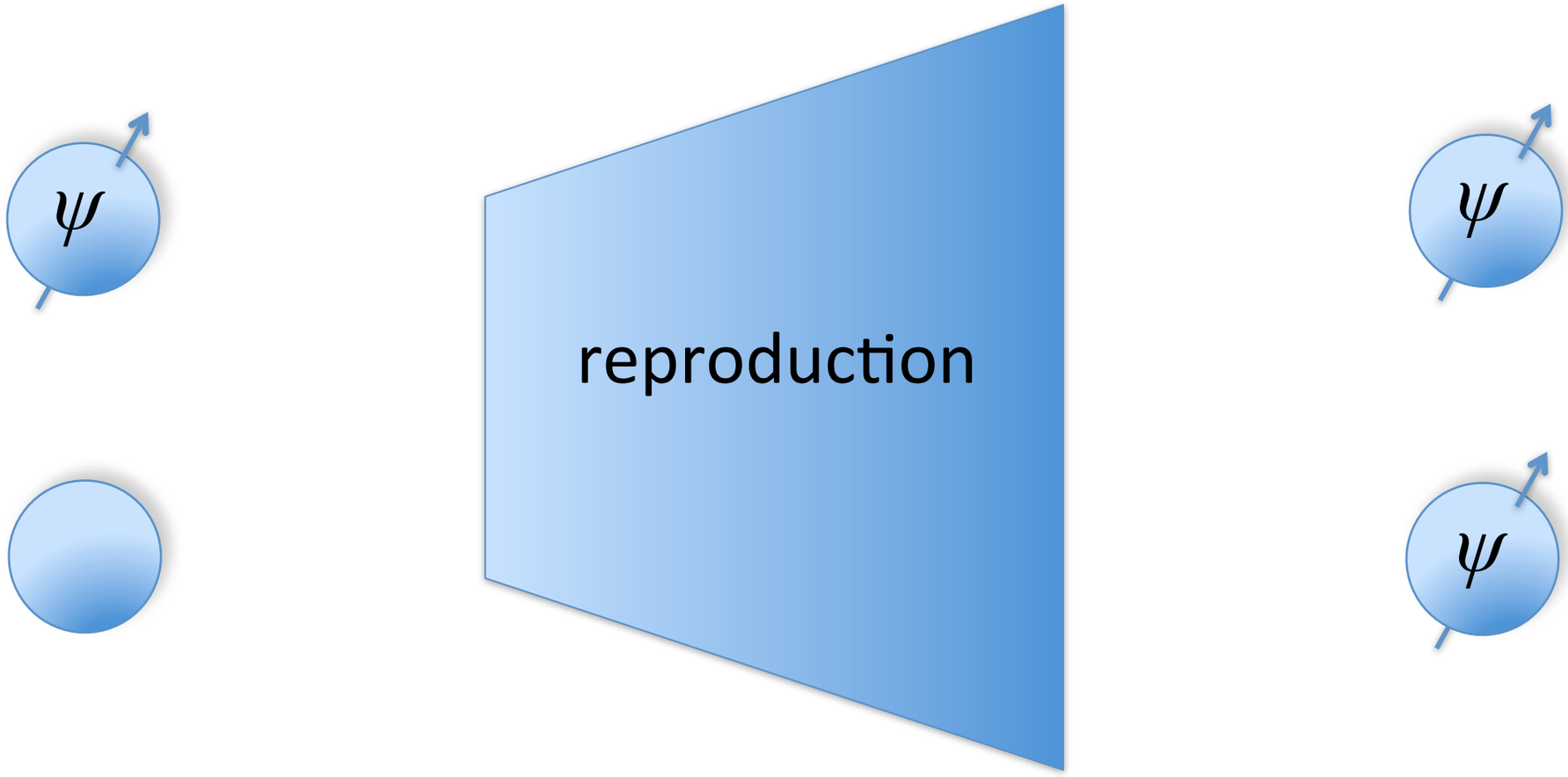
Quantum physics deviates from our day-to-day experience about the world around us

Example 2: No-cloning principle



Quantum physics deviates from our day-to-day experience about the world around us

Example 2: No-cloning principle



No-cloning theorem [Wootters und Zurek, 1982]

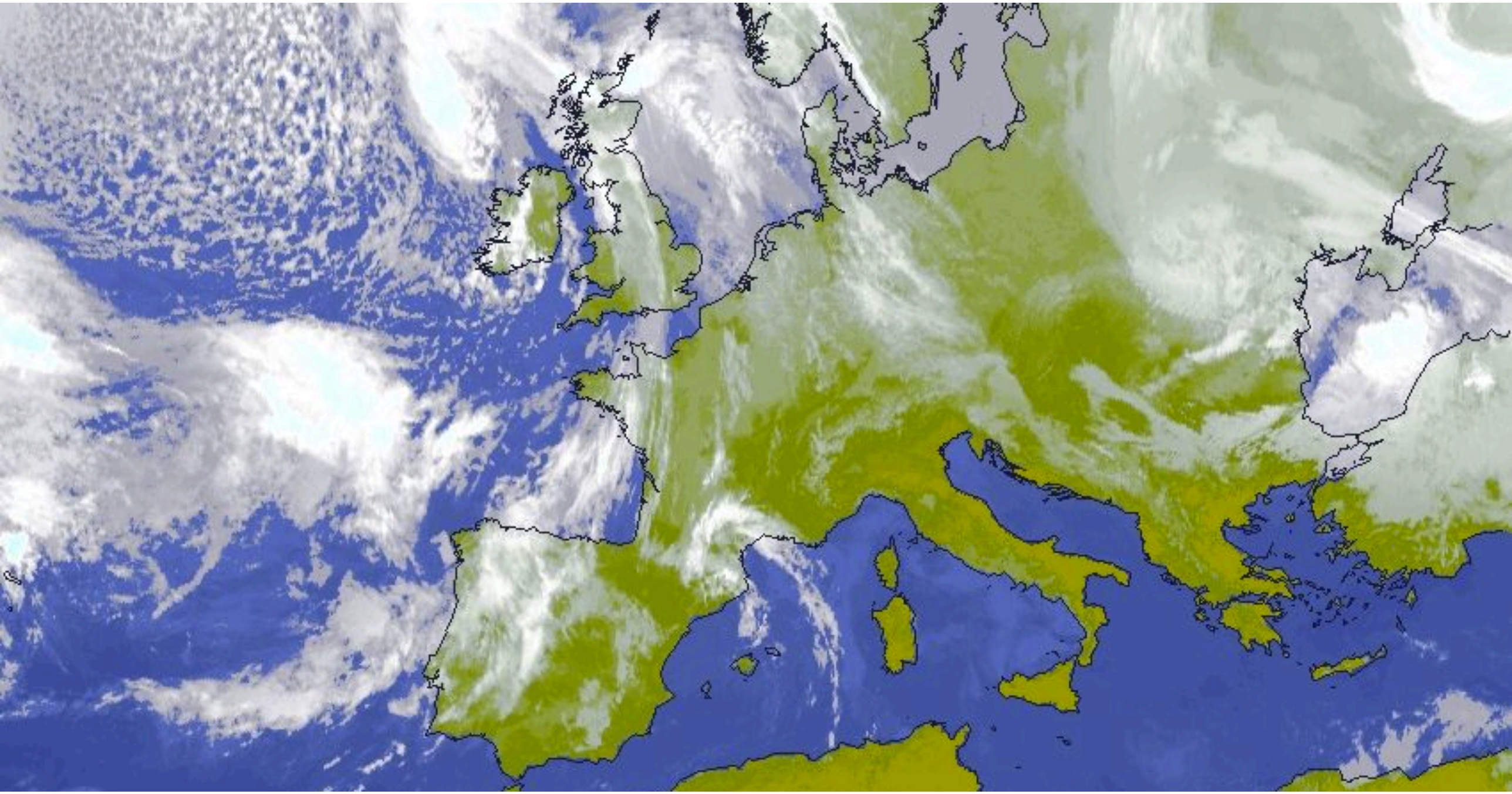
No physical device can copy the state of a quantum system (for arbitrary states ψ).

The no-cloning principle does not seem to be valid for macroscopic objects

reproduction

Quantum
Information Theory

What is “information”?



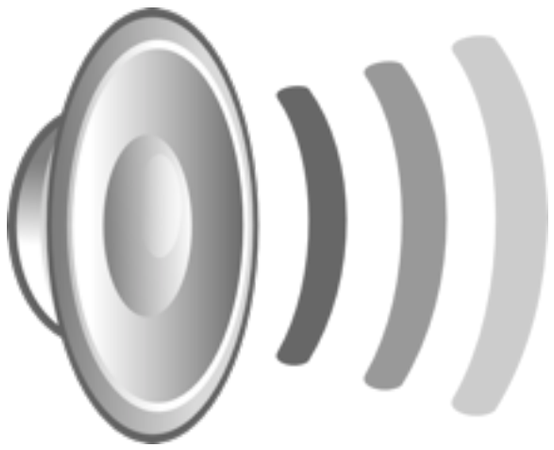
Two different approaches

Kolmogorov's notion:
based on the theory of computation

Shannon's notion:
based on probability theory

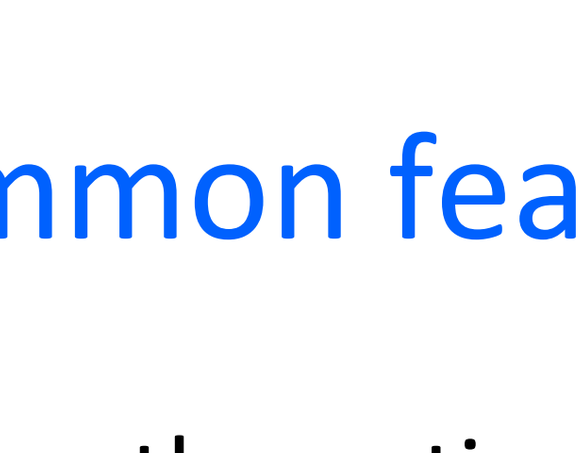
Common feature of both approaches

The mathematical theory should be independent of how information is represented.



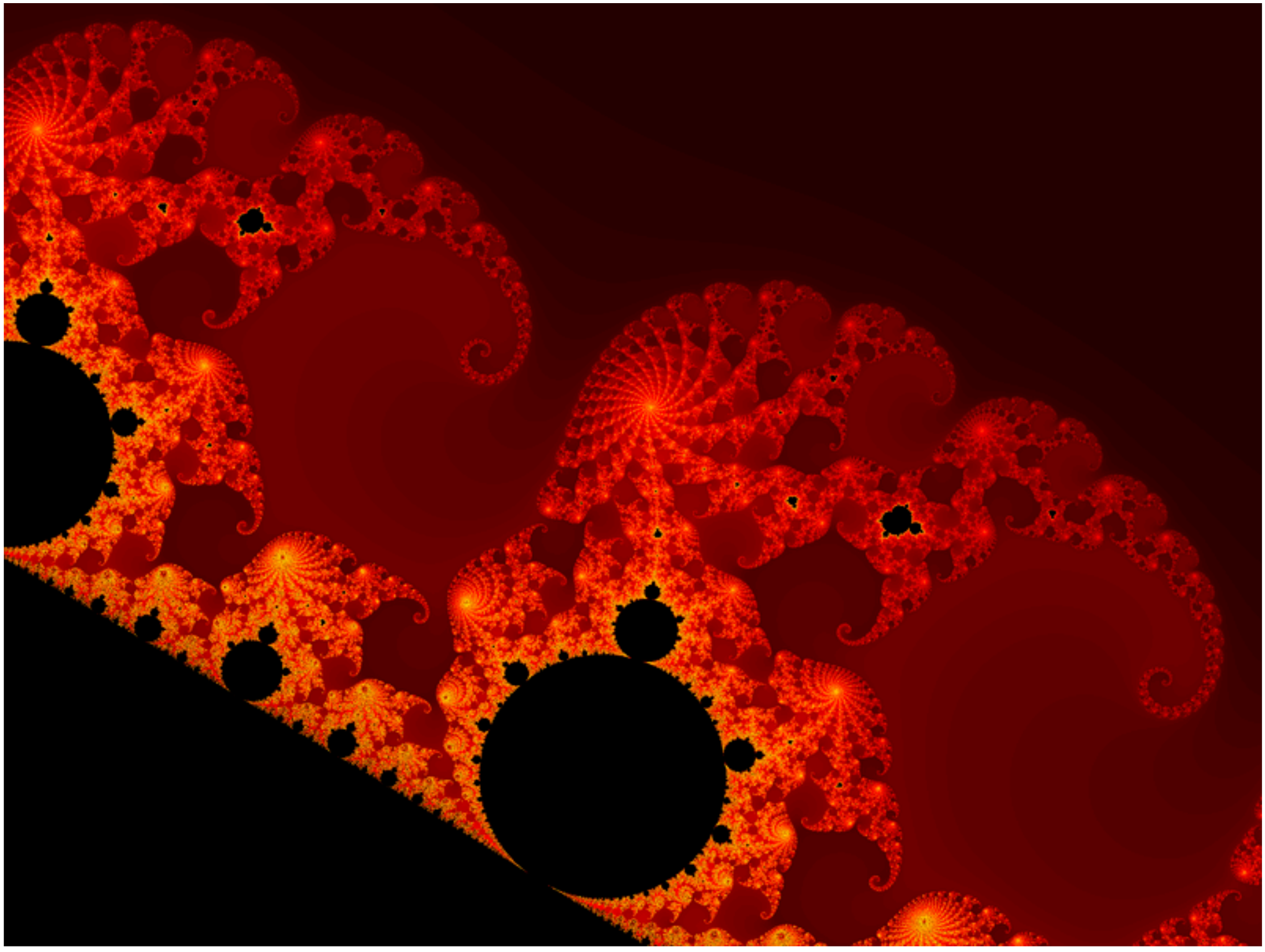
Common feature of both approaches

The mathematical theory should be independent of how information is represented.



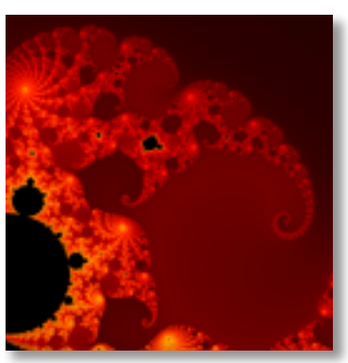
As we shall see, this idea is doomed to fail …

Kolmogorov’s notion of information



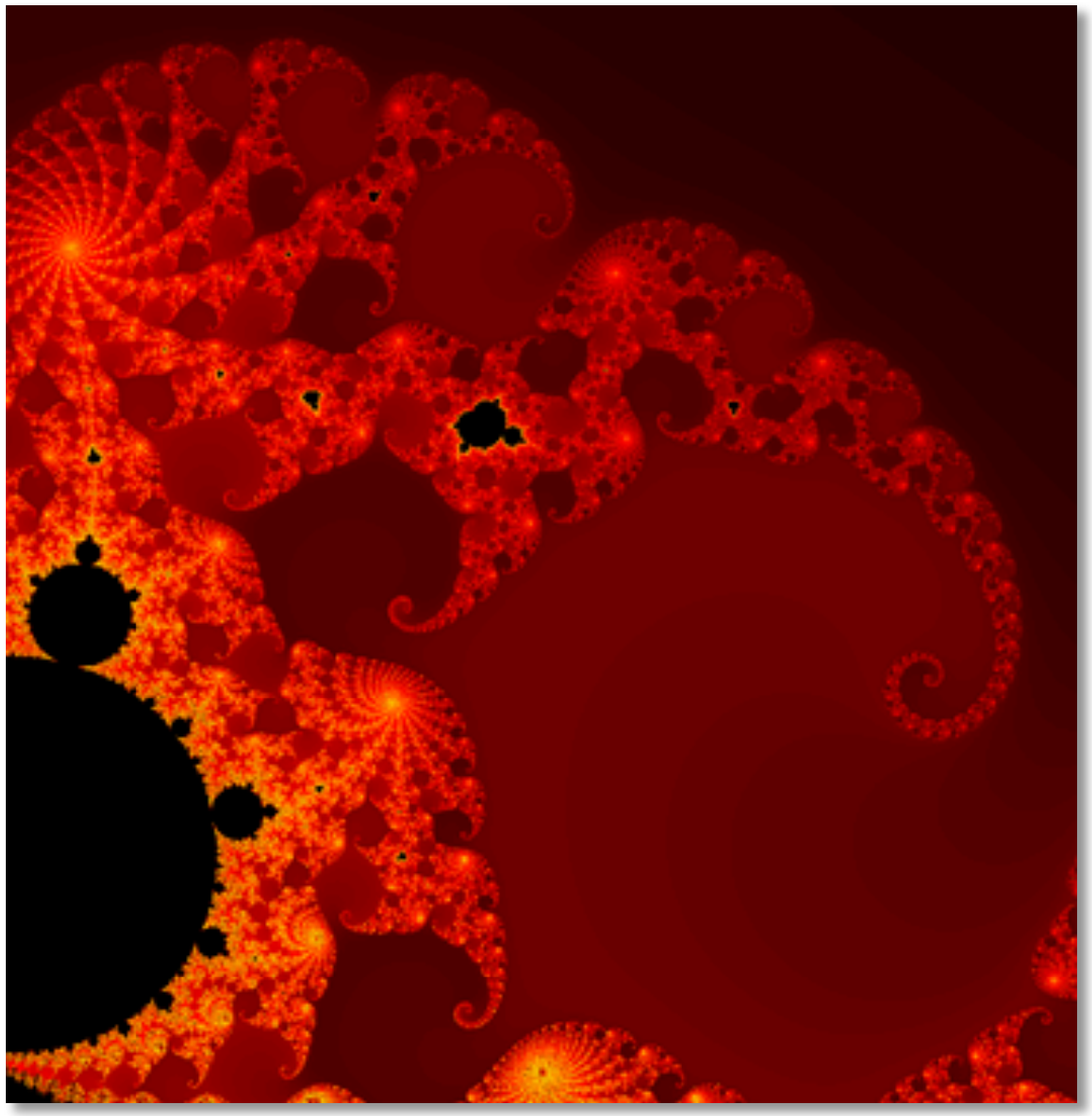
What is information?

```
For each pixel (x0,y0) on the screen do:
{  x = 0   y = 0
iteration = 0  max_iteration = 1000
while ( x*x + y*y <= (2*2)  AND  iteration < max_iteration )
{  xtemp = x*x - y*y + x0
y = 2*x*y + y0
x = xtemp
iteration = iteration + 1      }
if ( iteration == max_iteration )
then color = black
else  color = iteration
plot(x0,y0,color)    }
```



The algorithm reproduces this picture.

What is information?



≈

```
For each pixel on the screen do:
{  x = 0   y = 0
iteration = 0  max_iteration = 1000
while ( x*x + y*y <= (2*2)  AND
iteration < max_iteration )
{  xtemp = x*x - y*y + x0
     y = 2*x*y + y0
     x = xtemp
  iteration = iteration + 1      }
if ( iteration == max_iteration )
then color = black
else  color = iteration
plot(x0,y0,color)    }
```

Information can be represented in various equivalent ways.

Kolmogorov's notion of information

Definition [Kolmogorov]:

The "information content" of a "message" m is the length (in number of bits) of the shortest program that outputs m.

Kolmogorov's notion of information

Definition [Kolmogorov]:
The "information content" of a "message" m is the length (in number of bits) of the shortest program that outputs m.

Examples

Kolmogorov's notion of information

Definition [Kolmogorov]:
The "information content" of a "message" m is the length (in number of bits) of the shortest program that outputs m.

Examples

(1) m = 000000000000000000000000000000000000

Kolmogorov's notion of information

Definition [Kolmogorov]:
The "information content" of a "message" m is the length (in number of bits) of the shortest program that outputs m.

Examples

(1) m = 000000000000000000000000000000000000

(2) m = 000000000000100000000000010000000001

Kolmogorov's notion of information

Definition [Kolmogorov]:
The "information content" of a "message" m is the length (in number of bits) of the shortest program that outputs m.

Examples

(1) m = 000000000000000000000000000000000000

(2) m = 000000000000100000000000010000000001

(3) m = 15926535897932384626433832795028841 97

Kolmogorov's notion of information

Definition [Kolmogorov]:
The "information content" of a "message" m is the length (in number of bits) of the shortest program that outputs m.

Examples

(1) m = 000000000000000000000000000000000000

(2) m = 000000000000100000000000010000000001

(3) m = 15926535897932384626433832795028841 97

(4) m = 38458795016481354847647493584185001 47

Kolmogorov’s notion of information

Kolmogorov's notion of information

Kolmogorov's definition of "information content" has some remarkable properties:

Kolmogorov's notion of information

Kolmogorov's definition of "information content" has some remarkable properties:

- Model-independent: it is independent of the underlying "programming language" (up to an additive constant).

Kolmogorov's notion of information

Kolmogorov's definition of "information content" has some remarkable properties:

- Model-independent: it is independent of the underlying "programming language" (up to an additive constant).
- Incomputable: There is no algorithm that takes as input a message m and outputs its information content.

Shannon’s notion of information

Shannon's notion of information

Definition [Shannon]:

The "information content" $\mathrm{S}(m)$ of a "message" m is equal to the negative logarithm of its probability $\Pr[m]$, i.e., $\mathrm{S}(m) = -\log_2 \Pr[m]$.

Shannon's notion of information

Definition [Shannon]:
The "information content" $\mathrm{S}(m)$ of a "message" m is equal to the negative logarithm of its probability $\Pr[m]$, i.e., $\mathrm{S}(m) = -\log_2 \Pr[m]$.

Examples

Shannon's notion of information

Definition [Shannon]:
The "information content" $\mathrm{S}(m)$ of a "message" m is equal to the negative logarithm of its probability $\Pr[m]$, i.e., $\mathrm{S}(m) = -\log_2 \Pr[m]$.

Examples

(1) m: the lottery numbers

Shannon's notion of information

Definition [Shannon]:
The "information content" $\mathrm{S}(m)$ of a "message" m is equal to the negative logarithm of its probability $\Pr[m]$, i.e., $\mathrm{S}(m) = -\log_2 \Pr[m]$.

Examples

(1) m: the lottery numbers

(2) m: message whether you have won the lottery

Shannon's notion of information

Definition [Shannon]:
The "information content" $\mathrm{S}(m)$ of a "message" m is equal to the negative logarithm of its probability $\Pr[m]$, i.e., $\mathrm{S}(m) = -\log_2 \Pr[m]$.

Examples

(1) m: the lottery numbers

(2) m: message whether you have won the lottery

(3) $m = \pi$

Shannon's notion of information

Definition [Shannon]:
The "information content" $\mathrm{S}(m)$ of a "message" m is equal to the negative logarithm of its probability $\Pr[m]$, i.e., $\mathrm{S}(m) = -\log_2 \Pr[m]$.

Examples

(1) m: the lottery numbers

(2) m: message whether you have won the lottery

(3) $m = \pi$

(4) m: random bitstring of length n

Shannon’s notion of information

Shannon's notion of information

Some remarks on Shannon's definition of "information content":

Shannon's notion of information

Some remarks on Shannon's definition of "information content":

- Probabilistic definition: Requires an underlying probability distribution P_M on the set of messages M.

Shannon's notion of information

Some remarks on Shannon's definition of "information content":

- Probabilistic definition: Requires an underlying probability distribution P_M on the set of messages M.
- Easily computable.

Shannon's notion of information

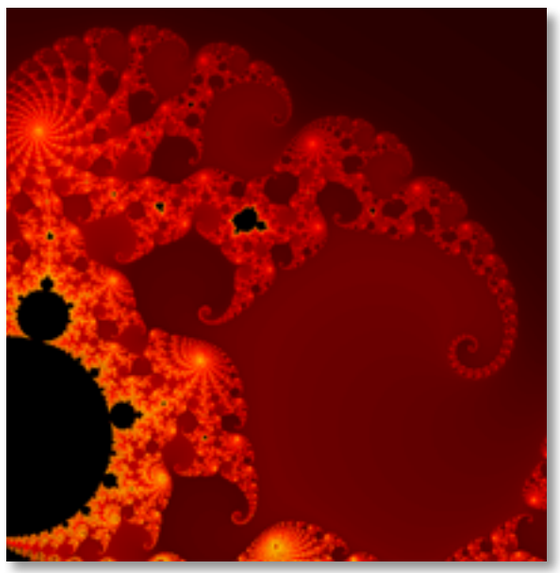
Some remarks on Shannon's definition of "information content":

- Probabilistic definition: Requires an underlying probability distribution P_M on the set of messages M.
- Easily computable.
- Widely used in modern information theory (in theory and practice).

The idea of information compression

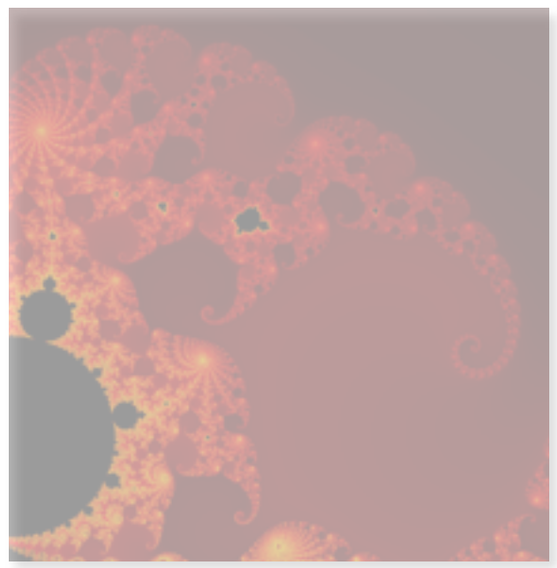
Suppose that we want to transmit the picture over a communication channel with limited capacity.

Sender



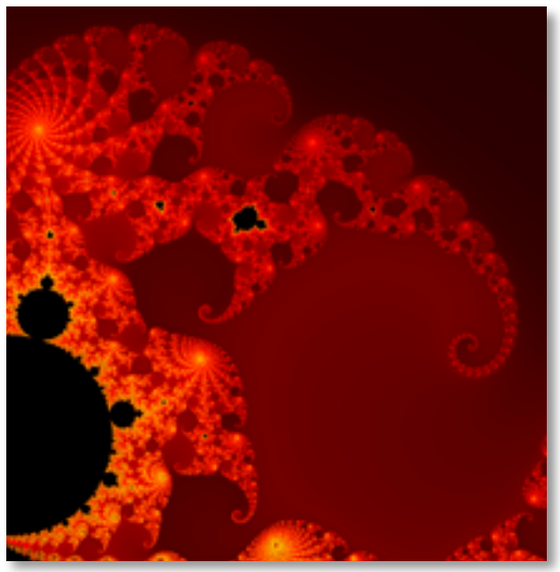
1000 bit channel

Receiver



The idea of information compression

Sender

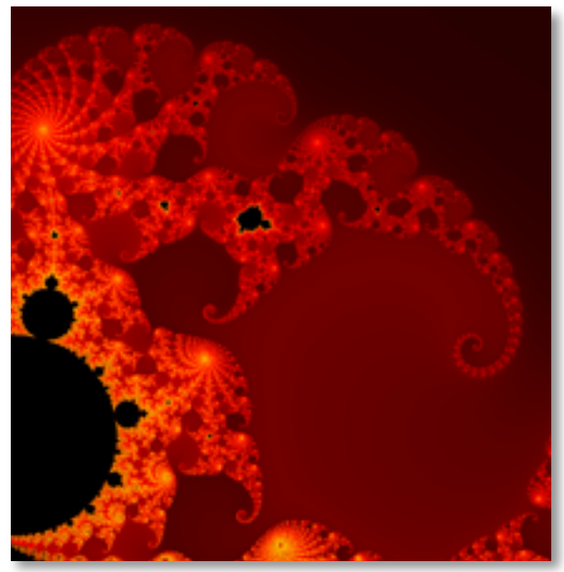


Compression

For each pixel on the screen do:
{ x = 0 y = 0
iteration = 0 max_iteration = 1000
while (x*x + y*y <= (2*2) AND iteration
< max_iteration)
{ xtemp = x*x - y*y + x0
y = 2*x*y + y0
x = xtemp
iteration = iteration + 1 }
if (iteration == max_iteration)
then color = black
else color = iteration
plot(x0,y0,color) }

1000 bit channel

Receiver

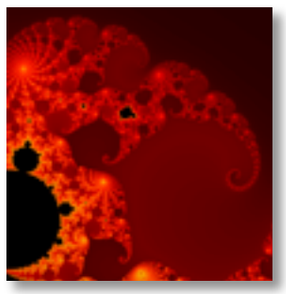


Decoding

For each pixel on the screen do:
{ x = 0 y = 0
iteration = 0 max_iteration = 1000
while (x*x + y*y <= (2*2) AND iteration
< max_iteration)
{ xtemp = x*x - y*y + x0
y = 2*x*y + y0
x = xtemp
iteration = iteration + 1 }
if (iteration == max_iteration)
then color = black
else color = iteration
plot(x0,y0,color) }

The idea of information compression

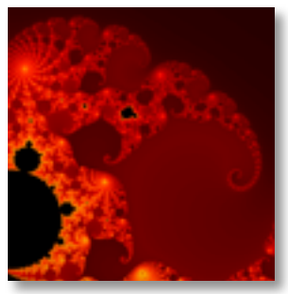
M



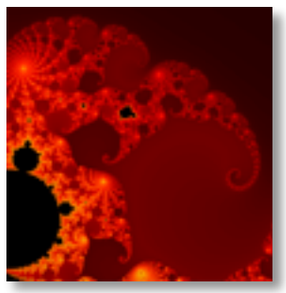
For each pixel on the screen do:
{ x = 0 y = 0
iteration = 0 max_iteration = 1000
while (x*x + y*y <= (2*2) AND iteration < max_iteration)
{ xtemp = x*x - y*y + x0
y = 2*x*y + y0
x = xtemp
iteration = iteration + 1 }
if (iteration == max_iteration)
then color = black
else color = iteration
plot(x0,y0,color) }

1000 bits

For each pixel on the screen do:
{ x = 0 y = 0
iteration = 0 max_iteration = 1000
while (x*x + y*y <= (2*2) AND iteration < max_iteration)
{ xtemp = x*x - y*y + x0
y = 2*x*y + y0
x = xtemp
iteration = iteration + 1 }
if (iteration == max_iteration)
then color = black
else color = iteration
plot(x0,y0,color) }



M



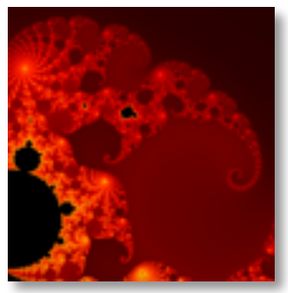
For abcdef
Hijklmnop
Qrstuvw
Xzy xyz

For abcdef
Hijklmnop
Qrstuvw
Xzy xyz

200 bits

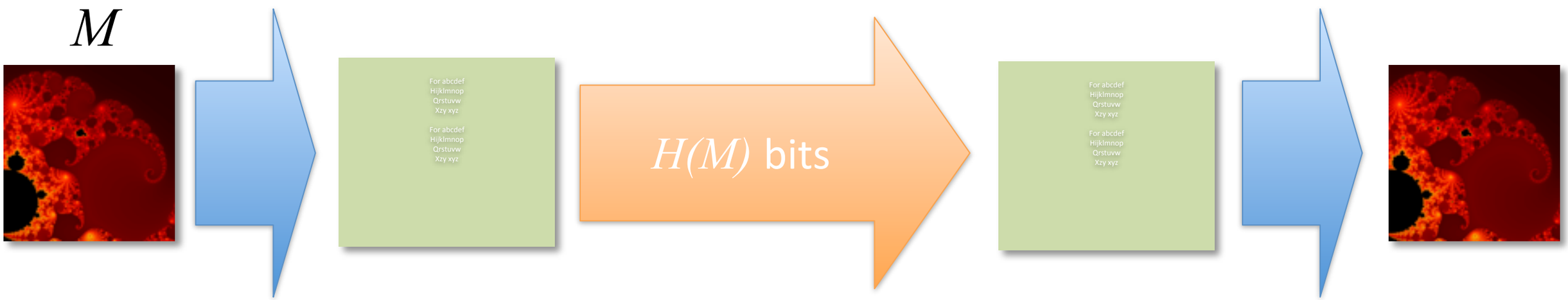
For abcdef
Hijklmnop
Qrstuvw
Xzy xyz

For abcdef
Hijklmnop
Qrstuvw
Xzy xyz



Quantify information content of a message M by the size (in # bits) of the minimal compression.

Shannon entropy and compression

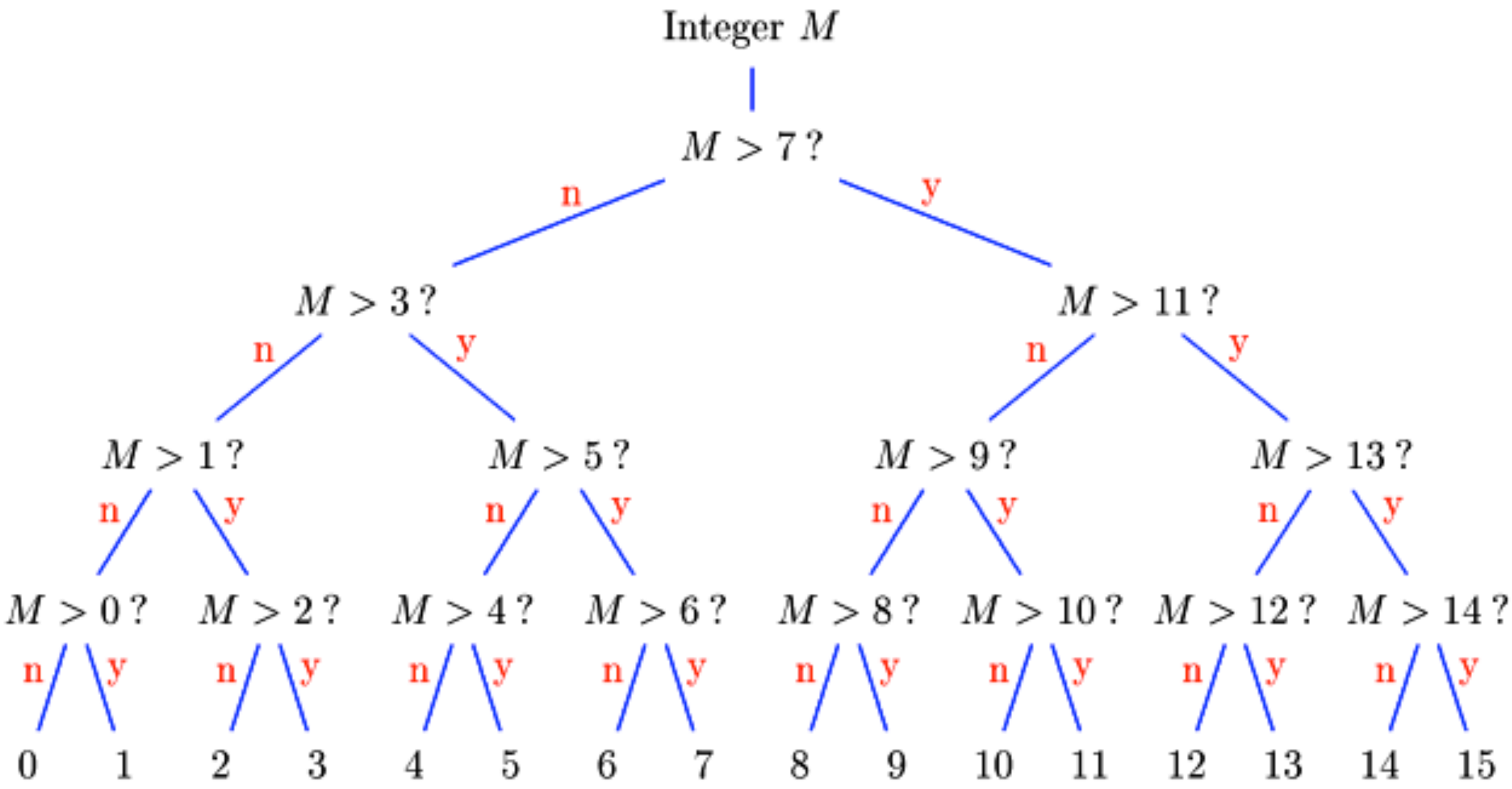


$$H(M) = -\sum_m p_m \log_2 p_m$$

Theorem [Shannon 1948]

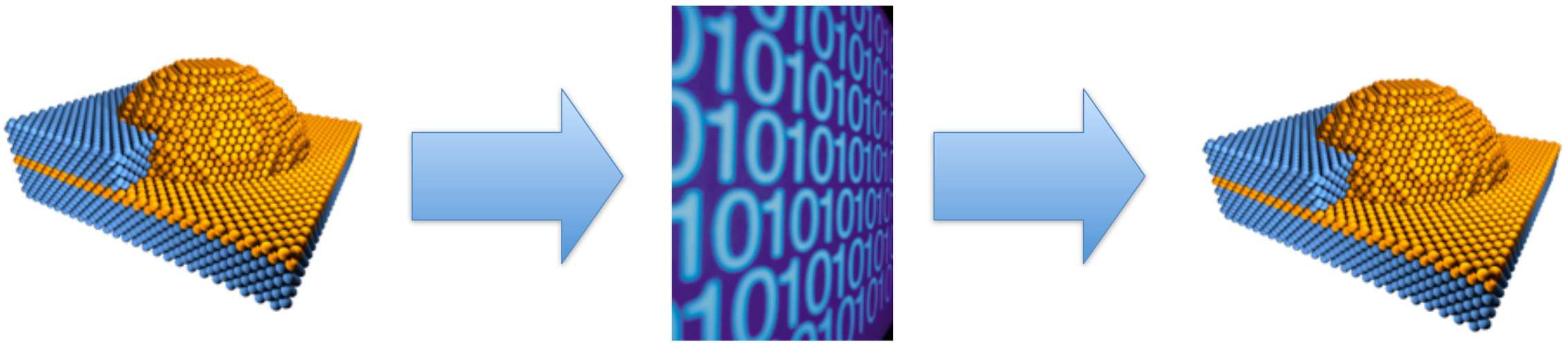
The Shannon entropy $H(M)$ corresponds to the minimum (average) compression length of M.

Compression according to Shannon

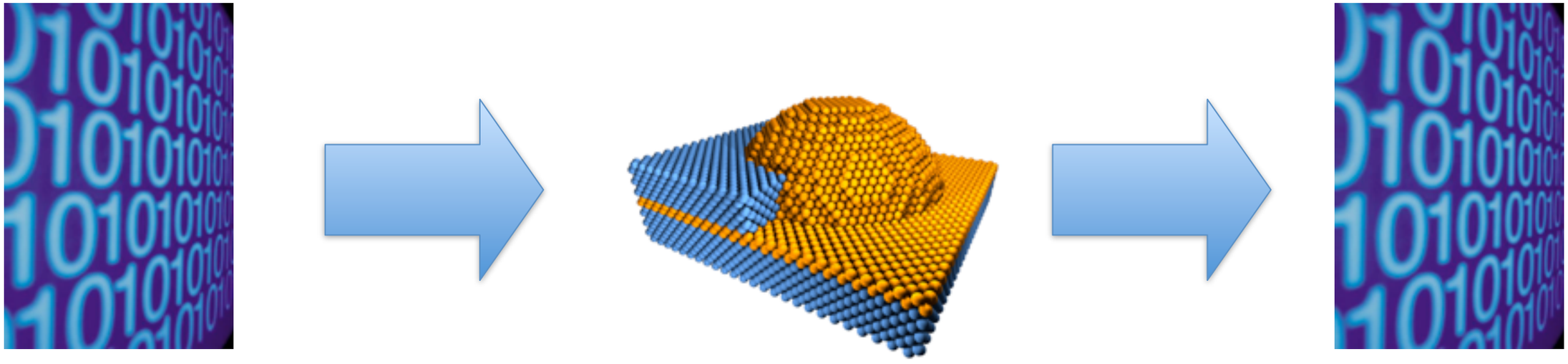


Operational relevance

- Given a physical object, how much information is required to describe it?



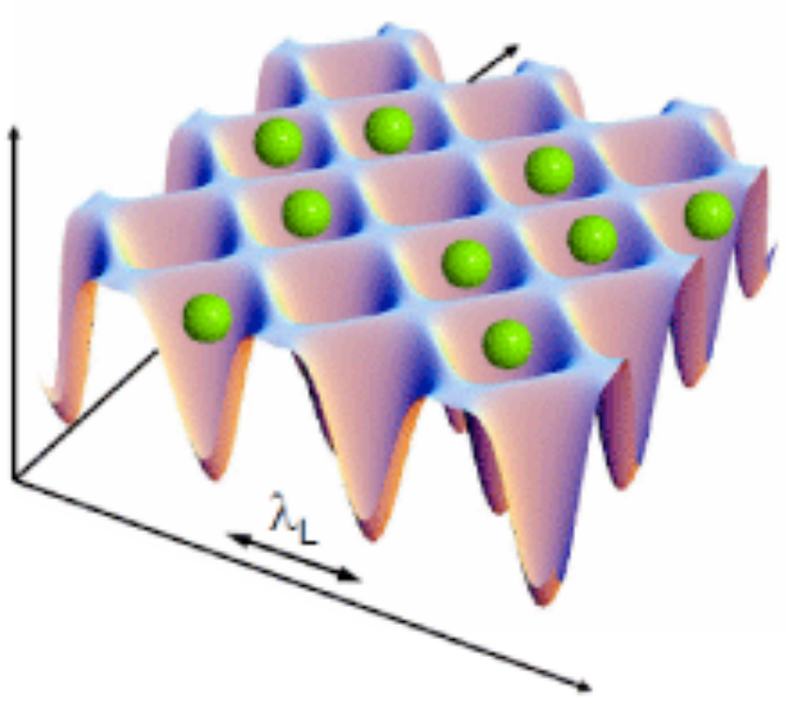
- Given a physical device, what is the maximum amount of information that can be stored reliably?



Why are such questions interesting?

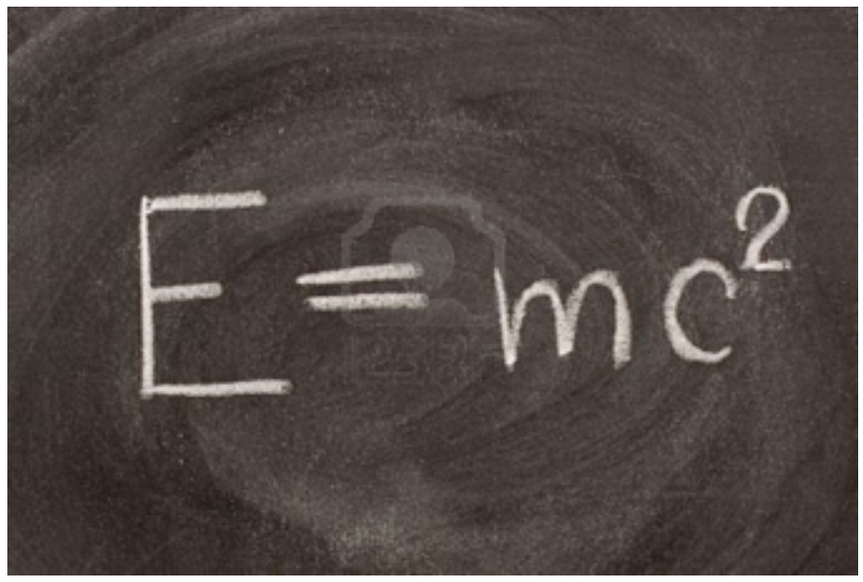
- Technological applications (information processing and transmission)

- Simulatability of physical systems



Why are such questions interesting? (cont'd)

- Development of physical theories



- Used in other areas of science (biology, finances, linguistics, …)

Linking Quantum Physics and Information Theory

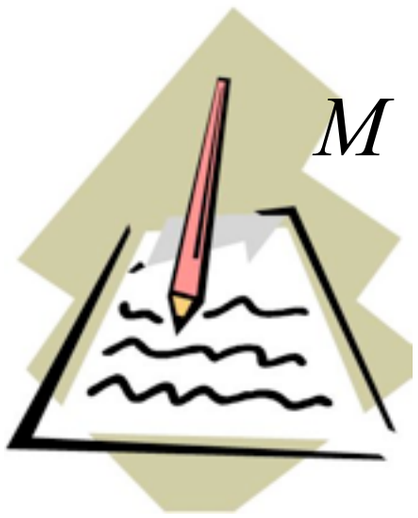
Information is physical

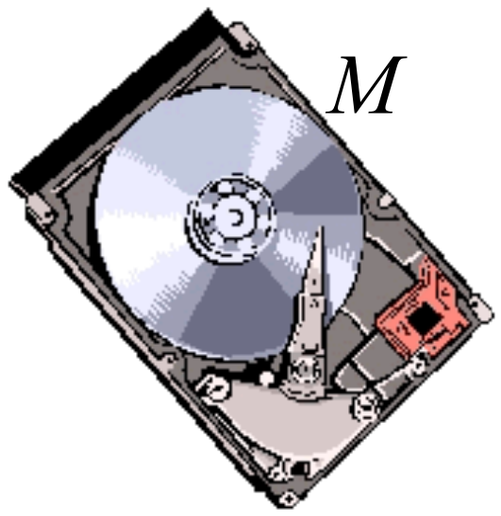
- Rolf Landauer:
  “information is always represented by the state of a physical system”.

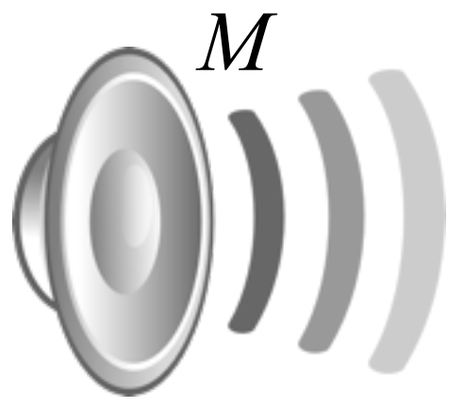
- If information is represented by a quantum system then it is by definition “quantum information”.

Independence of information carriers

According to Shannon's theory, information is independent of the "physical information carriers".





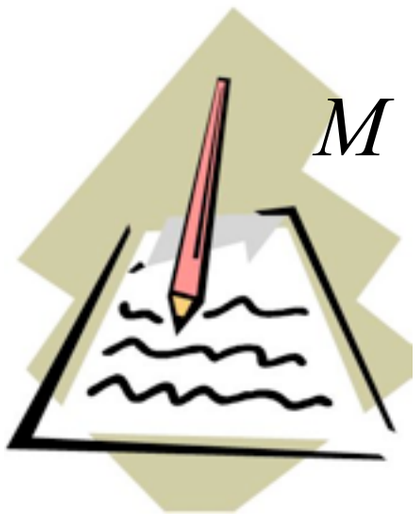


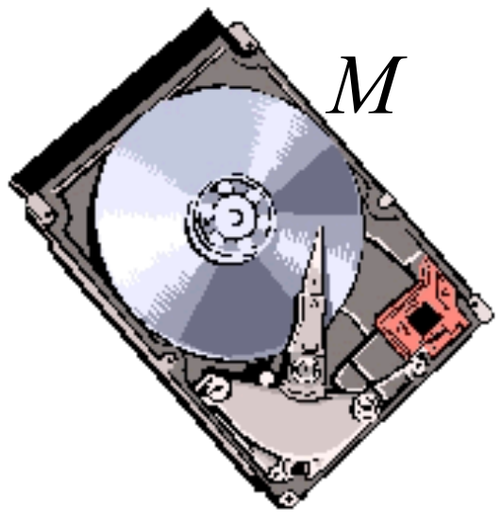
Representation of a message M

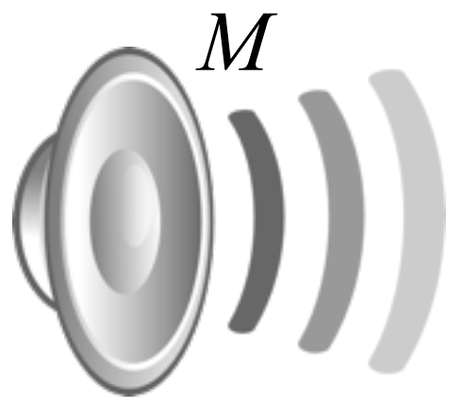
Each value $M=m$ is represented by a different physical state of the system.

Independence of information carriers

According to Shannon's theory, information is independent of the "physical information carriers".





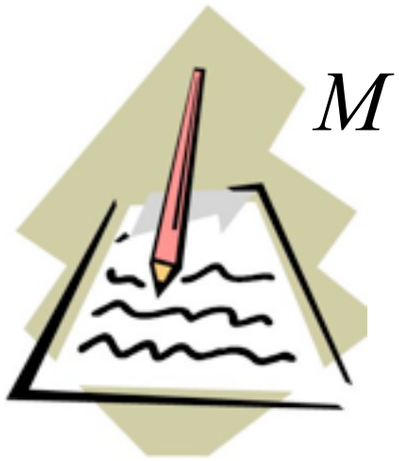


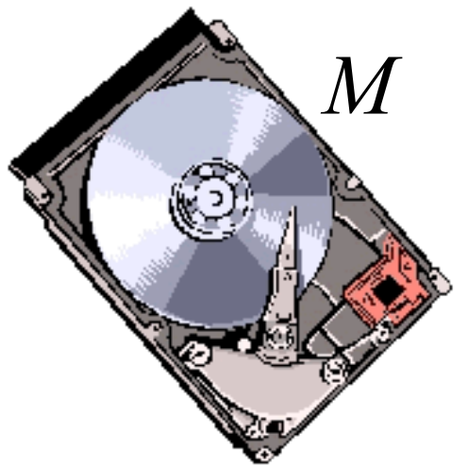
Representation of a bit

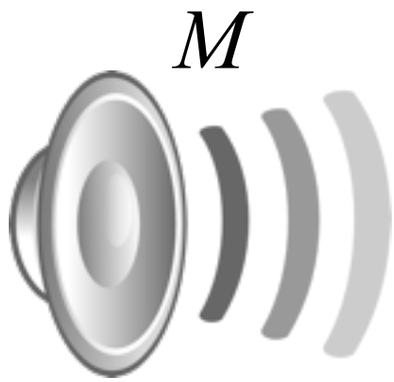
Each value of a bit ("0" or "1") is represented by two different (perfectly distinguishable) states of the information carrier.

Independence of information carriers?

According to Shannon's theory, information is independent of the "physical information carriers".

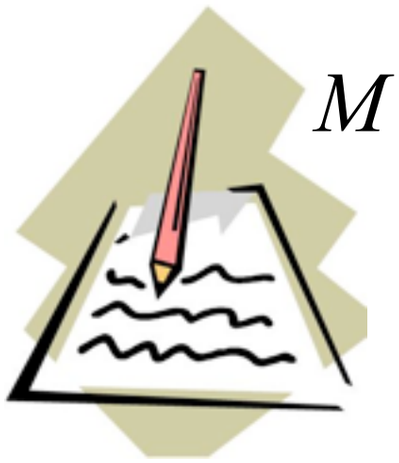


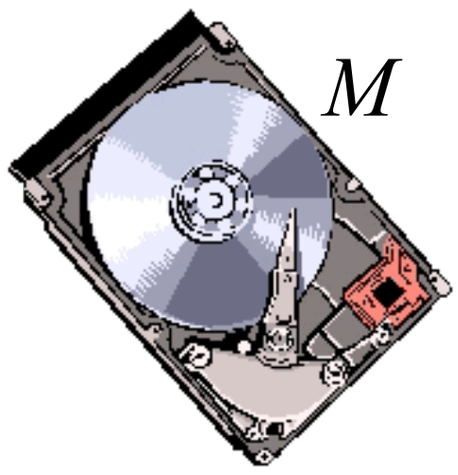


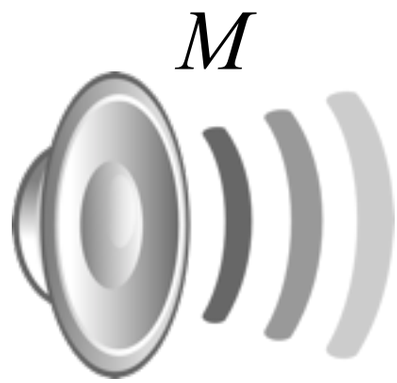


Independence of information carriers?

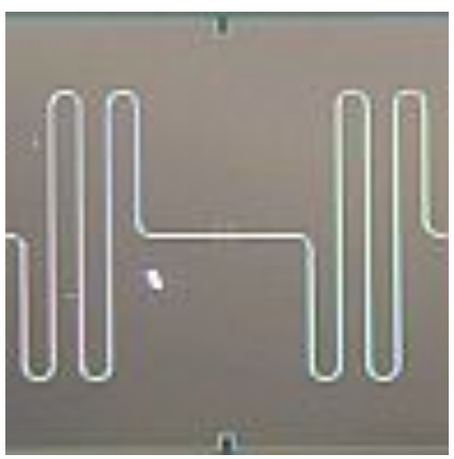
According to Shannon's theory, information is independent of the "physical information carriers".

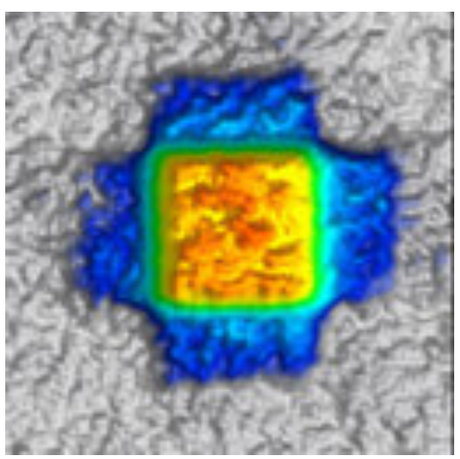


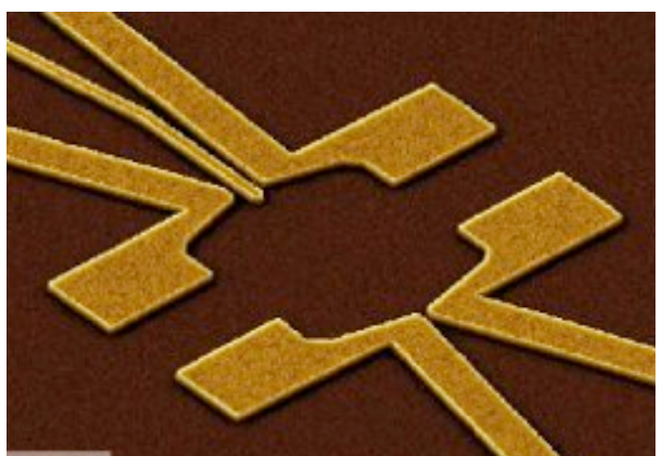




But does this paradigm also apply to information stored in quantum devices?







[Photos: QSIT]

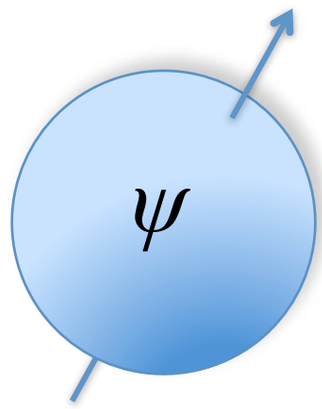
Classical information

Classically, information may always be represented as a sequence of binary numbers (the bits).

0 - 1

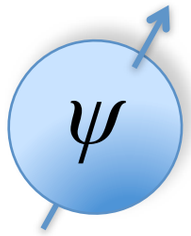
Quantum information

Quantum information is represented as the state of a quantum system, such as the polarization degree of freedom of a photon.



Qubit

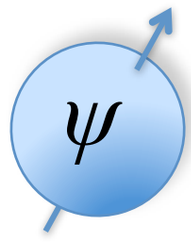
Although the smallest possible unit of quantum information is a that represented on a two-level system (a qubit), there is a continuum of states.



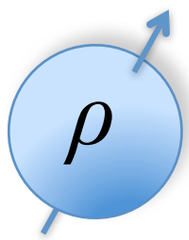
The state of a qubit is generally represented as a vector in C^2.

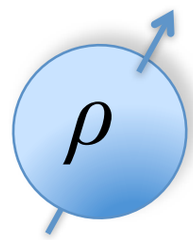
Qubits

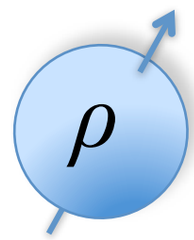
The state of a *single* system is specified by a 2-dimensional vector $\psi \in C^2$



The state of n qubits is specified by a 2^n-dimensional vector $\psi \in C^{2^n}$

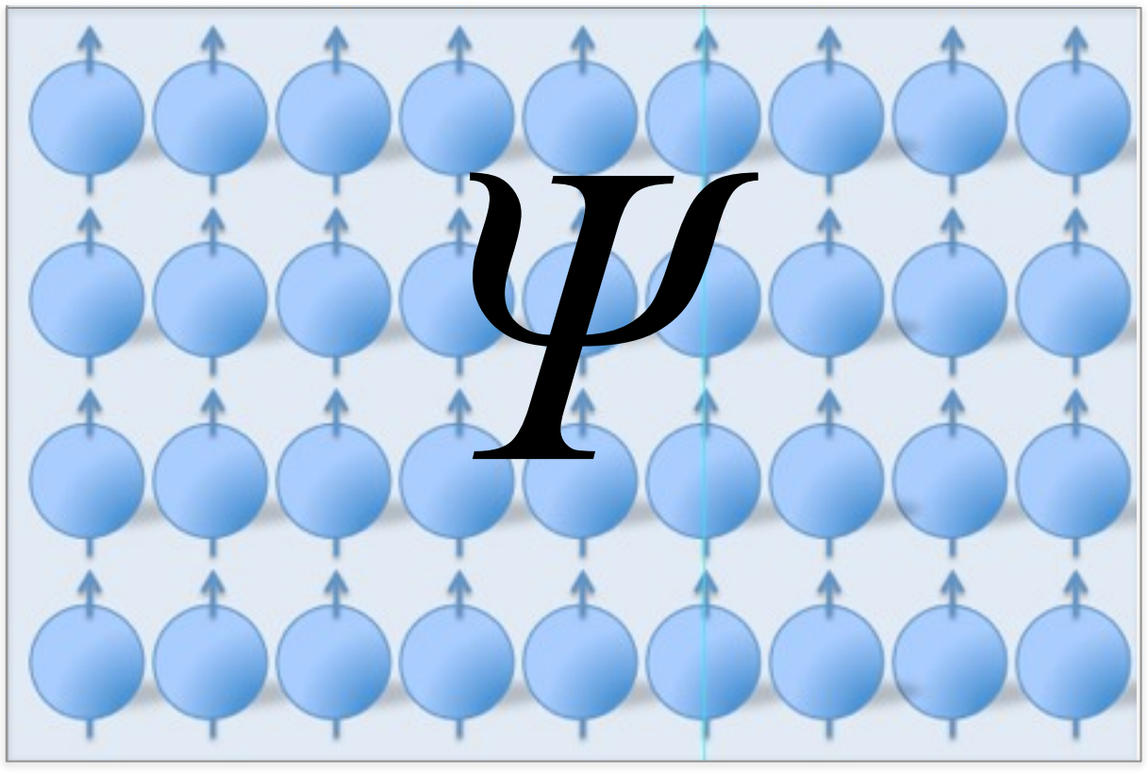






Comparison: bits vs qubits

36 qubits

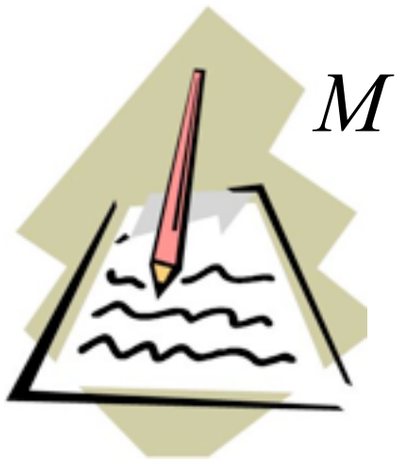


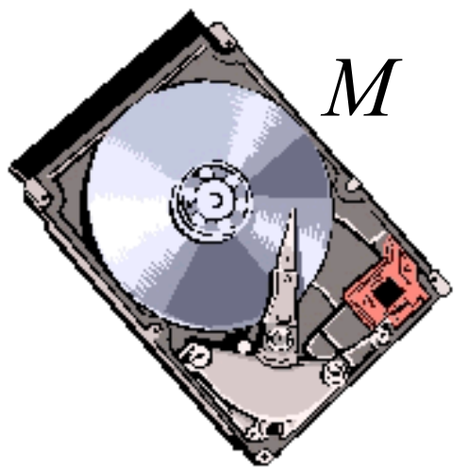
2^{36} coordinates

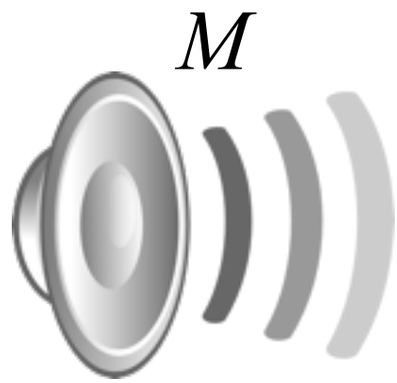
> 100 GByte

Independence of information carriers?

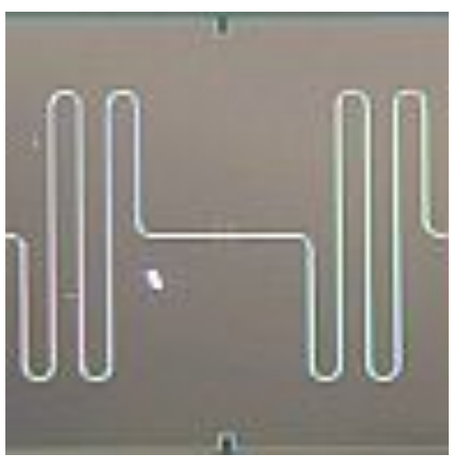
According to Shannon's theory, information is independent of the "physical information carriers".

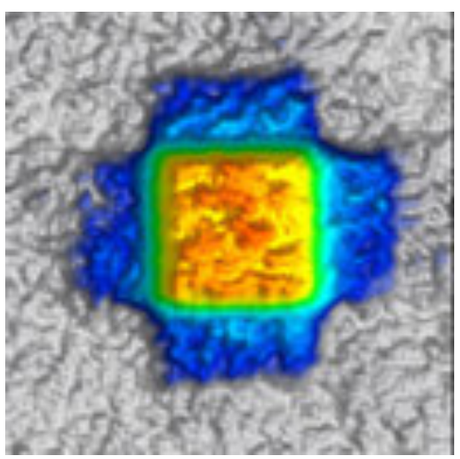


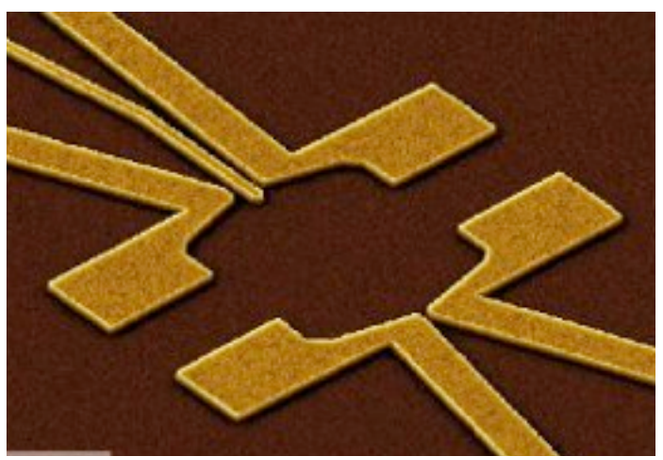




But does this paradigm also apply to information stored in quantum devices?

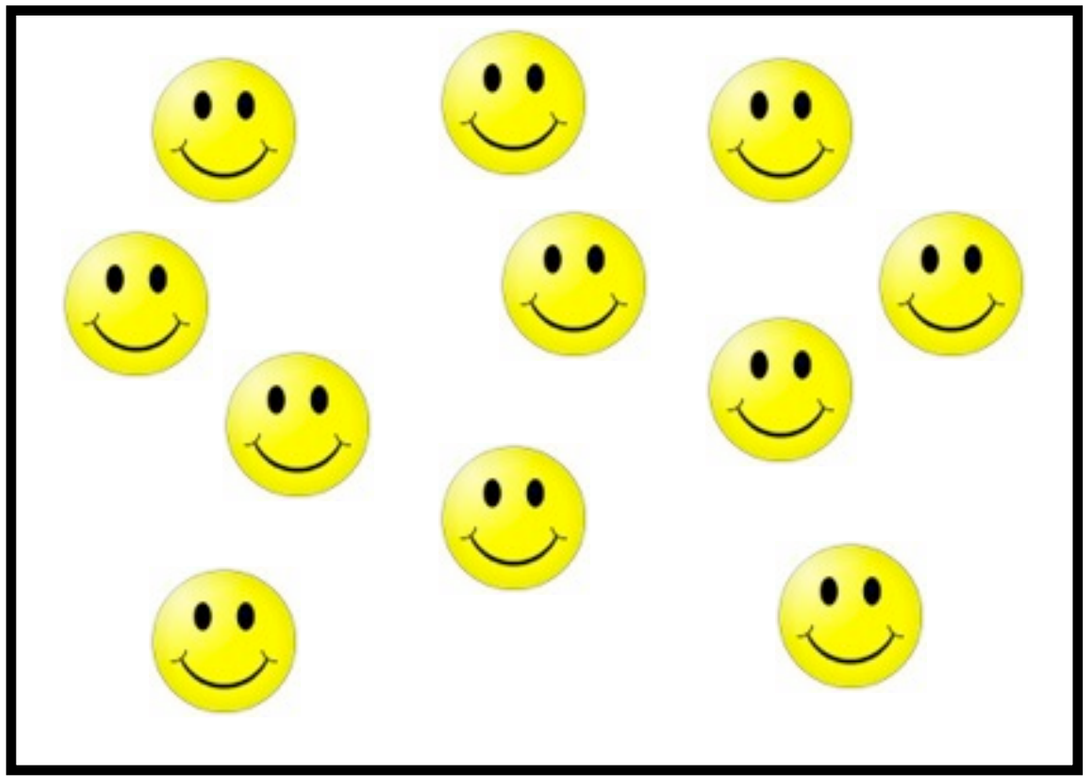


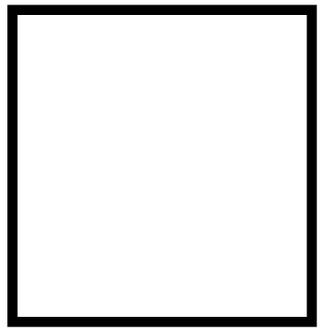


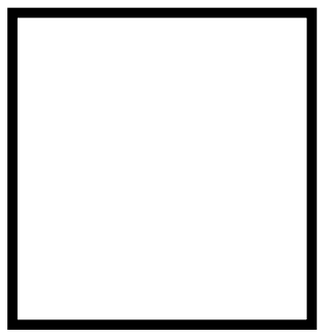


[Photos: QSIT]

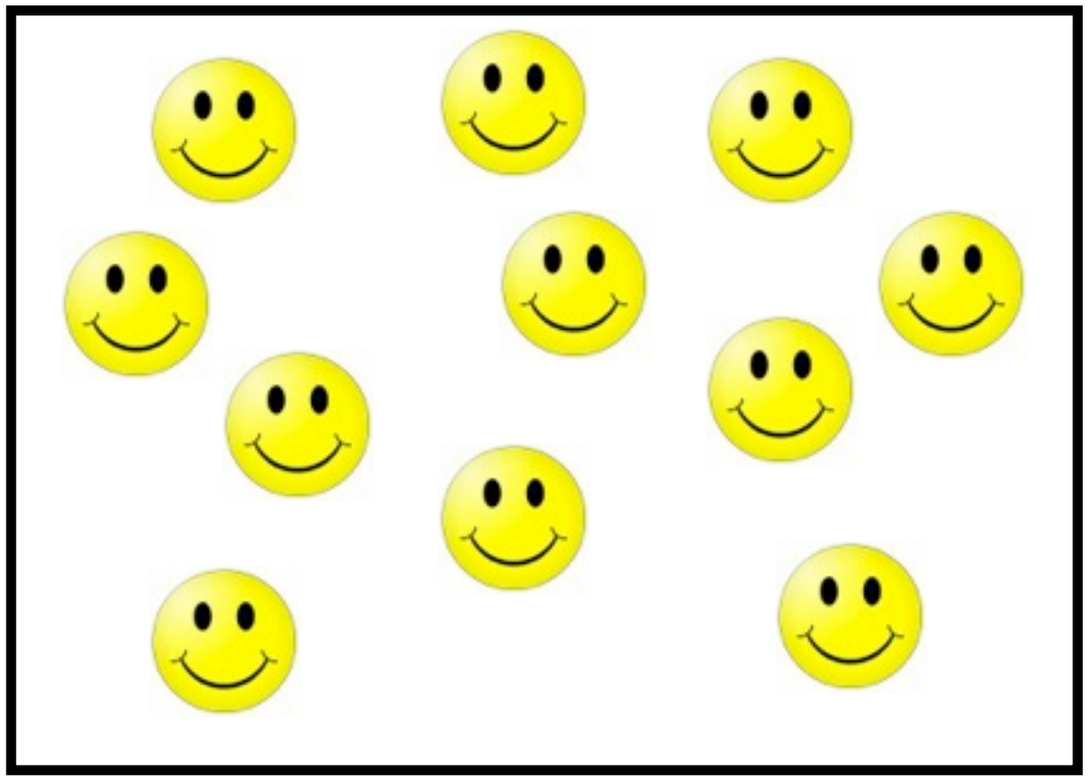
Toy example

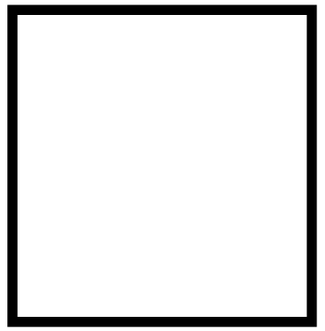


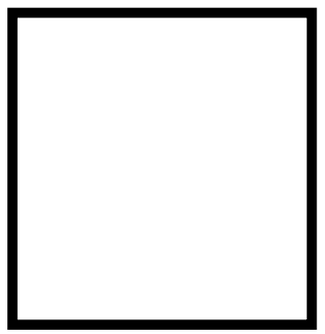




Toy example

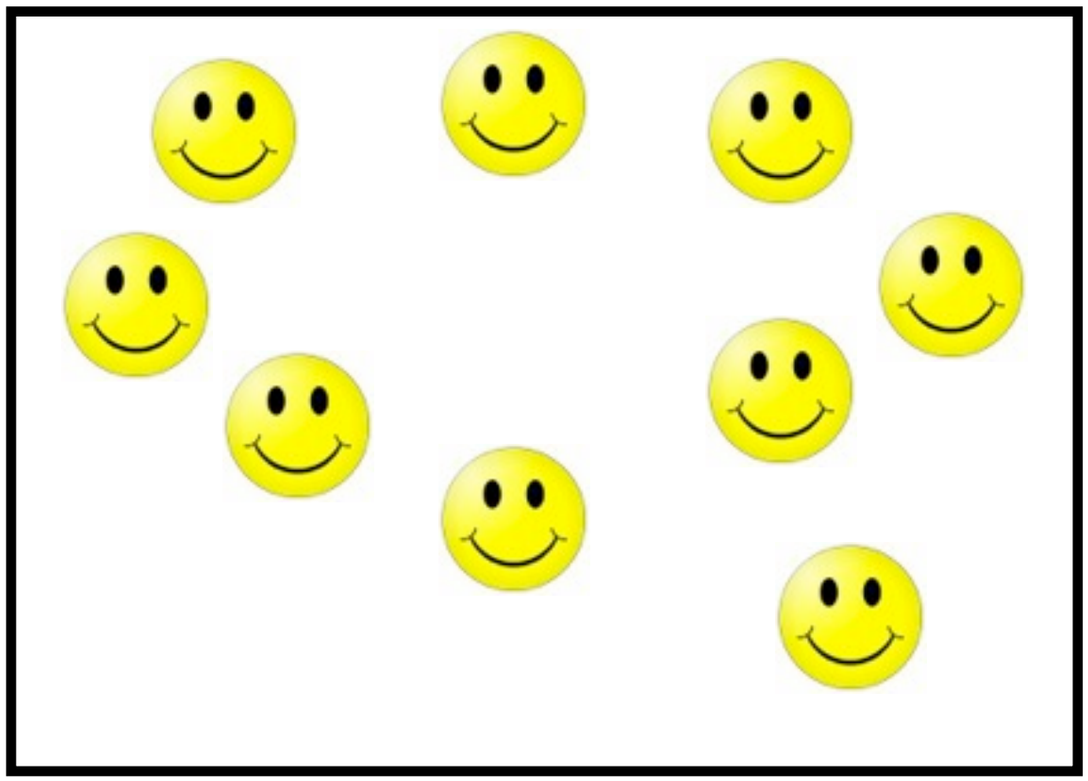






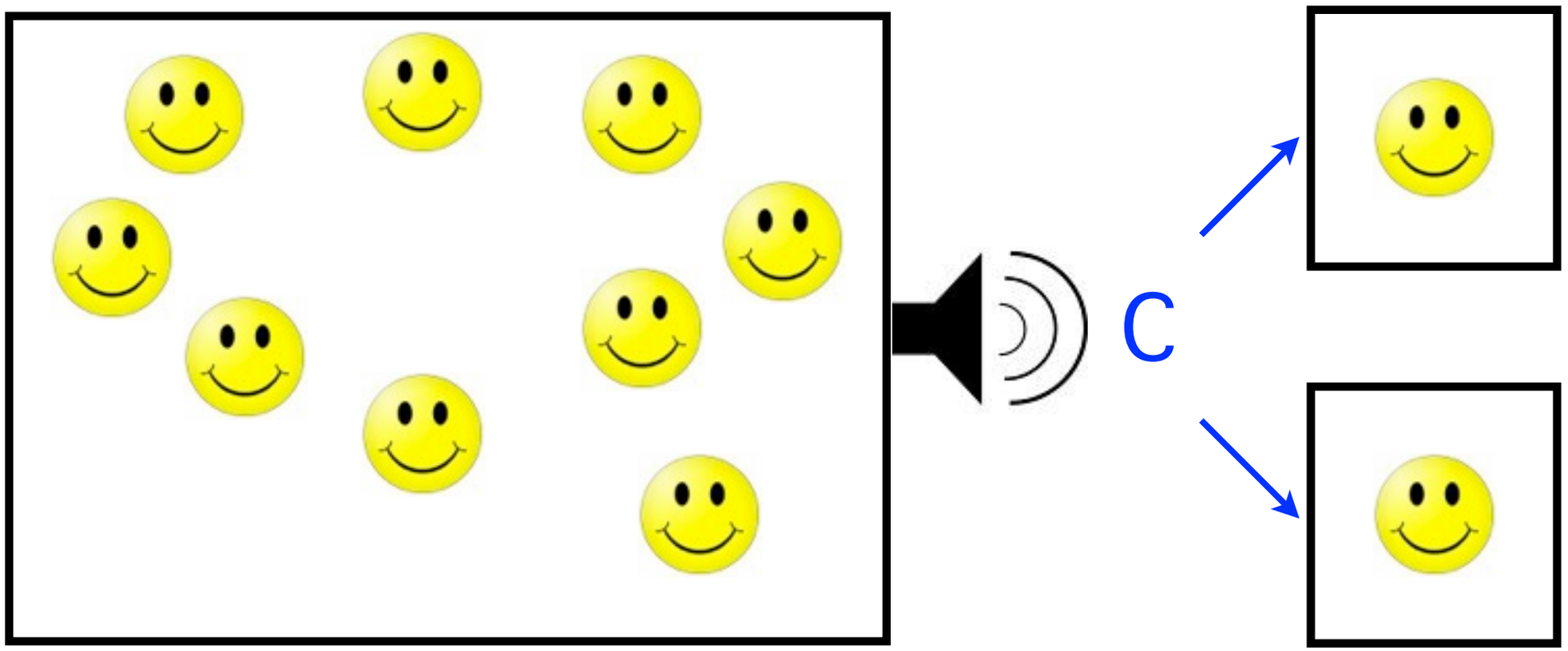
1. N collaborating players sitting in a room

Toy example



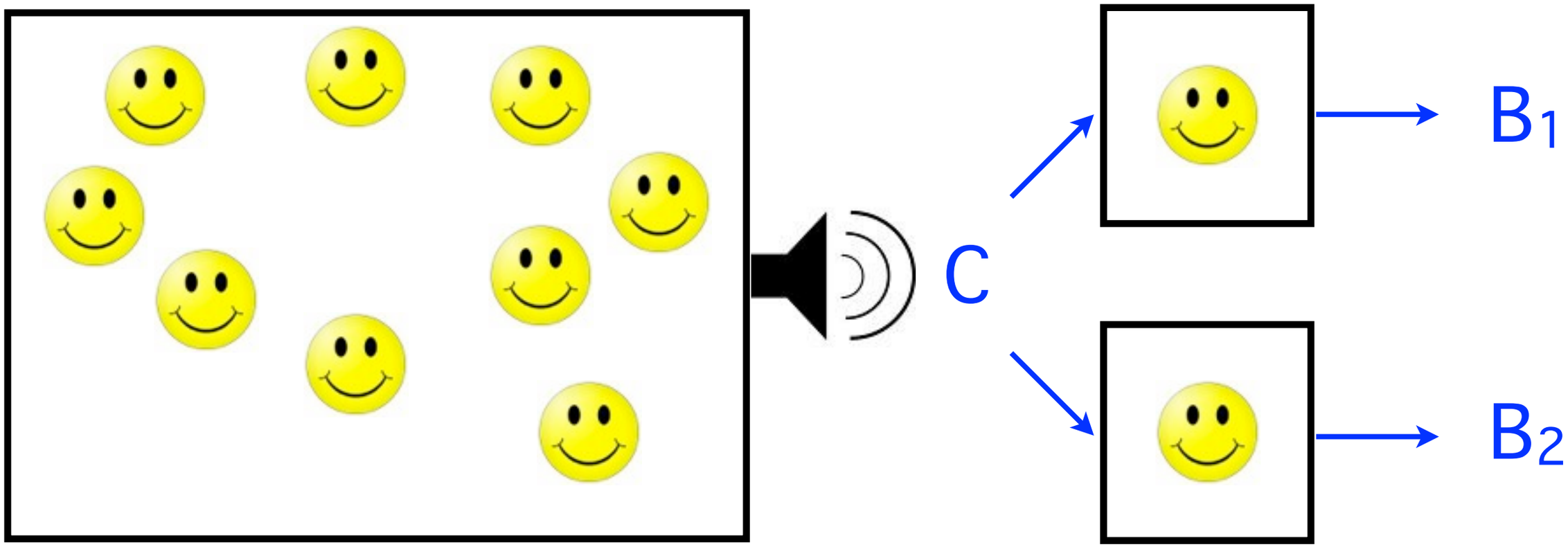
1. N collaborating players sitting in a room
2. 2 of them selected at random and put in separated rooms

Toy example



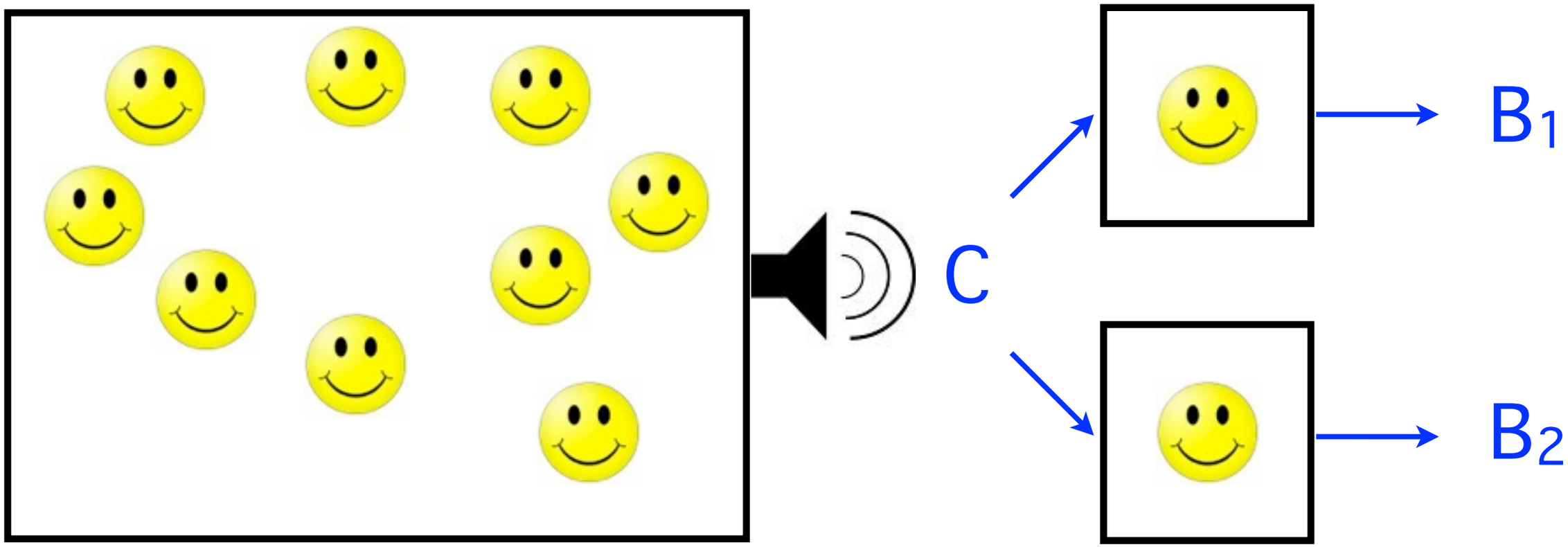
1. N collaborating players sitting in a room
2. 2 of them selected at random and put in separated rooms
3. N-2 remaining players announce a bit C of their choice

Toy example



1. N collaborating players sitting in a room
2. 2 of them selected at random and put in separated rooms
3. N-2 remaining players announce a bit C of their choice
4. separated players output bits B_1 and B_2

Toy example



1. N collaborating players sitting in a room
2. 2 of them selected at random and put in separated rooms
3. N-2 remaining players announce a bit C of their choice
4. separated players output bits B_1 and B_2

Game is won if $B_1 \neq B_2$.

Maximum winning probability

Strategies	B=0	B=1	B=C	B=1-C

Maximum winning probability

- Each player may choose one of the following four strategies (in case he is selected).

Strategies	B=0	B=1	B=C	B=1-C

(The strategy defines how the output B is derived from the input C.)

Maximum winning probability

- Each player may choose one of the following four strategies (in case he is selected).

Strategies	B=0	B=1	B=C	B=1-C

(The strategy defines how the output B is derived from the input C.)

- The game cannot be won if the two selected players follow identical strategies.

Maximum winning probability

- Each player may choose one of the following four strategies (in case he is selected).

Strategies	B=0	B=1	B=C	B=1-C

(The strategy defines how the output B is derived from the input C.)

- The game cannot be won if the two selected players follow identical strategies.
- This happens with probability ≈1/4 (for N large).

Maximum winning probability

- Each player may choose one of the following four strategies (in case he is selected).

Strategies	B=0	B=1	B=C	B=1-C

(The strategy defines how the output B is derived from the input C.)

- The game cannot be won if the two selected players follow identical strategies.
- This happens with probability ≈1/4 (for N large).
- Hence, the game is lost with probability (at least) 1/4.

What did we prove?

Claim

For any possible strategy, the game is lost with probability at least ≈1/4.

What did we prove?

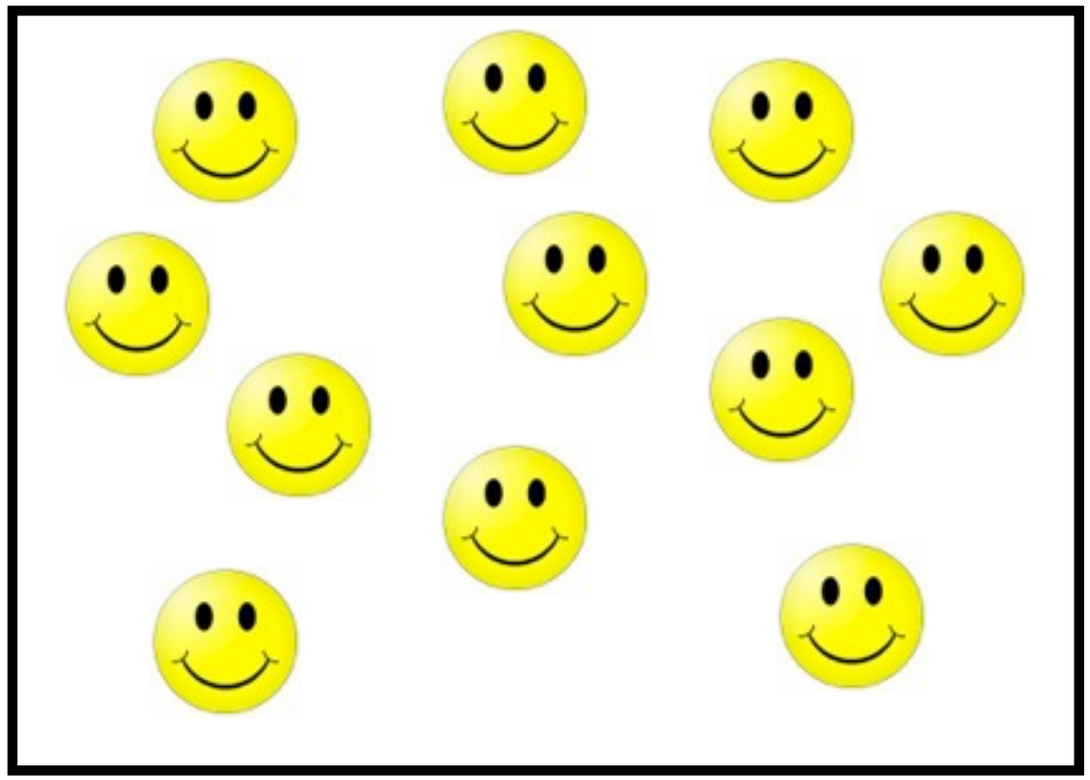
Claim

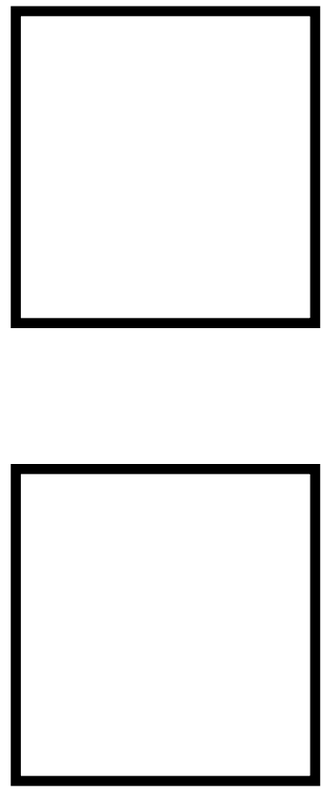
For any possible strategy, the game is lost with probability at least ≈1/4.

Additional implicit assumption

All information is encoded and processed classically.

Quantum strategies are stronger

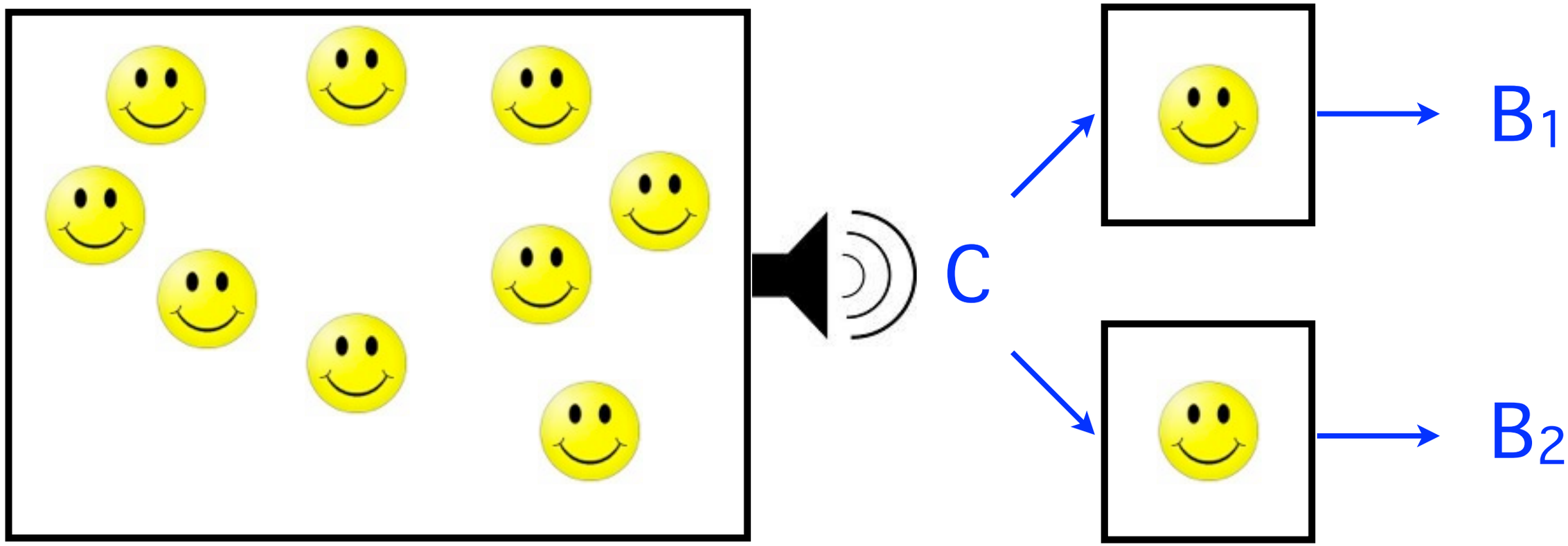




The game can be won with probability 1 if the players can use an internal quantum device.

Note: all communication during the game is still purely classical.

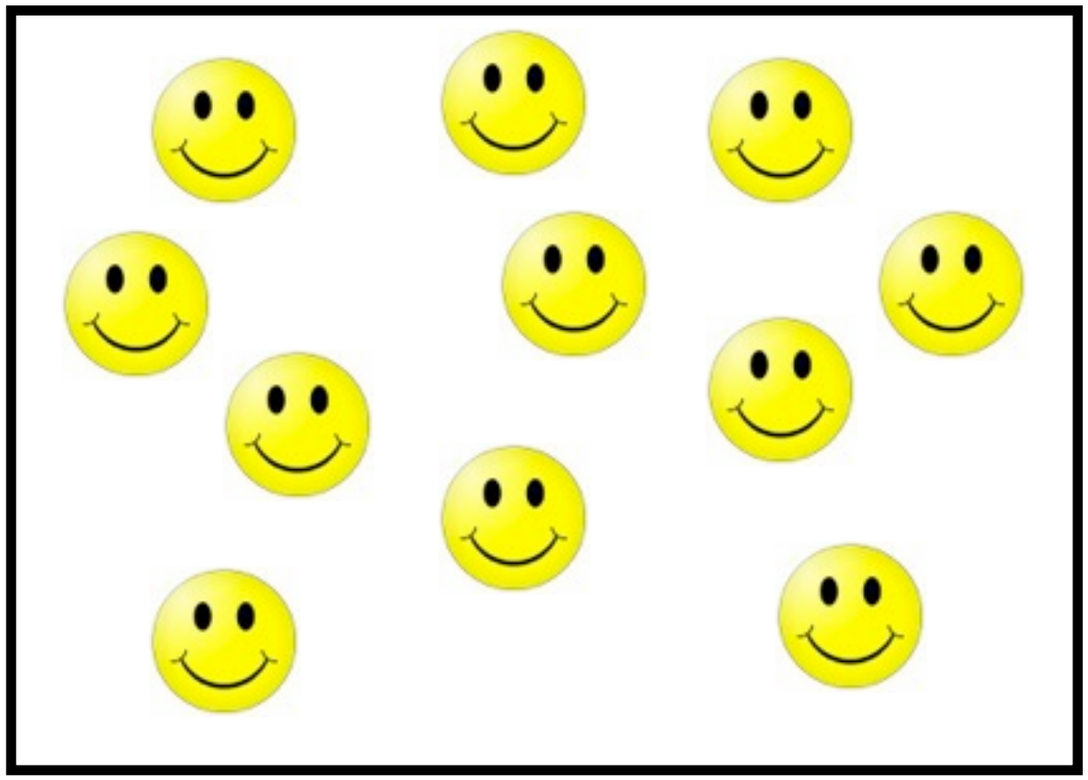
Quantum strategies are stronger

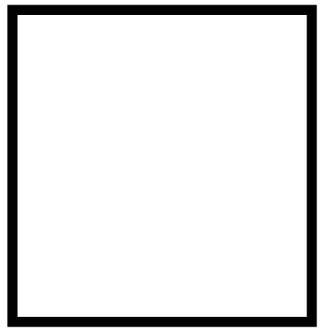


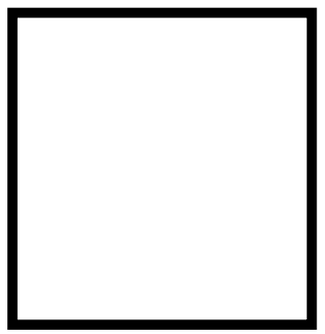
The game can be won with probability 1 if the players can use an internal quantum device.

Note: all communication during the game is still purely classical.

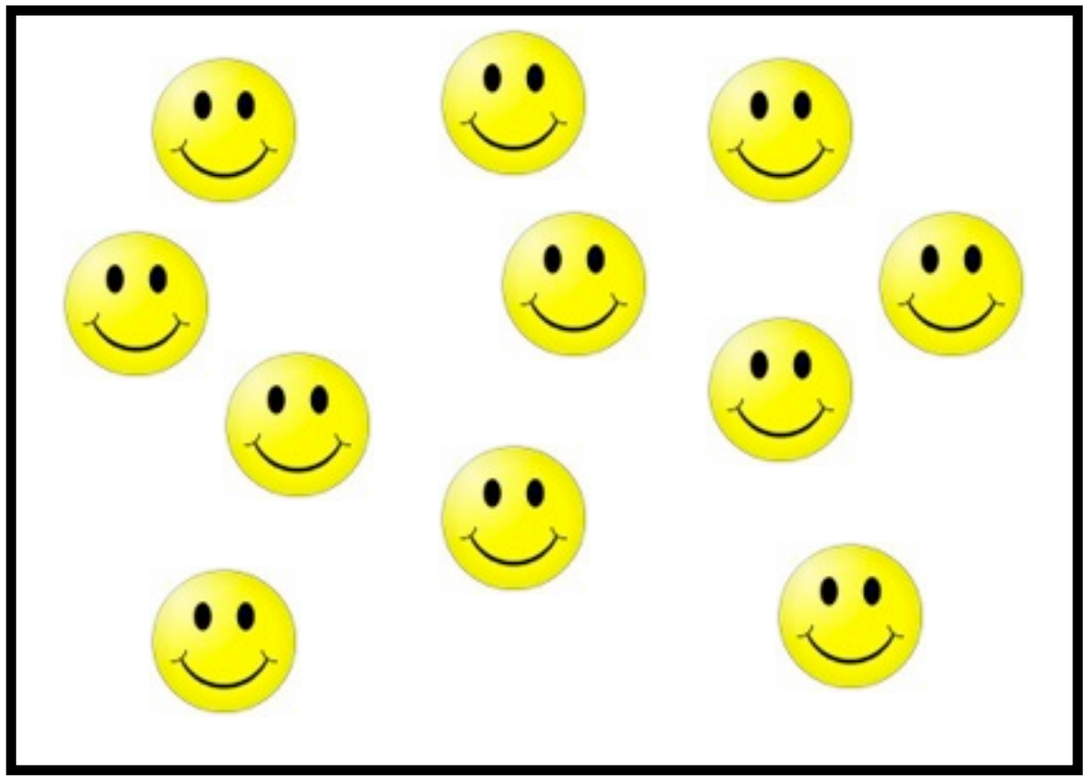
Quantum strategy

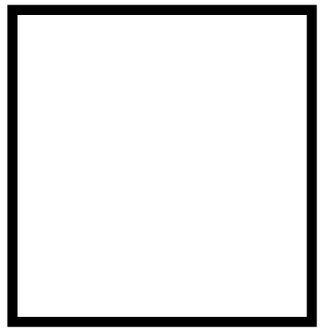


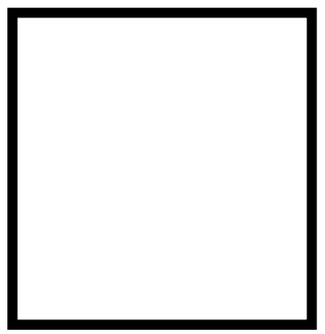




Quantum strategy

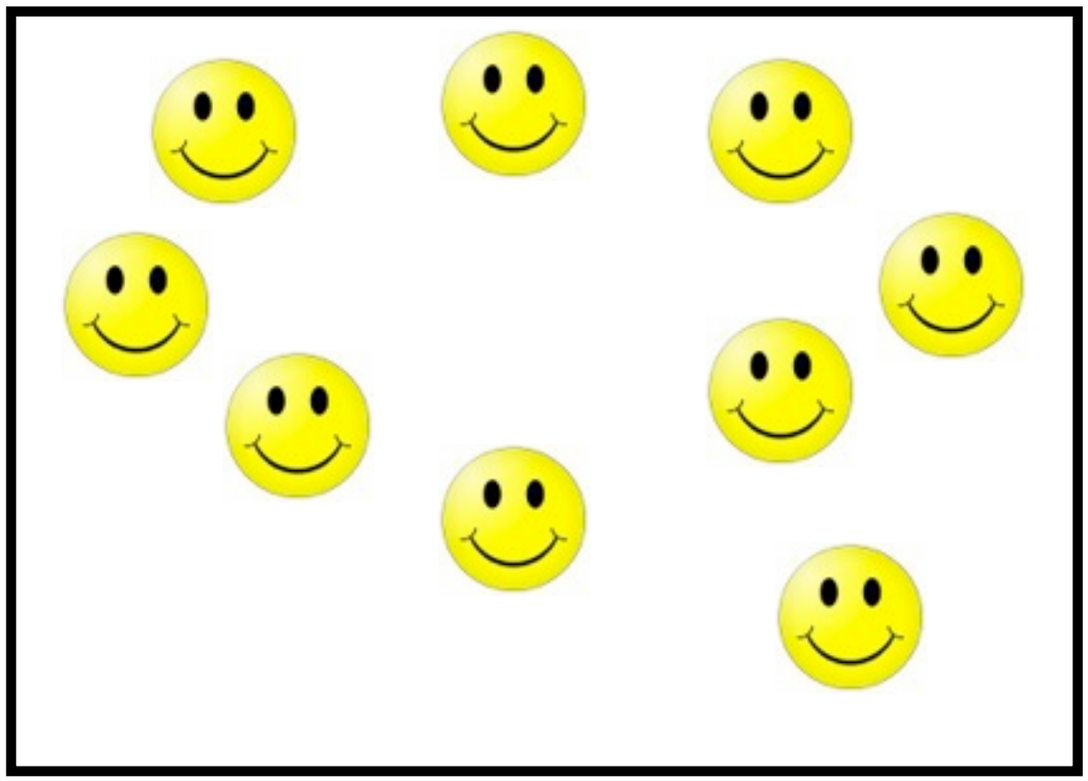






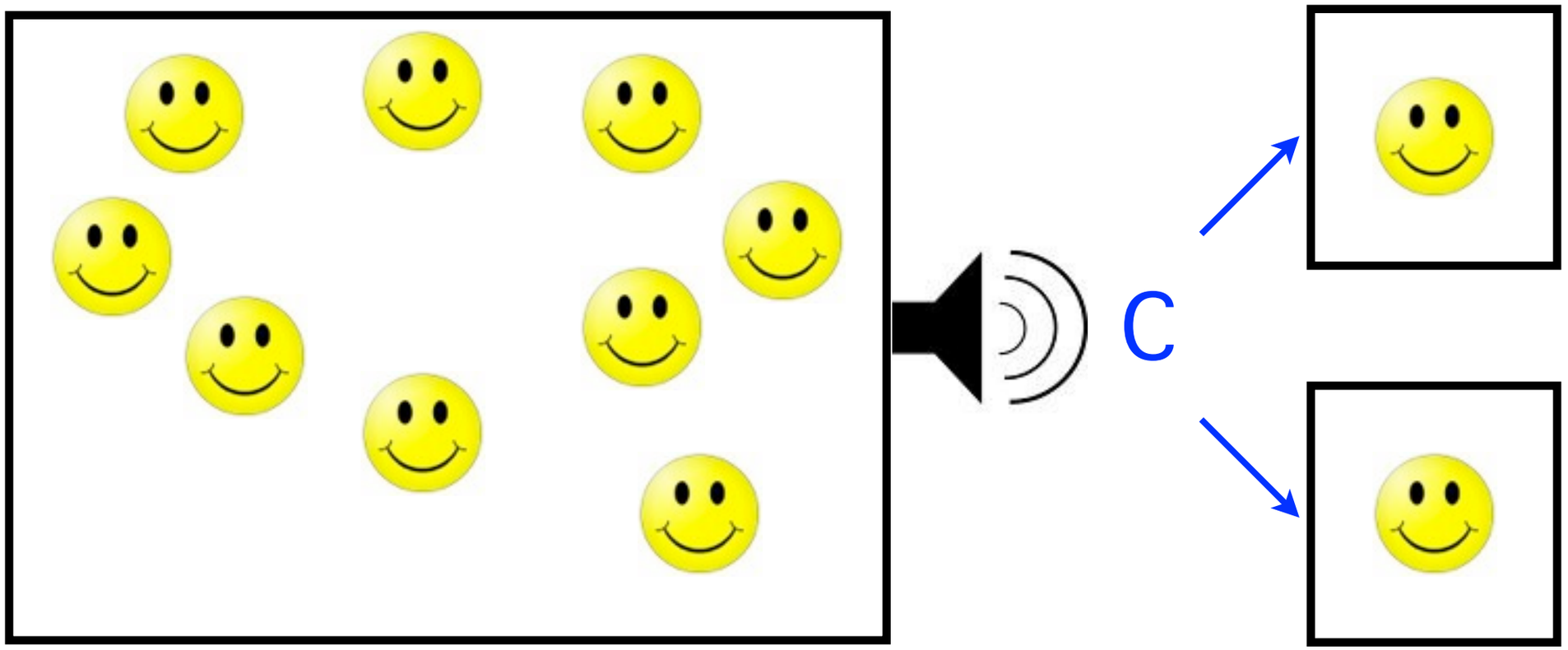
1. N players start with correlated state $\Psi = |0\rangle^{\otimes N} + |1\rangle^{\otimes N}$

Quantum strategy



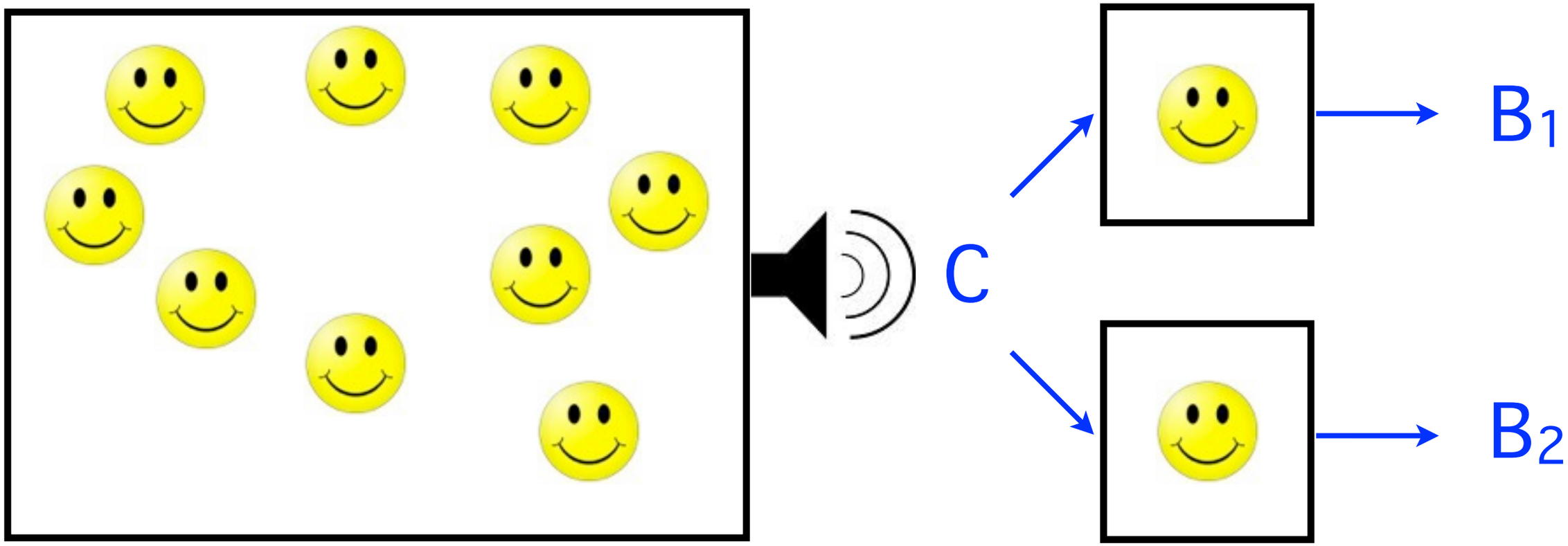
1. N players start with correlated state $\Psi = |0\rangle^{\otimes N} + |1\rangle^{\otimes N}$
2. keep state stored

Quantum strategy



1. N players start with correlated state $\Psi = |0\rangle^{\otimes N} + |1\rangle^{\otimes N}$
2. keep state stored
3. all remaining players measure in diagonal basis and choose C as the **xor** of their measurement results

Quantum strategy



1. N players start with correlated state $\Psi = |0\rangle^{\otimes N} + |1\rangle^{\otimes N}$
2. keep state stored
3. all remaining players measure in diagonal basis and choose C as the **xor** of their measurement results
4. separated players determine B_1 and B_2 by measuring in either the diagonal or the circular basis, depending on C.

What can we learn from this example?

What can we learn from this example?

- Quantum mechanics allows us to win games that cannot be won in a classical world
(examples known as "pseudo telepathy games").
(Telepathy is obviously dangerous from a cryptographic point of view.)

What can we learn from this example?

- Quantum mechanics allows us to win games that cannot be won in a classical world
  (examples known as "pseudo telepathy games").
  (Telepathy is obviously dangerous from a cryptographic point of view.)
- There is no physical principle that allows us to rule out quantum strategies.

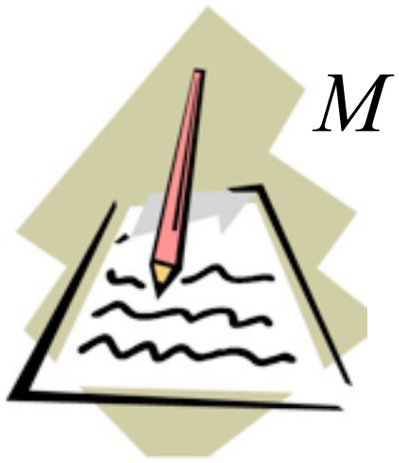
What can we learn from this example?

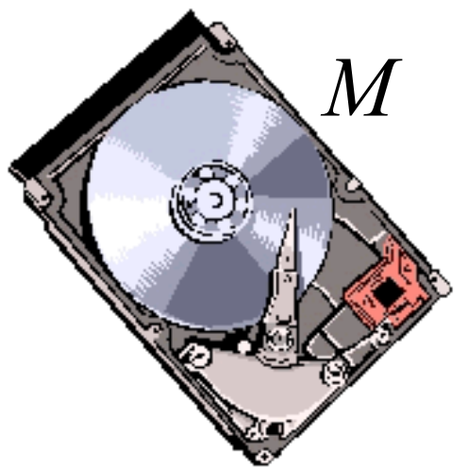
- Quantum mechanics allows us to win games that cannot be won in a classical world
  (examples known as "pseudo telepathy games").
  (Telepathy is obviously dangerous from a cryptographic point of view.)
- There is no physical principle that allows us to rule out quantum strategies.

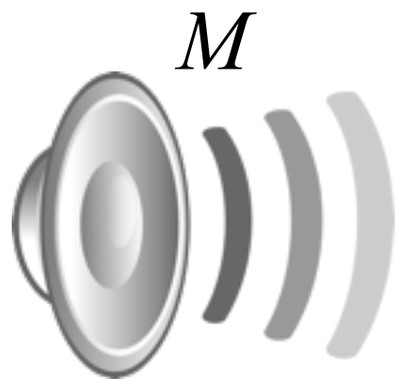
It is, in general, unavoidable to take into account quantum effects.

Independence of information carriers?

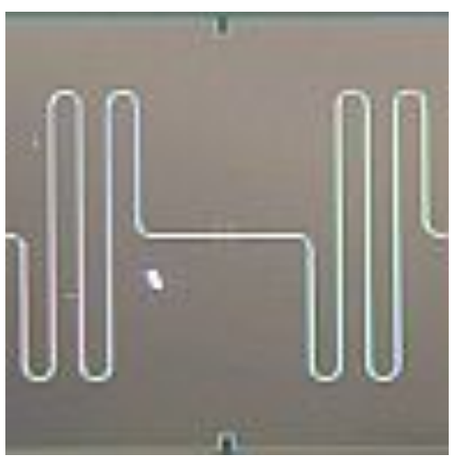
According to Shannon's theory, information is independent of the "physical information carriers".

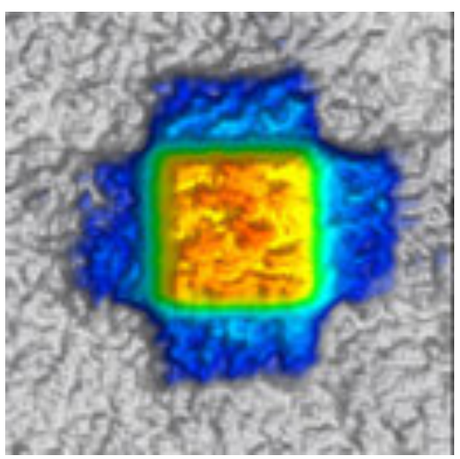


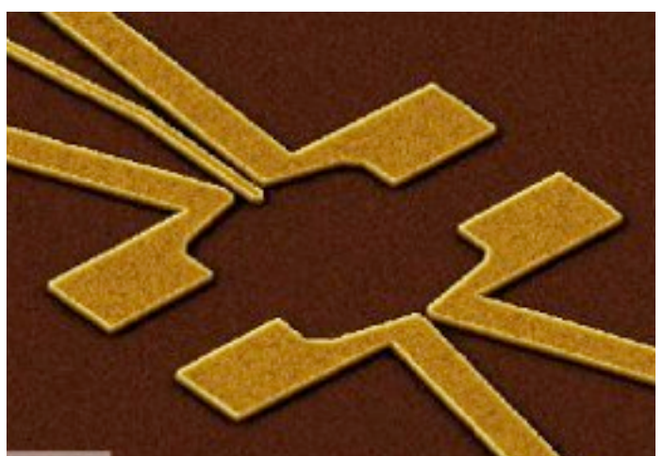




But does this paradigm also apply to information stored in quantum devices? **No!**







[Photos: QSIT]

Shannon's "impossibility result"

C = enc(M,S)

C

M = dec(C,S)

Theorem

For information-theoretically secure encryption, the key S needs to be at least as long as the message M.

In particular, *One-Time-Pad encryption* is optimal.

Proof of Shannon's theorem

Let M be a uniformly distributed n-bit message,
S a secret key, and C the ciphertext.

Requirements

- H(M | SC) = 0, since M is determined by S, C.
- H(M | C) = H(M) = n, since M is indep. of C.

Hence

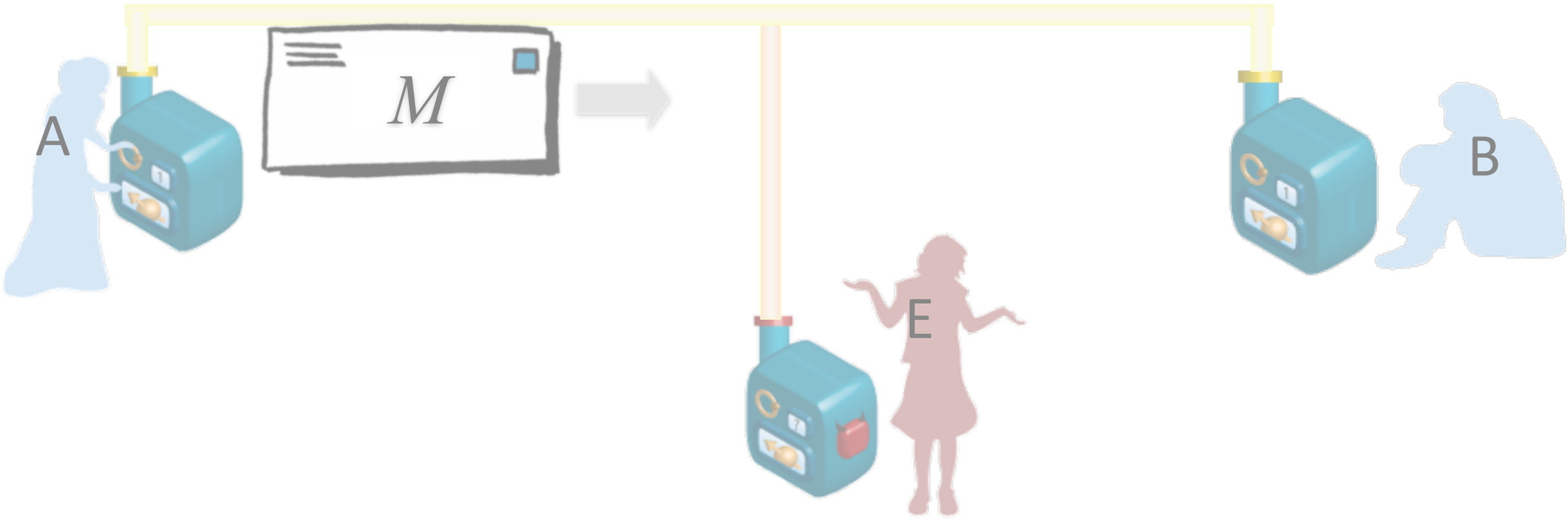
H(S) ≥ I(M : S | C) = H(M | C) - H(M | SC) = n.

Shannon's impossibility result

Theorem [Shannon, 1949]

Two parties connected via an insecure channel cannot exchange any messages secretly

(even if they have methods for authentication).



Bennett and Brassard's possibility result

C.H. Bennett

[Photo: ETH Zurich]

G. Brassard

[Photo: ETH Zurich]

If information cannot be cloned, then it can also not be stolen (without leaving traces).

Bennett and Brassard's possibility result

C.H. Bennett

[Photo: ETH Zurich]

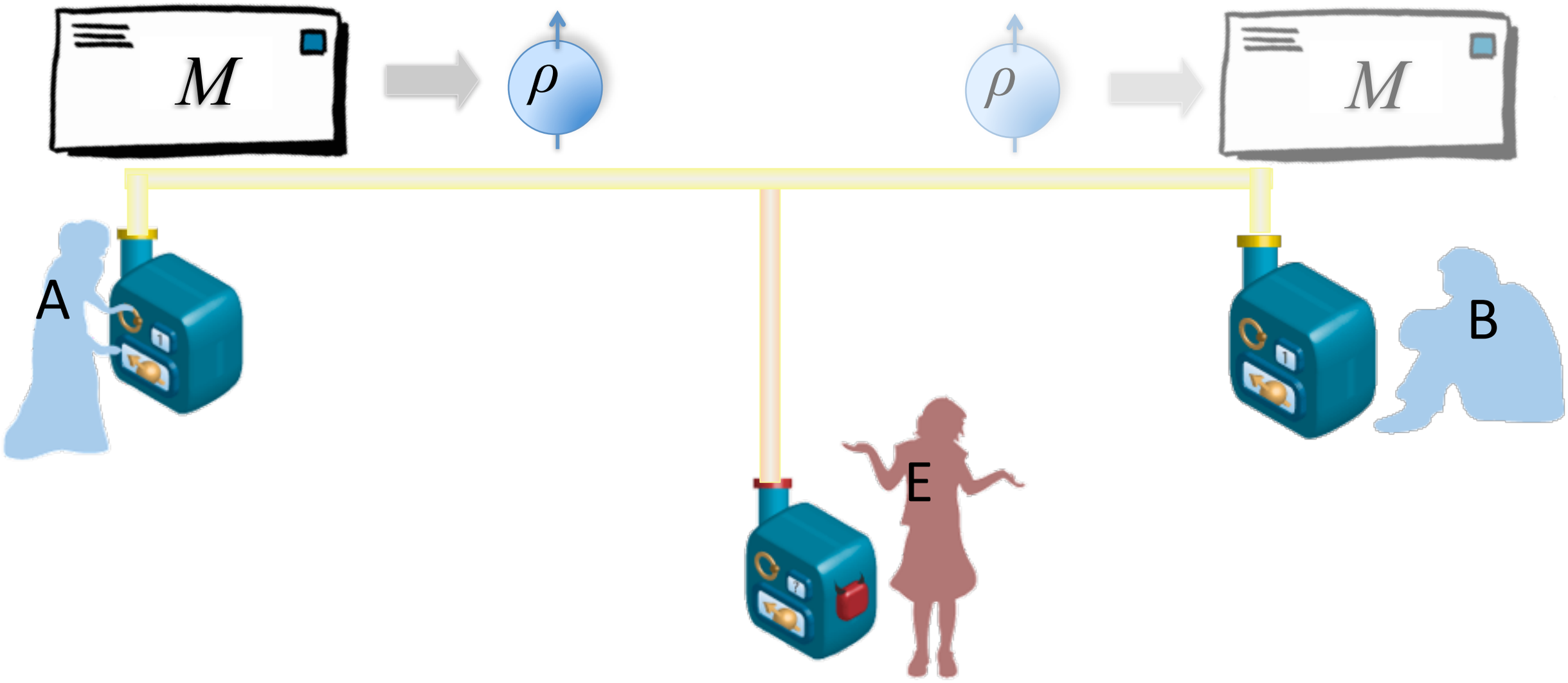
G. Brassard

[Photo: ETH Zurich]

If information cannot be cloned, then it can also not be stolen (without leaving traces).

This was the invention of quantum cryptography.

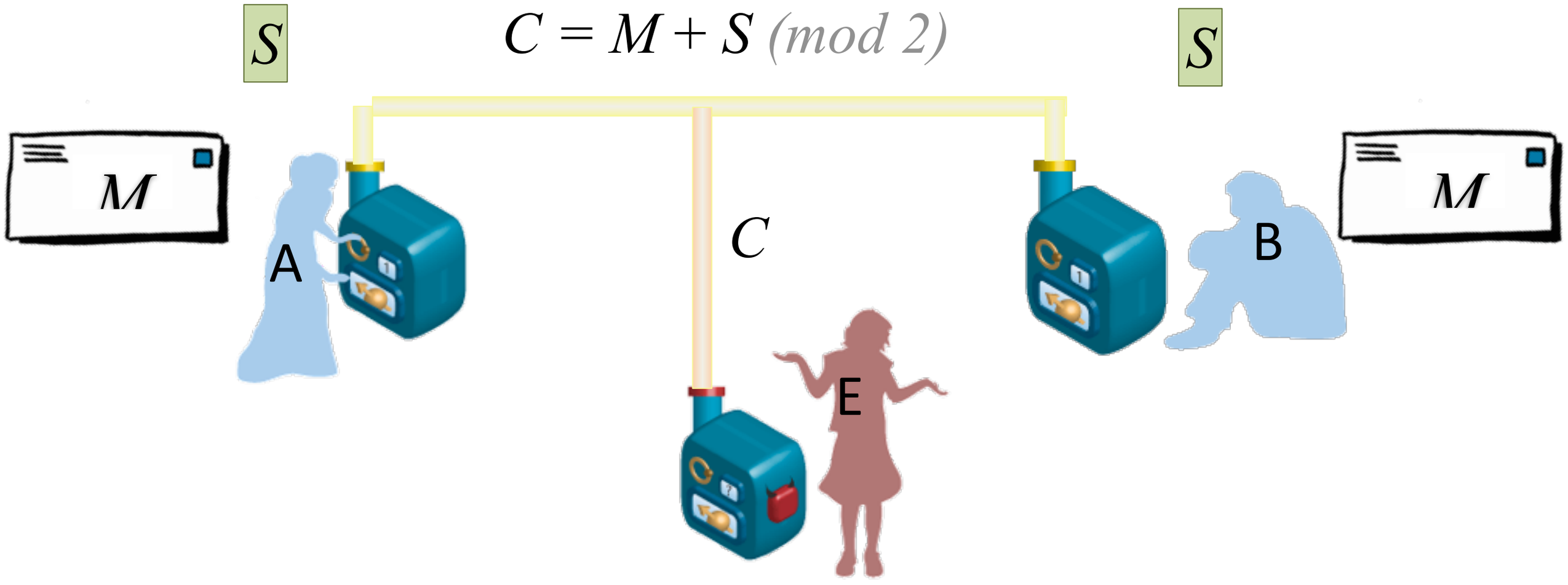
Quantum cryptography

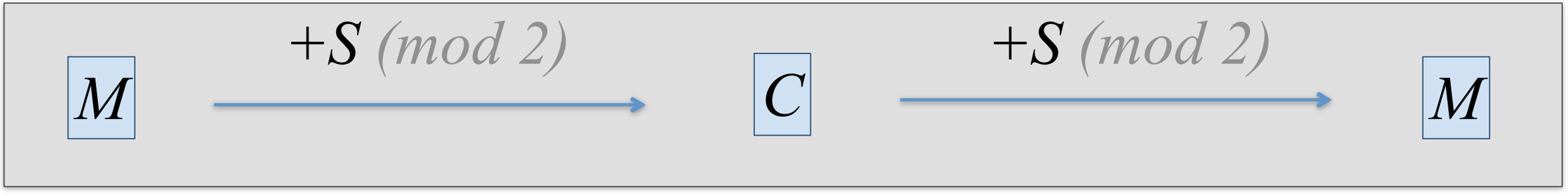


Idea: Use no-cloning principle to verify secrecy.

One-time-pad encryption

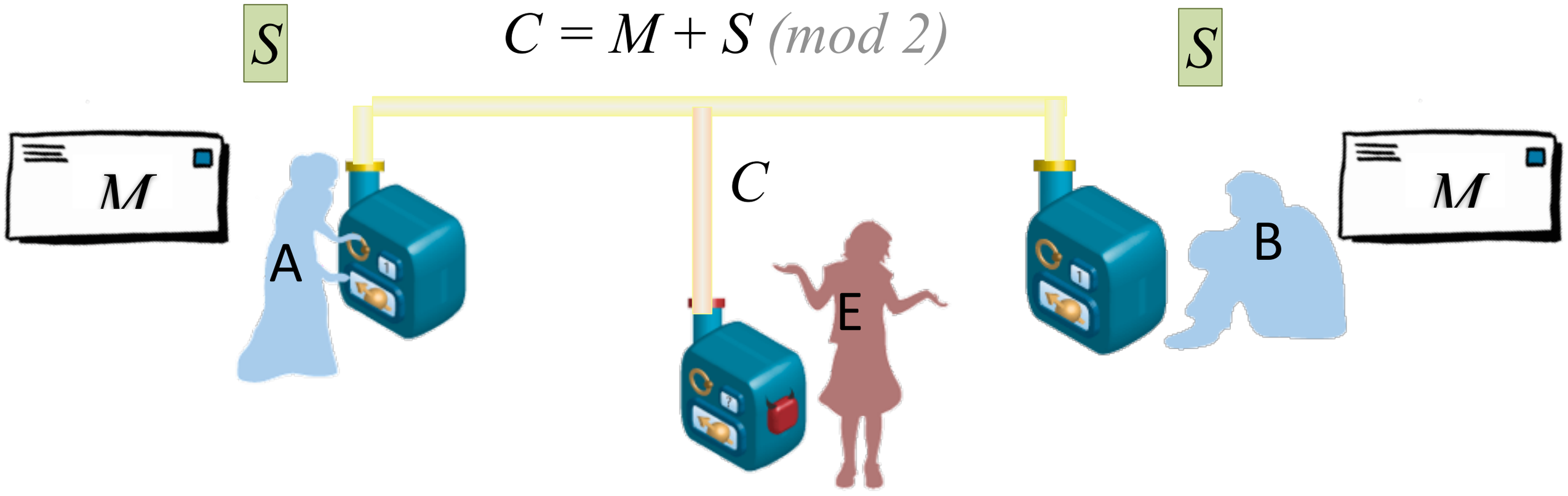
Let $M \in \{0,1\}$ be a message bit and $S \in \{0,1\}$ a "key bit".





One-time-pad encryption

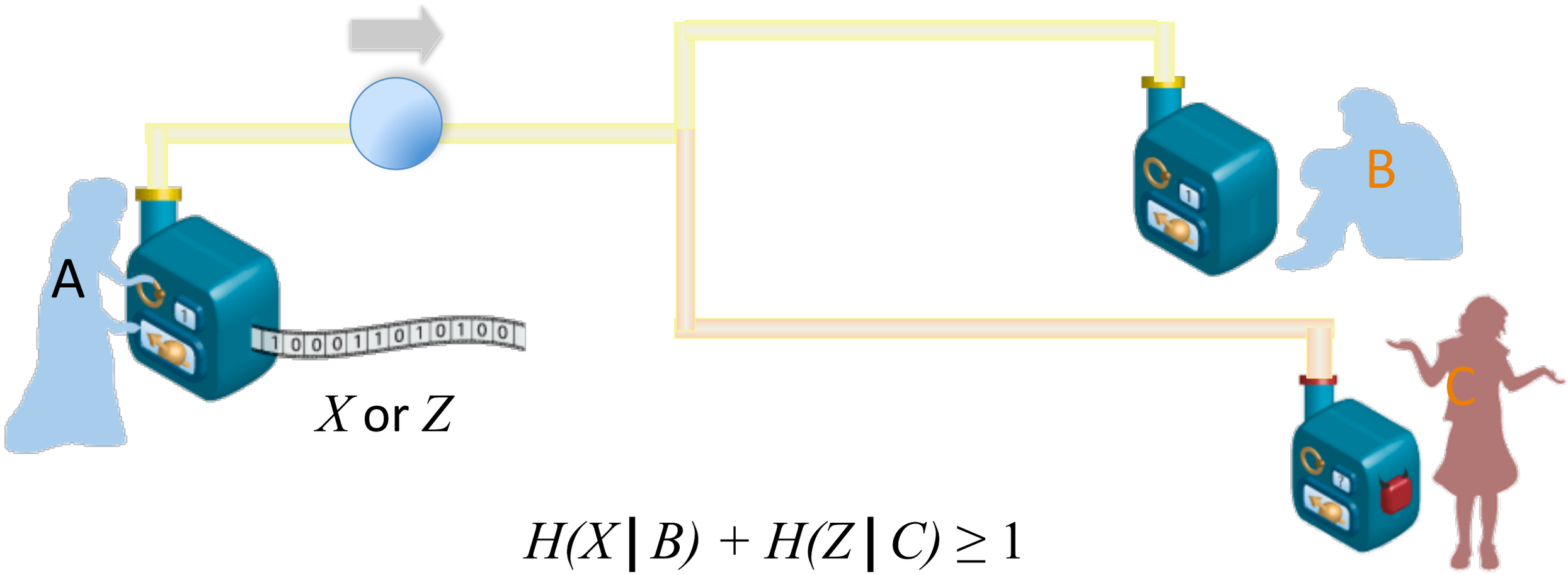
Let $M \in \{0,1\}$ be a message bit and $S \in \{0,1\}$ a "key bit".



Theorem

If S is uniformly distributed then C is uncorrelated to M.

No-cloning principle provides security



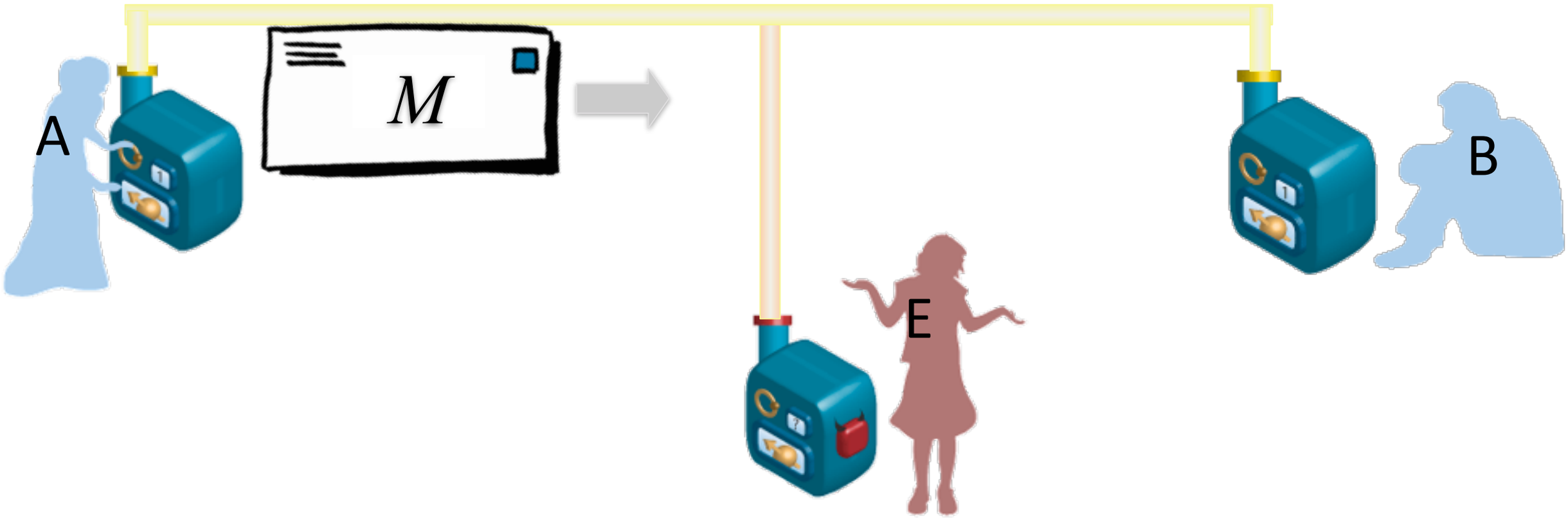
$$H(X|B) + H(Z|C) \geq 1$$

Idea

Check statistically that $H(X|B)$ is small. The generalized uncertainty principle then implies that $H(Z|C)$ is large.

[Tomamichel *et al.*, Nature Communications, 2012]

Quantum cryptography



Protocol

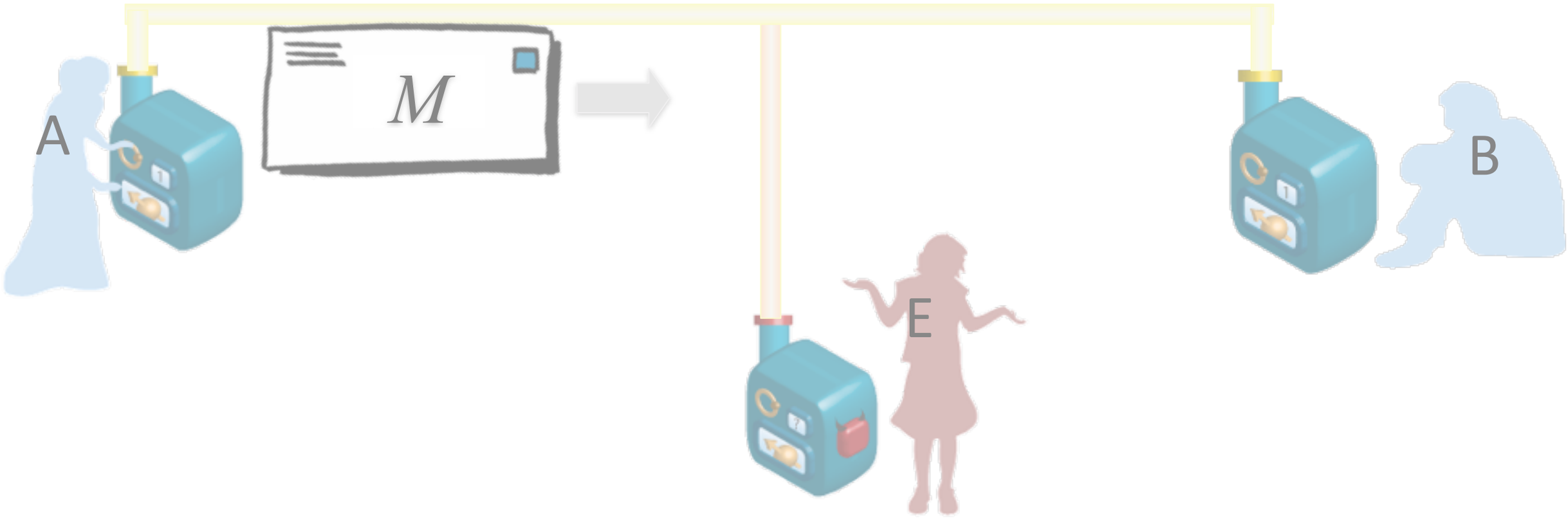
1. Use quantum communication to generate a key
   (the no-cloning principle guarantees that it is secure)
2. Use one-time-pad encryption to send message M.

An apparent contradiction

Theorem [Bennett and Brassard, 1984]

Two parties connected via an insecure channel can exchange messages secretly

(provided they have a method for authentication).



An apparent contradiction

Theorem [Bennett and Brassard, 1984]

Two parties connected via an insecure channel can exchange messages secretly

(provided they have a method for authentication).

Theorem [Shannon, 1949]

Two parties connected via an insecure channel cannot exchange any messages secretly

(even if they have methods for authentication).

Proof of Shannon's theorem

Let M be a uniformly distributed n-bit message, S a secret key, and C the ciphertext..

Requirements

- H(M | SC) = 0, since M determined by S, C.
- H(M | C) = H(M) = n, since M indep. of C.

Hence

H(S) ≥ I(M : S | C) = H(M | C) - H(M | SC) = n.

Proof of Shannon's theorem

Let M be a uniformly distributed n-bit message, S a secret key, and C the ciphertext..

Requirements

- H(M | SC) = 0, since M determined by S, C.
- H(M | C) = H(M) = n, since M indep. of C.

H(M | SC$_{Bob}$)

Hence

H(S) ≥ I(M : S | C) = H(M | C) - H(M | SC) = n.

Proof of Shannon's theorem

Let M be a uniformly distributed n-bit message, S a secret key, and C the ciphertext..

Requirements

- H(M | SC) = 0, since M determined by S, C.
- H(M | C) = H(M) = n, since M indep. of C.

H(M | SC_{Bob})

H(M | C_{Eve})

Hence

H(S) ≥ I(M : S | C) = H(M | C) - H(M | SC) = n.

Proof of Shannon's theorem

No cloning:
$C_{Bob} \neq C_{Eve}$ in general

Let M be a uniformly distribut
secret key, and C the ciphertext..

Requirements

$H(M|SC_{Bob})$

- $H(M|SC) = 0$, since M determined by S, C.
- $H(M|C) = H(M) = n$, since M indep. of C.

$H(M|C_{Eve})$

Hence

$H(S) \geq I(M : S|C) = H(M|C) - H(M|SC) = n.$

Properties of entangled qubits

$\Pr[X = Y] = \cos^2(\alpha-\beta)$

$\Pr[X \neq Y] = \sin^2(\alpha-\beta) \approx (\alpha-\beta)^2$ (for small angle differences)

Properties of entangled qubits

$\Pr[X = Y] = \cos^2(\alpha-\beta)$

$\Pr[X \neq Y] = \sin^2(\alpha-\beta) \approx (\alpha-\beta)^2$ (for small angle differences)

Note: If the left particle is measured with angle α and gives output 0 (or 1) then the right particle behaves as if it was prepared along α (or $\alpha+\pi/2$).

Conclusions

Conclusions

- Quantum vs. classical physical objects: The joint state space of object A and object B is not simply the cartesian product of the two individual state spaces.

Conclusions

- Quantum vs. classical physical objects: The joint state space of object A and object B is not simply the cartesian product of the two individual state spaces.

- Information is physical: Since information is physical, the physical properties of the underlying information carriers have to be taken into account when describing the laws of information.

Conclusions

- Quantum vs. classical physical objects: The joint state space of object A and object B is not simply the cartesian product of the two individual state spaces.

- Information is physical: Since information is physical, the physical properties of the underlying information carriers have to be taken into account when describing the laws of information.

- Implications: The resulting laws of information are fundamentally different from the corresponding classical laws. Examples include the no-cloning principle, which has applications, e.g., in cryptography.

Many thanks for your attention