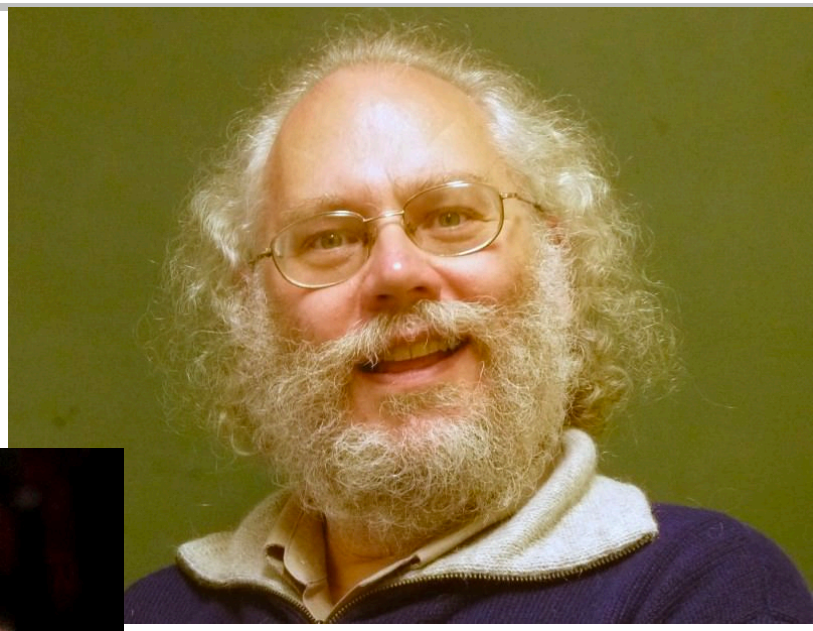
# The ultimate limits of privacy and randomness…

## …for the paranoid ones

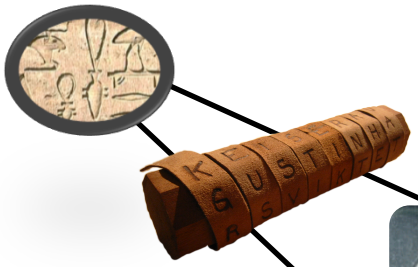
Artur Ekert

# Congratulations…



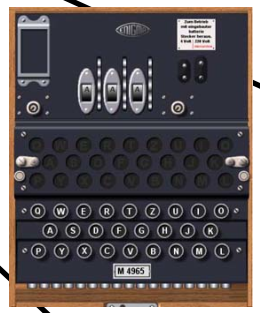
# Quantum speedup…

# Quest for a perfect cipher



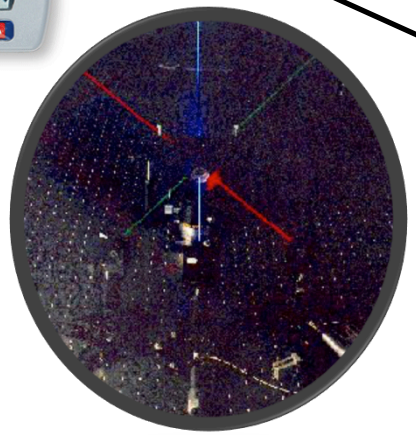
400BC
SCYTALE

1450
ALBERTI'S DISC



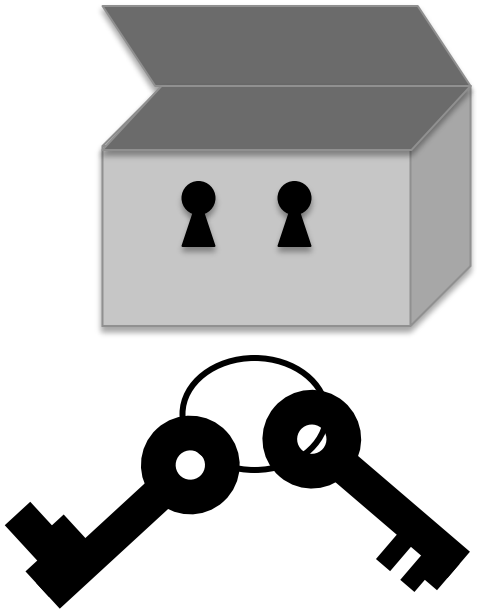
ENIGMA 1940


Public Keys



Quantum Crypto

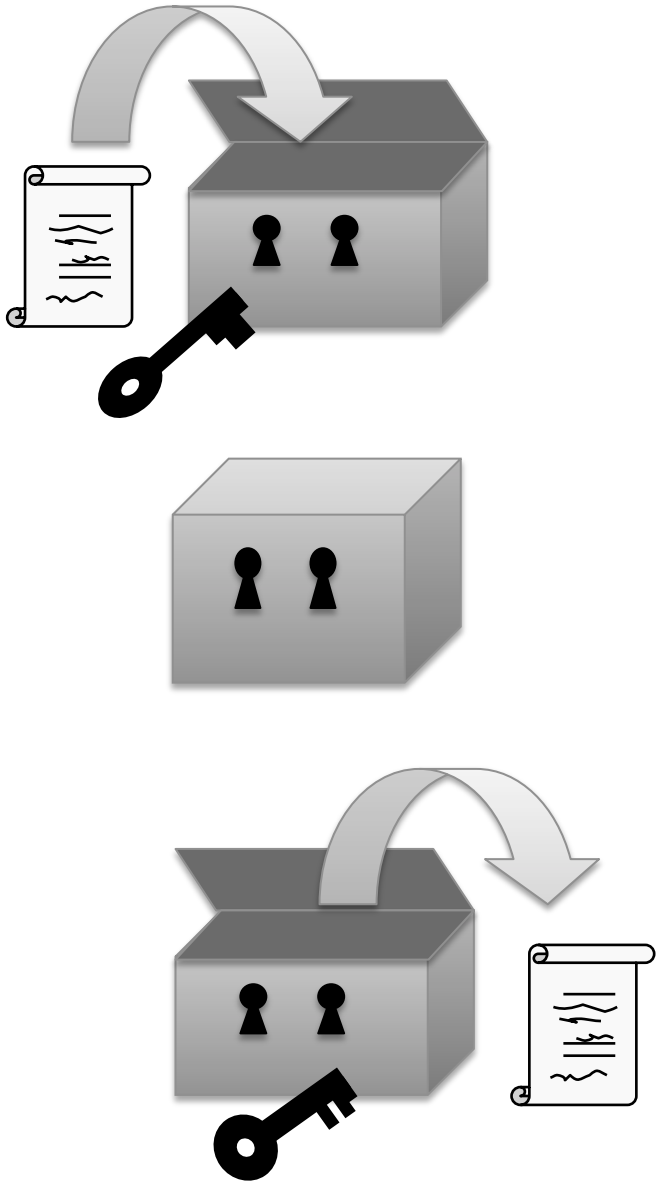
# Public Key Cryptosystems



Public key locks the box

Private key unlocks the box

FACTORING

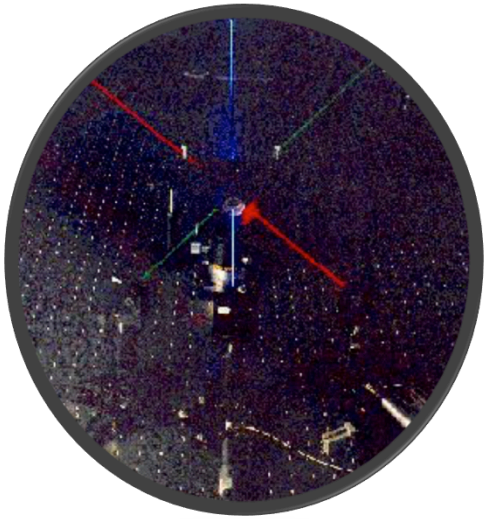


# Enter the quantum…

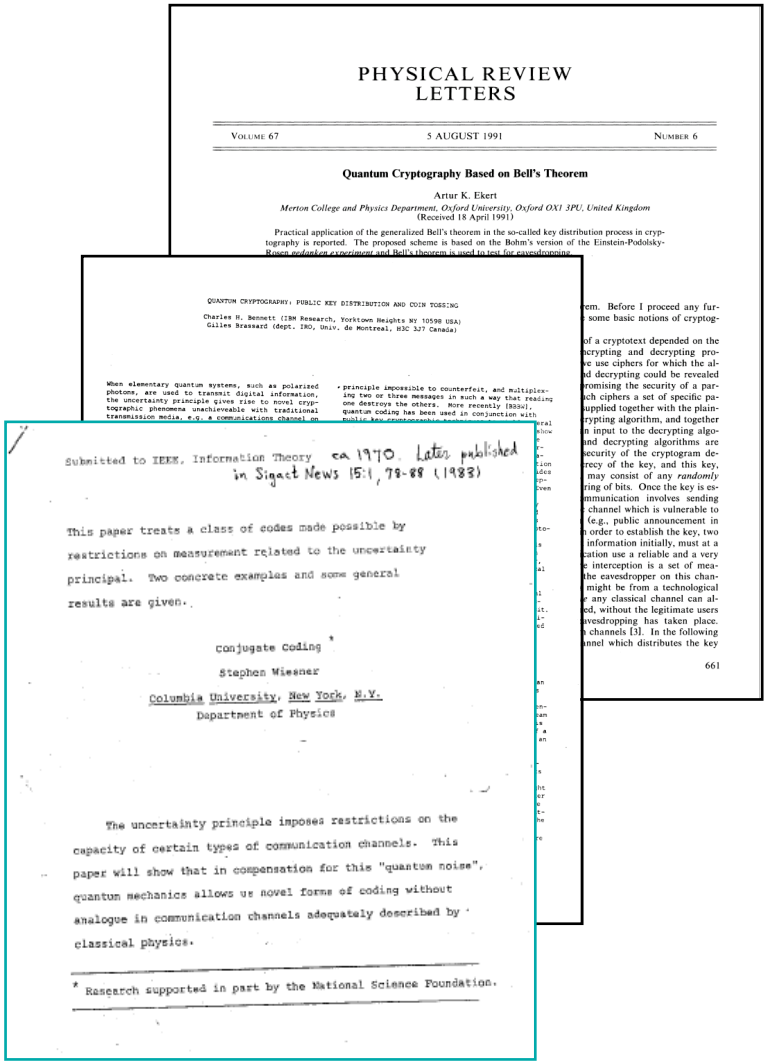
*The quantum taketh away…*


*…and the quantum giveth back!*

**QUANTUM CRYPTOGRAPHY** ➡



# Quantum cryptography



PHYSICAL REVIEW LETTERS

VOLUME 67 5 AUGUST 1991 NUMBER 6

**Quantum Cryptography Based on Bell's Theorem**

Artur K. Ekert

*Merton College and Physics Department, Oxford University, Oxford OX1 3PU, United Kingdom*

(Received 18 April 1991)

Practical application of the generalized Bell's theorem in the so-called key distribution process in cryptography is reported. The proposed scheme is based on the Bohm's version of the Einstein-Podolsky-Rosen *gedanken experiment* and Bell's theorem is used to test for eavesdropping.

QUANTUM CRYPTOGRAPHY: PUBLIC KEY DISTRIBUTION AND COIN TOSSING

Charles H. Bennett (IBM Research, Yorktown Heights NY 10598 USA)
Gilles Brassard (dept. IRO, Univ. de Montreal, H3C 3J7 Canada)

Submitted to IEEE, Information Theory ca 1970. Later published in Sigact News 15:1, 78-88 (1983)

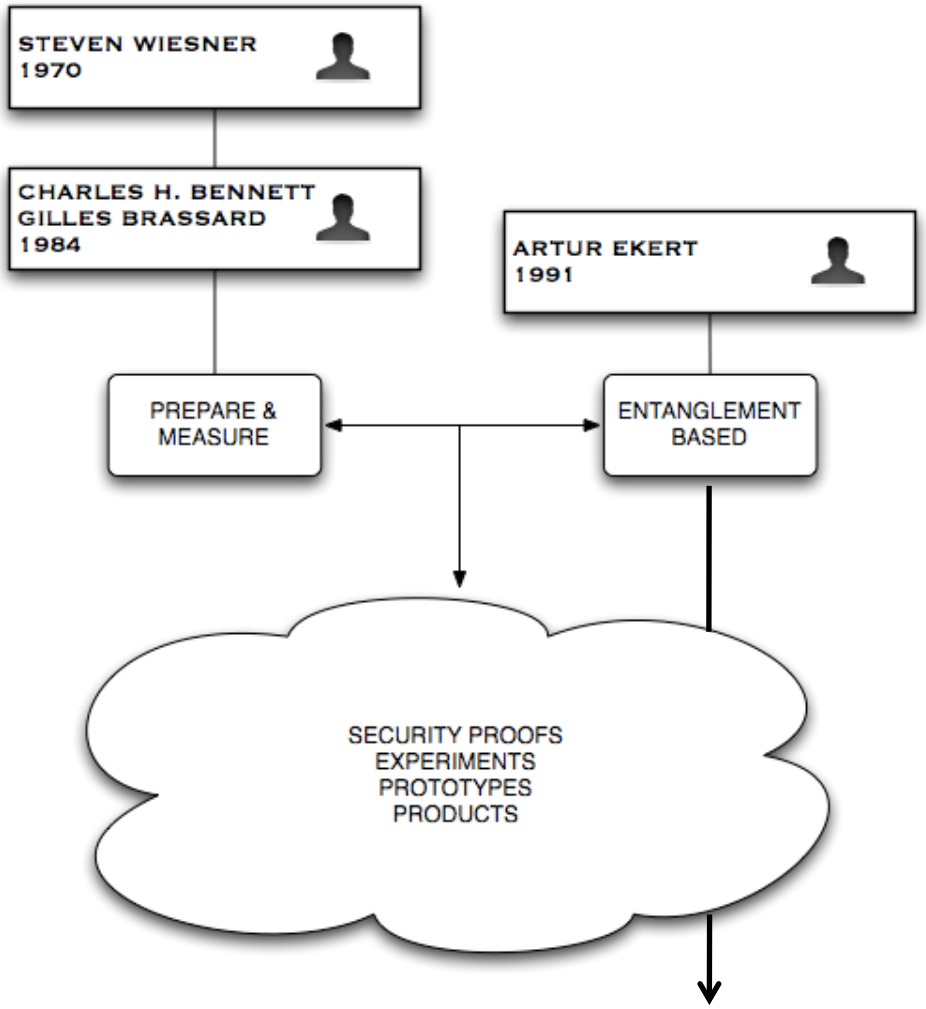
This paper treats a class of codes made possible by restrictions on measurement related to the uncertainty principal. Two concrete examples and some general results are given.

Conjugate Coding *

Stephen Wiesner
Columbia University, New York, N.Y.
Department of Physics

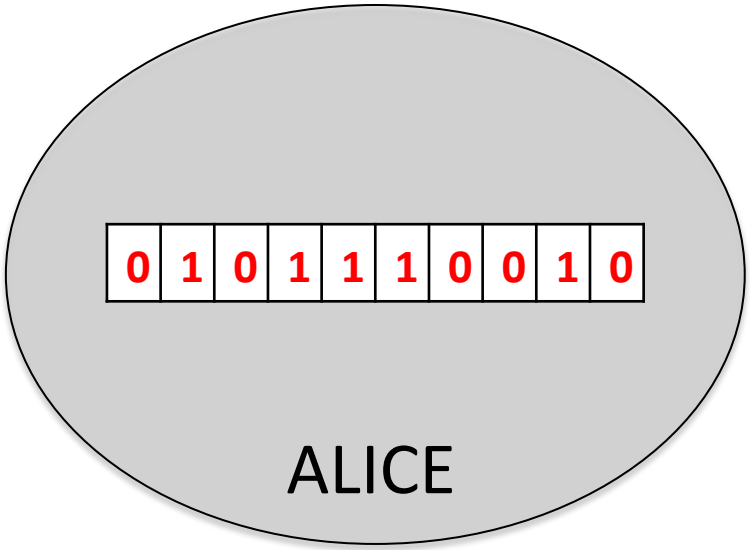
The uncertainty principle imposes restrictions on the capacity of certain types of communication channels. This paper will show that in compensation for this "quantum noise", quantum mechanics allows us novel forms of coding without analogue in communication channels adequately described by classical physics.

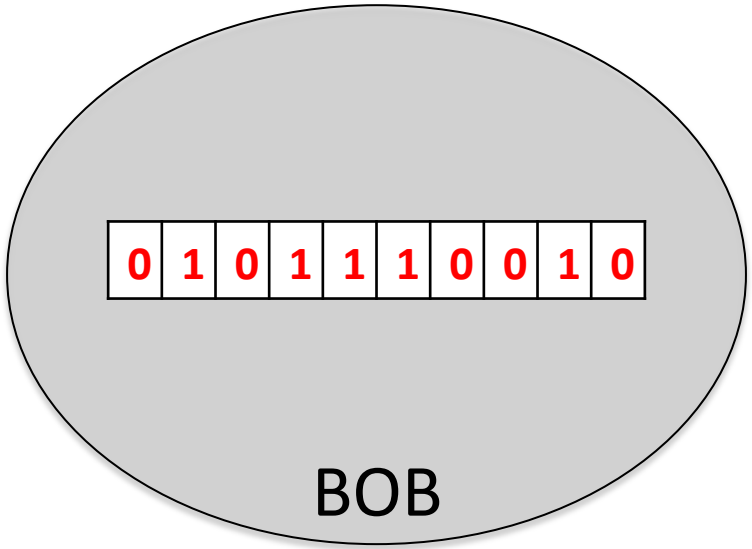
* Research supported in part by the National Science Foundation.




**Device independence etc**

# Secrecy = Shared Randomness




**UNIFORMLY DISTRIBUTED**

**UNPREDICTABLE / INDEPENDENT OF ANYTHING ELSE**

# One-time pad

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| message | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 |
| key | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 |
| cryptogram | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 |



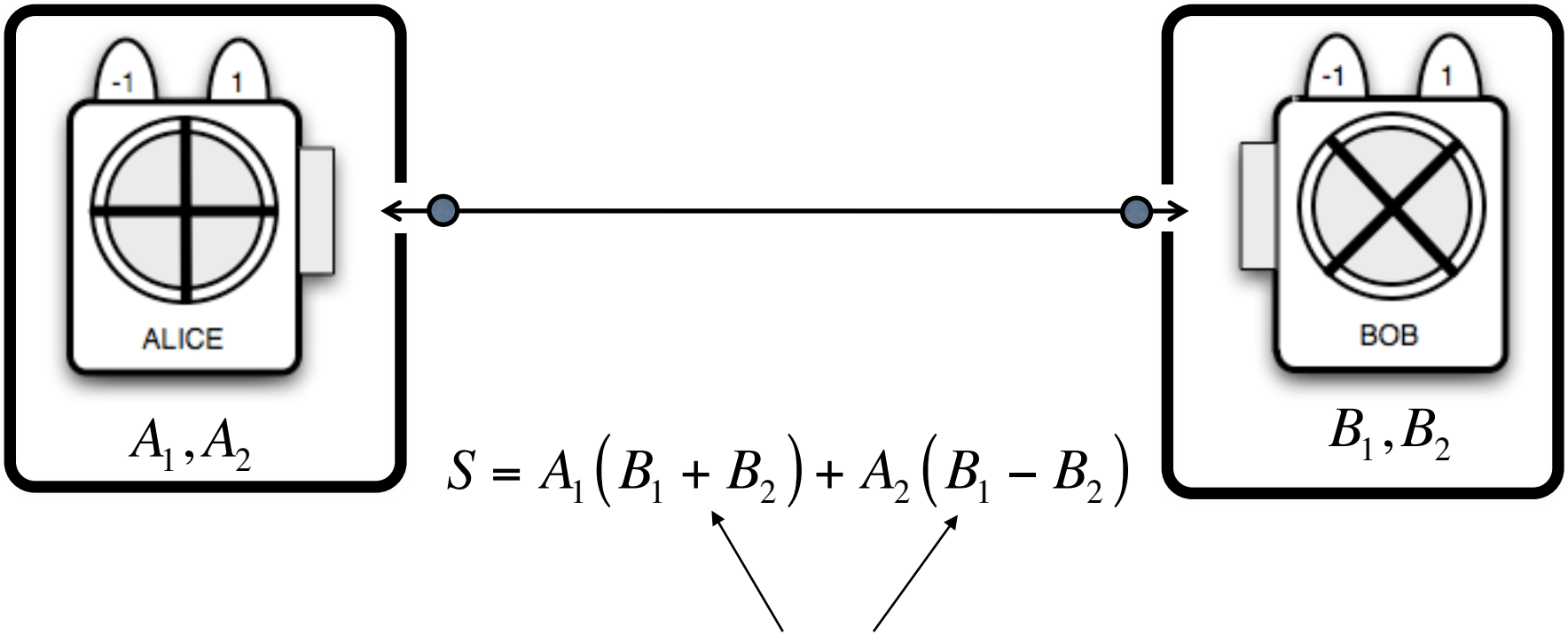
| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | cryptogram |
| 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | key |
| 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | message |

**Secure if the key is secret and uniformly distributed**

**Enter John Bell and a plethora of his inequalities…**

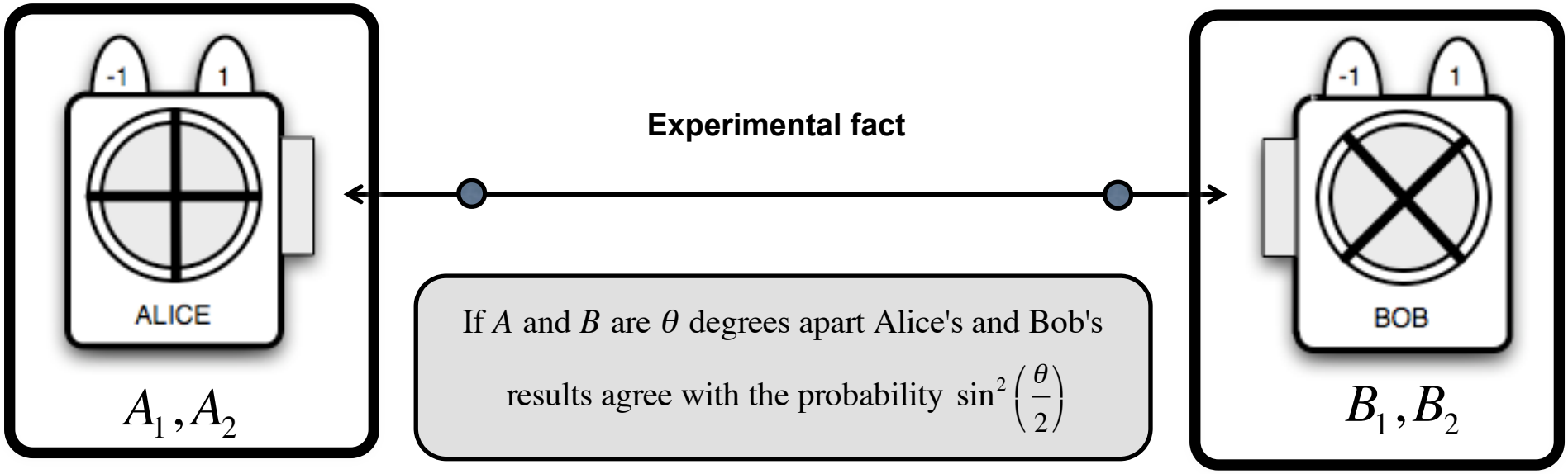
# Bell's inequalities…




**One of these terms is 0 and the other is ± 2**

$S = \pm 2$ **hence** $-2 \leq \langle S \rangle \leq 2$

# Local realism can be refuted…



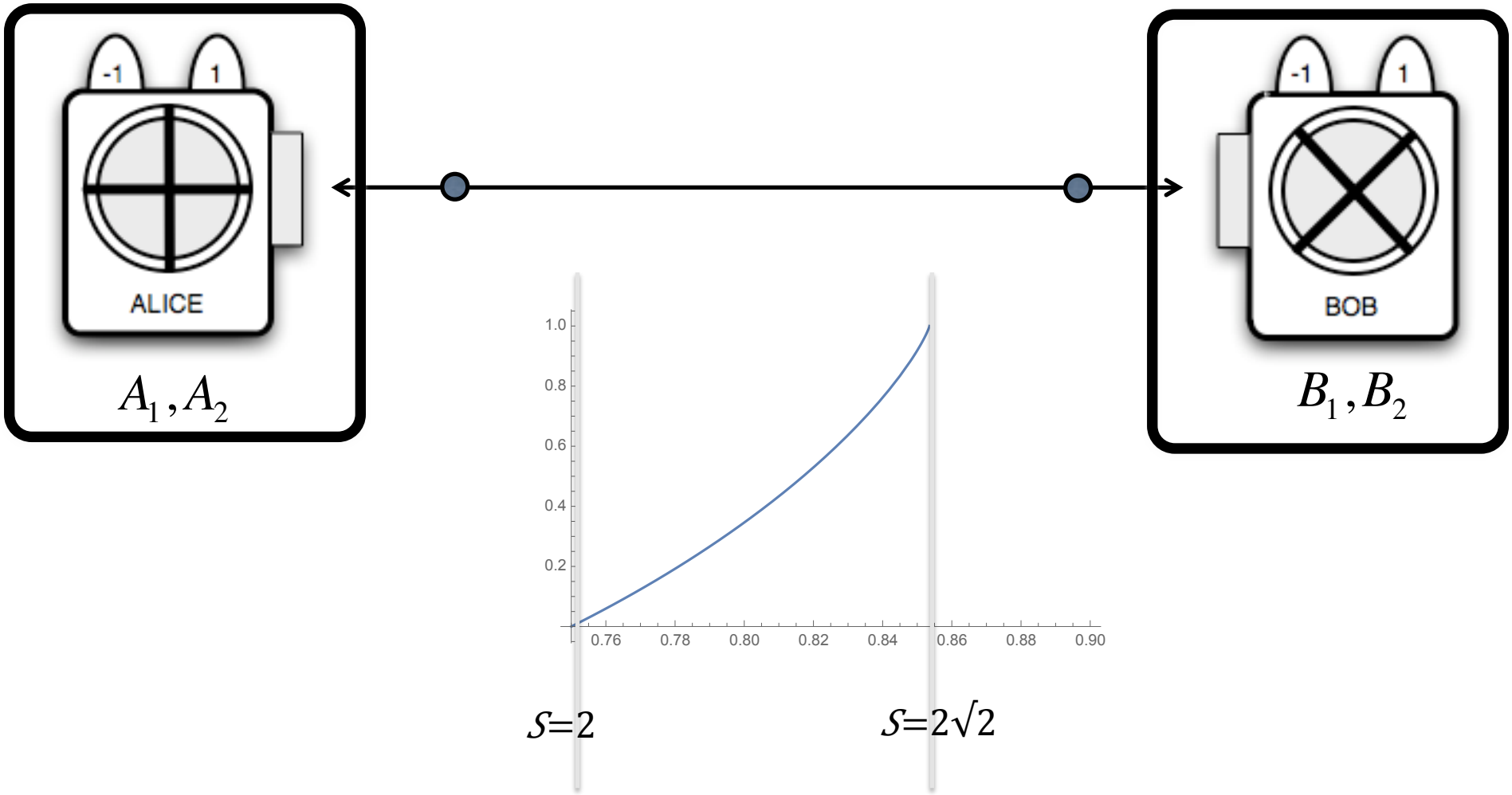

Results agree: $AB = 1$

Results disagree: $AB = -1$

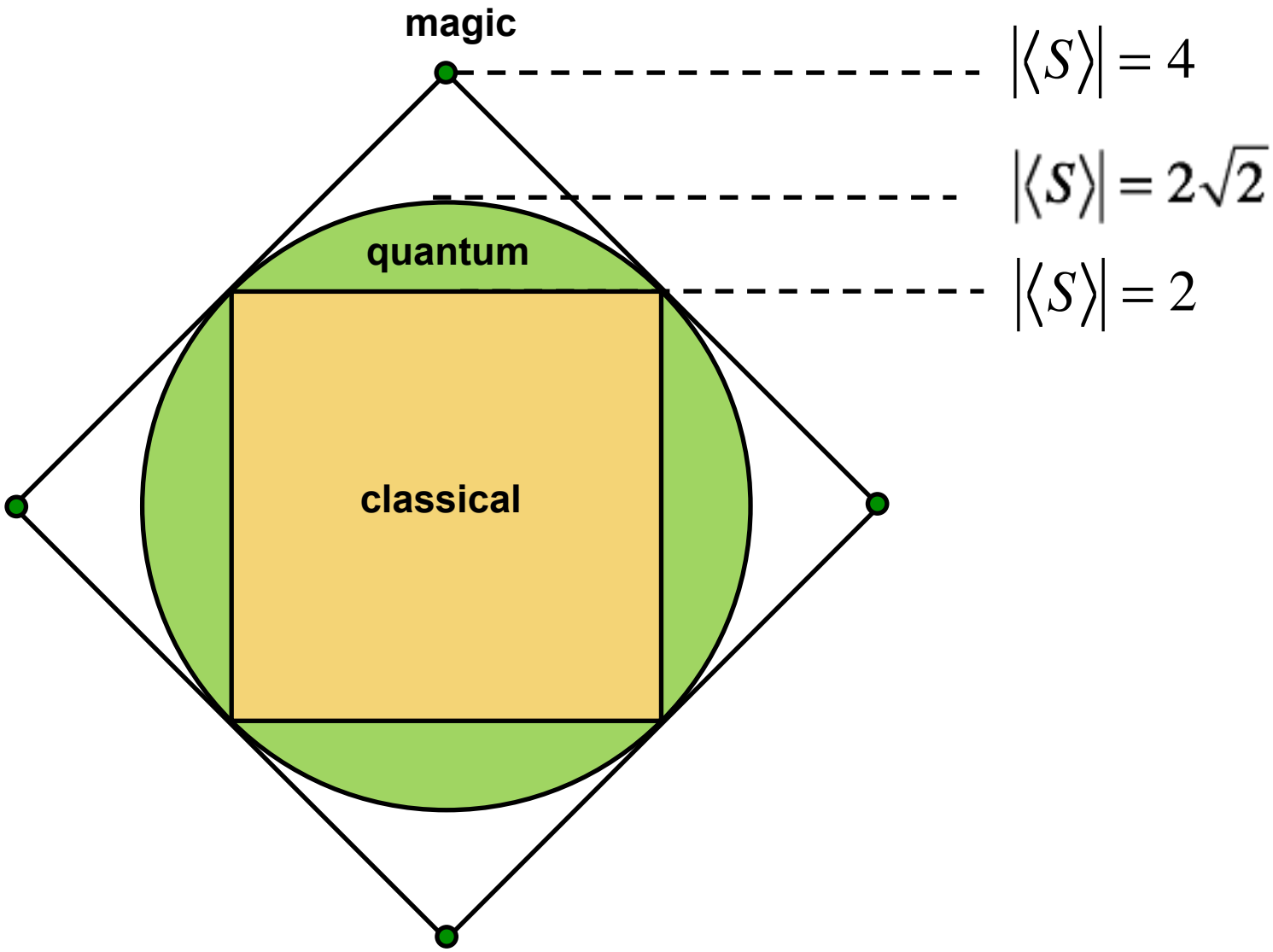
$$\langle AB \rangle = \sin^2\left(\frac{\theta}{2}\right) - \cos^2\left(\frac{\theta}{2}\right) = -\cos\theta$$

$$-2\sqrt{2} \le \langle A_1 B_1 \rangle - \langle A_1 B_2 \rangle + \langle A_2 B_1 \rangle + \langle A_2 B_2 \rangle \le 2\sqrt{2}$$

# Local realism can be refuted…

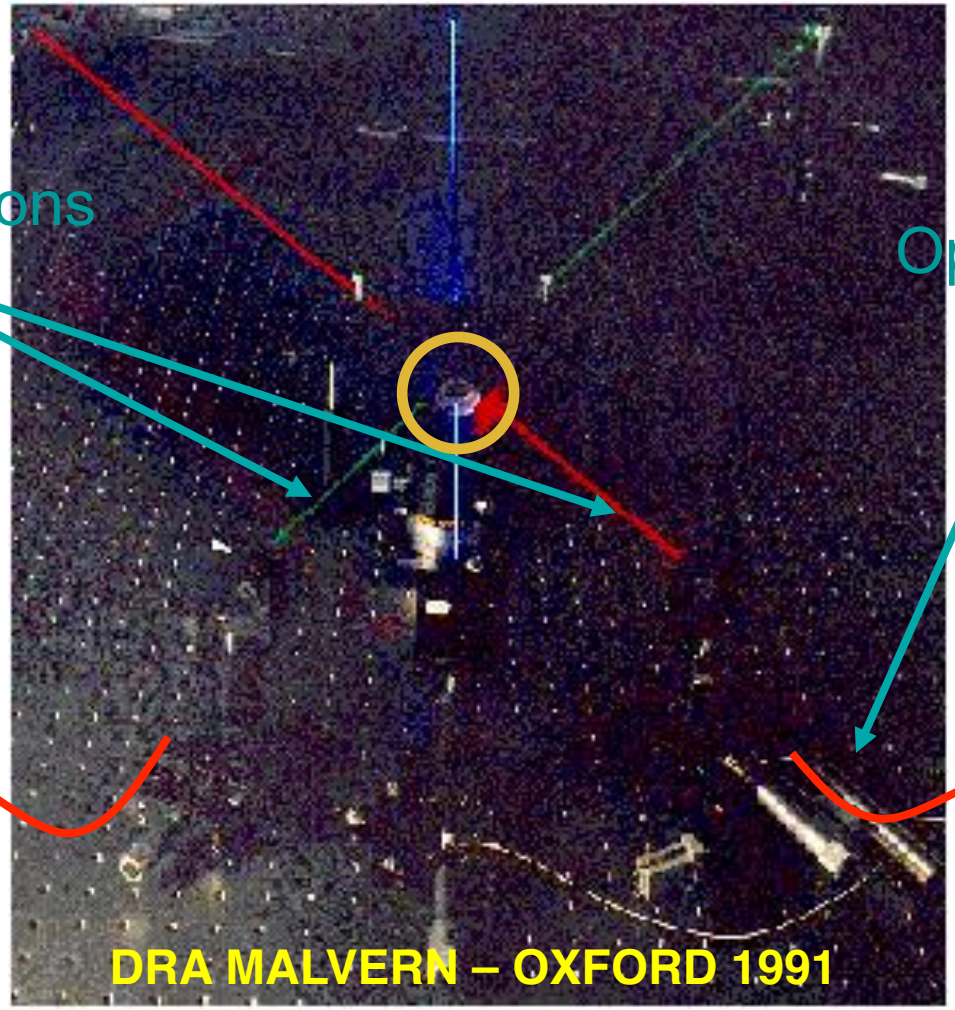


# Correlations galore



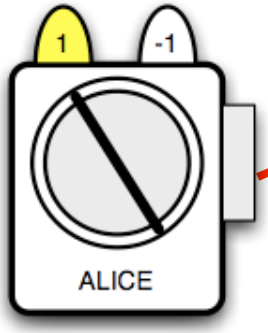
# And all this can be demonstrated…

## Parametric down conversion

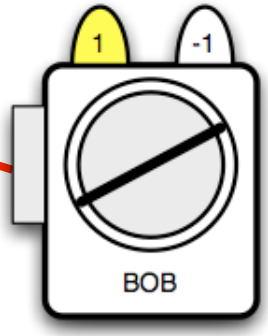



Entangled photons

Optical fibers




Polarizing filters
& photodetectors




Polarizing filters
& photodetectors

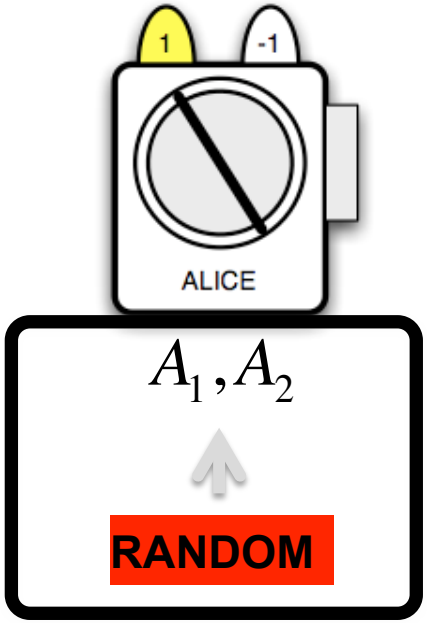
# Today commercial proposition…
# …but would you trust this product?

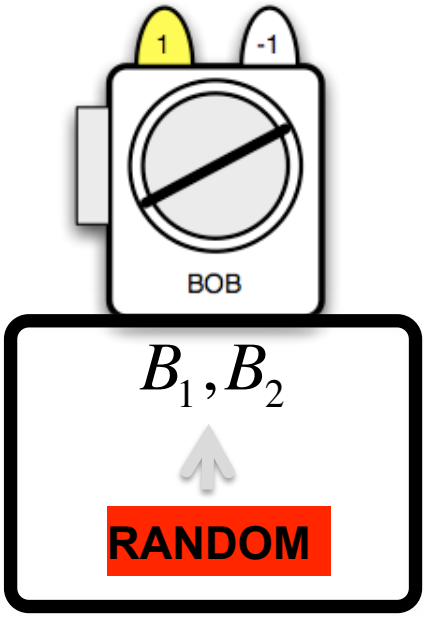

Courtesy Vadim Makarov

# Device independent cryptography

**LOOPHOLE FREE BELL TEST IS SUFFICIENT**

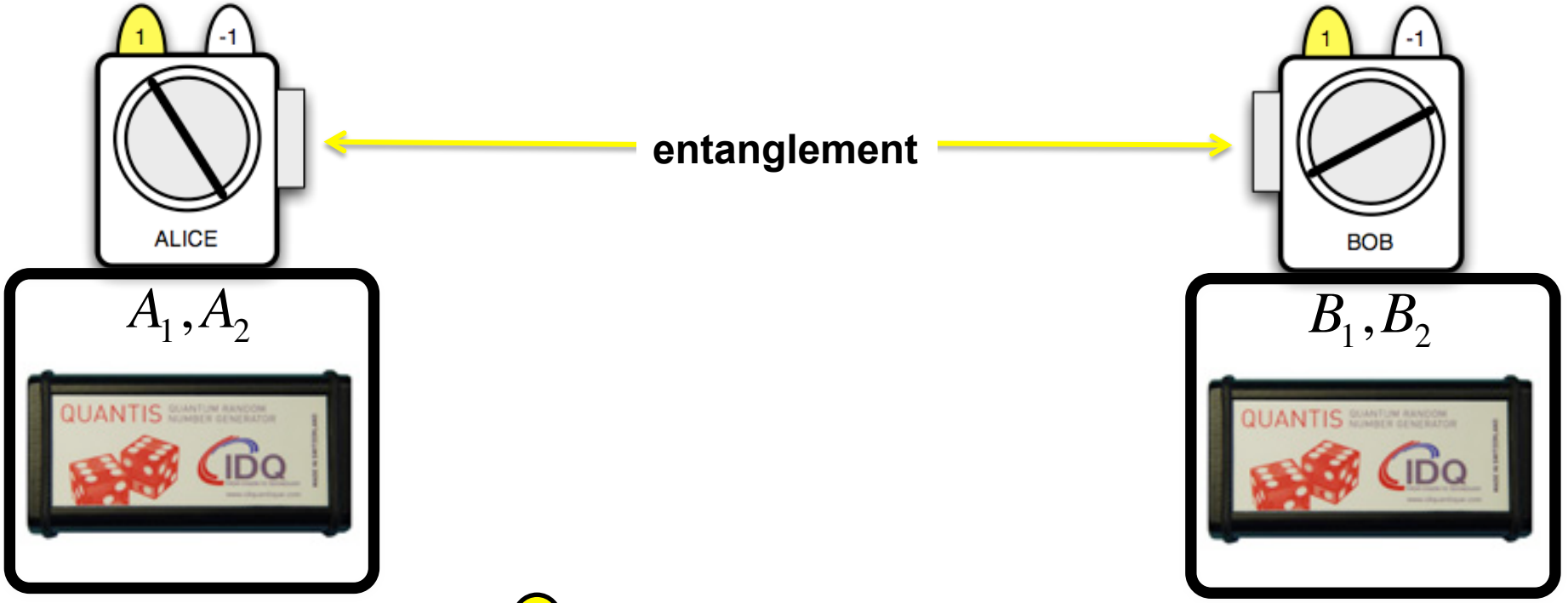
**No need to trust manufactures**
**No need to check what is in the box**




- **LOCAL RANDOMNESS**
- **LOCAL ISOLATION**
- **LOOPHOLE-FREE BELL TESTS**

# Good local randomness?




- QUANTUM RNG
- LOCAL ISOLATION
- LOOPHOLE-FREE BELL TESTS

# Uniformly distributed and unpredictable


01000101100111110010101000010…

**EACH BIT MUST BE**

**UNIFORMLY DISTRIBUTED**

**INDEPENDENT OF ANYTHING ELSE (OUTSIDE ITS FUTURE LIGHT CONE)**



**CERTIFICATION OF THE PROCESS**

# Trust the authorities?

CTL
COMPLIANCE TESTING LABORATORY

## Certificate of Compliance

This is to certify that the Random Number Generator

**Quantis-v10.10.08**

by

**ID Quantique SA**

*REF : CTL-037/37001*

has been tested by

**CTL, Compliance Testing Laboratory**

and has been found to be *suitably unpredictable and fit for purpose*

Issue Date: 30.03.2011

---

Technical Compliance Manager, CAST Limited

UKAS TESTING

CAST

PRIFYSGOL BANGOR UNIVERSITY 1884

CAST LTD Compliance Testing Laboratory,
A company approved and certified under the Online Gambling Regulation Act 2001 and accredited by UKAS for UK Testing

*Compliance Testing Laboratory, Tŷ Menai, Fford Penlan, Parc Menai Business Park, Bangor, Gwynedd LL57 4HJ*

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Justice and Police FDJP
**Federal Office of Metrology METAS**

## Certificate of Conformity No 151-04687

| | |
|---|---|
| *Object* | **Quantum Random Number Generator**<br>Quantis-USB S/N 070222A410<br>Quantis-PCI-1 S/N 08338A310<br>Quantis-PCI Express S/N 1002251A210 |
| *Applicant* | **id Quantique SA**<br>Ch. De la Marbrerie 3<br>1227 Carouge/Geneva<br>Switzerland |
| *Requirements* | The output of the Quantis random number generator has to pass all DIEHARD Battery of Tests, confirming that the random number generator distributes numbers with sufficient non-predictability, fair distribution and lack of bias to particular outcomes. Specifically: 10 data sets consisting of 1E8 bits per data set is considered to be random if none of the 234 p-values produced by the 15 DIEHARD Battery of Tests has a value between 1 and 1-epsilon, where epsilon is 1e-6. |
| *Confirmation* | The tested Quantis-USB, Quantis-PCI-1 and Quantis-PCI Express have passed all DIEHARD Battery of Tests.<br>The sequence of random bits generated cannot be predicted.<br>The sequence of random bits generated cannot be reproduced. |
| *Remarks* | The testing procedure used is described in the annex document "Annex_METAS_151-04687" |

CH-3003 Bern-Wabern, 10 May 2010

For the Test

Dr.Damian Twerenbold

Division Mechanics, Radiation and Time

Dr.Philippe Richard, Vice-Director

This document may not be published or forwarded other than in full.

1/1

METAS
Lindenweg 50, CH-3003 Bern-Wabern, Tel. +41 31 32 33 111, www.metas.ch

# Perhaps I can amplify weak randomness?


01001011001… → **Randomness Amplification** → 011010…

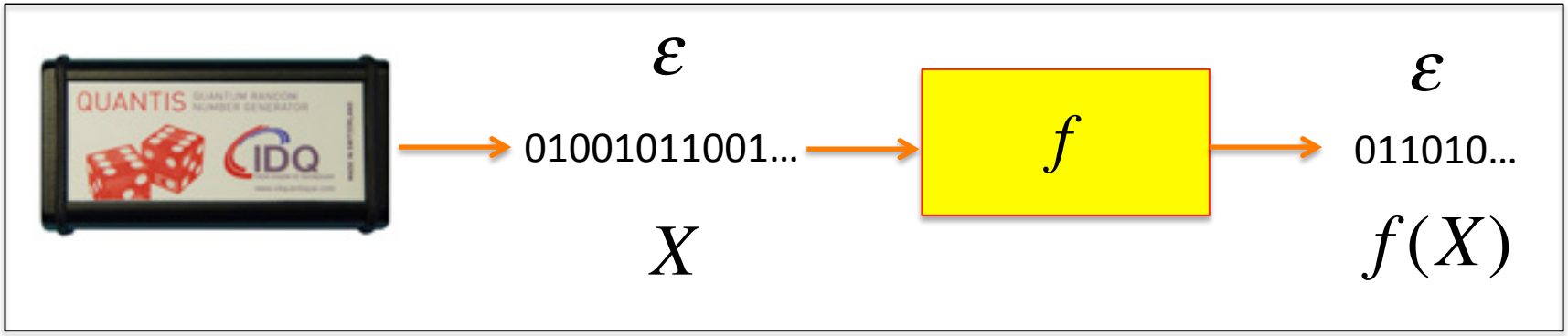
$X$ is $\varepsilon$-random if

**statistical distance**

$$\frac{1}{2}\left| P_{X|E} - P_U \right| \leq \varepsilon$$

where $E$ denotes everything outside the future of $X$

# No way…

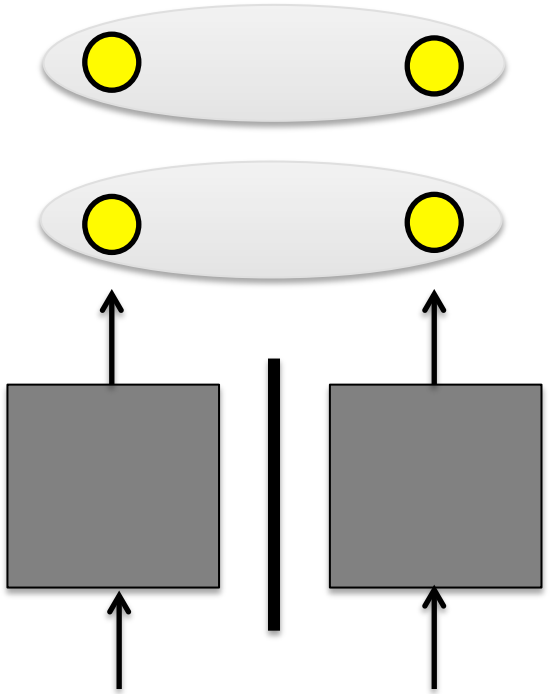



There exists no function $f$ such that the output $f(X)$ is uniform for any $\varepsilon$-random input $X$.

Santha & Vazirani (1984)

# …unless we use monogamous correlations

For any $\varepsilon < \varepsilon_0$ there exists a device-independent protocol whose output $f(X)$ is uniform for any $\varepsilon$-random input $X$.



$\varepsilon$-random source

Colbeck & Renner (2011)

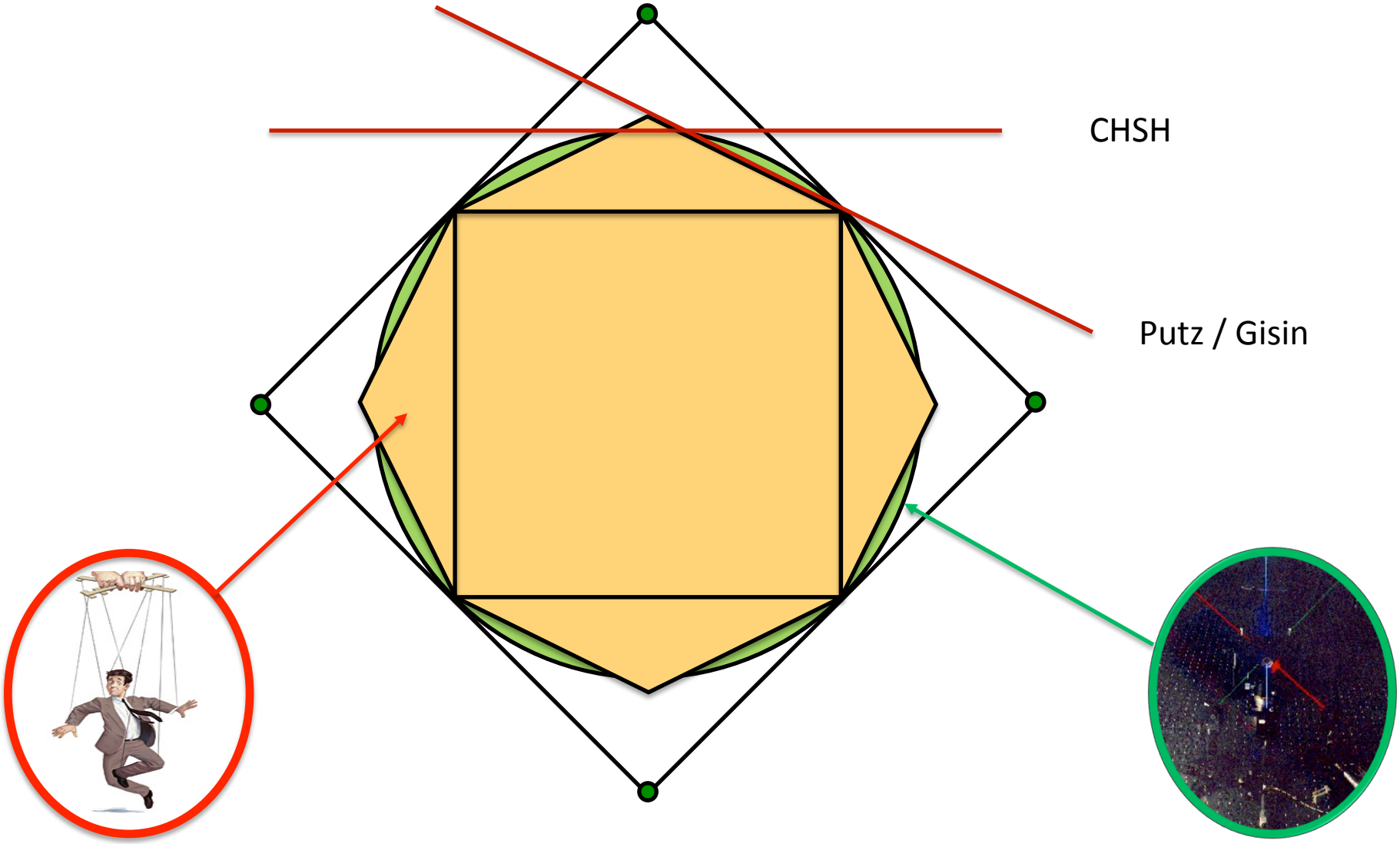
$$\varepsilon < 0.08$$

Galego et al (2012)

$$\varepsilon < 0.5$$

**MONOGAMOUS CORRELATIONS**
**CHAINED BELL INEQUALITIES**

# Beyond CHSH

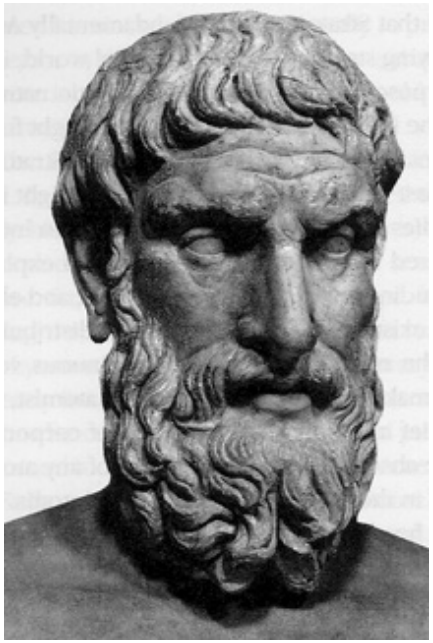


# Many open questions

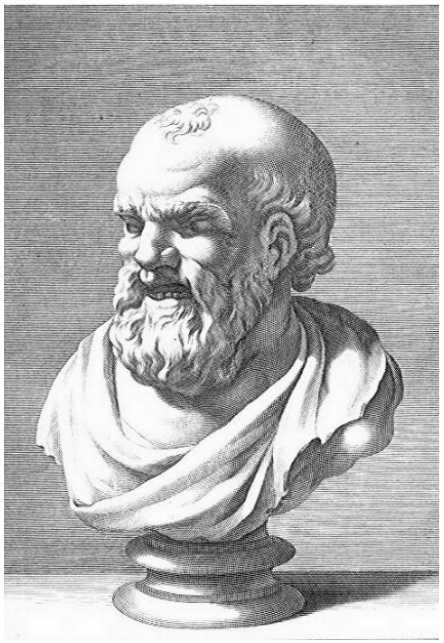
**EPR VISION OF REALITY IS TOO SIMPLISTIC**

**SECURITY AND RANDOMNESS IN THE MULTIVERSE**

# Origins of randomness



Why random?



**EPICURUS**
**(300 BC)**

**OBJECTIVE**

atoms *swerve* at random along their paths

**DEMOCRITUS**
**(400 BC)**

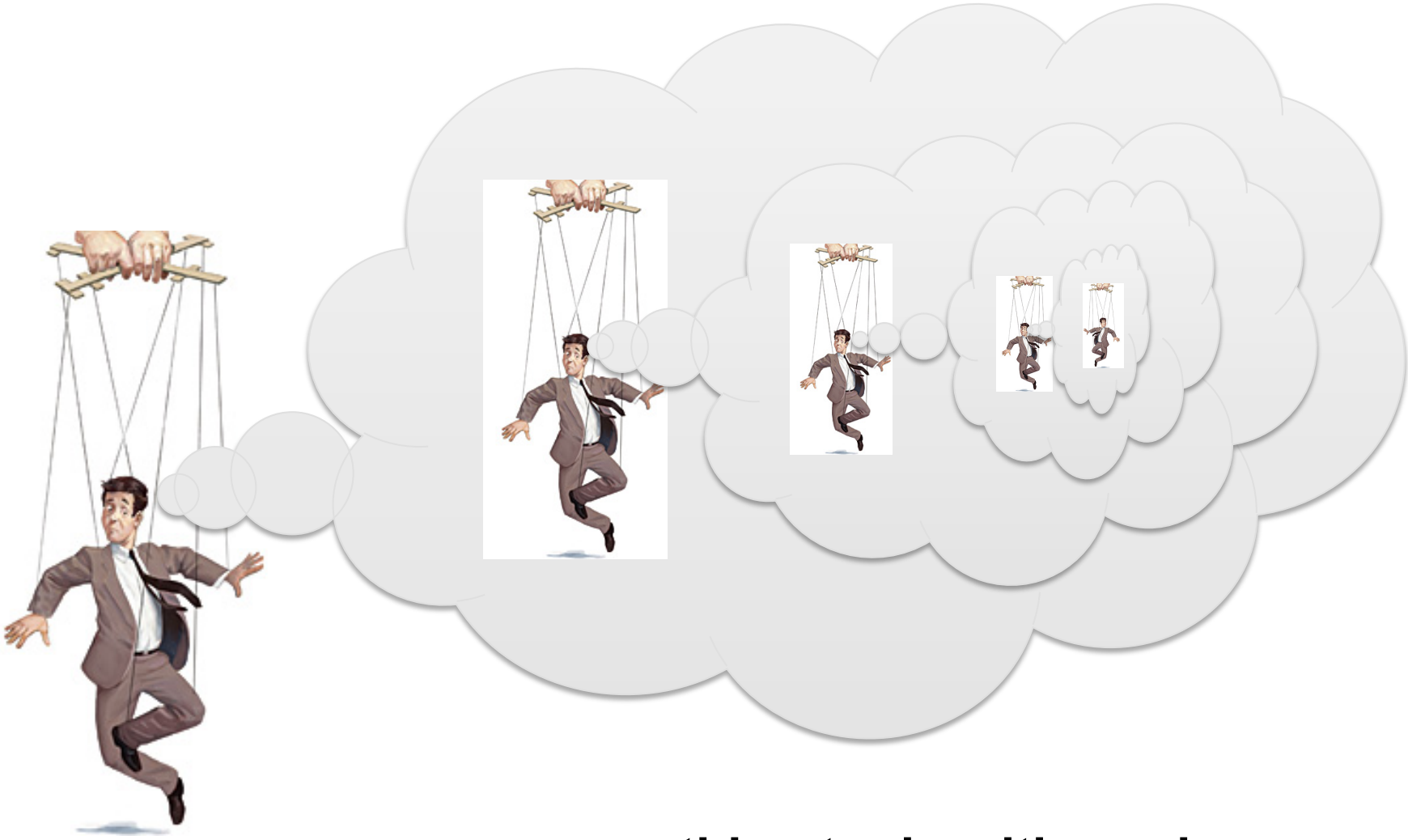
**SUBJECTIVE**

atoms follow predetermined paths

**But I do not trust myself !**

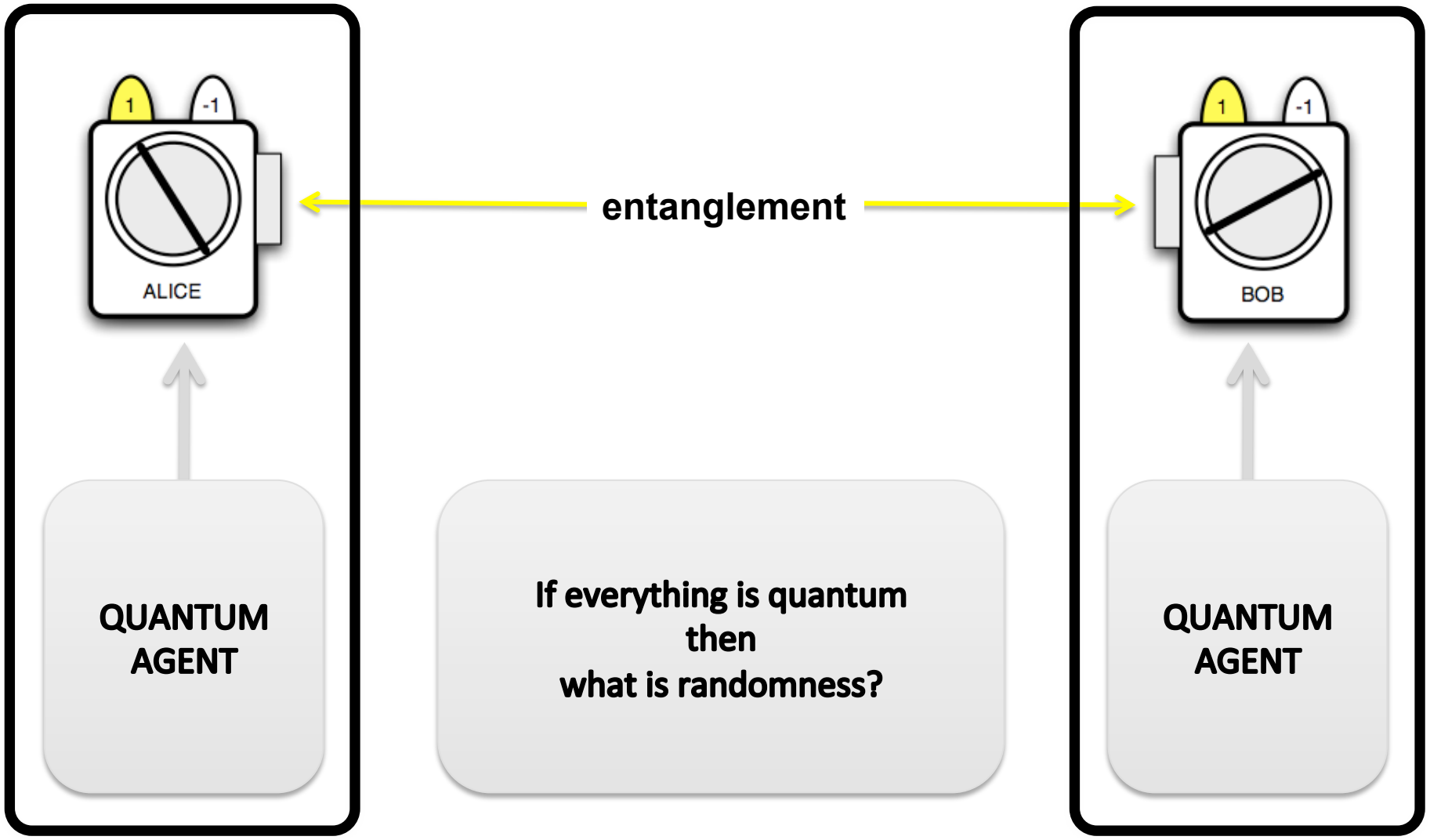
**I feel I am manipulated!**

# Free will within deterministic system

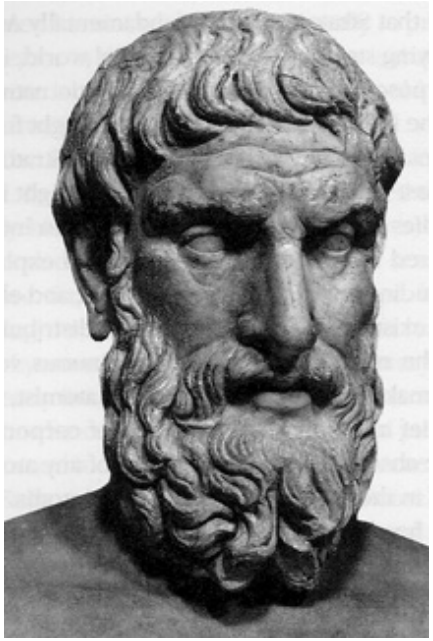


nothing to do with randomness

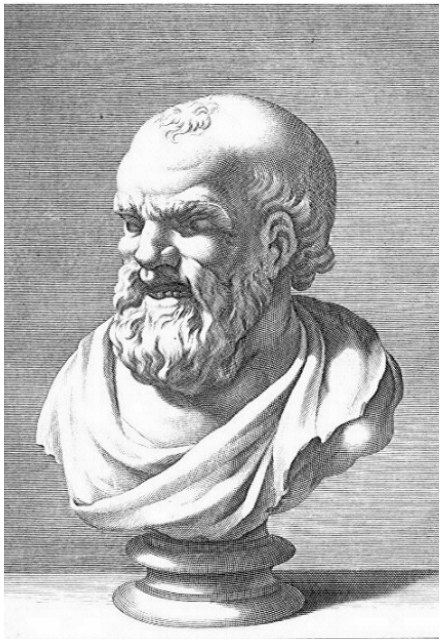
# Beyond the simplistic mathematical model



# Beyond the simplistic mathematical model



**If everything is quantum**
**then**
**what is randomness?**



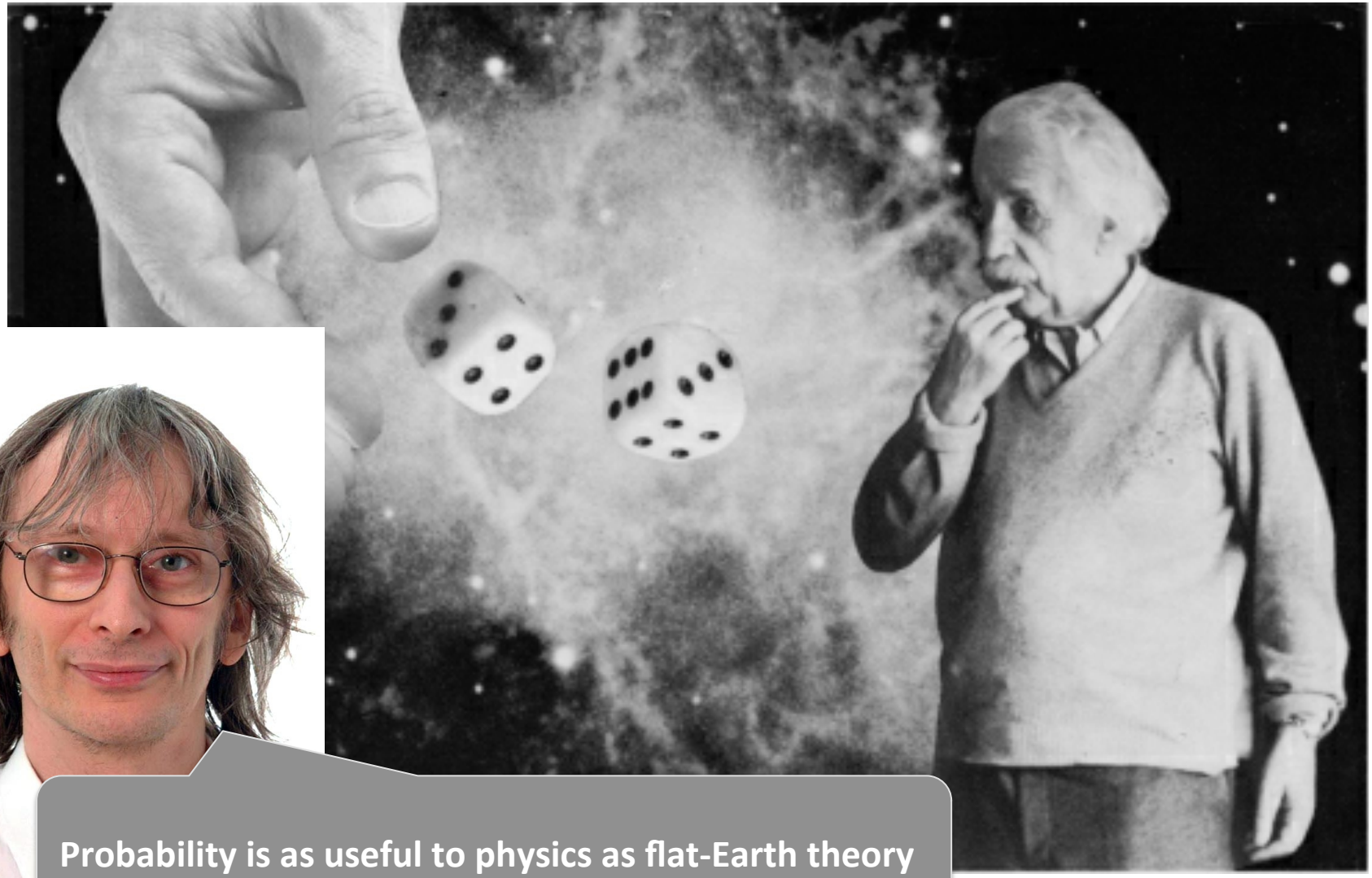
**EPICURUS**
**(300 BC)**

**OBJECTIVE**

**DEMOCRITUS**
**(400 BC)**

**SUBJECTIVE**

# Do we really need probability…





Probability is as useful to physics as flat-Earth theory

nature

THE INTERNATIONAL WEEKLY JOURNAL OF SCIENCE

# HOW TO KEEP A SECRET

Quantum cryptography, randomness and cunning can outfox the snoopers

PAGE 443

ARCHAEOGENETICS

## THE WAY WE WERE

*Ancient DNA is rewriting human prehistory*

PAGE 414

QUANTUM PHYSICS

## WHY IT'S ALL ABOUT ME

*On the physical nature of the Now*

PAGE 421

BIOMEDICINE

## MAKE THE MOST OF MICE

*Better use of disease models can save human lives*

PAGE 423

NATURE.COM/NATURE

27 March 2014 £10

Vol. 507, No. 7493

9 770028 083095 13