Bell inequalities

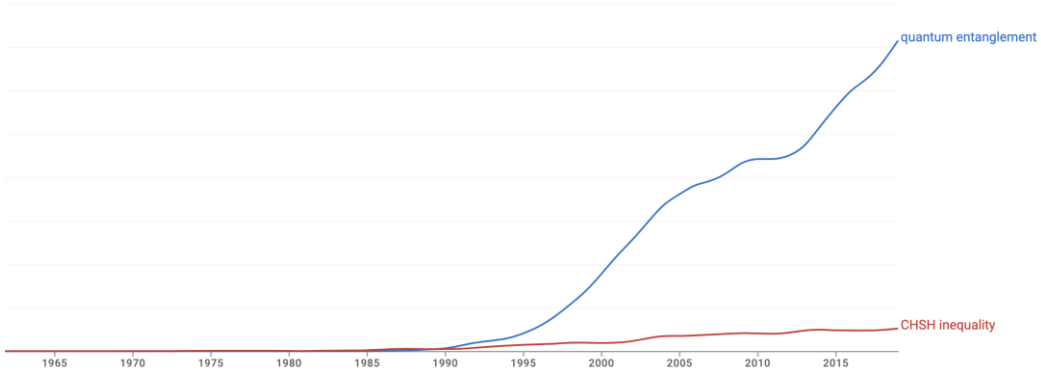
From curiosity to security

Artur Ekert

Spoiler – two narratives

1935

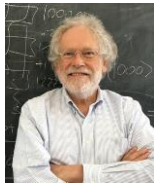
1972



curiosity

1964

1982



1918

Gilbert Vernam

~ 1970

James Ellis

~ 1980

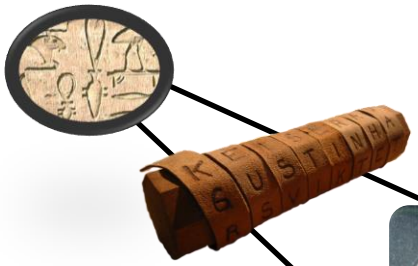
Stephen Wiesner

E91

BB84

security

Quest for a perfect cipher

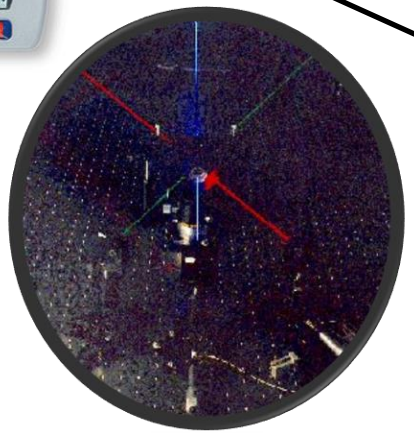


400BC
SCYTALE

1450
ALBERTI'S DISC

ENIGMA 1940

Public Keys



Quantum Crypto

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

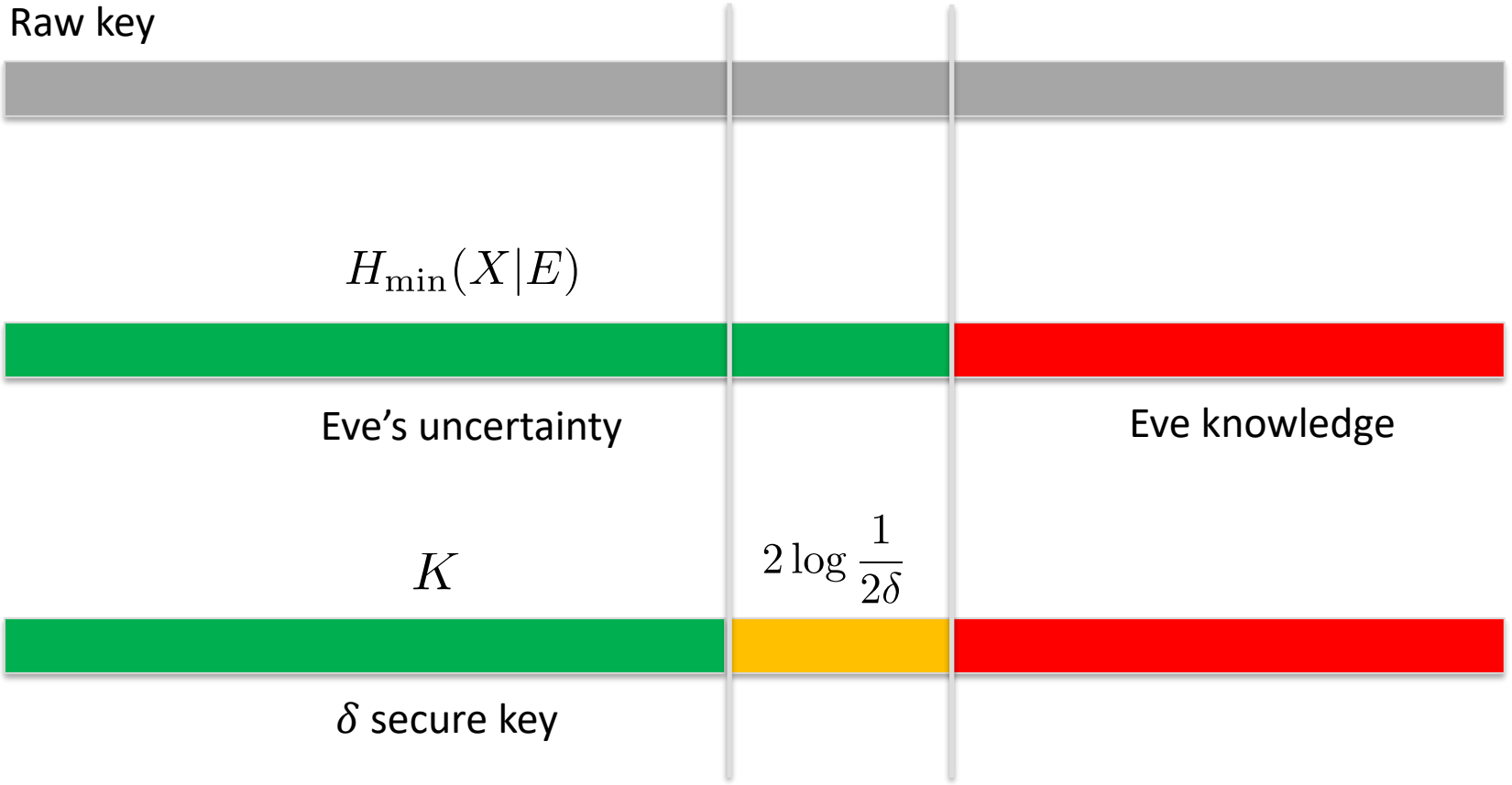
	0	0	1	0	1	0	0	0	0	1

	0	0	1	0	1	0	0	0	0	1

cryptogram	0	0	1	0	1	0	0	0	0	1
key	0	1	0	1	1	1	0	0	1	0
message	0	1	1	1	0	1	0	0	1	1

KEY DISTRIBUTION PROBLEM

Privacy amplification



$$l = H_{\min}(X|E) - 2\log\frac{1}{2\delta}$$

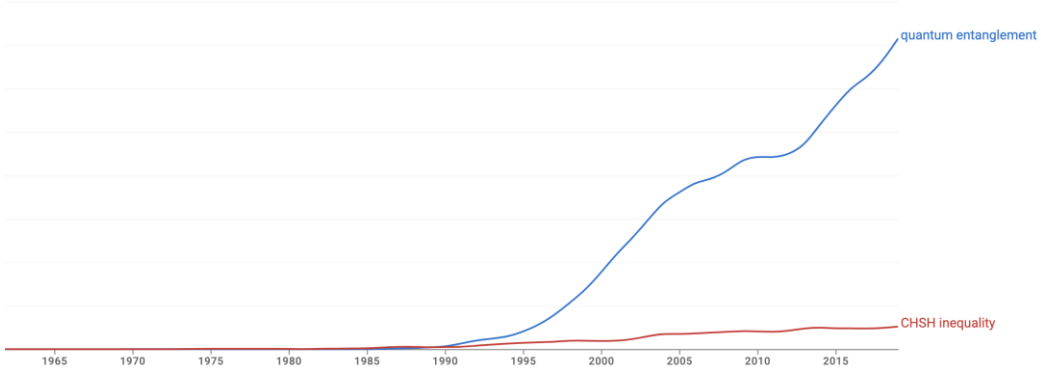
But how much does Eve know?

$$H_{\min}(X|E)$$

The other narrative

1935

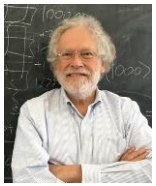
1972



curiosity

1964

1982



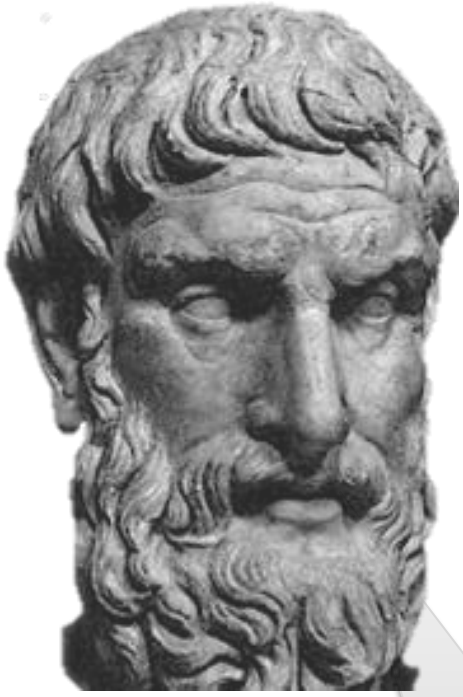
E91

security

BB84

Randomness – objective or subjective?

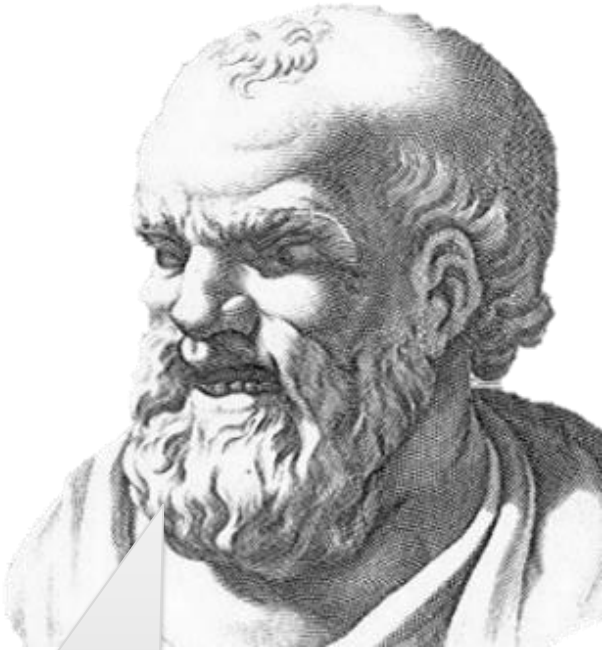
EPICURUS (300 BC)



atoms *swerve* at random along their paths

OBJECTIVE

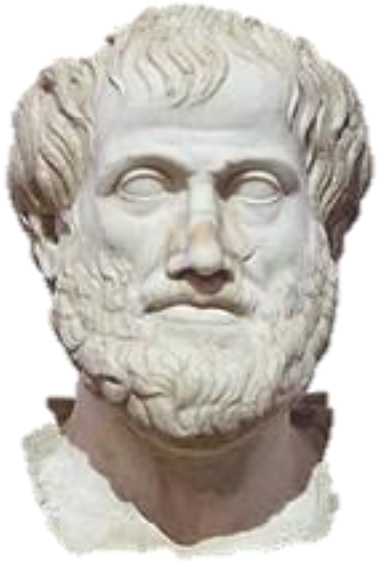
DEMOCRITUS (400 BC)



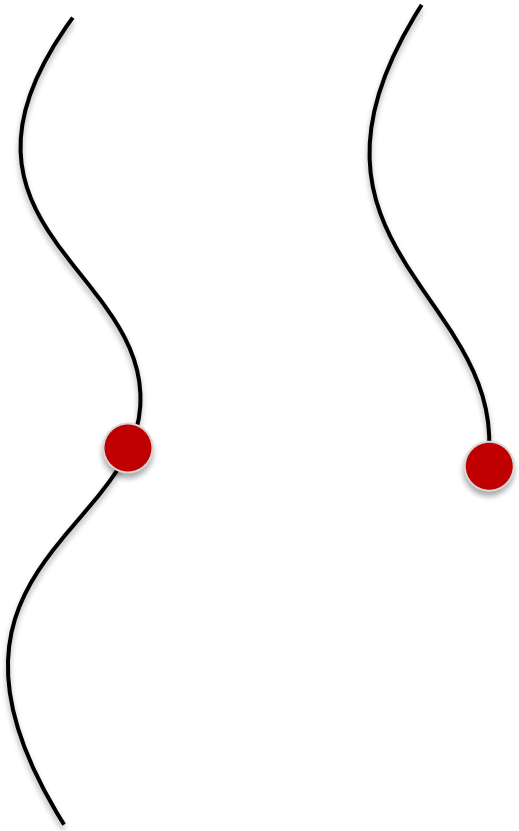
atoms follow predetermined paths

SUBJECTIVE

Beyond rational domain

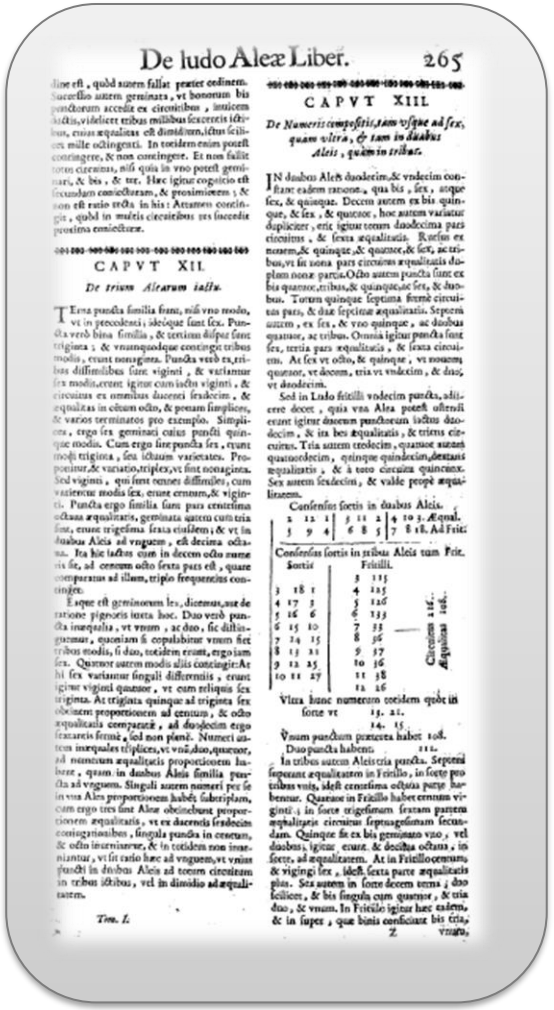


Aristotle 384–322 BC



Science by its own nature is causal
Chance = break of causality
Hence chance cannot be studied by science

But if you are a rational gambler…



De ludo Aleæ Liber. 265

CAPVT XII.

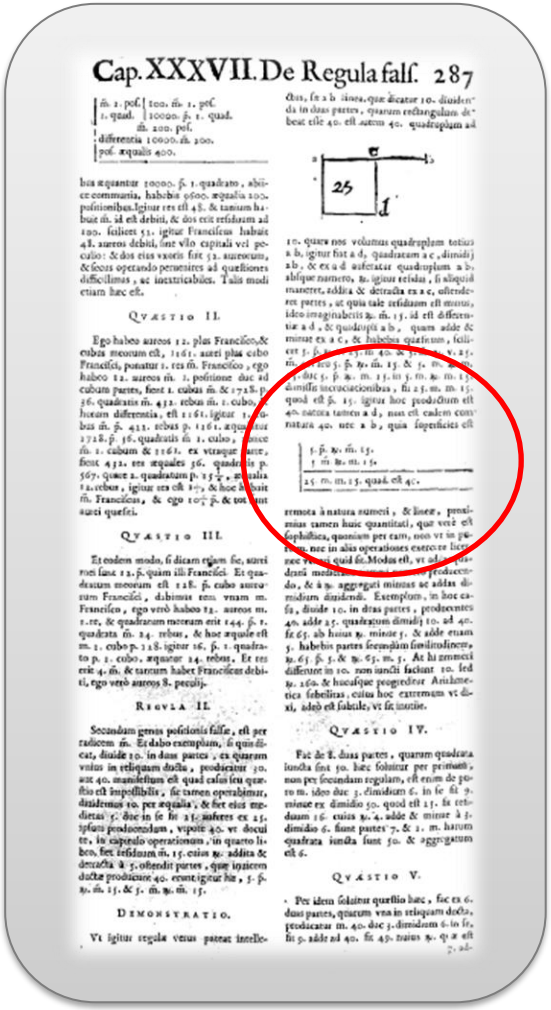
De trium Alearum iactu.

CAPVT XIII.

De Numeris compositis, quam vsque ad sex, quam vltra, & tam in duabus Aleis, quàm in tribus.

Girolamo Cardano

1501-1576



Cap. XXXVII. De Regula falf. 287

QVÆSTIO II.

QVÆSTIO III.

REGVLA II.

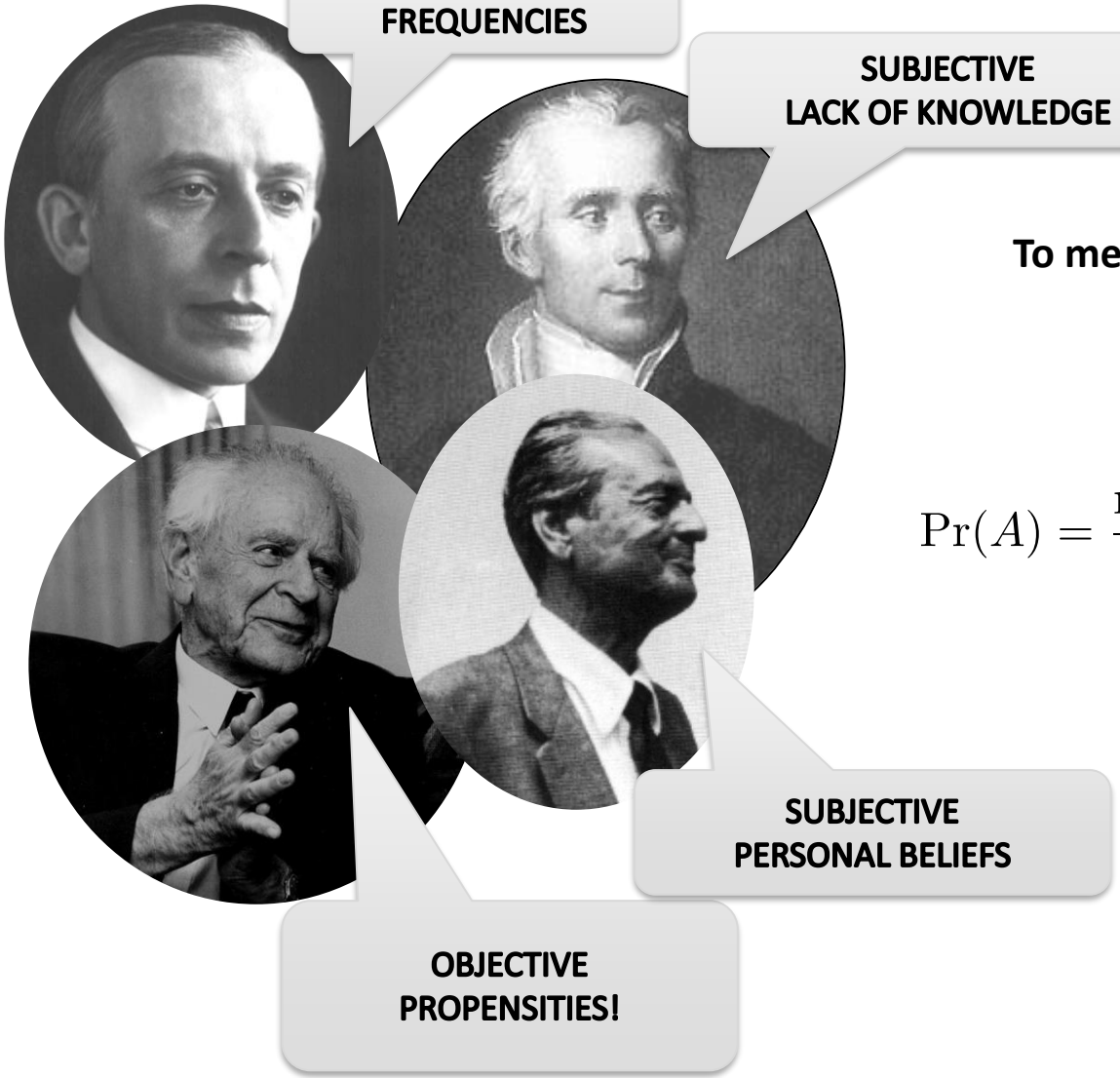
QVÆSTIO IV.

QVÆSTIO V.

PROBABILITY
Liber de Ludo Aleae

COMPLEX NUMBERS
Ars Magna

How to understand probability?



To measure probability find equally probable cases and count them

$$\Pr(A) = \frac{\text{no. of cases in which A occurs}}{\text{total no. of cases}}$$

And then came Kolmogorov…

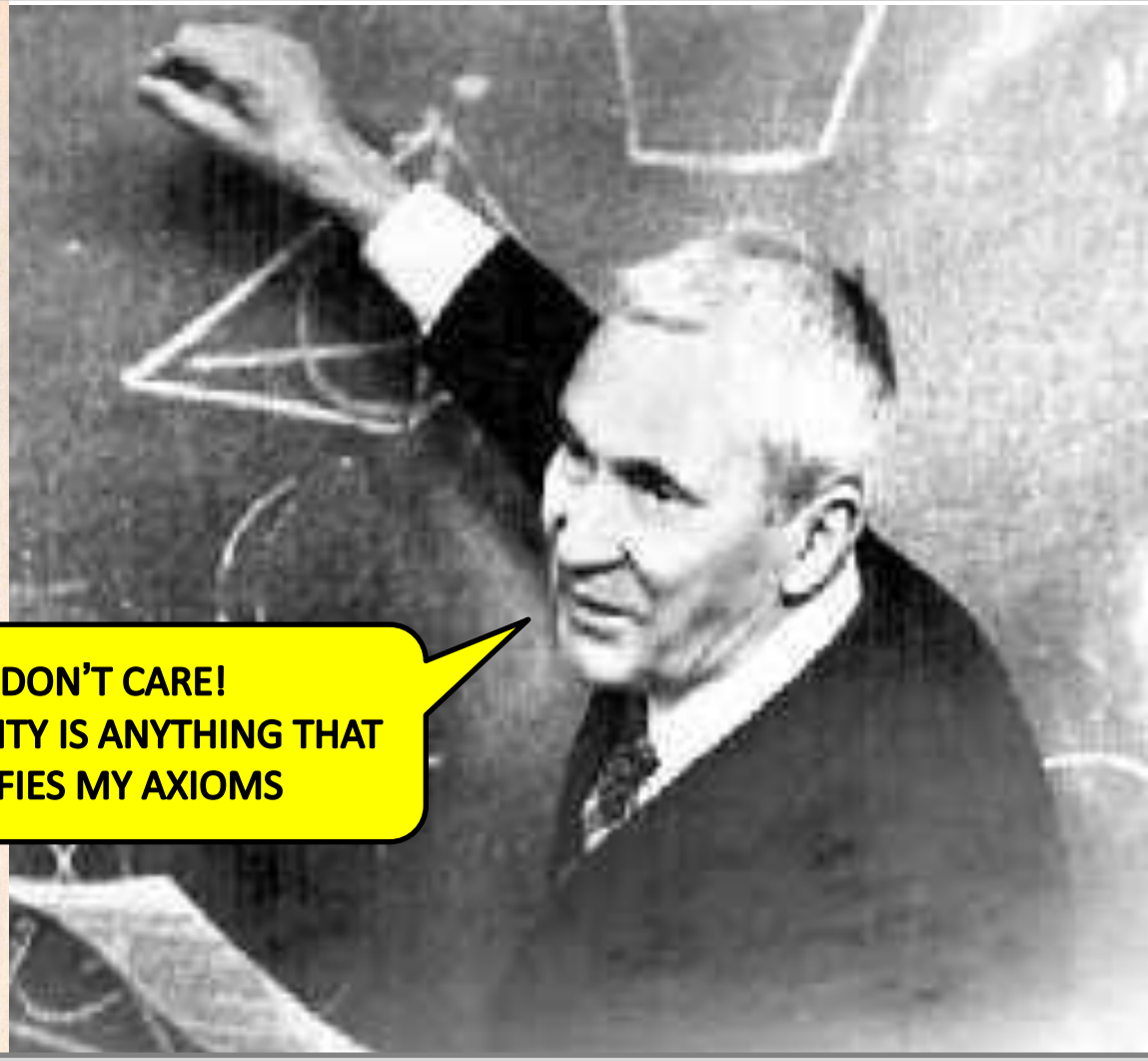
ERGEBNISSE DER MATHEMATIK
UND IHRER GRENZGEBIETE
HERAUSGEGEBEN VON DER SCHRIFTLEITUNG
DES
„ZENTRALBLATT FÜR MATHEMATIK"
ZWEITER BAND
3

GRUNDBEGRIFFE DER
WAHRSCHEINLICHKEITS-
RECHNUNG

VON

A. KOLMOGOROFF

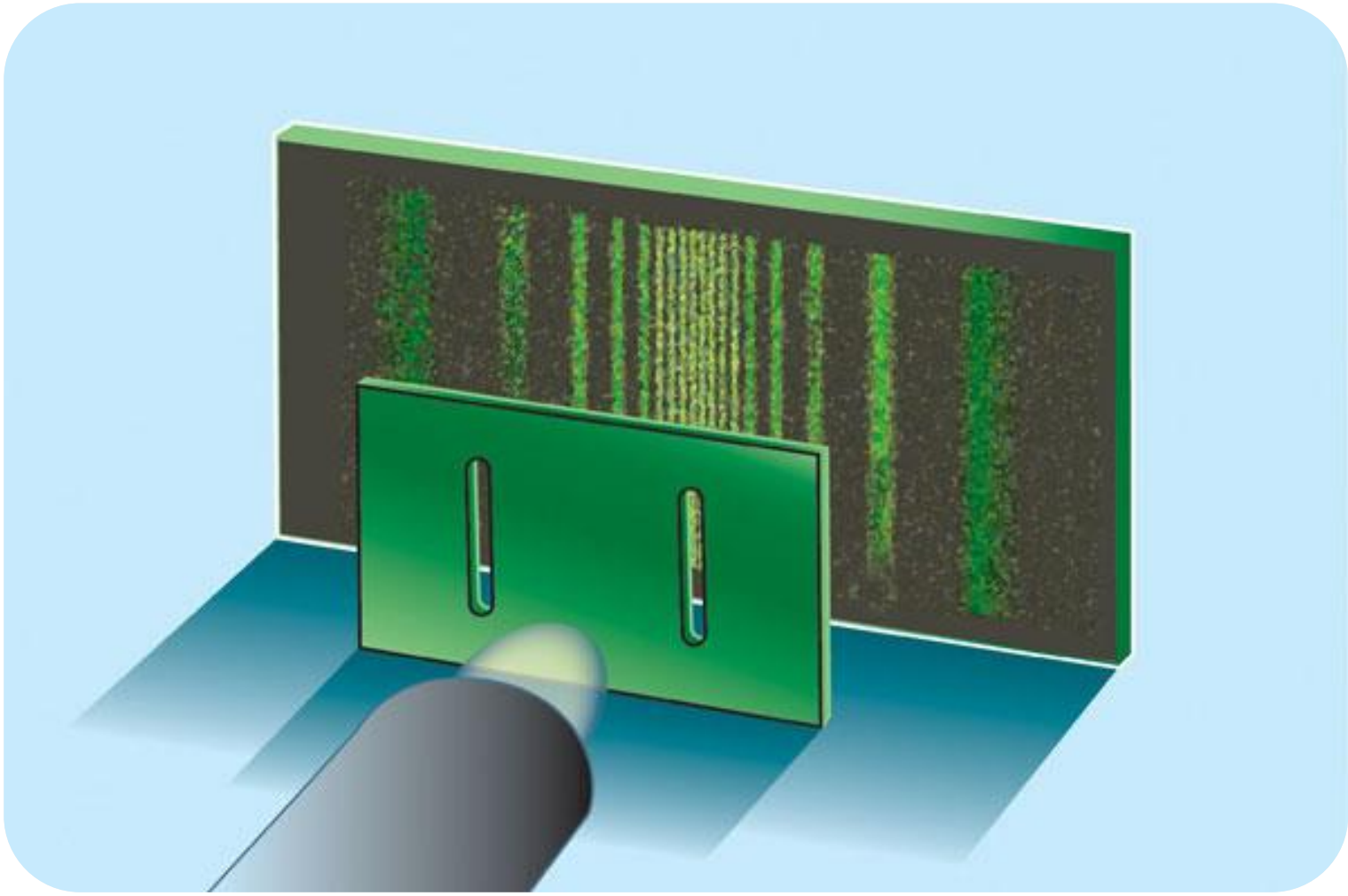
BERLIN
VERLAG VON JULIUS SPRINGER
1933



I DON'T CARE!
PROBABILITY IS ANYTHING THAT
SATIFIES MY AXIOMS

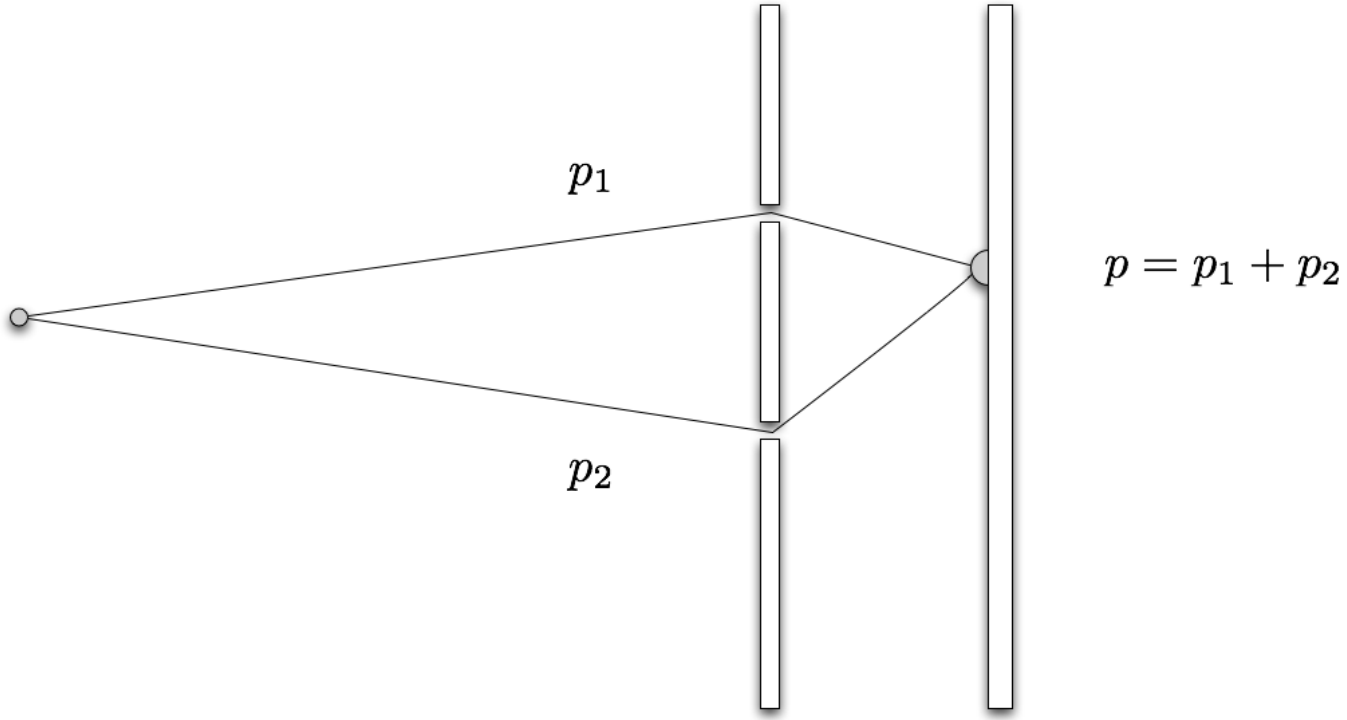
Probability is a non-negative number
Probability that something happens is 1
Probabilities of exclusive events add up

It’s all very well, except that…

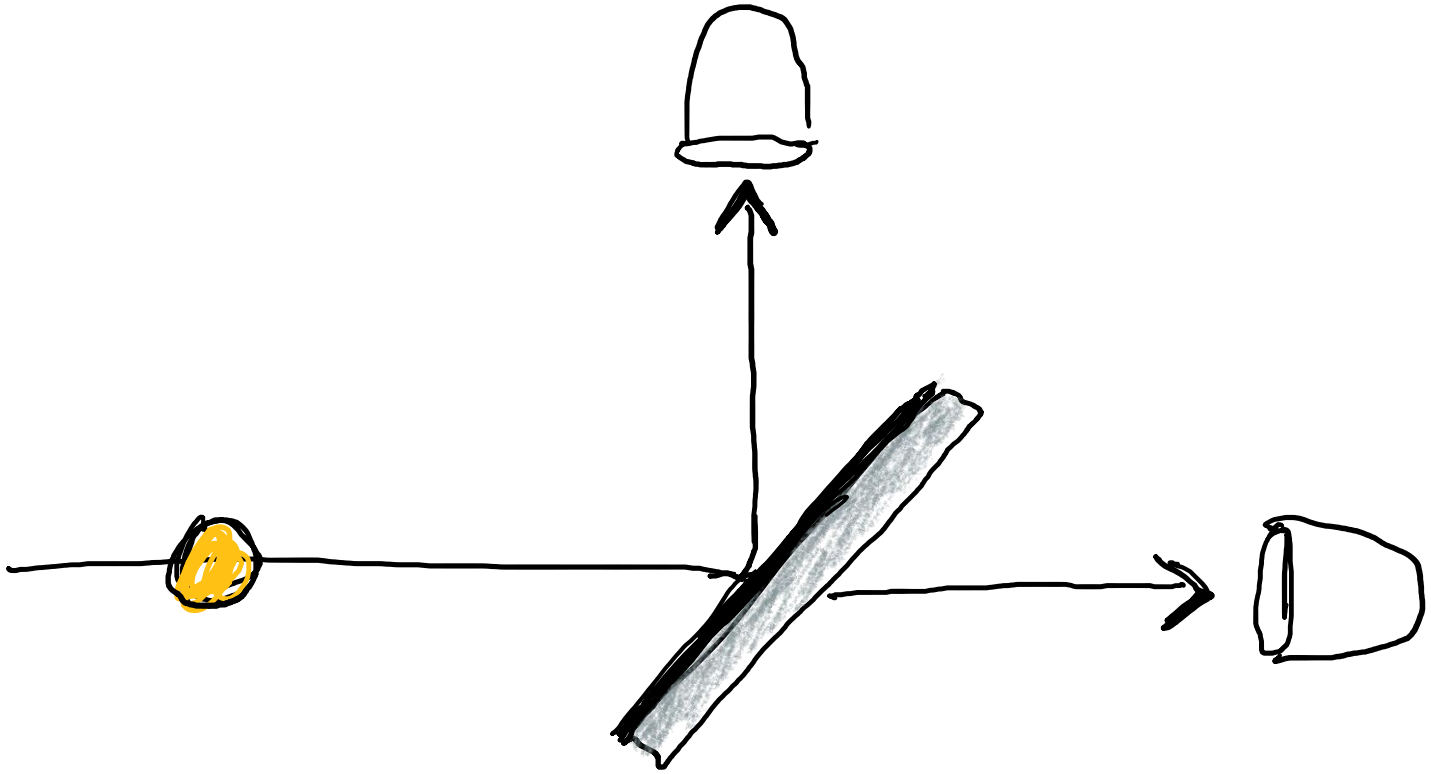


…Nature ignores additivity axiom

Whenever an event can occur in several mutually exclusive ways, the probability for the event is the sum of the probabilities for each way considered separately.



Quantum randomness seems to be different



The story of worry

MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

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

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

(Received March 25, 1935)

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

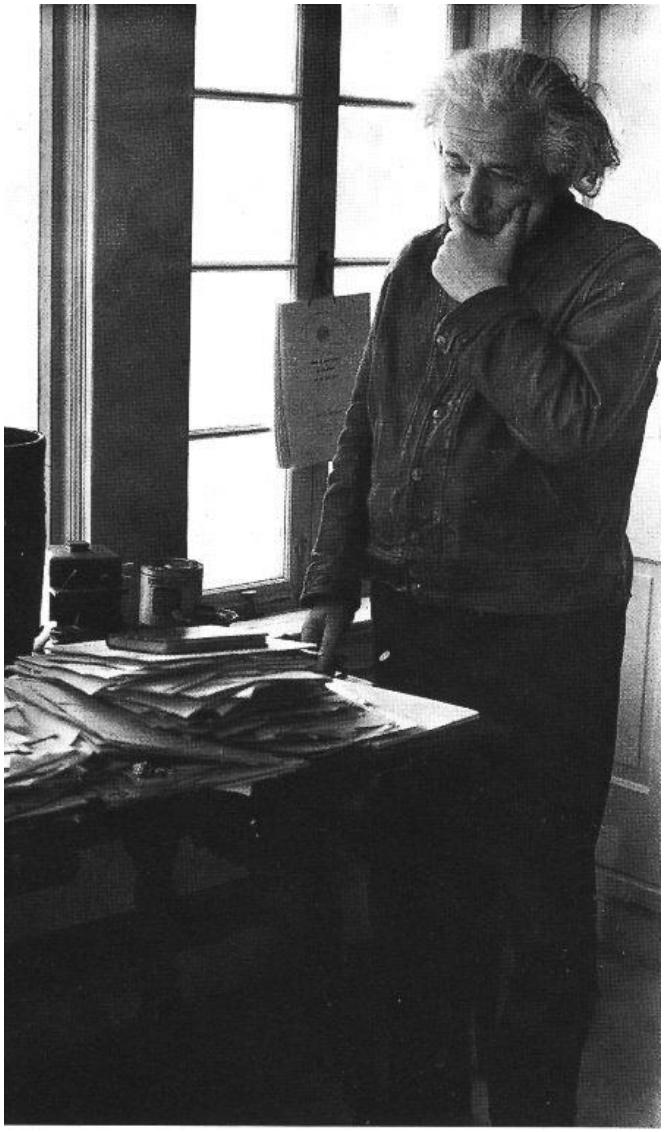
1.

ANY serious consideration of a physical theory must take into account the distinction between the objective reality, which is independent of any theory, and the physical concepts with which the theory operates. These concepts are intended to correspond with the objective reality, and by means of these concepts we picture this reality to ourselves.

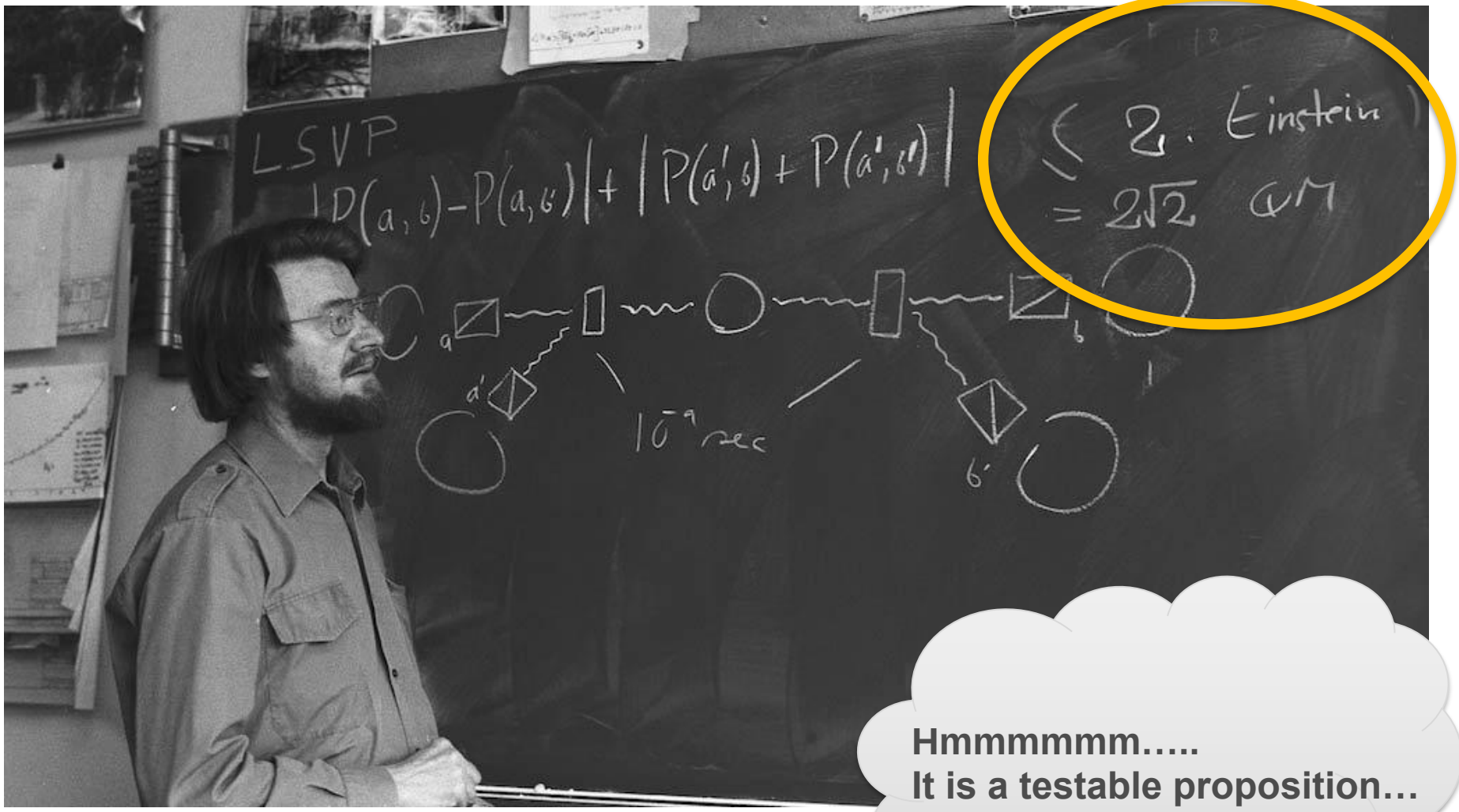
In attempting to judge the success of a physical theory, we may ask ourselves two questions: (1) "Is the theory correct?" and (2) "Is the description given by the theory complete?" It is only in the case in which positive answers may be given to both of these questions, that the concepts of the theory may be said to be satisfactory. The correctness of the theory is judged by the degree of agreement between the conclusions of the theory and human experience. This experience, which alone enables us to make inferences about reality, in physics takes the form of experiment and measurement. It is the second question that we wish to consider here, as applied to quantum mechanics.

Whatever the meaning assigned to the term *complete*, the following requirement for a complete theory seems to be a necessary one: *every element of the physical reality must have a counterpart in the physical theory*. We shall call this the condition of completeness. The second question is thus easily answered, as soon as we are able to decide what are the elements of the physical reality.

The elements of the physical reality cannot be determined by *a priori* philosophical considerations, but must be found by an appeal to results of experiments and measurements. A comprehensive definition of reality is, however, unnecessary for our purpose. We shall be satisfied with the following criterion, which we regard as reasonable. *If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity.* It seems to us that this criterion, while far from exhausting all possible ways of recognizing a physical reality, at least provides us with one

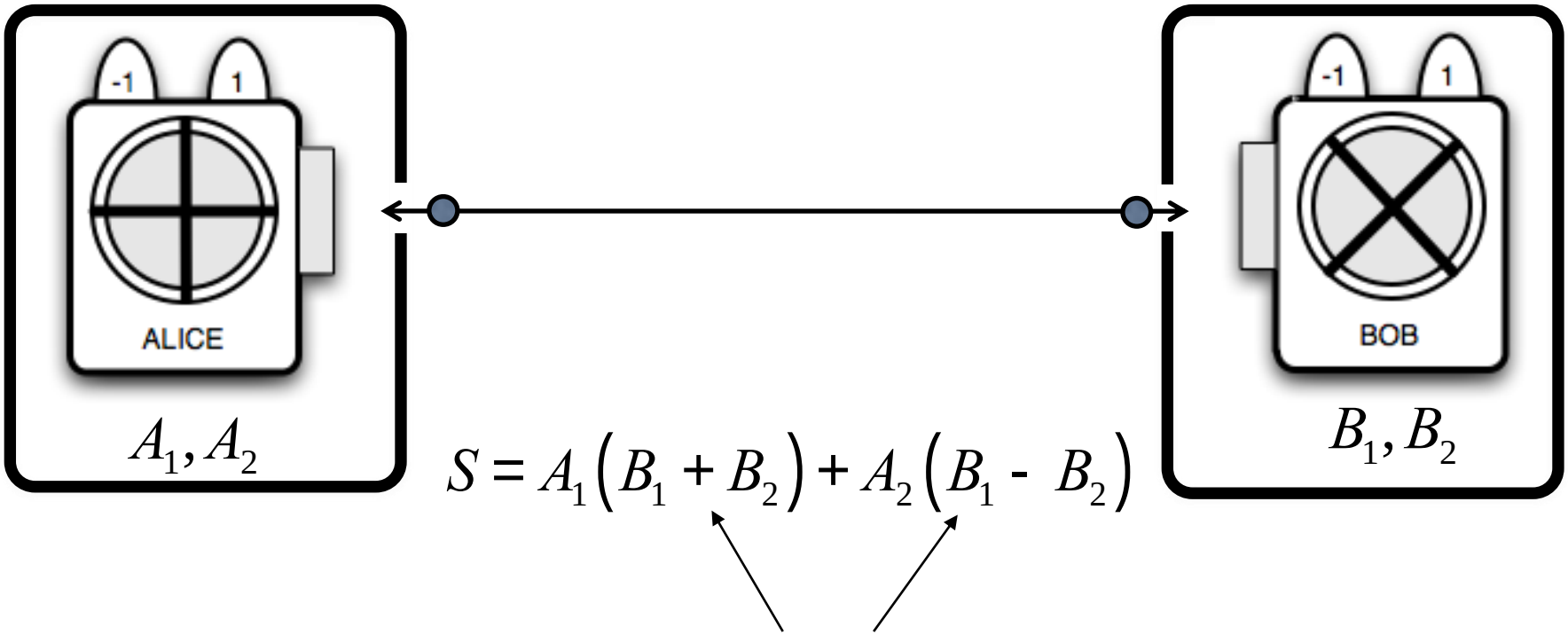


Enter John Bell



year 1964

Bell's inequalities…



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

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

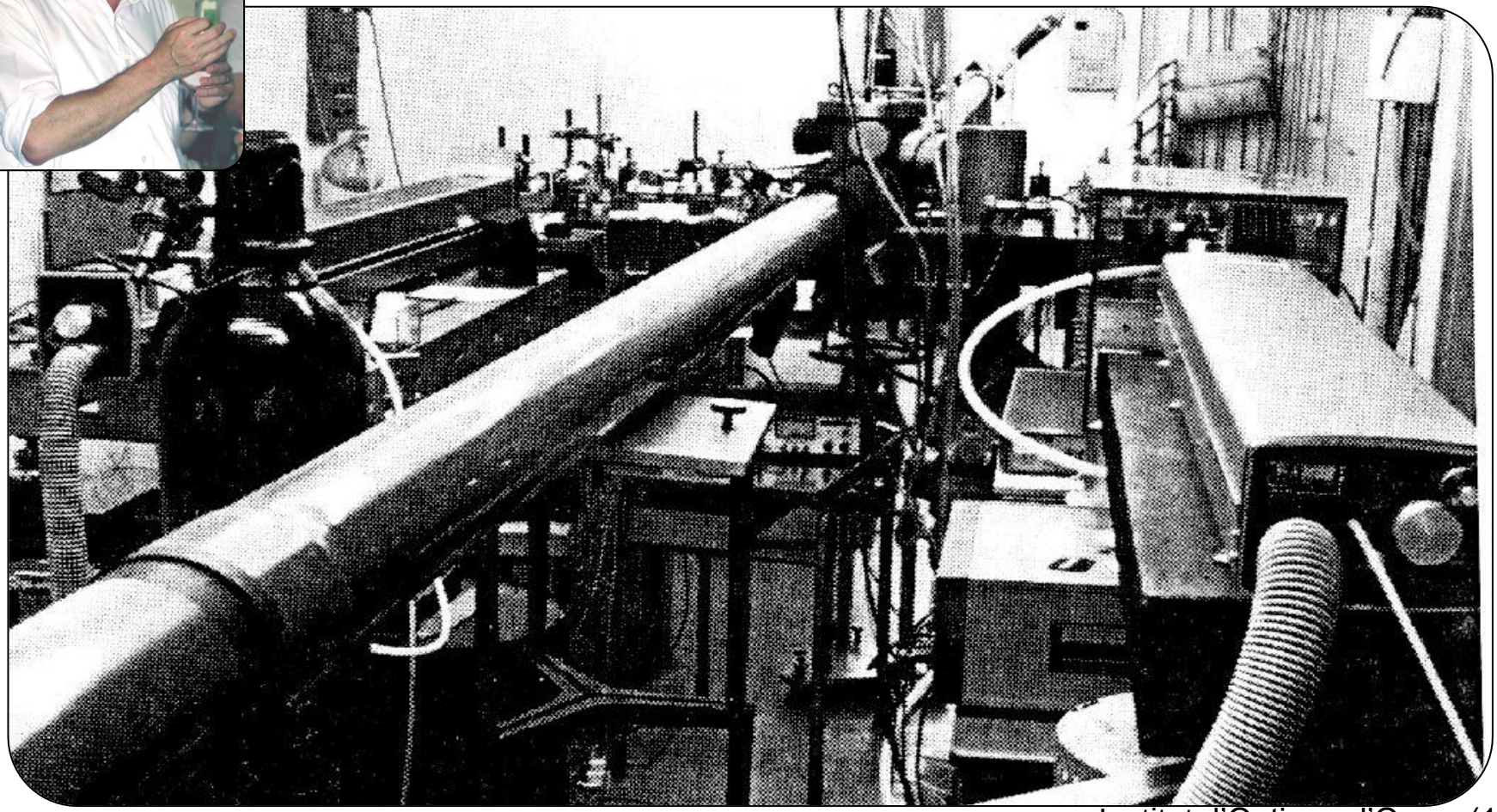
John Clauser

Berkeley (1972**)**

Alain Aspect and his quantum magic

$S > 2$

Et voilà!

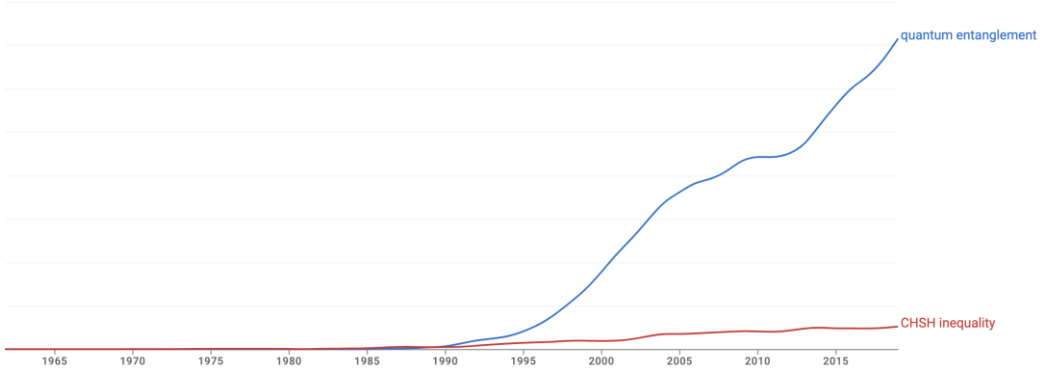


Institut d'Optique d'Orsay (1982)

Fusion

1935

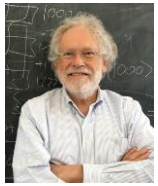
1972



curiosity

1964

1982



1918

Gilbert Vernam

~ 1970

James Ellis

~ 1980

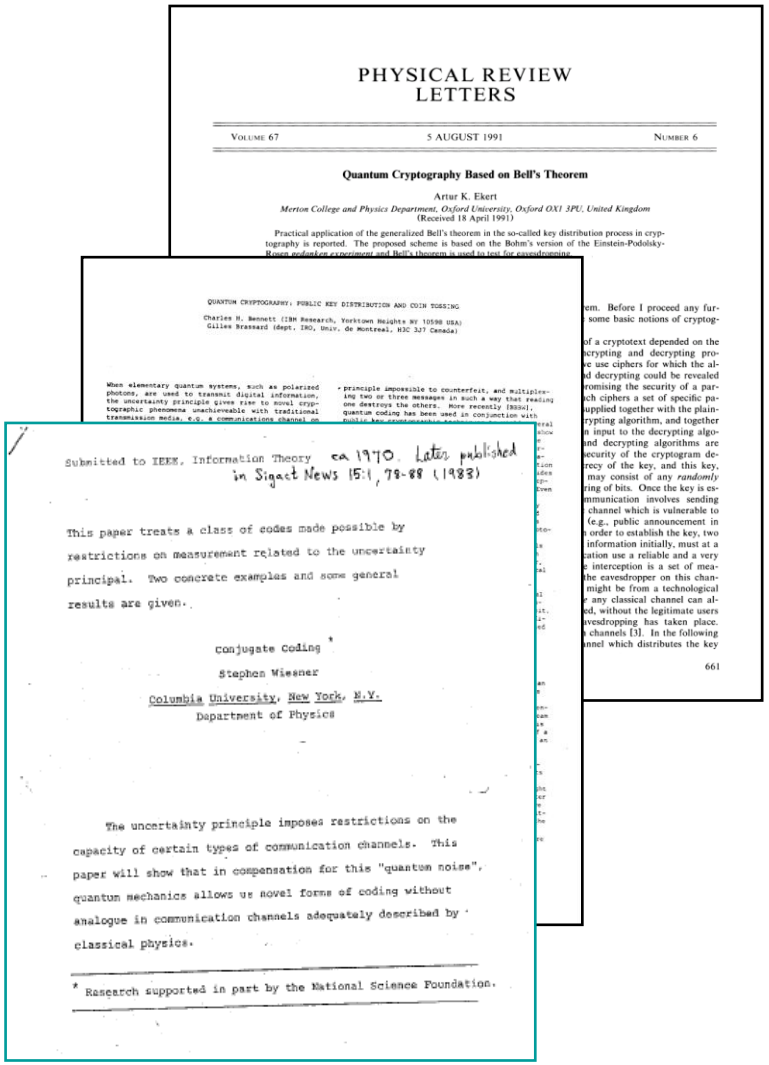
Stephen Wiesner

E91

BB84

security

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-

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.

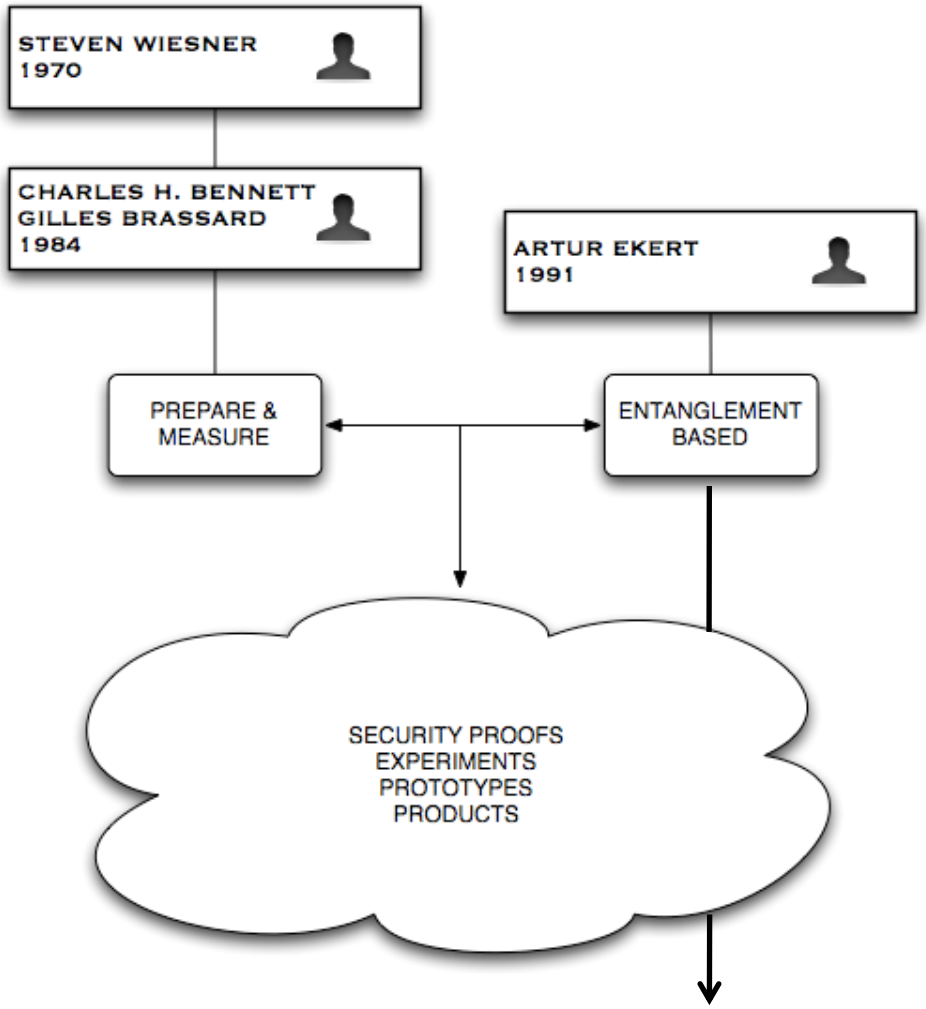
Conjugate Coding *

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

The story of worry

MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

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

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

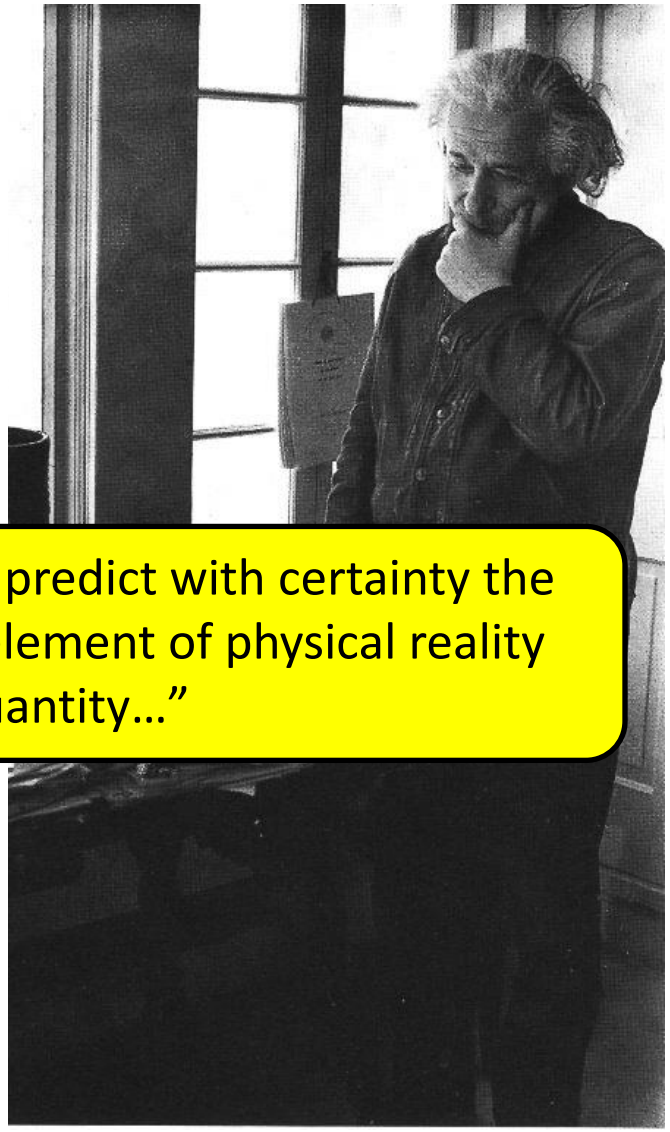
(Received March 25, 1935)

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

1.

ANY serious consideration of a physical theory must take into account the distinction between the objective reality, which is independent of any theory, and the physical

Whatever the meaning assigned to the term *complete*, the following requirement for a complete theory seems to be a necessary one: *every element of the physical reality must have a counterpart in the physical theory.* We shall call this the



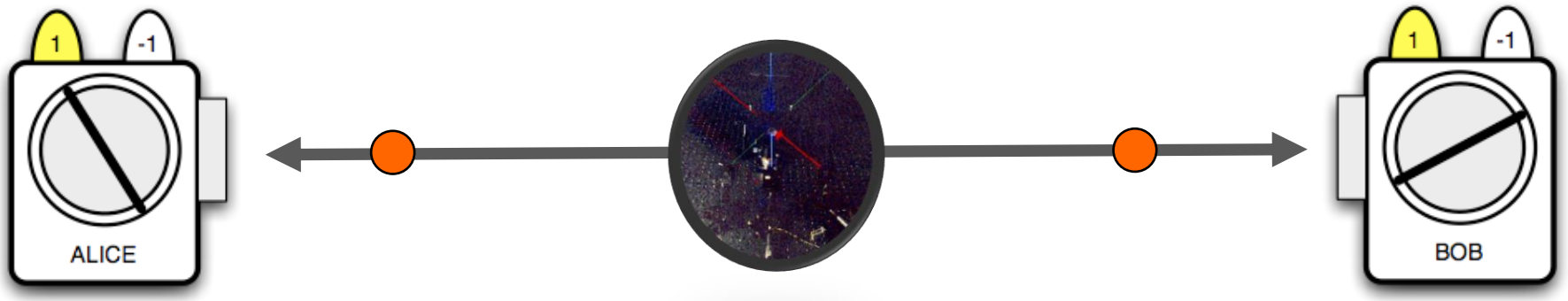
"…If without any way disturbing a system, we can predict with certainty the value of a physical quantity then there exists an element of physical reality corresponding to this physical quantity…"

It is only in the case in which positive answers may be given to both of these questions, that the concepts of the theory may be said to be satisfactory. The correctness of the theory is judged by the degree of agreement between the conclusions of the theory and human experience. This experience, which alone enables us to make inferences about reality, in physics takes the form of experiment and measurement. It is the second question that we wish to consider here, as applied to quantum mechanics.

comprehensive definition of reality is, however, unnecessary for our purpose. We shall be satisfied with the following criterion, which we regard as reasonable. *If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity.* It seems to us that this criterion, while far from exhausting all possible ways of recognizing a physical reality, at least provides us with one

DEFINITION OF EAVESDROPPING

Less reality more security



PHOTONS DO NOT CARRY PREDETERMINED VALUES OF POLARIZATIONS

IF THE VALUES DID NOT EXIST PRIOR TO MEASUREMENTS THEY WERE NOT AVAILABLE TO ANYBODY INCLUDING EAVESDROPPERS

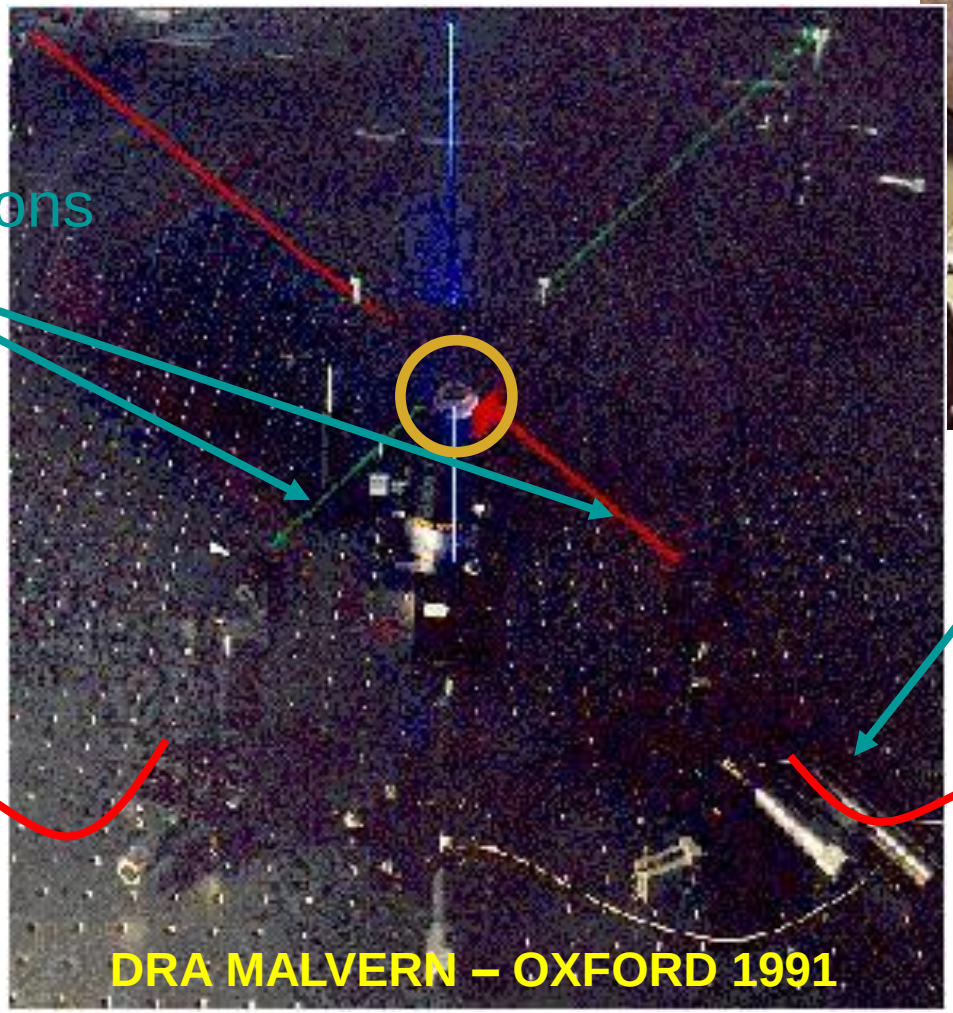
TESTING FOR THE VIOLATION OF BELL'S INEQUALITIES = **TESTING FOR EAVESDROPPING**

A. Ekert 1991

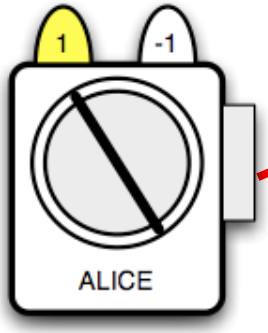
And all this can be demonstrated…

Parametric down conversion

Entangled photons

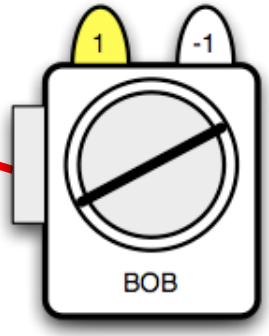


Optical fibers



Polarizing filters
& photodetectors

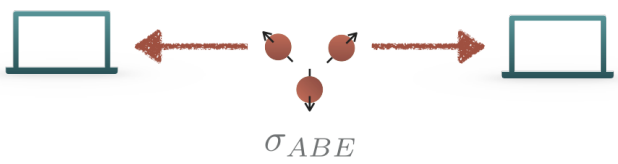
DRA MALVERN – OXFORD 1991



Polarizing filters
& photodetectors

You need some mathematical gymnastics

Eve uses the same strategy in each round, independently of all other rounds

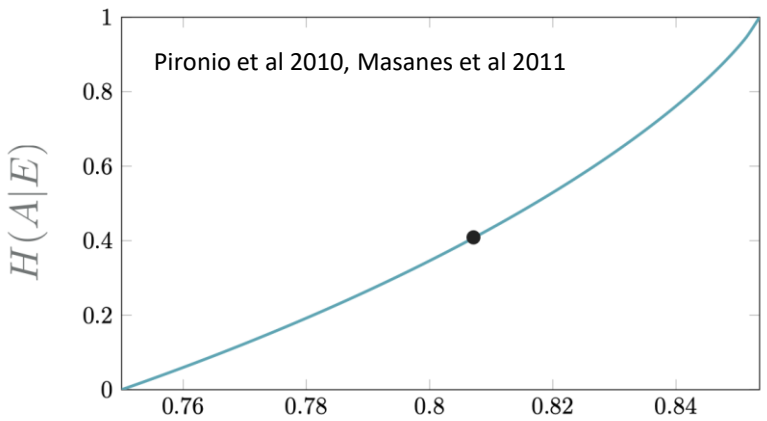


$$S$$

$$H_{\min}^{\varepsilon}(\mathbf{A}|\mathbf{E})_{\rho} \geq nH(A|E)_{\sigma} - c_{\varepsilon}\sqrt{n}$$

Extractors

Secret key



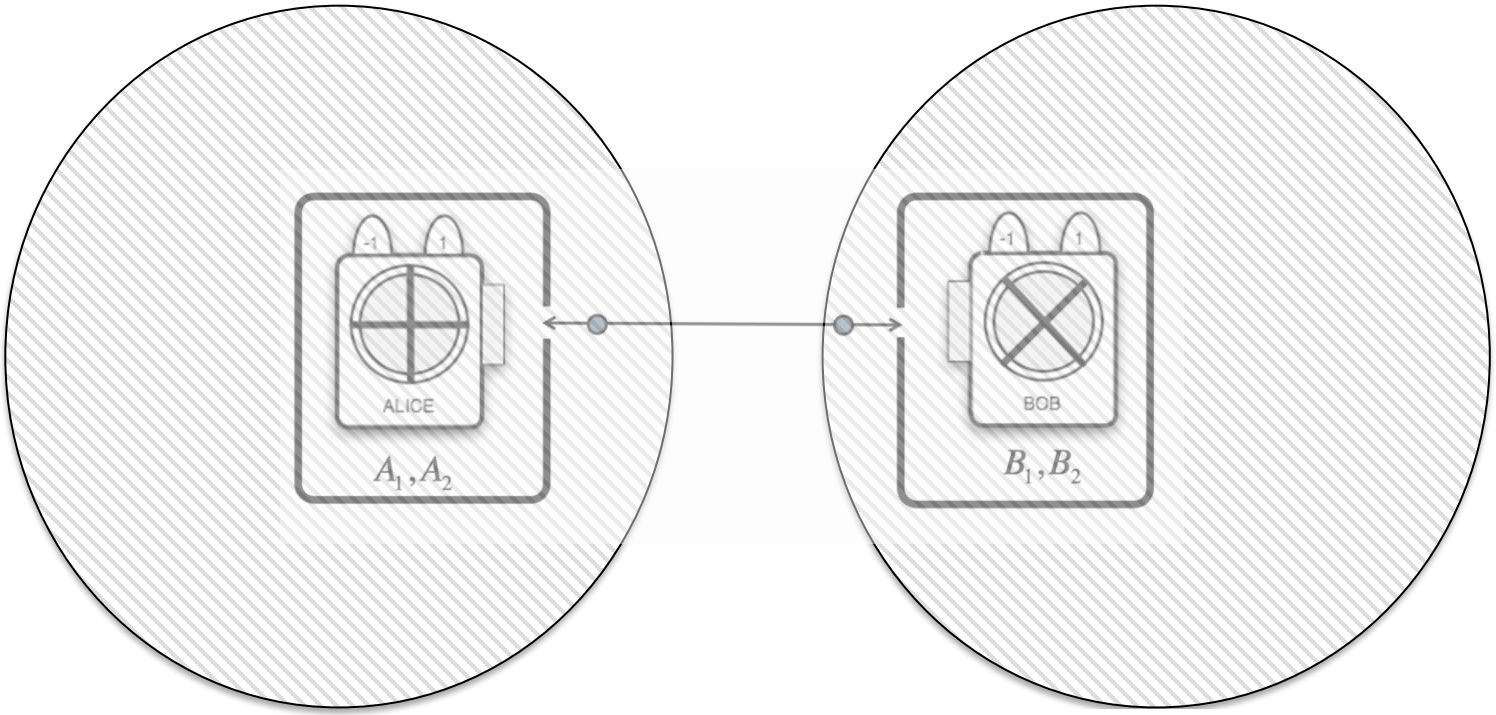
$$\omega = (S+4)/8$$

Quantum Asymptotic Equipartition Property
M. Tomamichel et al (2009) IDD CASE

Eve distributes the key!

(Maximal) violation of Bell's inequalities is rigid

$$|S| = |A_1B_1| + |A_1B_2| + |A_2B_1| - |A_2B_2| = 2\sqrt{2}$$

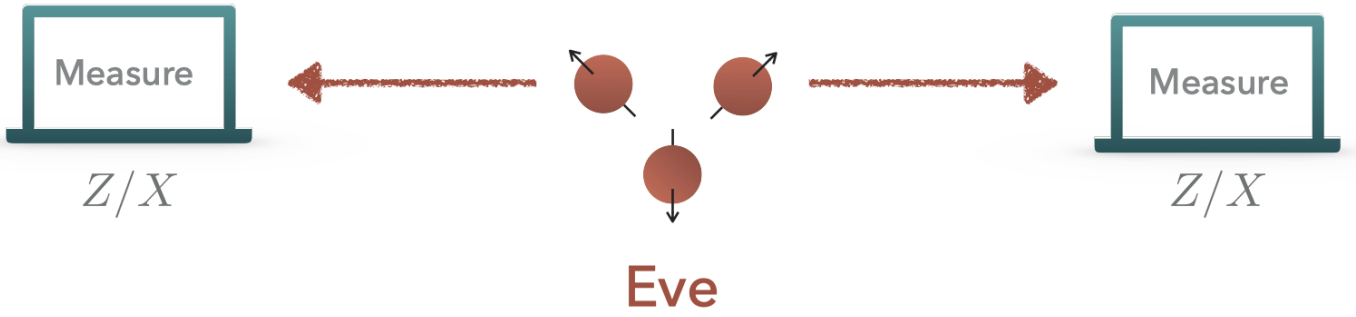


A_1, A_2

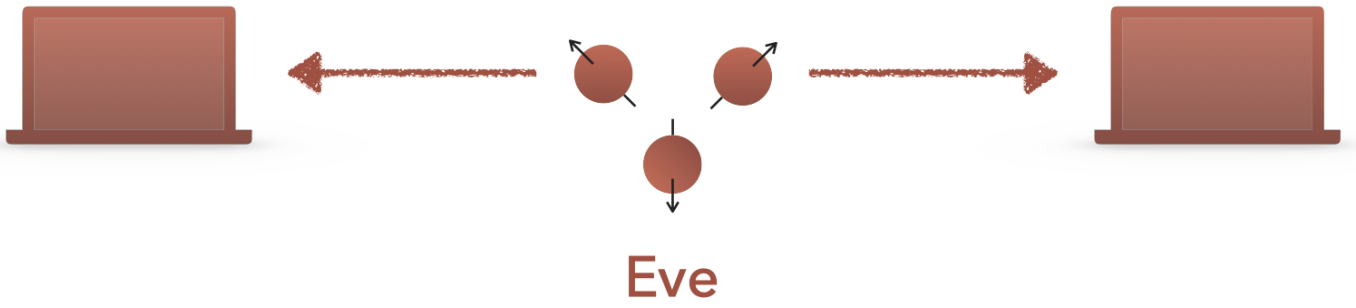
B_1, B_2

At the mercy of Eve

Ekert 91

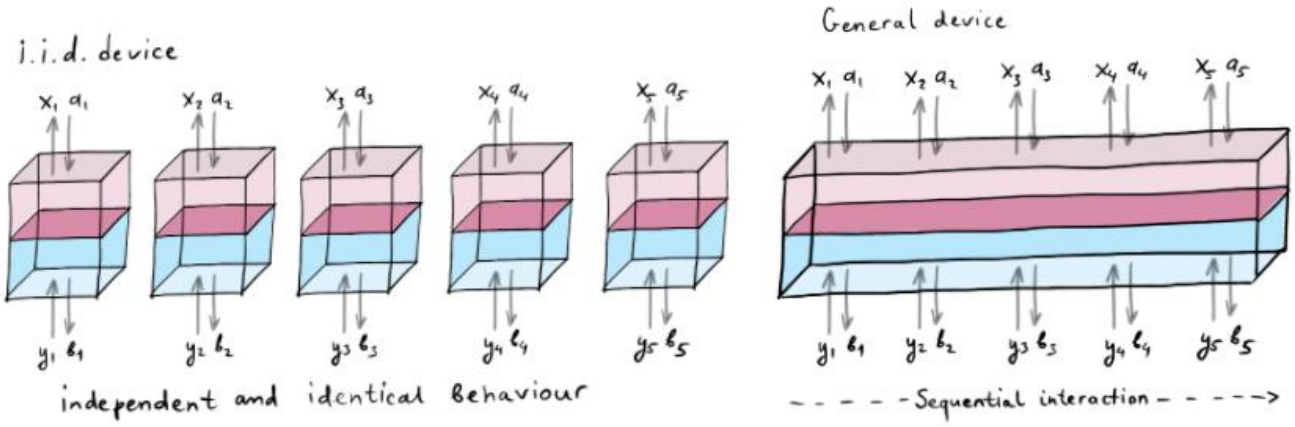


Device-independent

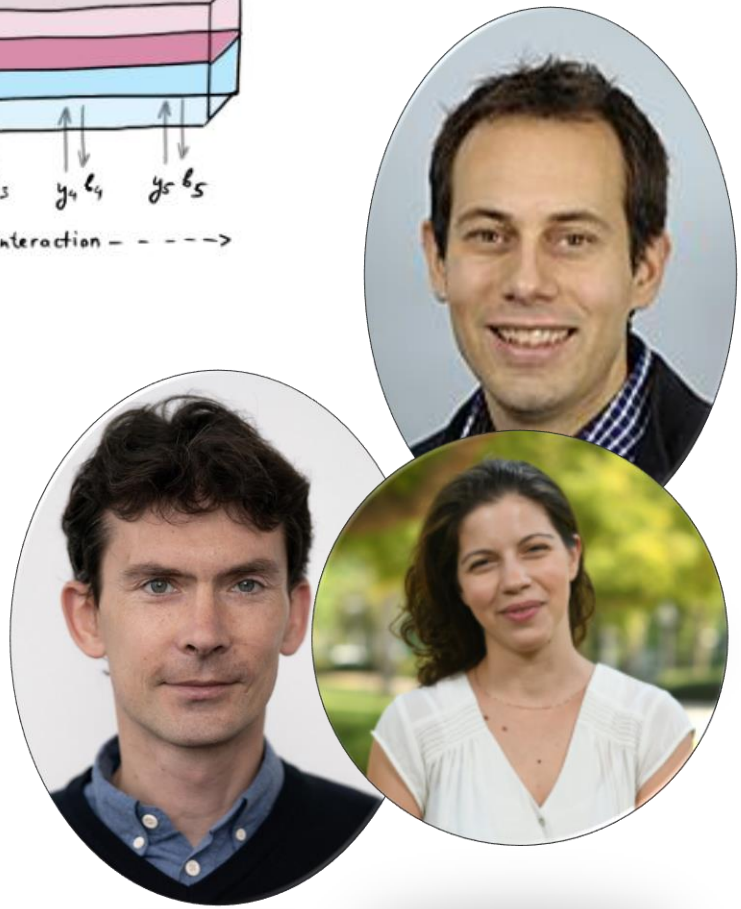


Courtesy Rotem Arnon-Friedman

EAT your key to make it secure



Entropy Accumulation Theorem (EAT) allows us to reduce arbitrary strategies to i.i.d. strategies and enables simple device-independent security proofs.



Rotem Arnon-Friedman, Renato Renner and Thomas Vidick. Simple and tight device-independent security proofs. *SIAM J. Comput.* **48**, 181 (2019). doi: 10.1137/18M1174726

And this is for real…

95884 secret bits in 8 hours

Article

Experimental quantum key distribution certified by Bell's theorem

https://doi.org/10.1038/s41586-022-04941-5
Received: 29 September 2021
Accepted: 7 June 2022
Publis
Ch

D. P. Nadlinger[1✉], P. Drmota[1], B. C. Nichol[1], G. Araneda[1], D. Main[1], R. Srinivas[1], D. M. Lucas[1], C. J. Ballance[1✉], K. Ivanov[2], E. Y.-Z. Tan[3], P. Sekatski[4], R. L. Urbanke[2], R. Renner[3], N. Sangouard[5✉] & J.-D. Bancal[5✉]

It is because of quantum crypto we still keep testing Bell inequalities…

PHYSICAL REVIEW LETTERS

Highlights Recent Accepted Collections Authors Referees Search Press About E

Featured in Physics | Editors' Suggestion

Access by Uni

Toward a Photonic Demonstration of Device-Independent Quantum Key Distribution

Wen-Zhao Liu, Yu-Zhe Zhang, Yi-Zheng Zhen, Ming
Jian-Wei Pan

Phys. Rev. Lett. **129**, 050502 – Published 27 July 2(

Physics See Research News: Hiding Secrets Using Qua

Article

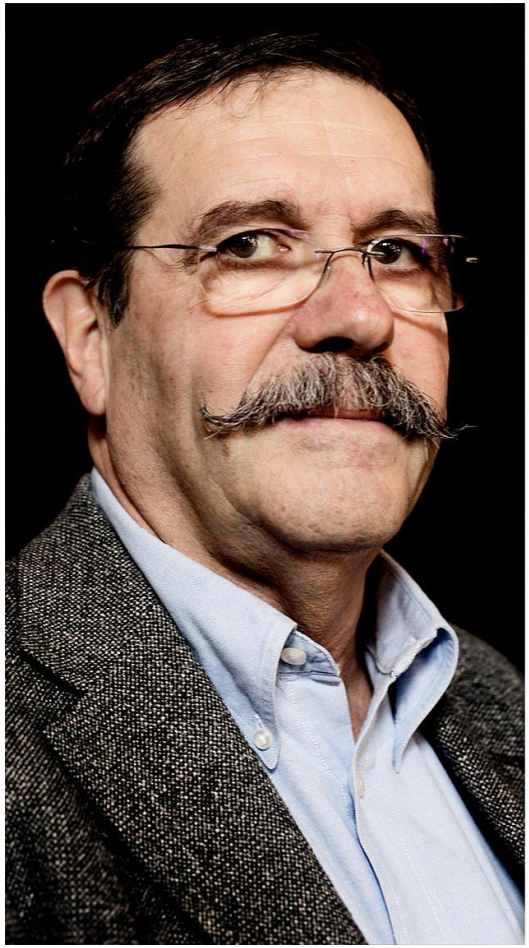
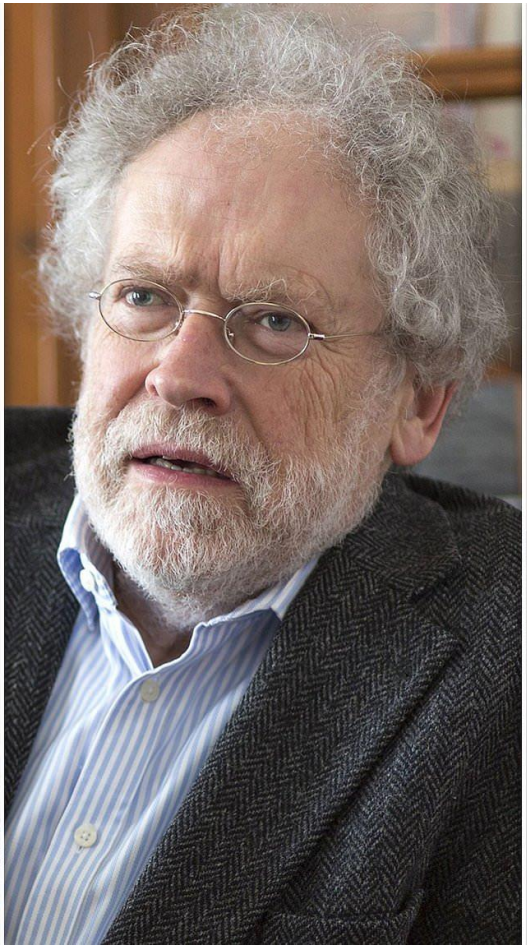
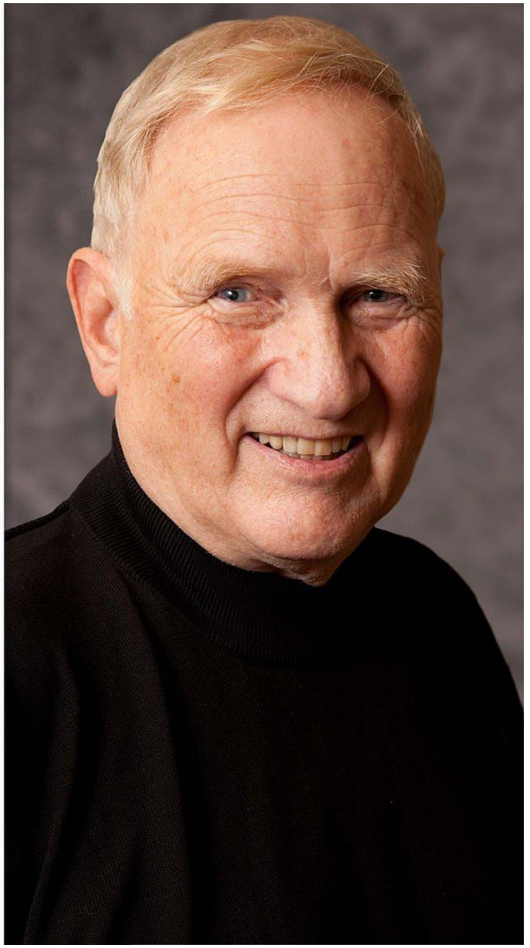
A device-independent quantum key distribution system for distant users

https://doi.org/10.1038/s41586-022-04891-y
Received: 8 October 2021
Accepted: 20 May 2022
Published online: 27 July 2022
Open access
Check for updates

Wei Zhang[1,2,9], Tim van Leent[1,2,9], Kai Redeker[1,2,9], Robert Garthoff[1,2,9], René Schwonnek[3,4], Florian Fertig[1,2], Sebastian Eppelt[1,2], Wenjamin Rosenfeld[1,2], Valerio Scarani[5,6], Charles C.-W. Lim[4,5,8✉] & Harald Weinfurter[1,2,7✉]

Device-independent quantum key distribution (DIQKD) enables the generation of secret keys over an untrusted channel using uncharacterized and potentially untrusted devices[1–9]. The proper and secure functioning of the devices can be certified by a statistical test using a Bell inequality[10–12]. This test originates from the foundations of quantum physics and also ensures robustness against implementation

Nobel 2022

End of worries?

You need perfect randomness, right ?

Einstein again - connections to relativity

New Journal of Physics
The open access journal at the forefront of physics

PAPER • OPEN ACCESS

Quantum principle of relativity

Andrzej Dragan[1,2] and Artur Ekert[2,3]

Published 24 March 2020 • © 2020 The Author(s). Published by IOP Publishing Ltd on behalf of the Institute of Physics and Deutsche Physikalische Gesellschaft
New Journal of Physics, Volume 22, March 2020
Citation Andrzej Dragan and Artur Ekert 2020 *New J. Phys.* **22** 033038
DOI 10.1088/1367-2630/ab76f7

Article PDF Article ePub

Classical and Quantum Gravity

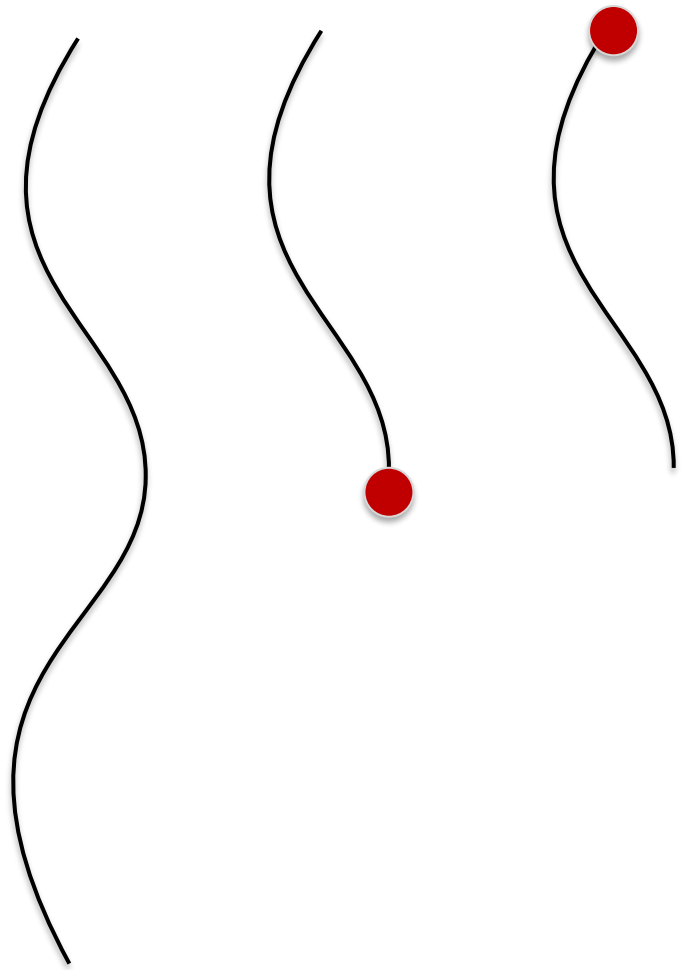
PAPER • OPEN ACCESS

Relativity of superluminal observers in 1+3 spacetime

Andrzej Dragan[6,1,2], Kacper Dębski[1], Szymon Charzyński[3], Krzysztof Turzyński[1] and Artur Ekert[2,4,5]

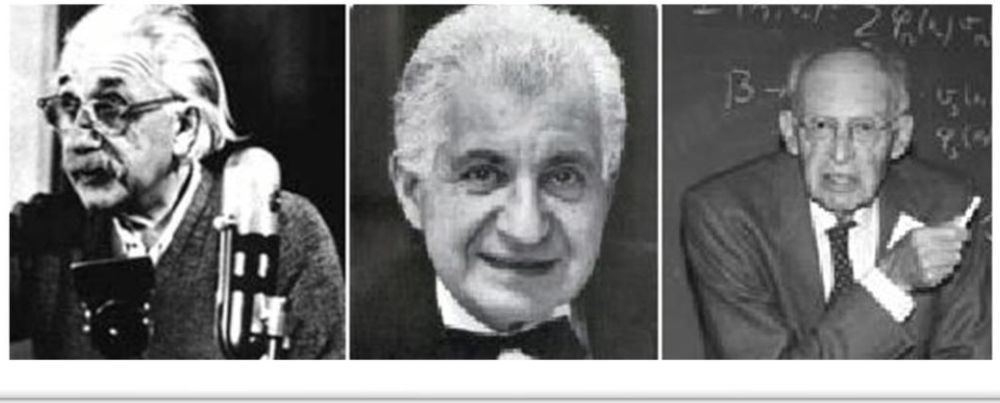
Published 30 December 2022 • © 2022 The Author(s). Published by IOP Publishing Ltd
Classical and Quantum Gravity, Volume 40, Number 2
Citation Andrzej Dragan *et al* 2023 *Class. Quantum Grav.* **40** 025013
DOI 10.1088/1361-6382/acad60

Article PDF



Random event, their past and their future

Many open questions

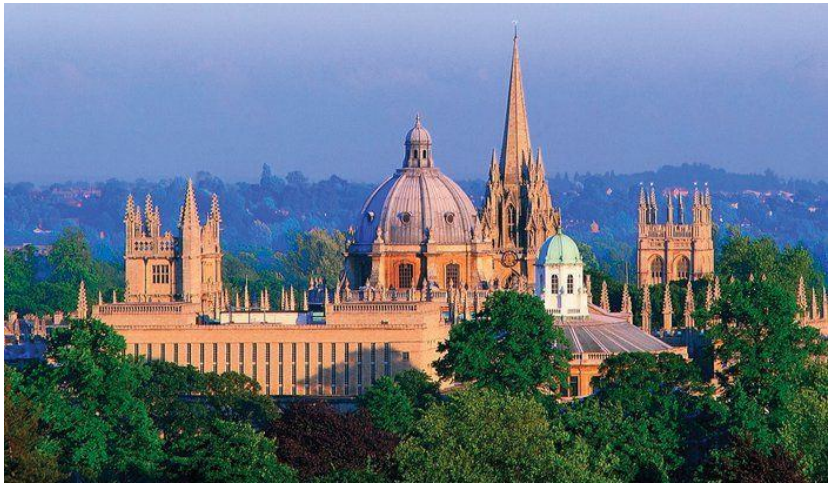


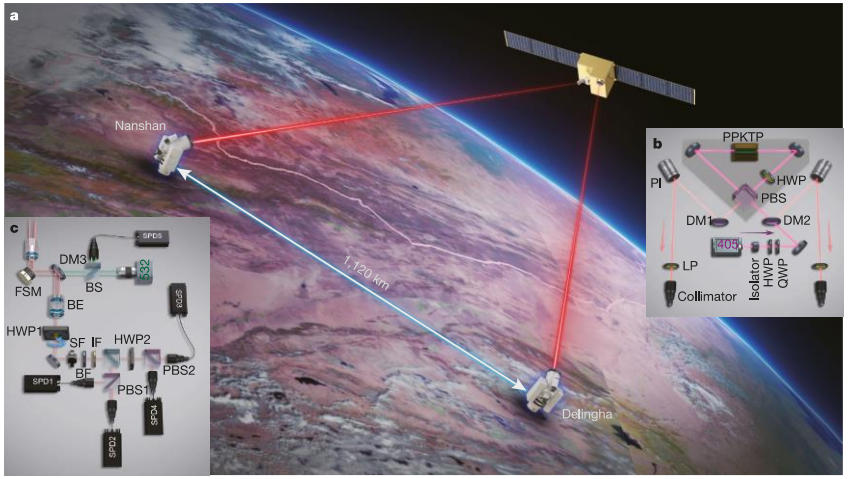
EPR VISION OF REALITY IS TOO SIMPLISTIC

SECURITY AND RANDOMNESS IN THE MULTIVERSE

In the superdeterministic world the notion of privacy or security makes no sense…

The sky's the limit!





From Oxford in 1991…

…to China in 2019

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.

PACS numbers: 03.65.Bz, 42.80.Sa, 89.70.+c

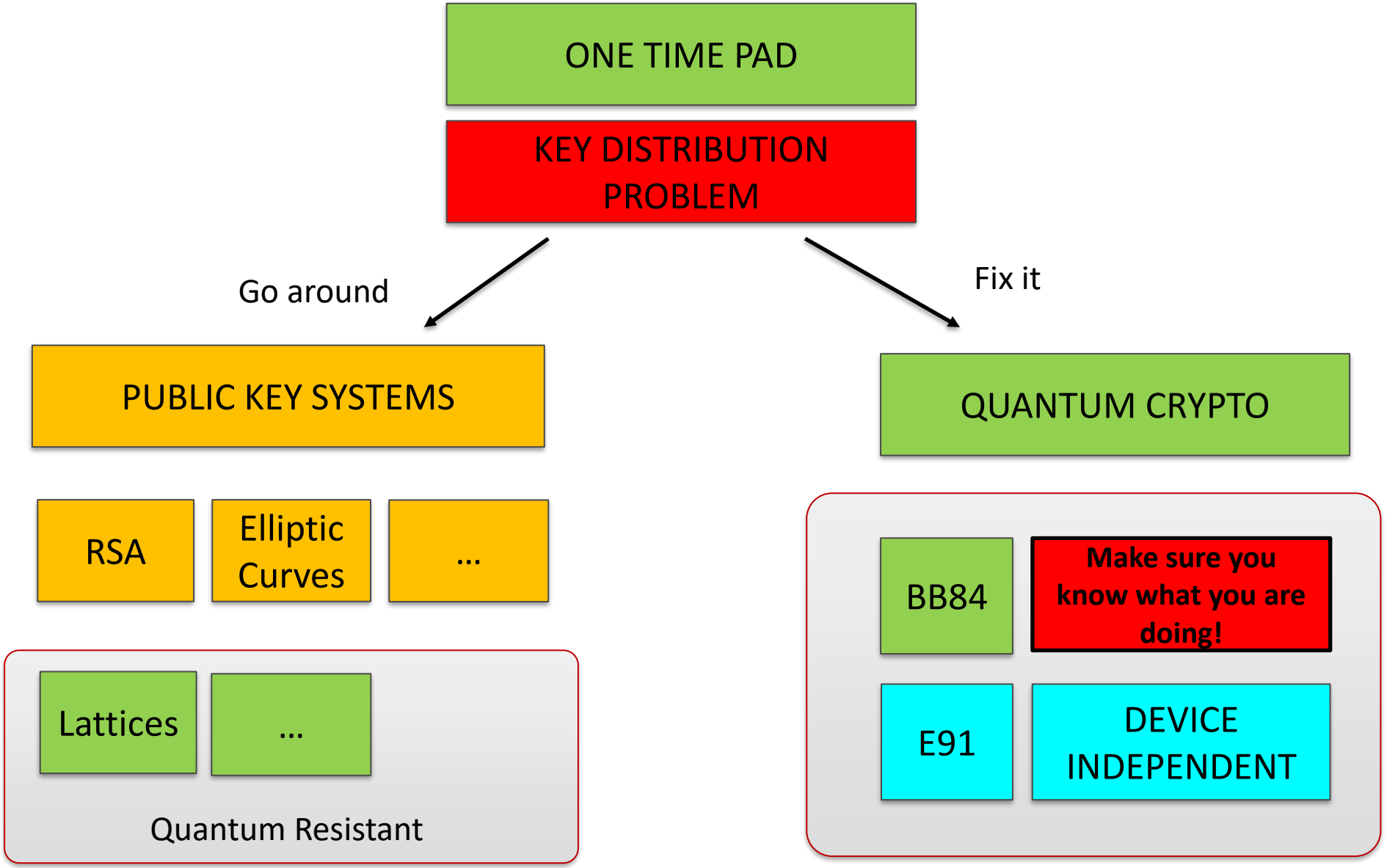
Article

Entanglement-based secure quantum cryptography over 1,120 kilometres

https://doi.org/10.1038/s41586-020-2401-y
Received: 15 July 2019
Accepted: 13 May 2020
Published online: 15 June 2020
Check for updates

Juan Yin[1,2,3], Yu-Huai Li[1,2,3], Sheng-Kai Liao[1,2,3], Meng Yang[1,2,3], Yuan Cao[1,2,3], Liang Zhang[2,3,4], Ji-Gang Ren[1,2,3], Wen-Qi Cai[1,2,3], Wei-Yue Liu[1,2,3], Shuang-Lin Li[1,2,3], Rong Shu[2,3,4], Yong-Mei Huang[5], Lei Deng[6], Li Li[1,2,3], Qiang Zhang[1,2,3], Nai-Le Liu[1,2,3], Yu-Ao Chen[1,2,3], Chao-Yang Lu[1,2,3], Xiang-Bin Wang[2], Feihu Xu[1,2,3], Jian-Yu Wang[2,3,4], Cheng-Zhi Peng[1,2,3]✉, Artur K. Ekert[7,8] & Jian-Wei Pan[1,2,3]✉

Quest for perfect secrecy



Post-quantum: there is still room for improvement

Report on the Security of LWE:
Improved Dual Lattice Attack

The Center of Encryption and Information Security – MATZOV*†
IDF

Abstract

Many of the leading post-quantum key exchange and signature schemes rely on the conjectured hardness of the Learning With Errors (LWE) and Learning With Rounding (LWR) problems and their algebraic variants, including 3 of the 6 finalists in NIST's PQC process. The best known cryptanalysis techniques against these problems are primal and dual lattice attacks, where dual attacks are generally considered less practical.

In this report, we present several algorithmic improvements to the dual lattice attack, which allow it to exceed the efficiency of primal attacks. In the improved attack, we enumerate over more coordinates of the secret and use an improved distinguisher based on FFT. In addition, we incorporate improvements to the estimates of the cost of performing a lattice sieve in the RAM model, reducing the gate count of random product
Comb
Saber an
olds defi

SOLILOQUY: A CAUTIONARY TALE

Peter Campbell, Michael Groves and Dan Shepherd
CESG, Cheltenham, UK

1. Introduction

The Soliloquy primitive, first proposed by the third author in 2007, based on cyclic lattices. It has very good efficiency properties, both terms of public key size and the speed of encryption and decryption. The are straightforward techniques for turning Soliloquy into a key exchan or other public-key protocols. Despite these properties, we abandoned search on Soliloquy after developing (2010 to 2013) a reasonably efficie quantum attack on the primitive. A similar quantum algorithm has been