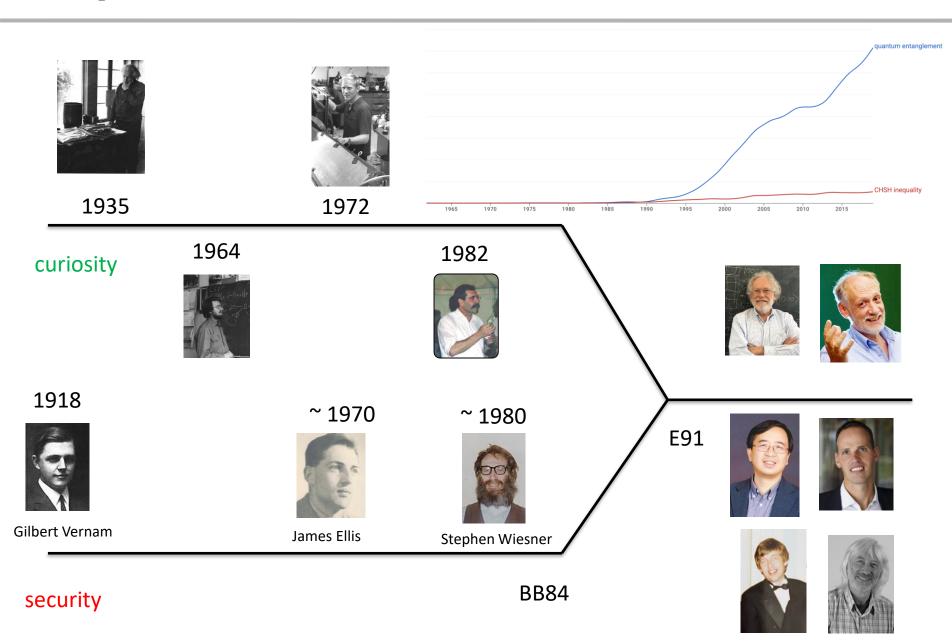
Bell inequalities

From curiosity to security

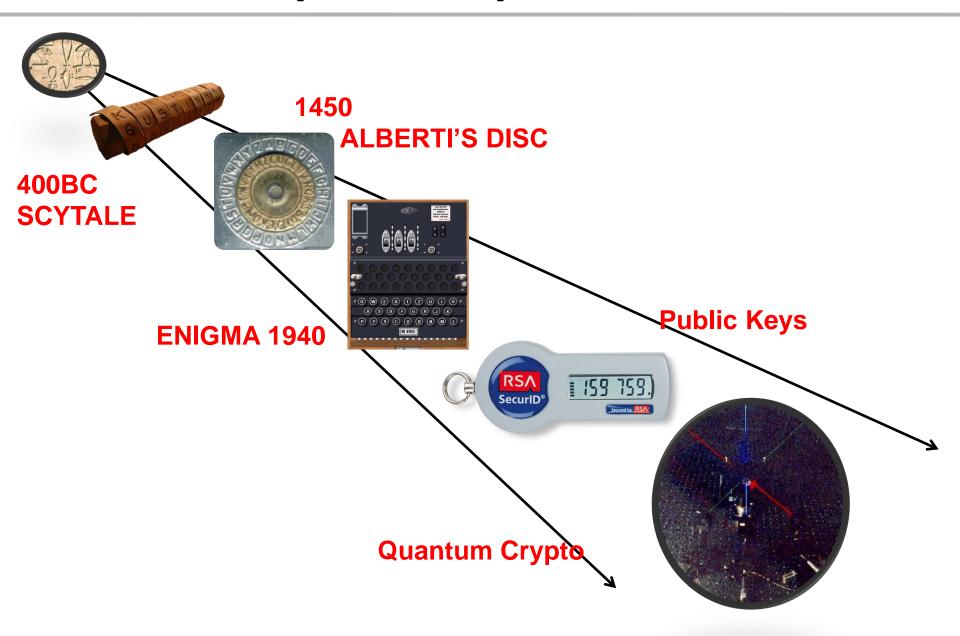


Artur Ekert

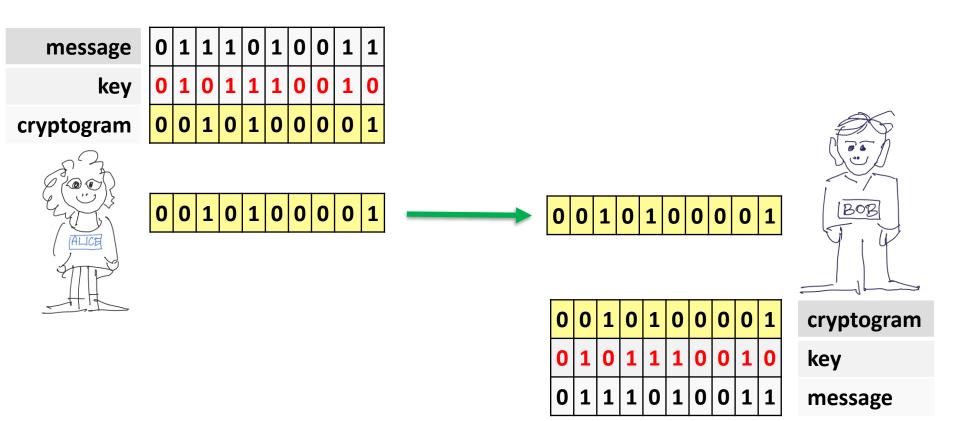
Spoiler – two narratives



Quest for a perfect cipher

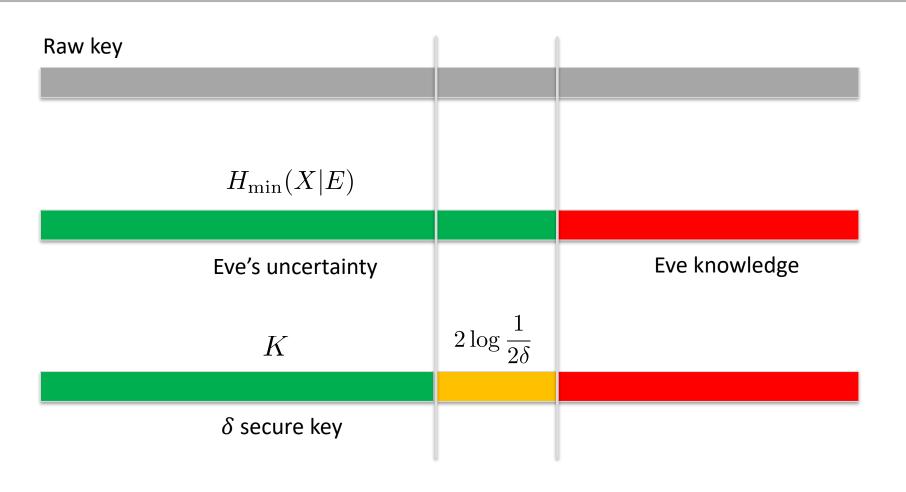


One-time pad



KEY DISTRIBUTION PROBLEM

Privacy amplification



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

But how much does Eve know?

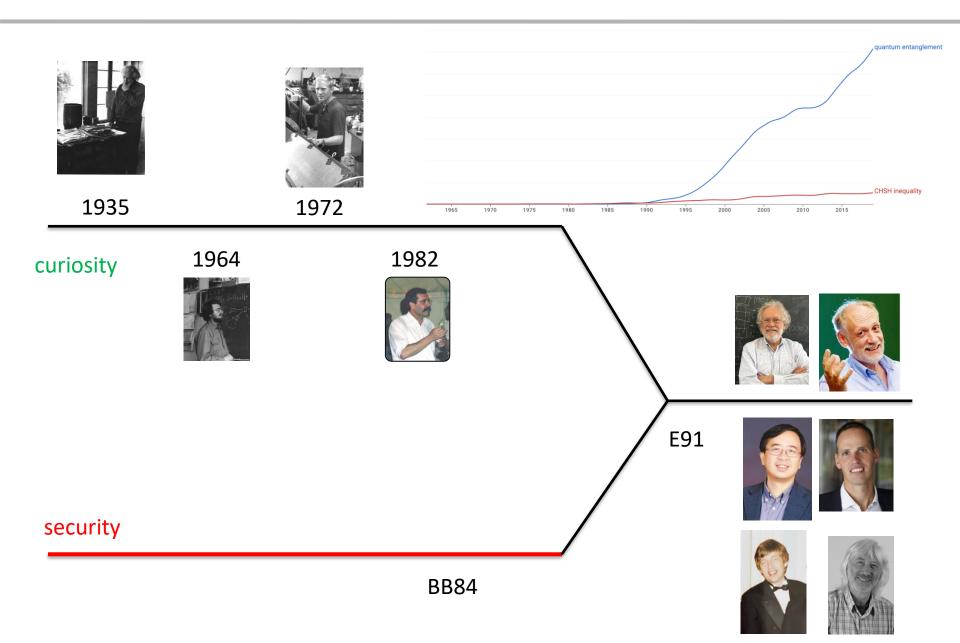






$$H_{\min}(X|E)$$

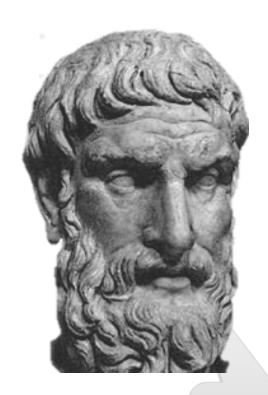
The other narrative



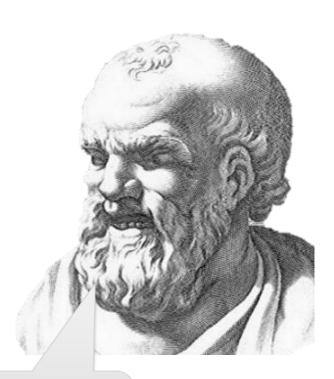
Randomness – objective or subjective?

EPICURUS (300 BC)

DEMOCRITUS (400 BC)



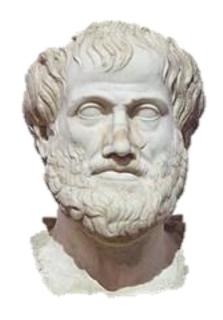
atoms swerve at random along their paths



atoms follow predetermined paths

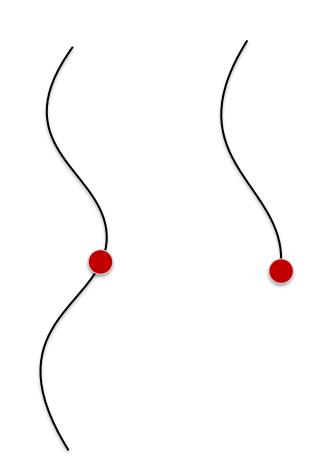
SUBJECTIVE

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 Alex Liber.

265

dine eft , quòd surem fallet penter cedinem-Succellio autem geninata , ve bonorum bis punctorum accedit ex circuitibus , inuicem atis, videlicet eribus milibus fesceretis ichiun, cuia staditas el dintátum, ictus feilion mile oftingenti. In toridem enim poteft contingere, & non contingere. Et non fallit totus carentau, nili quia in vno potest gemi-mari, & bis , & ter. Har igitus cognicio est freundam consolturam, & proximierem ; & git , qubd in multis ciecuitibus pes incendit cima emicétiere.

-----CAPVT XII.

De trium Alearum ially.

T Ema punda fimilia frant, nife vno modo, ve in precedenti i sterque funt fex. Pun-da verò bina fimilia , & tertinu dispar func triginta : & vnunquodque continge tribus modis, crunt nonsginta. Pundta verò es riifex modin,ecent igitut cam incht viginti . &c circuitus ex ammitus ducenti fexdecim . &c qualitas in cerum octo, & penam fimplices, 5c varios terminatos pro exemplo. Simpliora, ergo fea gerninaci cuius puncti quin-que modis. Cum ergo fire puncta fea, cyunt modi trigima, fea ichum varietates. Proponitur et variatio triplex, ve fint nonaginea. Sed viginti qui funt oranes diffimiles , cum atientu modis fex, erunt ernoum,& vigin-Puncha ergo fimilia funt para centefima oftens requalitaris, gereinata queen cum tria tushus Aleis ad vaguem, eft decima octait fit, ad centum ofto fexta pats eft , quare emparatus ad illum, triplo frequencius con-

Exone eft acminorum les, dicemus sur de Esque eft geminorum les, dicemus, six ou ratione pignotis intra hoc. Das verò pan-da invegalia, vt venur , ac deo, fic diffin-guemus, queniam fi copulabinar venur fice tribus stodis, fi dan, totidem esant, ergo iam Quarmor autren modis allis contingie: At hi fex variantur finguli differentiis , erunt girur viginti quatsor, ve cam reliquis fex riginta. At triginta quinque ai triginta fex obcinem proportionem al centum, & odio equilitaria comparate ad doodecim engo fexareta ferne a fod non plane. Numeri un-tem interquales triplices, vt vna, duo, quaenor, teen mequates terptices, ve viriados, quescor, ad nemerum aqualitesis proportionem haber, quano in dunbus Aleis familia pracha ad vegueme. Singuli aucem numeri per le invus Ales proportionem habet, fabriripiam, cam engo uris fant Ales obtendeunt proportionem exqualitatis, ve ter discretis fradecim coniggranulos, fingula punda in ocetum, Sc. ofin interniareme, de in totalem non insecu. niantur, vt fit ratio hac ad voguem, vt vnian functi in dividus Aleis ad toesm circutesm in tribus ictibus, vel in dimidio ad aquali-

CAPVT XIIL

De Nameris compositis, tam ofque ad fex, quam vitra, & tam in duabus Aleis , quien in tribat.

IN daubos Aleis duodecim, & vrdecim con-fignt eadem rationes, qua bis , fee , atque fee, & quinque. Decen autem es bis quin-que, & fee , & quirnot , hoc autem variatur dapliciter, erit igitus tenum daodecima para circuitus , de fexta arqualitatis. Rocfus ex nonem & quinque & quamer,& fex, actribus, ve fit nona pars circuitus requalitatis da-plam nonz partis. Octo autem puncha funt ex primi none particoles satin patien non interesta de dis-bia quanto, tribas, & quinque, ao feta & dis-bia. Tortum quinque foptima firmé circui-na para, & das feptima aqualisatis. Septim autem, ex fet, & vro quinque, ac disolus quantos, ac tribus. Omnià igilut punda fina-fet, territa para sequilitatis , & festa circuiem. At fex vt ofto, & quinque, vt nouem, questor, vt docum, tria vt vnáctim, & dno;

Sed in Ludo fritilli vodecim puncha, aditerre decet , quia van Alea potest oftensi ecant igitus duceum punchecum inclus duo-decim , & ita bes equalitatis , & triens ciecuirtes. Tria sottem tredecim, quamor sucara quatocedecim, quinque quindecim, destant condination. At a toto circulta cuincana. Sex antem feudecim, & valde peopè mqua-

3 9 4 6 8 5 7 8 18. Ad Friti

Confentas fortis in stibus Aleis tum Prit. 18 r 115 133 7 33 8 36 9 37 to 36 6 15 10 8 13 11 9 12 15 10 11 17 11 38 12 16

Vlera hune numeram totidem quòt in force vt it. at.

form wt 15. a.s.

Visum parcham presents shabet 10d.
Dao punch shabers 11s.
In tribus satom Alcistoria puncha. Septem
forecast equalization in Ferdina, in force por
talban with, sleft constrain orbitals punch
forecast equalization in Ferdina, forces
formus. Quarter in Ferdina, forces
formus. Quarter in Ferdina, forces
formus. Quarter in Ferdina, forces
formus puncha
forces, and qualitation years year
(dockness, typica; cutus. & dockless octure), in
force, and qualitatem. As in Fridinocemum,
& visging; for , idedi fectus purte equalitation
glius. Stat suttern in forte decent ment; dos
fection, de visual, in Fridinoi gipta the
& the forces
& (and forces), in Fridinoi gipta the
& (in faper , que baits certificant the
visite,

visite,

Girolamo Cardano

1501-1576

Cap. XXXVII. De Regula falf. 287

m. 1. pol. 1000 m. 1. pol. 1. quad. | 10000 p. 1. quad. m. 100 pol. differentia 10000. ft. 100. pol aqualis 400.

bes equantite 10000. f. 1. quadrato, abiina upantur (2005. p. 1. quantur 20. sep-ceommunia, habelis egoc. sepaña 100. pofitionibas. Igitur ere eft 48. 8. tanium ha-buie ih. id est debiti, & dos ceit refishum ad 100. fallete 51. igitur Francifem habaie 48. zareos debiti, fine vilo capitali vel peculio: & dos eius vxoris frit (2. aureorum, & feors operando persenires ad queftiones difficillmes, ac inextricabiles. Talis modietiam hac eft.

QVESTIO IL

Ego habeo aureos 12. plus Franciico,& enbes meorum est, 1161, aurei plus cabo Francifci, ponatur 1, res m. Francico, ego haboo ta. sureos m. 1. pefitione duc ad cubam partes, fiert 1. cubas m. & 1718-p 36. quadratis m. 432. rebus m. 1. cubo, hotum diferentia, eft 1161. igitur 1. bas m. p. 411. tebus p. 1161. aqui 1718. p. 16. quadratis m 1. cubo, mice m. 1. cubum & 1161. ex vtraque utre, fient 432, ses requales 56, quadr is p. 567, quaer a quadratum p. 15 1, p. qualia fa. rebus , igitur ers eft 14, & hoe h buit agrei quefei.

QYASTIO IIL

Et codem modo, fi dicam etjam fie, surei roci fanc 1 a. p. quam illi Francisci. Et quadestum meorum eft 118. p. cubo autro-tum Francisci, dabimus tem vnam m. Francisco, ego verò habeo ta. aureos m. 1.10, & quadrarum moreum erit 144. f. 1. quadrata fi. 14. rebus, & hoc aquale est m. 1. cubo p. 118. igitur 16, p. 1. quadra-to p. 1. cubo, aquatur 14. rebus, Et res erit 4. m. & tantum habet Franciscus debi-ti, ego verò aureos 8. peculij.

RIGVLA IL

Sociadam genis policionis faille, ell per tadicem m. Et dabo exemplum, in qua si-cat, diade a c. in dans pares; et quaram vates in etiquam decla, peodiciatur qua-aret qua maniettum et qua casa icu qua-tio ett impedibilis, se tamen operabimar, detidemes to per equalis , & fet eins engofficial produced as a specie of a property of a property of the produced as a property of the produced as a produced as a produced as a produced as a produced of the produced as a produced of the produced as a p

DIMONSTRATIO.

Vt igitur regula verus pateat intelle-

Ous, fe a b lines, que dicator 10. diuiden-da in duas partes , quanum rectangulum de best elle 40. ell autem 40. quadruphum ad



igitur fiat a d, quadratum a c "dimidi) ab, & ex a d aufetater quadroplum a b; abique numero, & igitus teidas, fi sliquid maneret, addita & detracha ex a c. oftenderet partes , at quia tale refiduem eft monts, ideo imaginaberis 3. m. 15. id eft differen tiz a d , & quidespii a b , quam adde & minue ex a c , & habebia quafitum , felliduc c. p. ac. m. 1 t. in c. m. ac. m. quod eft 5. 15. igitus hoc productum elt 40. nacrea tamen a d., nan est cadem com riatura 40. nec a b, quia foperficies eft

15 m. m. 15. qual ch 40.

remota à natura sumeri . Scliner . proximiss tamen huic quantitati, que verè eft ophilica, quanium per earn, non vr in pe-rora, nec in alis operationes exercise lices nec ve vi quid fit. Modas ell, vt adio do, & à 30 aggregati mittoss se addas di-midium disidendi. Esemplum, in hoc cafig., divide 10. in dras partes, producentes 40. adde 25. quadratum dimidi 10. ad 40. fit 65. ab hoisa 30. minute 3. & adde ensur 3. habebis partes fecundum fimilitudiocus, habetos parera secundan mentostores,
 6.5 f. 5. 8 t. 6.5 n. s. A. ha semuci different in 10. non iunchi faciant 10. led 10. 160. de hacafque peopredior Arialmetica fabelitas, cuita hoc extremam v. dirak, adeb elt faballe, vr. fir inutile.

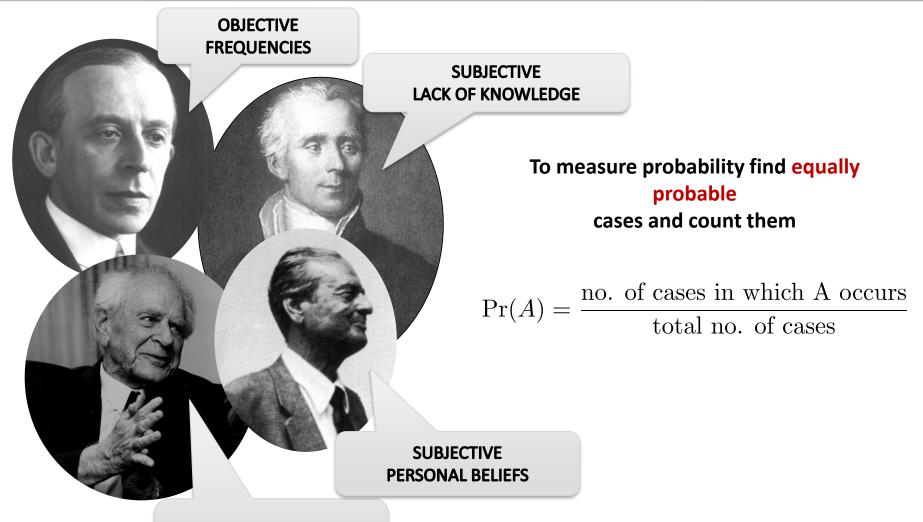
Fat de E. duss partes , quarum quadrata iundia fint 50. hier folutiur per primant, mon per focundam regularo, eft enim de po-ro m. ideo duc 3. climidium 6. in fe fit 9. minue ex dimidio 50. quod eft 15. fa cet-daum 16 cuits p. 4. adde & minue à 5. dimidio 6. fiunt partes 7. & 1. m. harum quafrata iun@a funt 50. & aggregatum

. Per idea folging ourflip has , fac ex 6. dus panes, quarum vna in reliquam docha, producaras m. 40. dac 3. direidrem 6. in fr. fit 5. adde ad 40. fit 49. trains 40. q. x eft

PROBABILITY Liber de Ludo Aleae

COMPLEX NUMBERS Ars Magna

How to understand probability?



OBJECTIVE PROPENSITIES!

And then came Kolmogorov...

ERGEBNISSE DER MATHEMATIK UND IHRER GRENZGEBIETE

HERAUSGEGEBEN VON DER SCHRIFTLEITUNG
DES
"ZENTRALBLATT FÜR MATHEMATIK"
ZWEITER BAND

GRUNDBEGRIFFE DER
WAHRSCHEINLICHKEITSRECHNUNG

VON

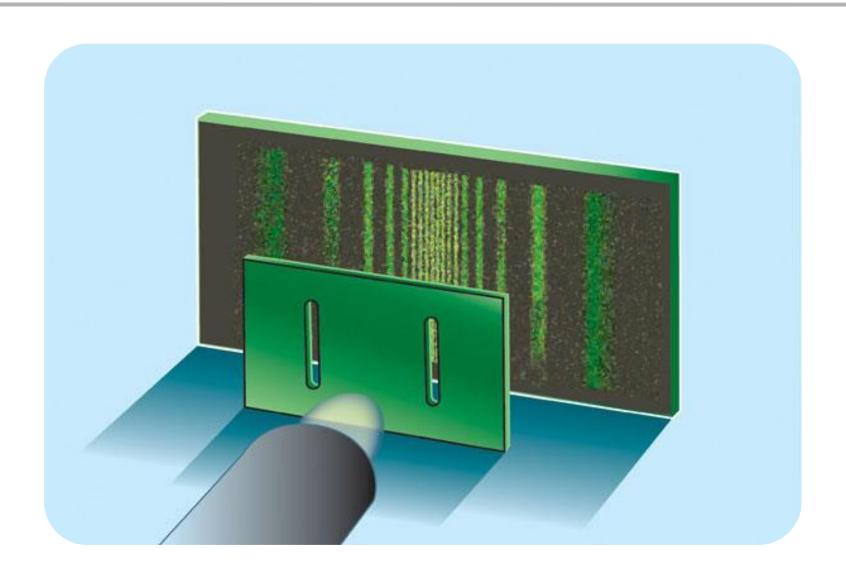
A. KOLMOGOROFF

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



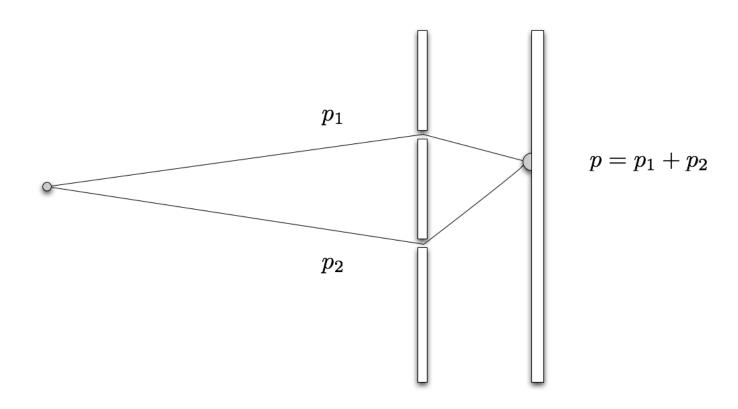
BERLIN VERLAG VON JULIUS SPRINGER 1933 Probability is a non-negative number Probability that something happens is 1 Probabilities of exclusive events add up

It's all very well, except that...

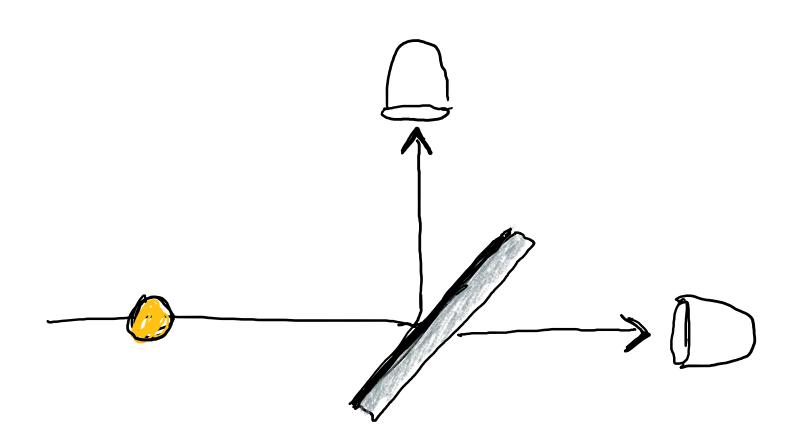


...Nature ignores additivity axiom

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.

τ.

A NY 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.

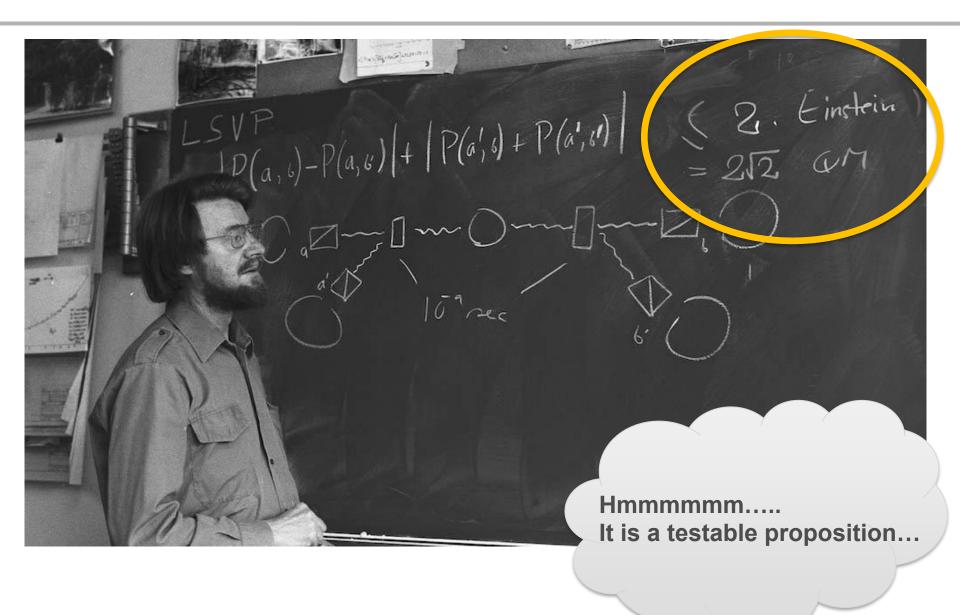
In attempting to judge the success of a physical theory, we may ask ourselves two questions: (1) "Is the theory correct?" and (2) "Is the description given by the theory complete?" It is only in the case in which positive answers may be given to both of these questions, that the concepts of the theory 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.

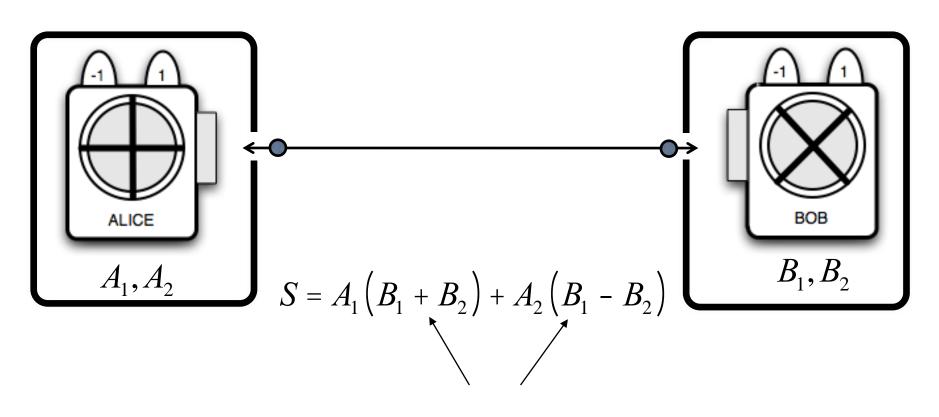
The elements of the physical reality cannot be determined by a priori philosophical considerations, but must be found by an appeal to results of experiments and measurements. A comprehensive definition of reality is, however, unnecessary for our purpose. We shall be satisfied with the following criterion, 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



Bell's inequalities...



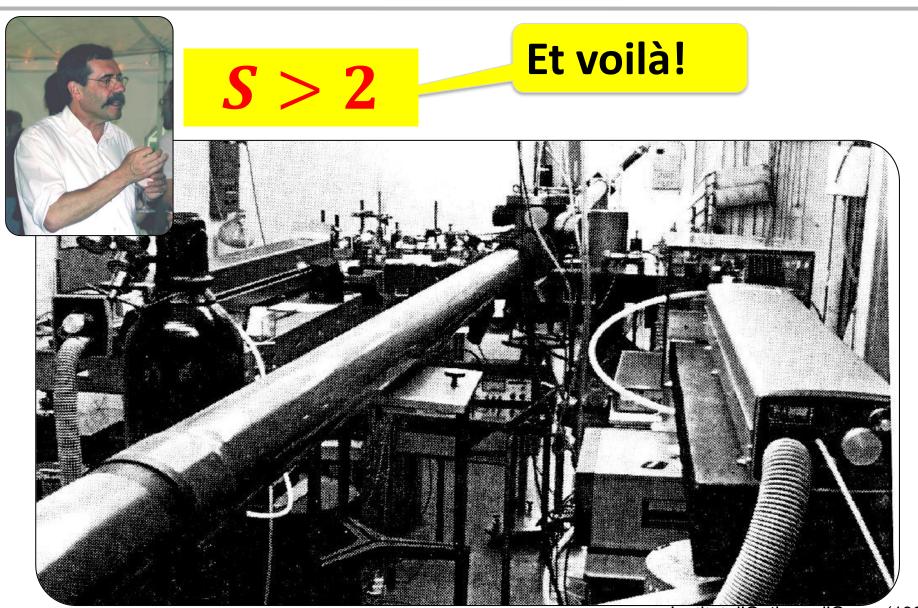
One of these terms is 0 and the other is ± 2

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

John Clauser

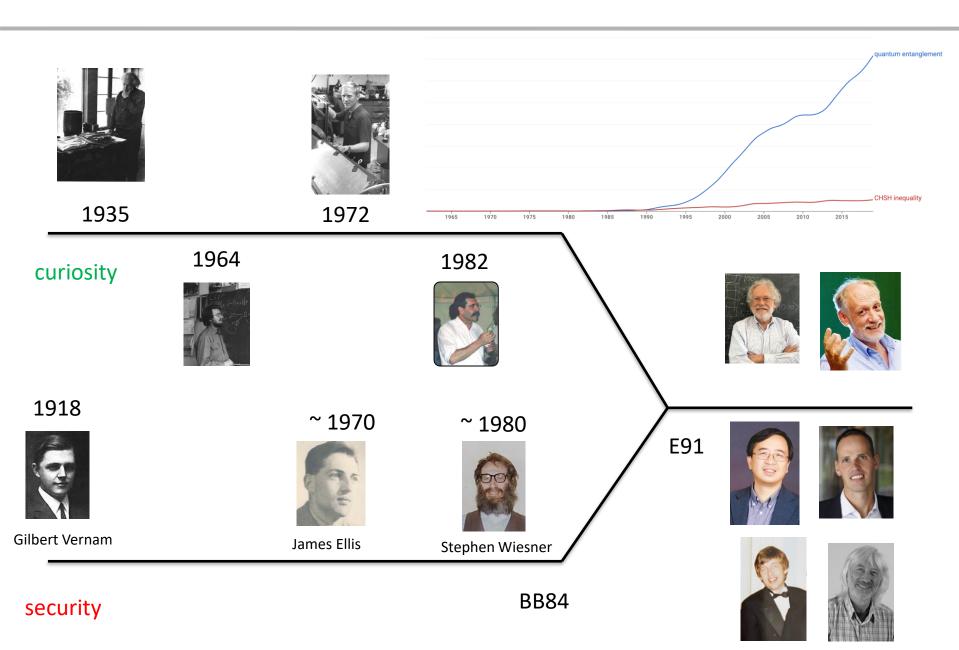


Alain Aspect and his quantum magic

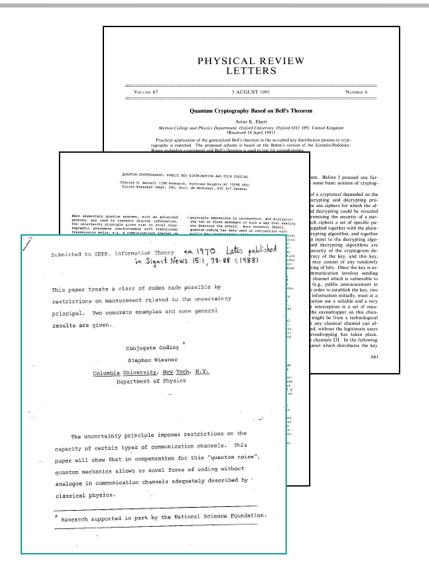


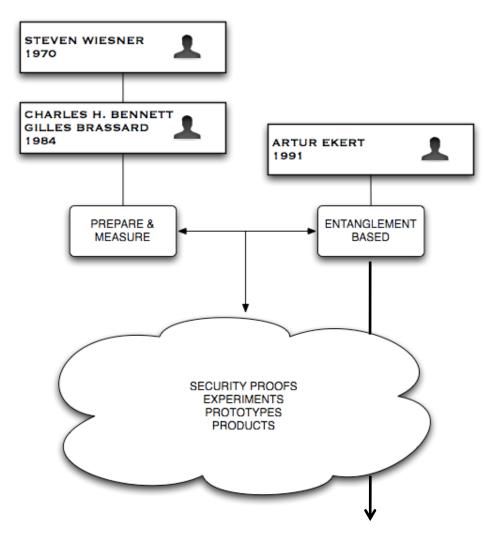
Institut d'Optique d'Orsay (1982)

Fusion



Quantum cryptography





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)

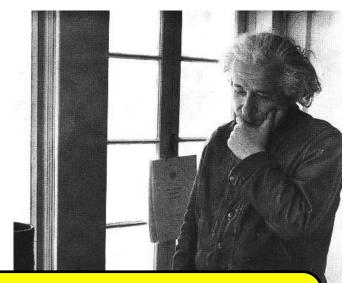
In a complete theory there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system. In quantum mechanics in the case of two physical quantities described by 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

A NY 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.

unnecessary for our purpose. We shall be satisfied with the following criterion, which we regard as

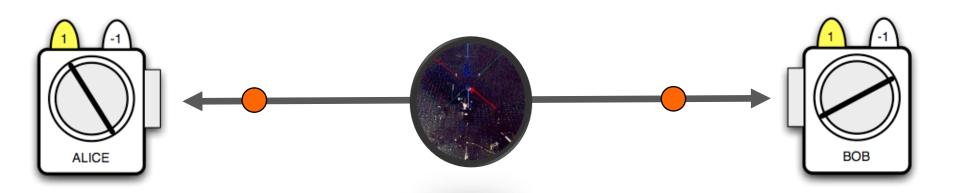
reasonable. If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity. It

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



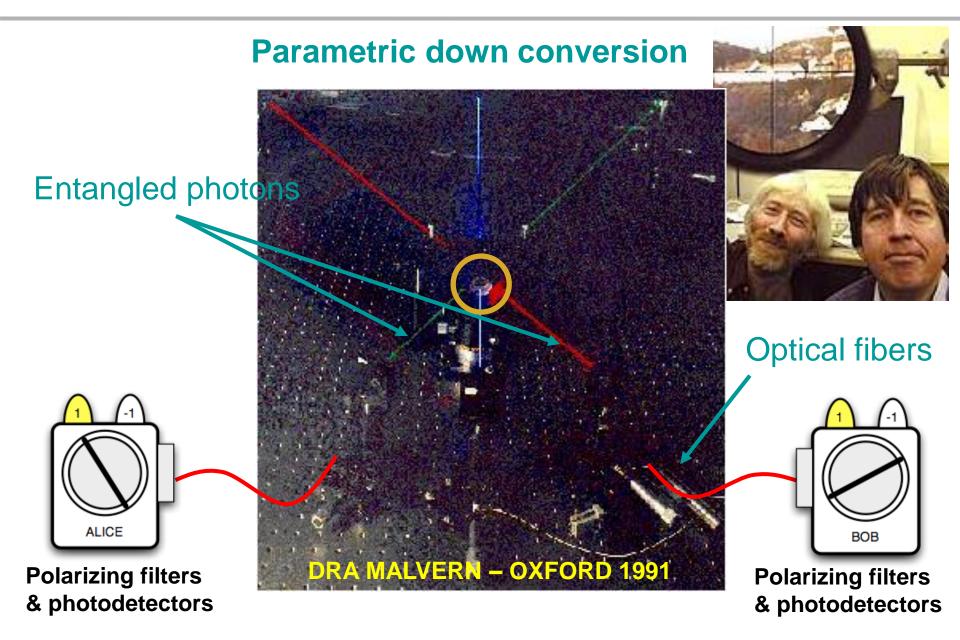
PHOTONS DO NOT CARRY PREDETERMINED VALUES OF POLARIZATIONS

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

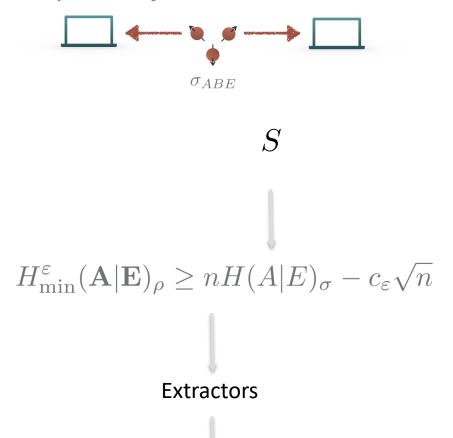
TESTING FOR EAVESDROPPING

And all this can be demonstrated...

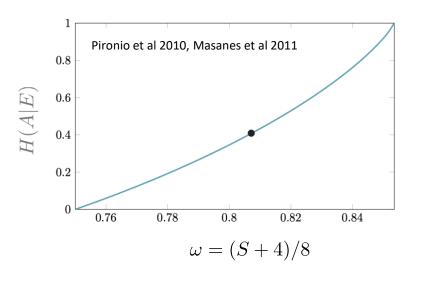


You need some mathematical gymnastics

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



Secret key

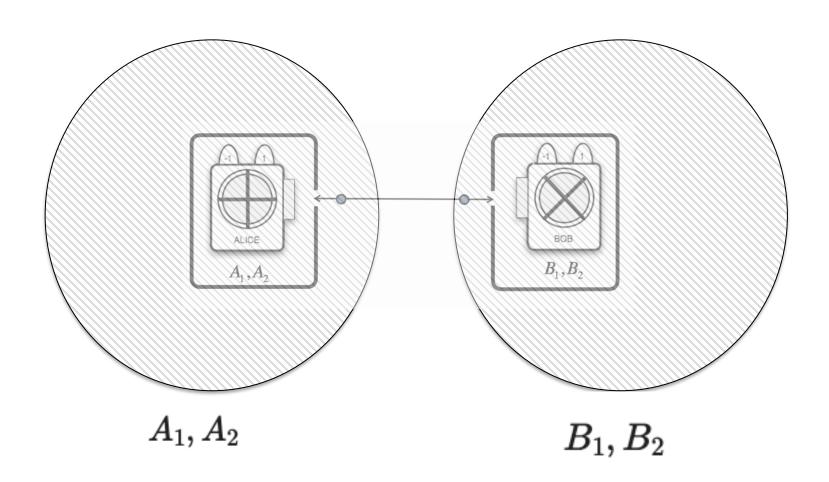


Quantum Asymptotic Equipartition Property M. Tomamichel et al (2009) IDD CASE

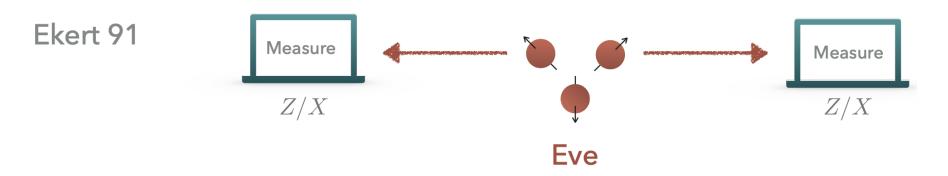
Eve distributes the key!

(Maximal) violation of Bell's inequalities is rigid

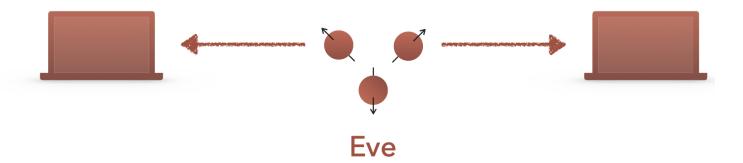
$$|S| = |A_1B_1| + |A_1B_2| + |A_2B_1| - |A_2B_2| = 2\sqrt{2}$$



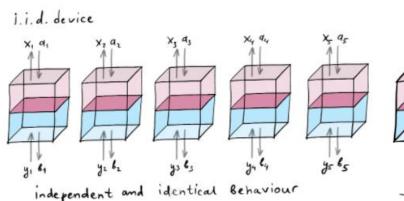
At the mercy of Eve

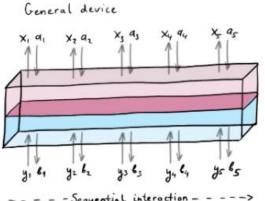


Device-independent



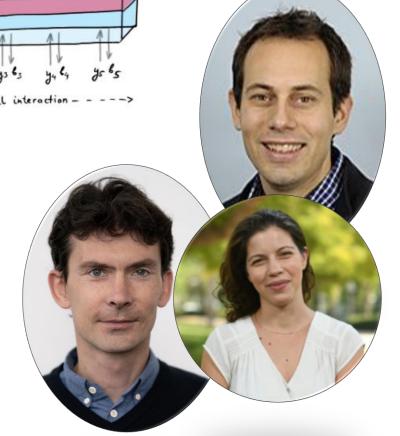
EAT your key to make it secure



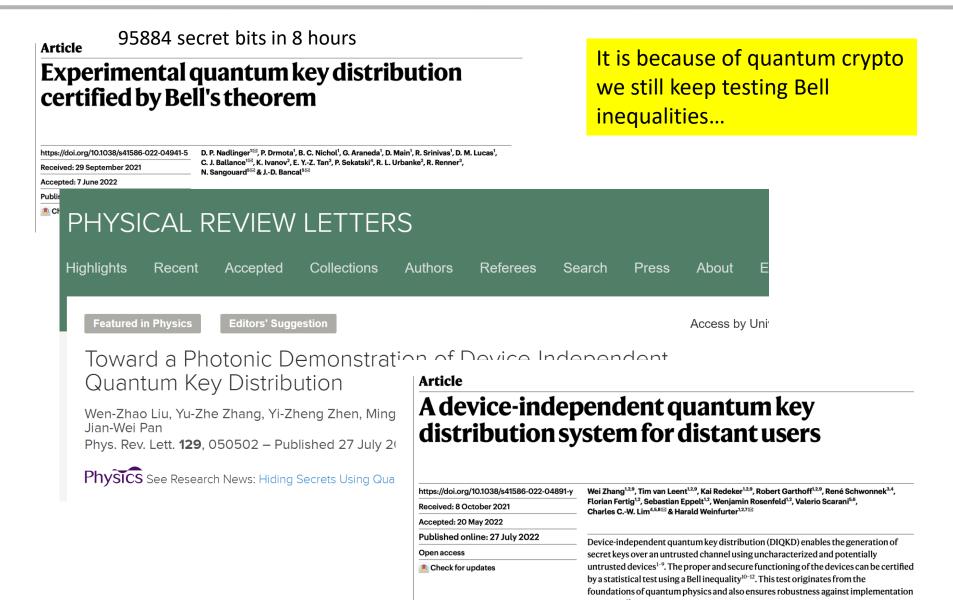


Entropy Accumulation Theorem (EAT) allows us to reduce arbitrary strategies to i.i.d. strategies and enables simple device-independent security proofs.

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...



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





Classical and Quantum Gravity

PAPER • OPEN ACCESS

Relativity of superluminal observers in 1+3 spacetime

Andrzej Dragan^{6,1,2} , Kacper Dębski¹, Szymon Charzyński³ , Krzysztof Turzyński¹ and Artur Ekert^{2,4,5}

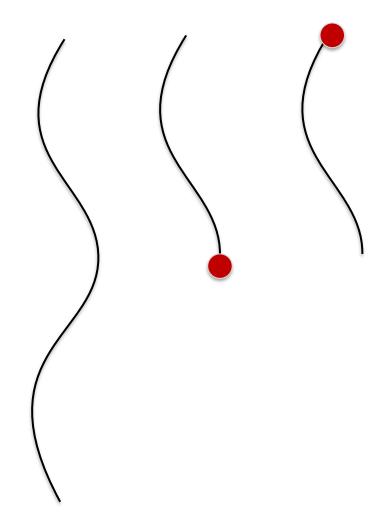
Published 30 December 2022 • © 2022 The Author(s). Published by IOP Publishing Ltd

Classical and Quantum Gravity, Volume 40, Number 2

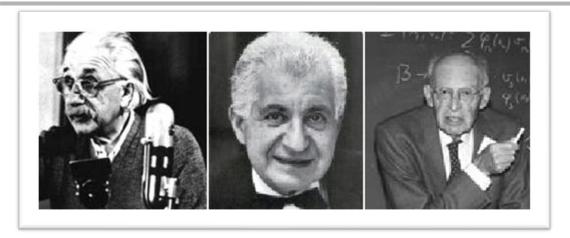
Citation Andrzej Dragan et al 2023 Class. Quantum Grav. 40 025013

DOI 10.1088/1361-6382/acad60

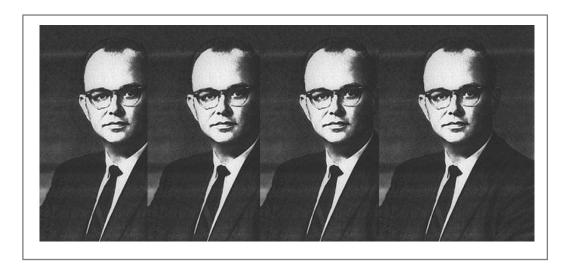




Many open questions



EPR VISION OF REALITY IS TOO SIMPLISTIC



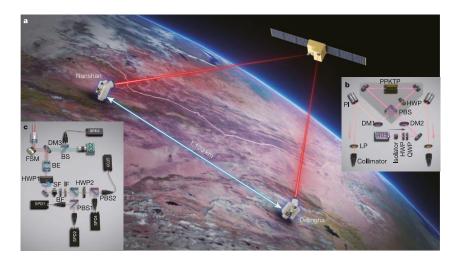
SECURITY AND RANDOMNESS IN THE MULTIVERSE

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

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

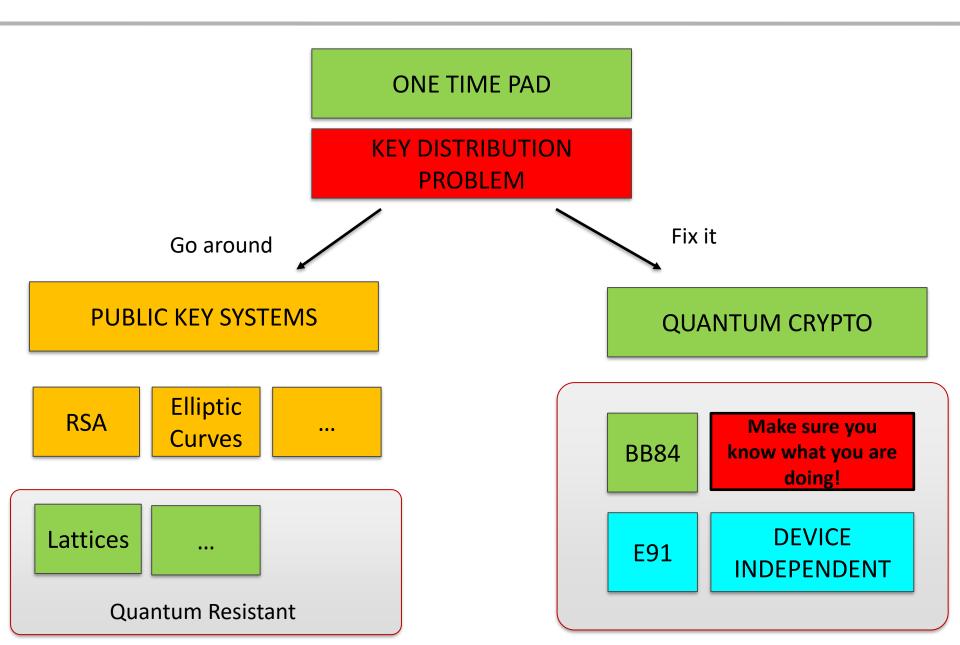
Accepted: 13 May 2020

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 Huang⁵, Lei Deng⁶, 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 Wang², Feihu Xu^{1,2,3}, Jian-Yu Wang^{2,3,4}, Cheng-Zhi Peng^{1,2,3,2,4}, 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 size in the DAM model reducing the gate count of rendem product.

Comb Saber an olds defir

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 exchar 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





Cryptology ePrint Archive

Paper 2022/975

An efficient key recovery attack on SIDH (preliminary version)

Wouter Castryck, KU Leuven Thomas Decru, KU Leuven

Abstract

We present an efficient key recovery attack on the Supersingular Isogeny Diffie-Hellman protocol (SIDH), based on a "glue-and-split" theorem due to Kani. Our attack exploits the existence of a small non-scalar endomorphism on the starting curve, and it also relies on the auxiliary torsion point information that Alice and Bob share during the protocol. Our Magma implementation breaks the instantiation SIKEp434, which aims at security level 1 of the Post-Quantum Cryptography standardization process currently ran by NIST, in about one hour on a single core. This is a preliminary version of a longer article in preparation.

Pa