QUANTUM CONNECTIONS
PART 2

Artur Ekert

The ultimate limits of privacy …

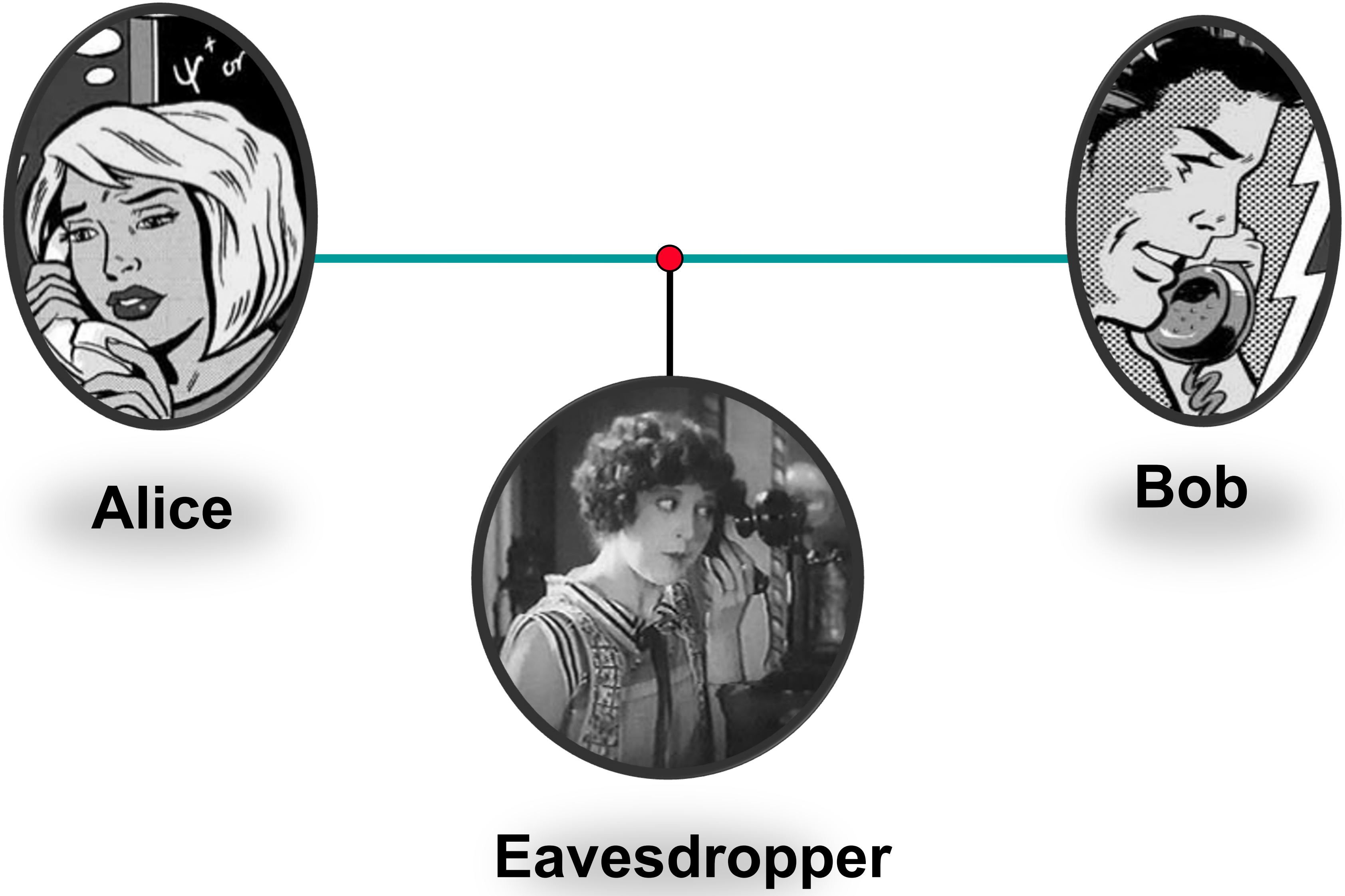
…for the paranoid ones

Artur Ekert

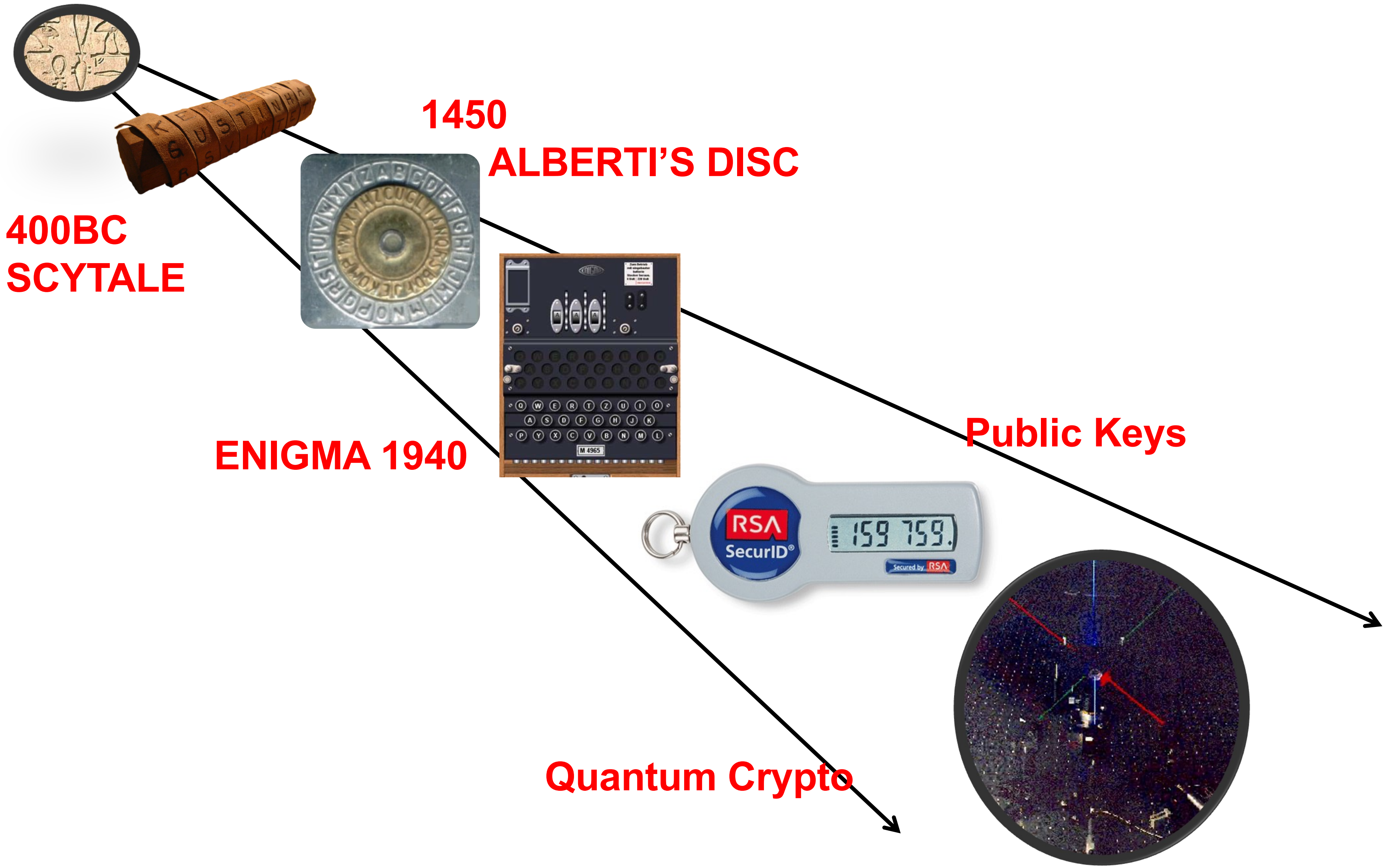
Outline

- Is there a perfect cipher?
- Key distribution – the holy grail of cryptography
- Privacy amplification / randomness extraction
- For whom the Bell tolls
- Less reality more security
- Device independent cryptography

We all have secrets…



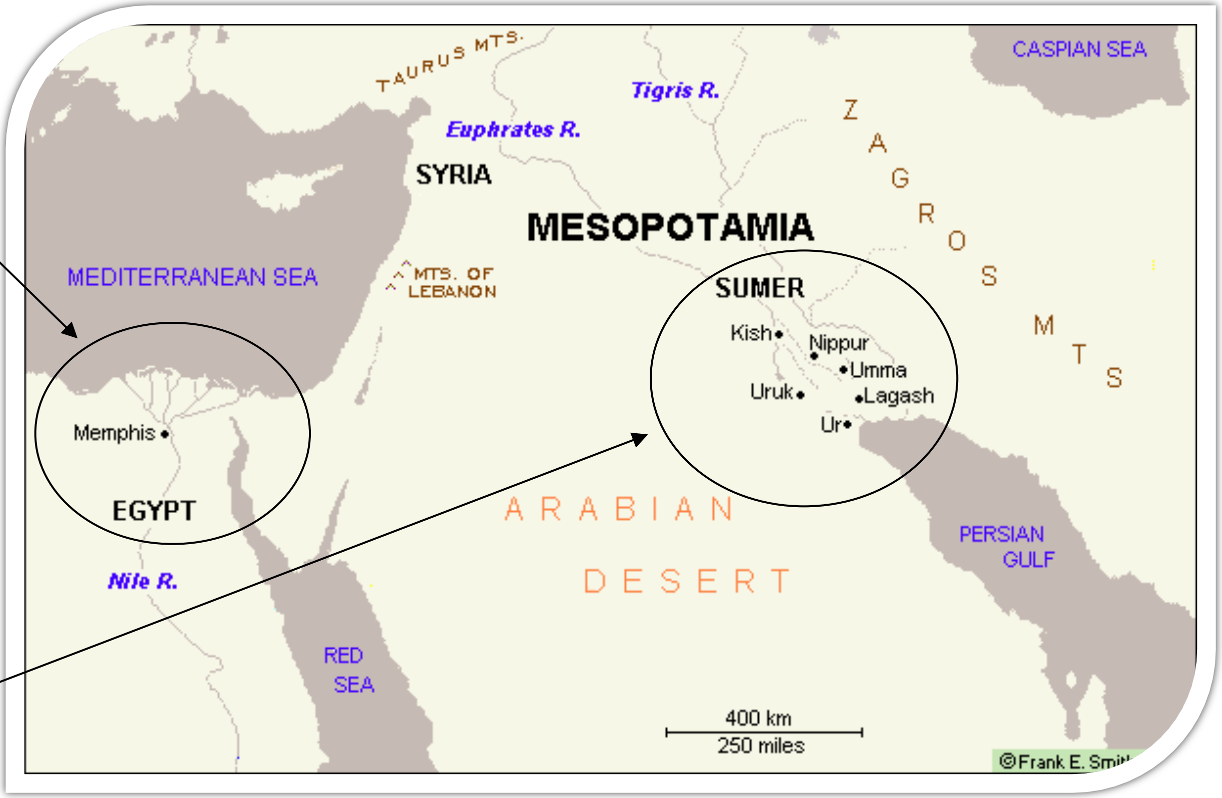
Quest for a perfect cipher



It starts with writing…

Hieroglyphs
Egypt, circa 3300 BC

Cuneiform
Sumer, circa 3300 BC

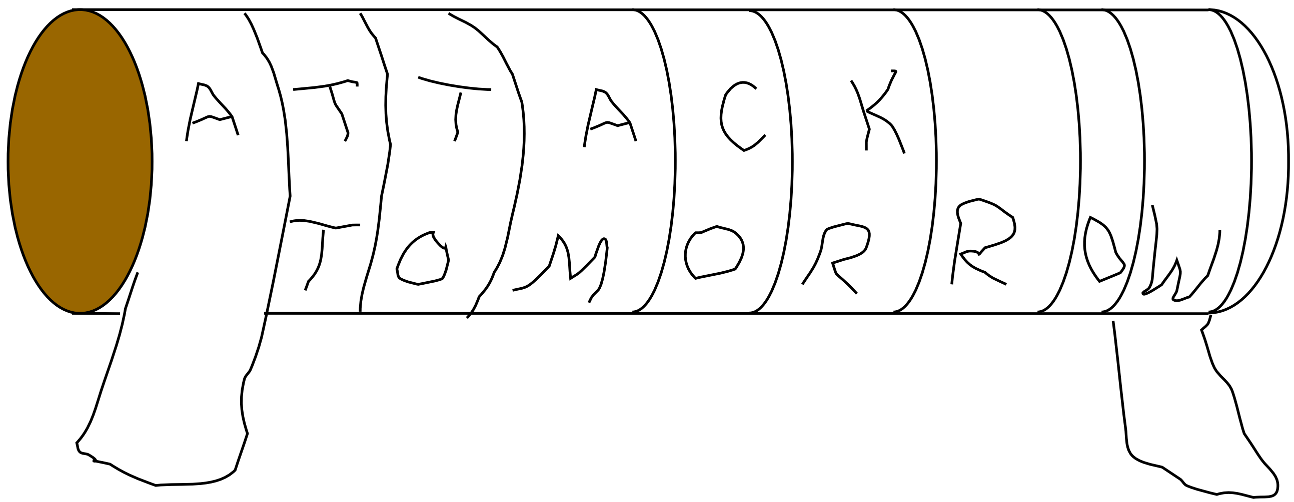


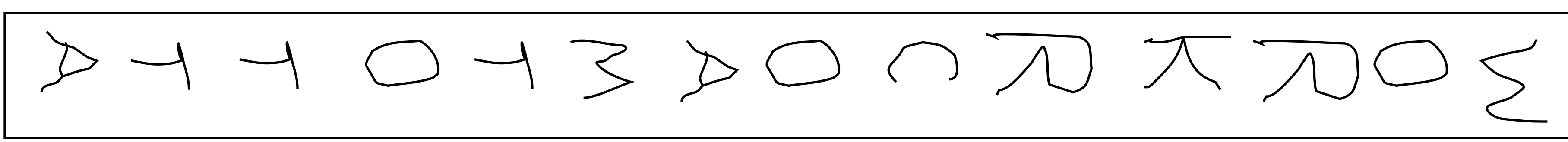
Basic techniques

- PERMUTATIONS
  - SCYTALE (400 BC)
- SUBSTITUTIONS
  - CAESAR SIPHER (50 BC)
- PERMUTATIONS + SUBSTITUTIONS

Scytale

400 BC
SPARTA





Permutation of characters

Caesar ciphers

50 BC
ROME

ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ

ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC

A T T A C K T O M O R R O W
D W W D F N W R P R U U R Z

Code-makers versus code-breakers

Julius Caesar
(100-44 BC)

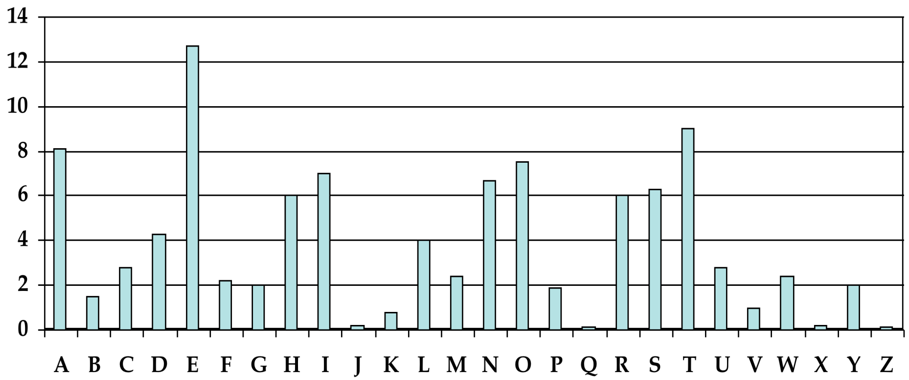
ABCDEFGHIJKLMNOPQRSTUVWXYZ

⇓

NWDEAPYFGTIJUKLMOZQRSBVCXH

$\approx 4 \times 10^{26}$ SUBSTITUTIONS

Al Kindi
(800-873)



Counterexamples - Lipograms

That's right - this is a lipogram - a book, paragraph or similar thing in writing that fails to contain a symbol, particularly that symbol fifth in rank out of 26 (amidst 'd' and 'f') and which stands for a vocalic sound such as that in 'kiwi'. I won't bring it up right now, to avoid spoiling it…

The most famous lipogram: Georges Perec, La Disparition (1969) 85000 words without the letter e:

Tout avait l'air normal, mais tout s'affirmait faux. Tout avait l'air normal, d'abord, puis surgissait l'inhumain, l'affolant. Il aurait voulu savoir où s'articulait l'association qui l'unissait au roman : sur son tapis, assaillant à tout instant son imagination, …

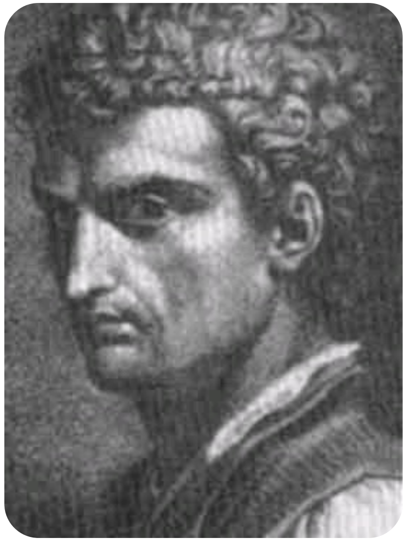
English translator, Gilbert Adair, in A Void, succeeded in avoiding the letter e as well

Gottlob Burmann (1737-1805) R-LESS POETRY. An obsessive dislike for the letter r; wrote 130 poems without using that letter, he also omitted the letter r from his daily conversation for 17 years…

Polyalphabetic ciphers

CODEMAKERS

CODEBREAKERS



Leone Battista Alberti (1404-1472)

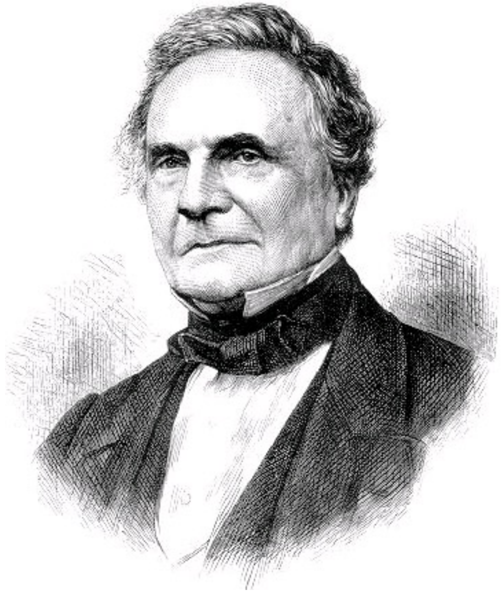
Johannes Trithemius (1462-1516)
Blaise de Vigenere (1523-1596)

Alberti's encryption disk

Sequence of substitutions e.g. 7, 14, 19

Plaintext: **S E L L**

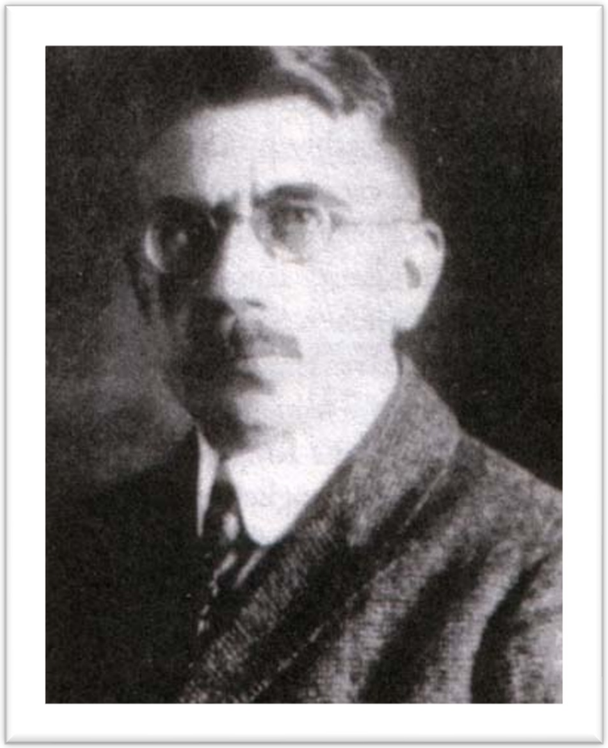
Cryptogram: **Z S E S**



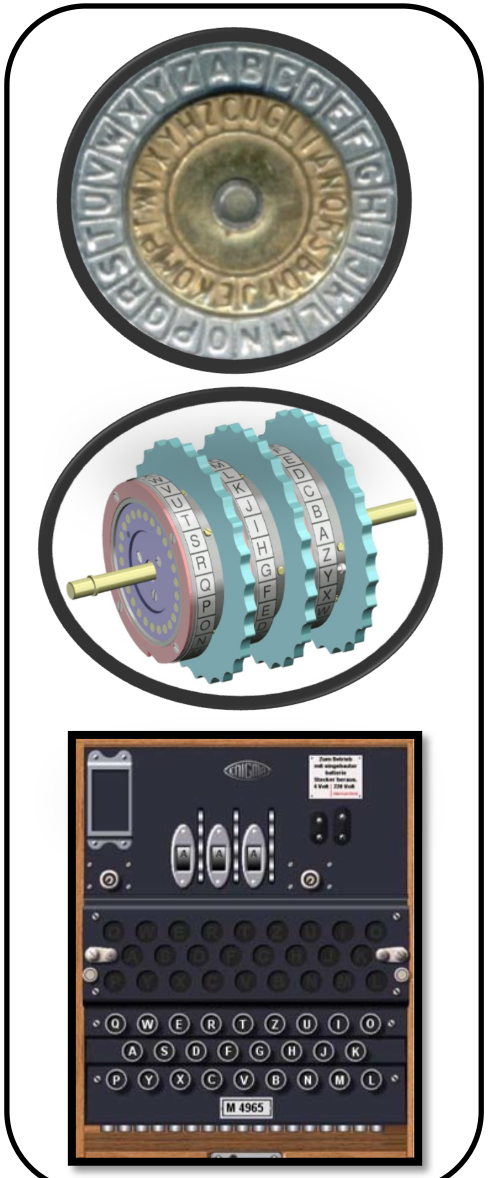
Charles Babbage (1791-1871)

From Alberti's disk to rotor machines

CODEMAKERS



Arthur Scherbius
(1878-1929)



CODEBREAKERS

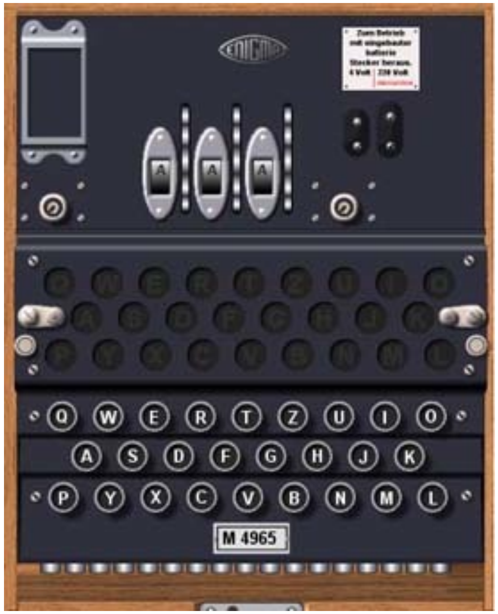
Marian Rejewski
(1905-1980)

The Poles who broke Enigma (BS-4 Section)

Is there a perfect cipher ?

SCYTALE 400BC

ALBERTI'S DISC 1450



ENIGMA 1940

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

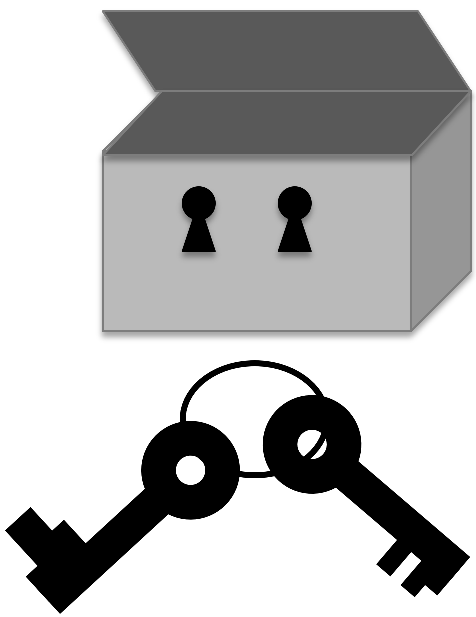
0	0	1	0	1	0	0	0	0	1

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

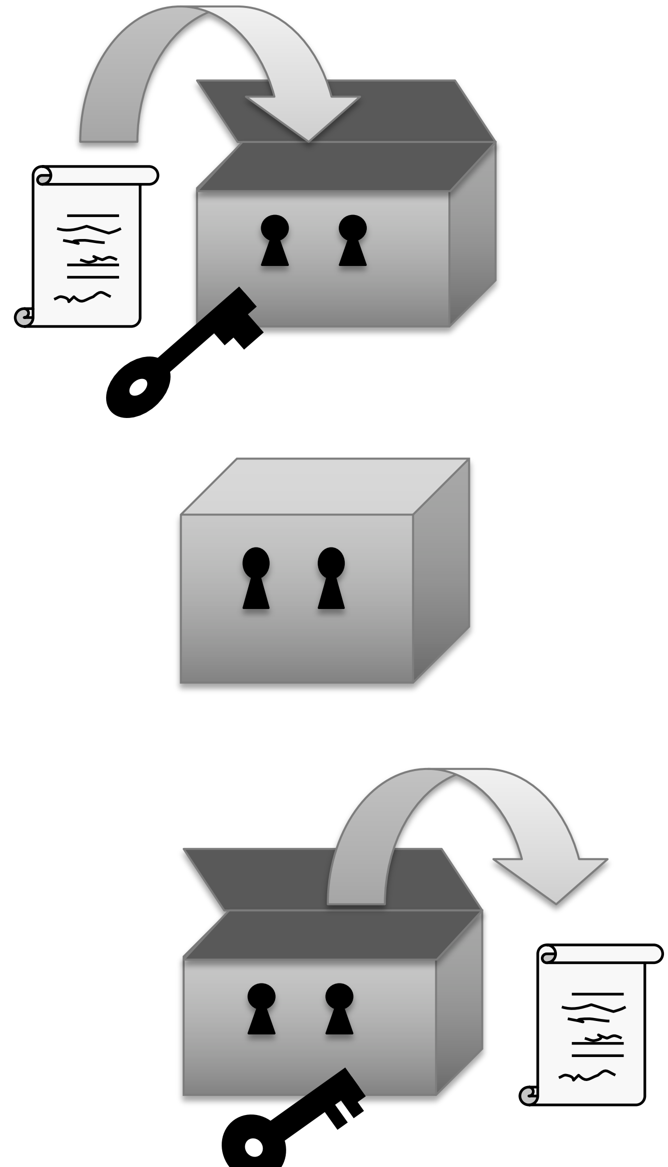
KEY DISTRIBUTION PROBLEM

Public Key Cryptosystems

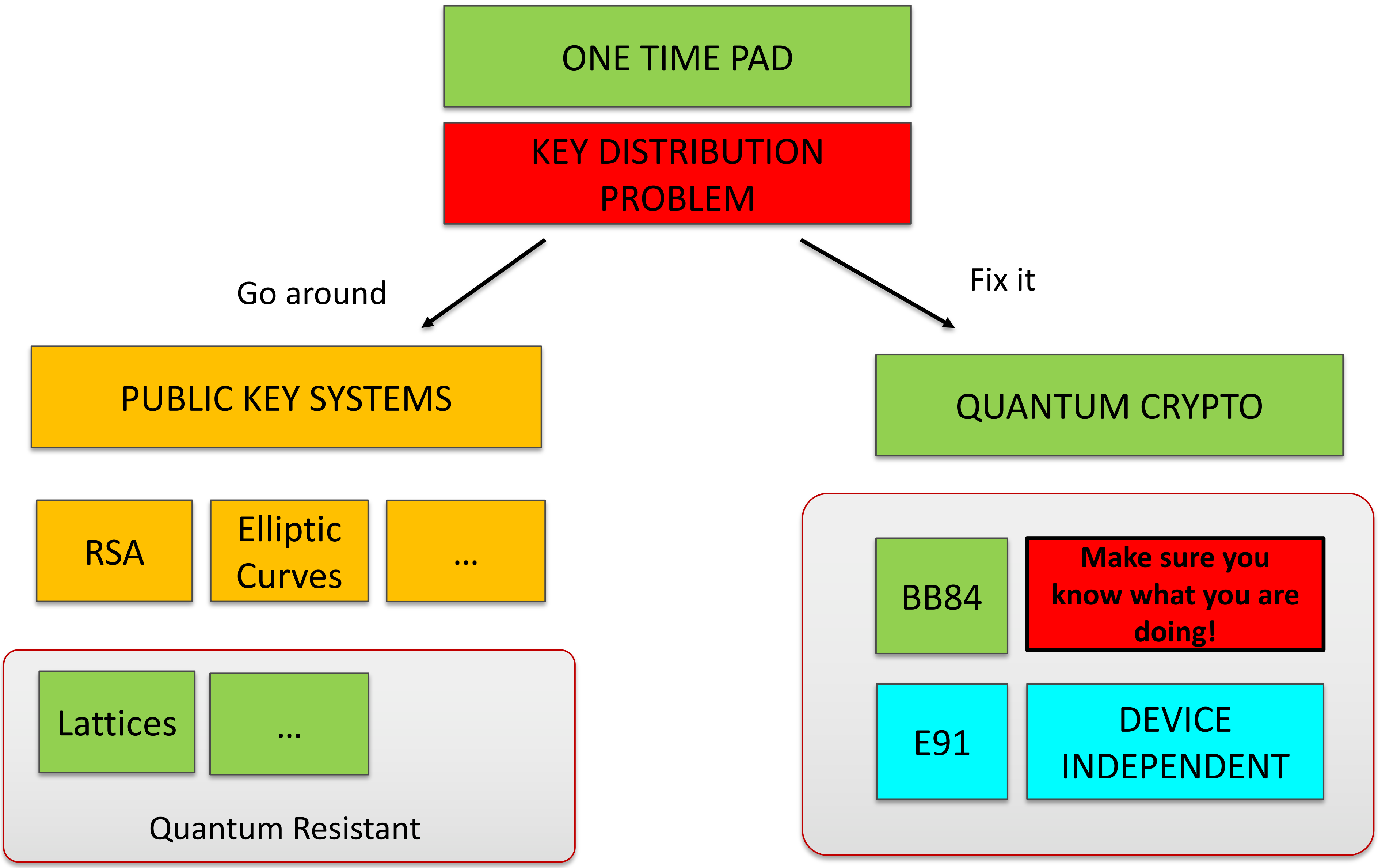


Public key locks the box → **Private key unlocks the box**

FACTORING



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 perfor

product

Comb

Saber an

olds defi

Cryptology ePrint Archive

Paper 2022/214

Breaking Rainbow Takes a Weekend on a Laptop

Ward Beullens, IBM Research - Zurich

Abstract

This work introduces new key recovery attacks against the Rainbow signature scheme, which is one of the three finalist signature schemes still in the NIST Post-Quantum Cryptography standardization project. The new attacks outperform previously known attacks for all the parameter sets submitted to NIST and make a key-recovery practical for the SL 1 parameters. Concretely, given a Rainbow public key for the SL 1 parameters of the second-round submission, our attack returns the corresponding secret key after on average 53 hours (one weekend) of computation time on a standard laptop.

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 effici 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.

Key distribution problem

The key should be random, sufficiently long and secret (known only to Alice and Bob)

0	1	0	1	1	1	0	0	1	0

X

0	1	0	1	1	1	0	0	1	0

X

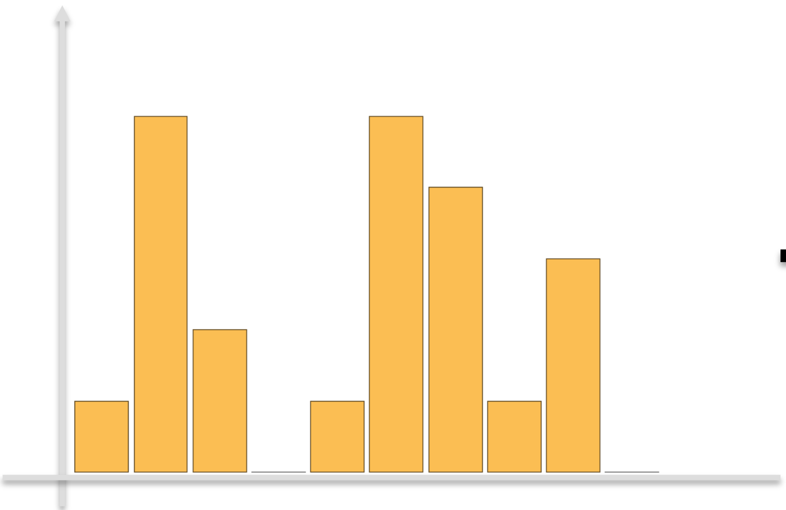
0	?	?	1	?	0	0	?	?	?

E

Probability of Eve guessing the key correctly should be very close to $\frac{1}{2^n}$

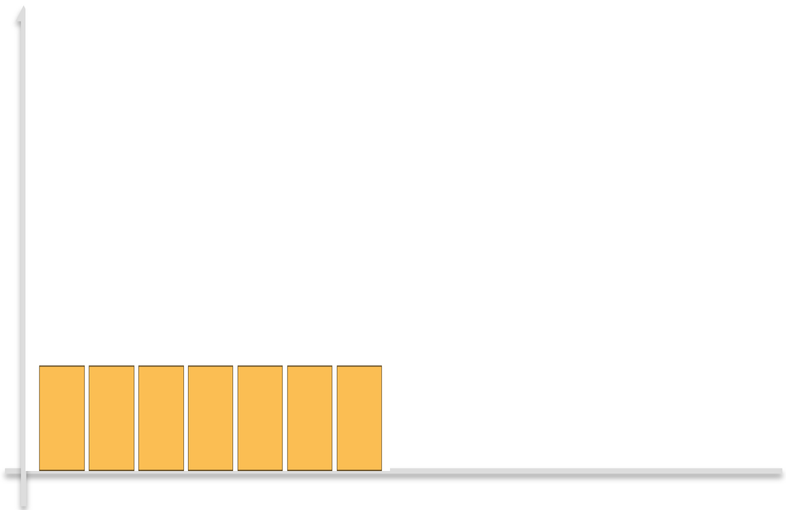
Privacy amplification

$P(X|E)$



$x \in \{0,1\}^n$

$U(K|E)$



$k \in \{0,1\}^l$

For independent bits try parity

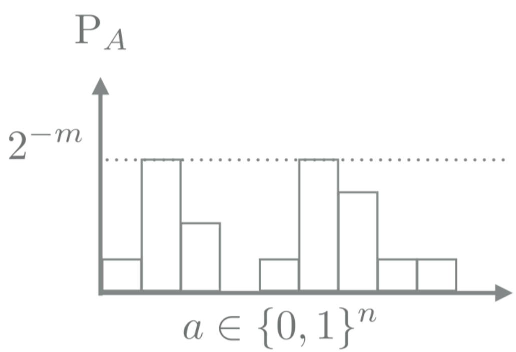
$$x_1 \oplus x_2 \oplus x_3 \ldots$$

Suppose Eve knows one of the two bits, but Alice and Bob are not sure which one

$$k = x_1 \oplus x_2$$

Randomness extraction

Weak source of randomness



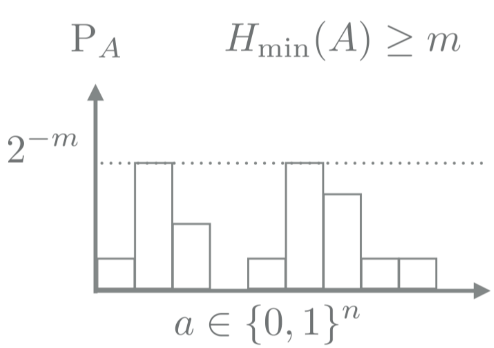
Min-entropy:

$$H_{\min}(A) = -\log\left(\overbrace{\max_a \Pr[a]}^{p_{\text{guess}}(A)}\right)$$

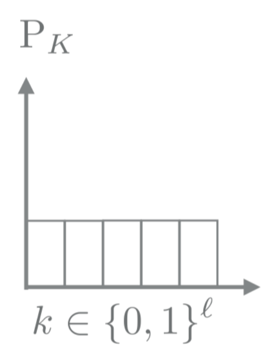
$H_{\min}(A) \geq m$:

$$\forall a \in \{0,1\}^n, \quad \Pr[a] \leq 2^{-m}$$

Weak source of randomness

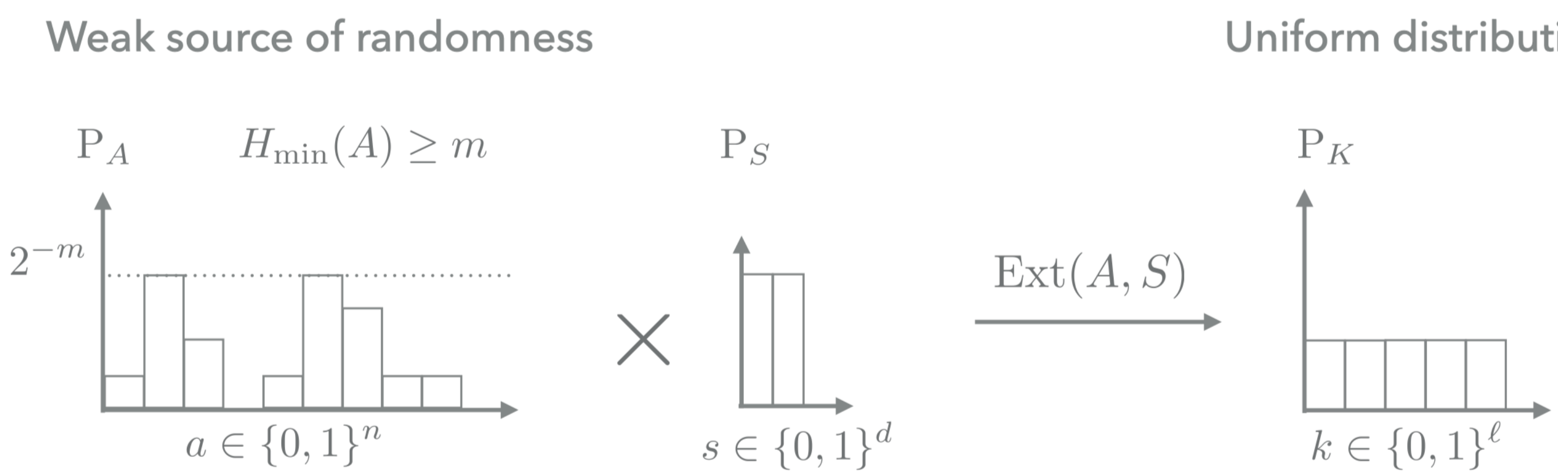


Uniform distribution



Randomness extraction

- Impossible to achieve deterministically
- Possible with an additional short random seed



Randomness extraction

- Def. [Randomness extractor]: A function $\mathrm{Ext}(A,S) : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^\ell$ is called a **strong** (m,ε)-randomness extractor if for

   1. $S = U_d$

   2. any P_A with $H_{\min}(A) \geq m$

   we have

$$\|\mathrm{Ext}(A,S)S - U_\ell \times S\| \leq \varepsilon$$

Eve?

Output of the extractor

Uniform key

(Strong extractor: the seed is made public during the QKD protocol)

Privacy amplification

Alice and Bob can turn their partially secure key into a secure key as long as they can estimate how much Eve knows about the raw key.

0	1	0	1	1	1	0	0	1	0

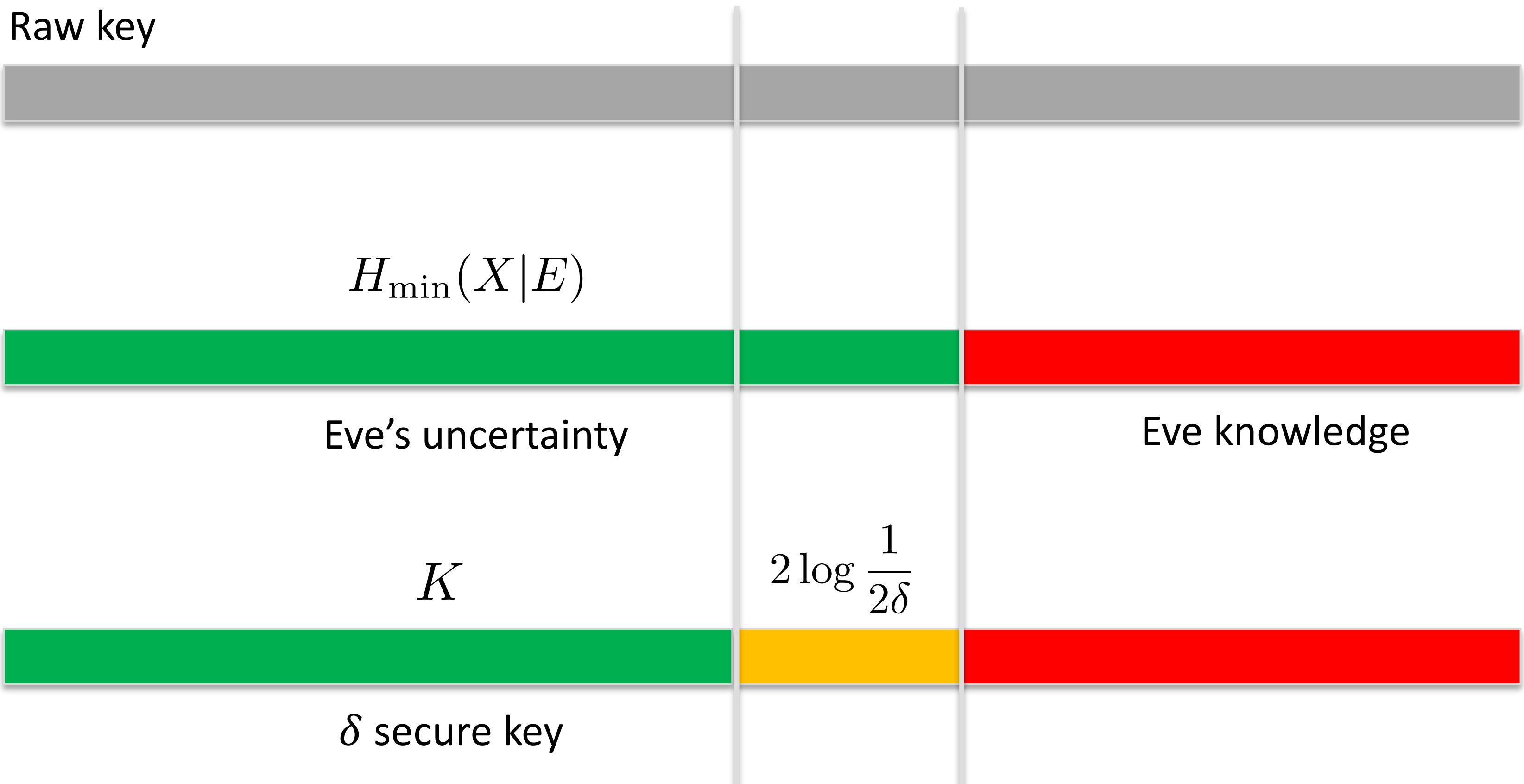
0	1	0	1	1	1	0	0	1	0

Probability of Eve guessing the key correctly should be very close to $\frac{1}{2^n}$

$$H_{\min}(X|E) = -\log p_{\text{guess}}(X|E)$$

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

Extractors



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

How to find out how much Eve knows?

0	1	0	1	1	1	0	0	1	0

X

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

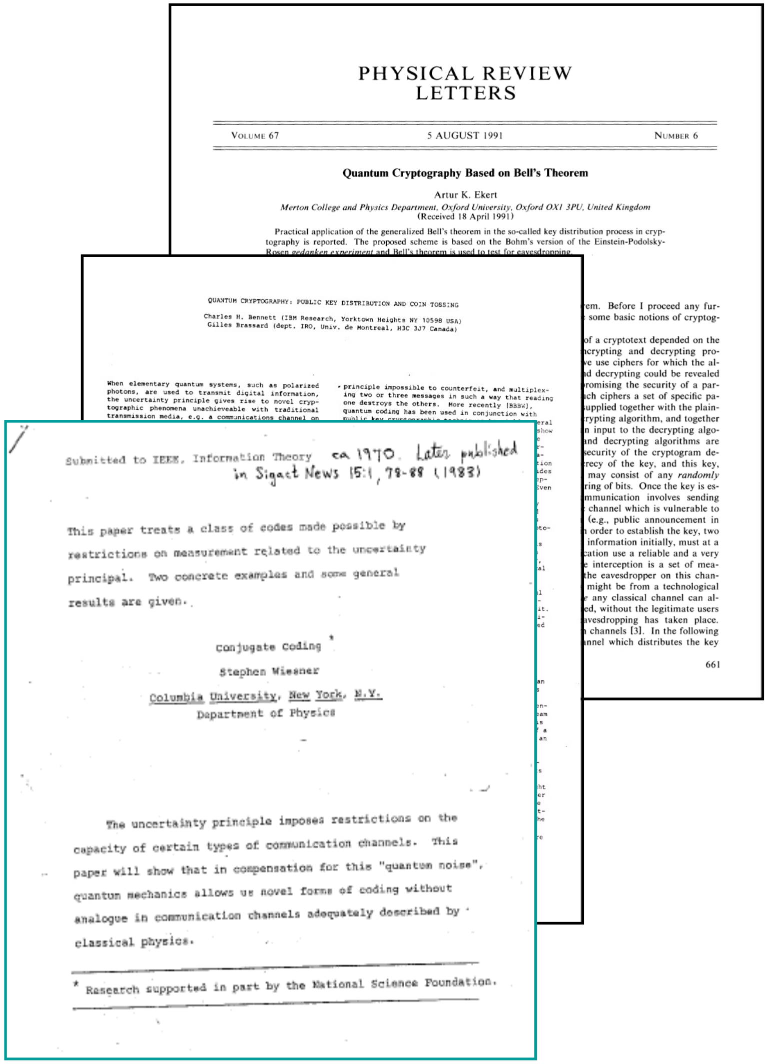
0	1	0	1	1	1	0	0	1	0

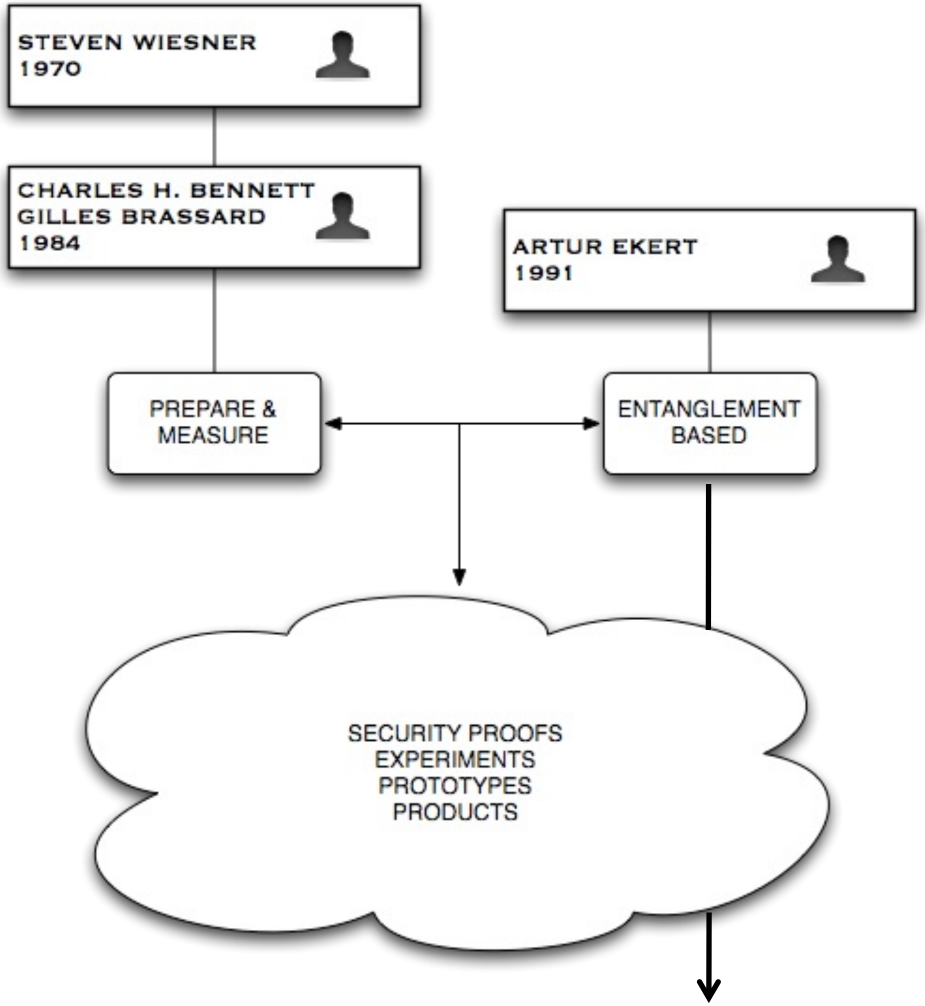
X

0	?	?	1	?	0	0	?	?	?

E

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.

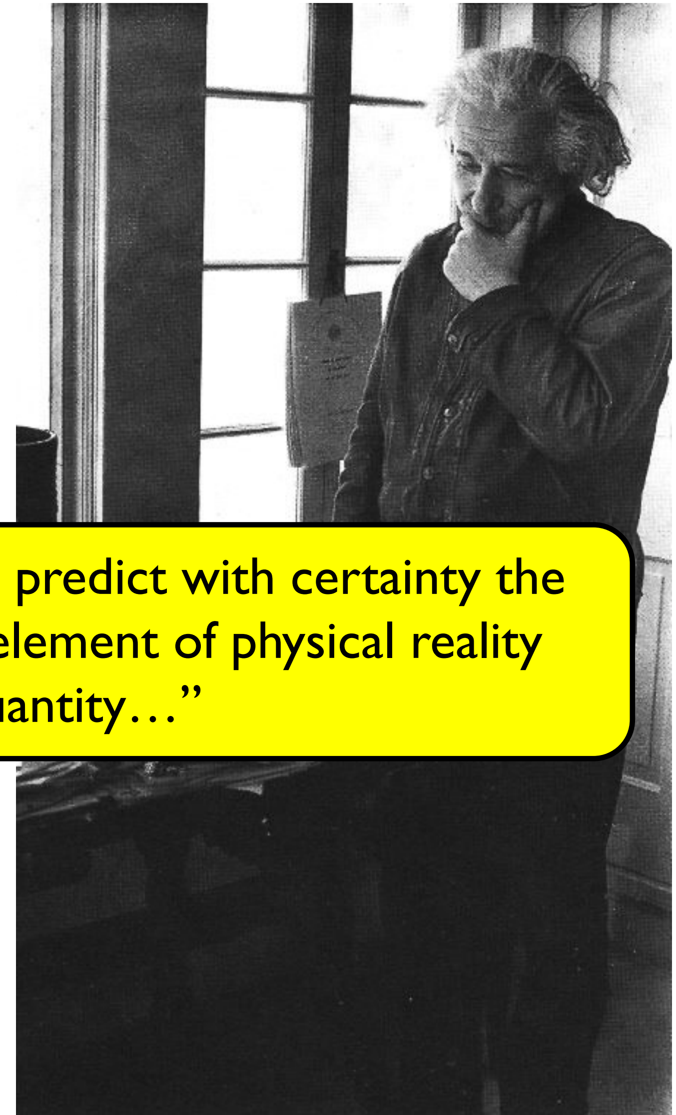
ANY serious consideration of a physical theory must take into account the distinction between the objective reality, which is independent of any theory, and the physical

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

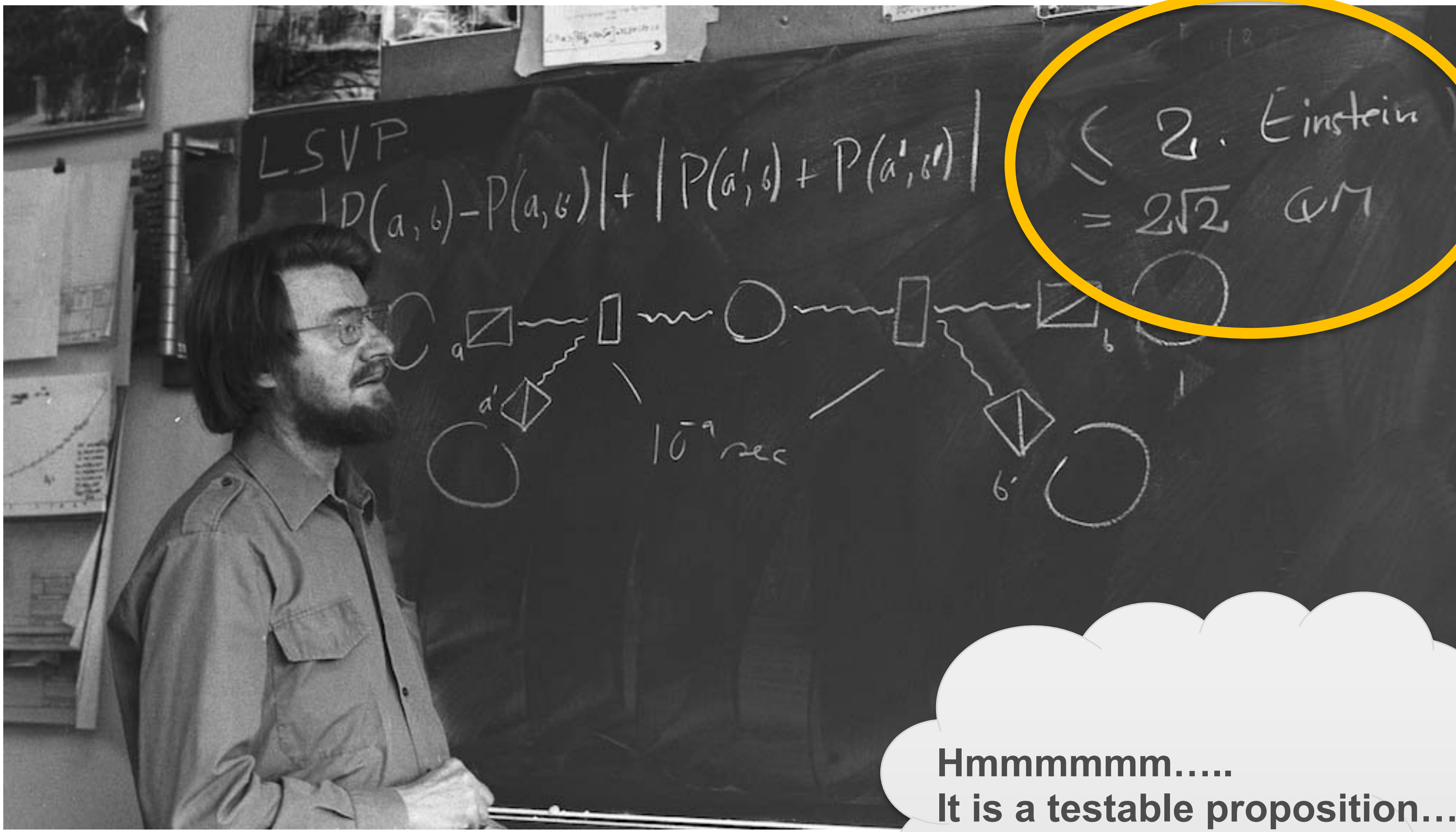
comprehensive definition of reality is, however, unnecessary for our purpose. We shall be satisfied with the following criterion, which we regard as reasonable. *If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, 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

"…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…"



DEFINITION OF EAVESDROPPING

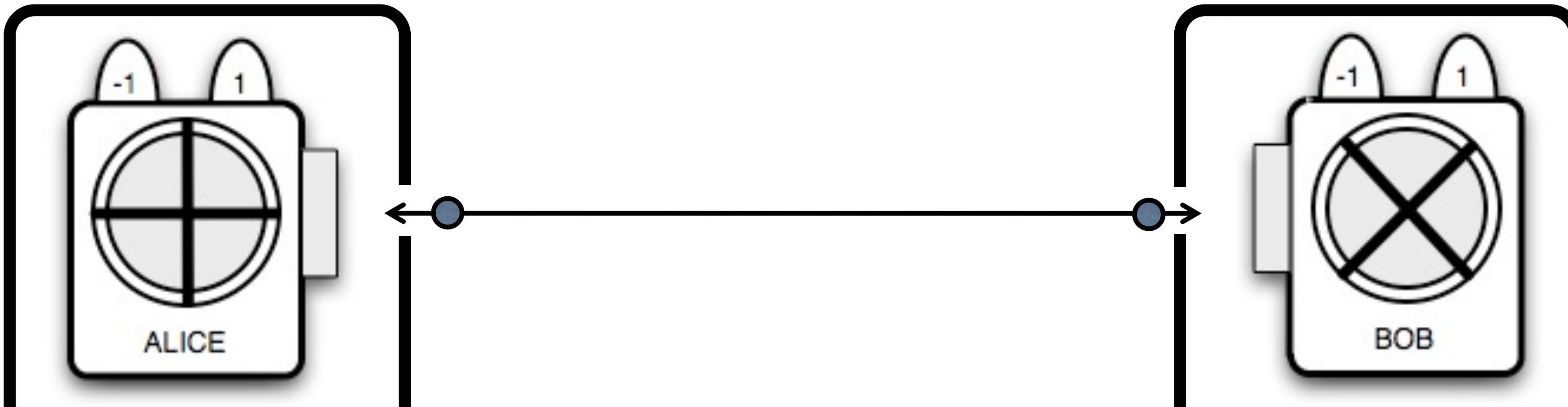
Enter John Bell



Hmmmmmm…..
It is a testable proposition…

year 1964

Bell's inequalities...



A_1, A_2

B_1, B_2

$$S = A_1\left(B_1 + B_2\right) + A_2\left(B_1 - B_2\right)$$

One of these terms is 0 and the other is $\pm$ 2

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

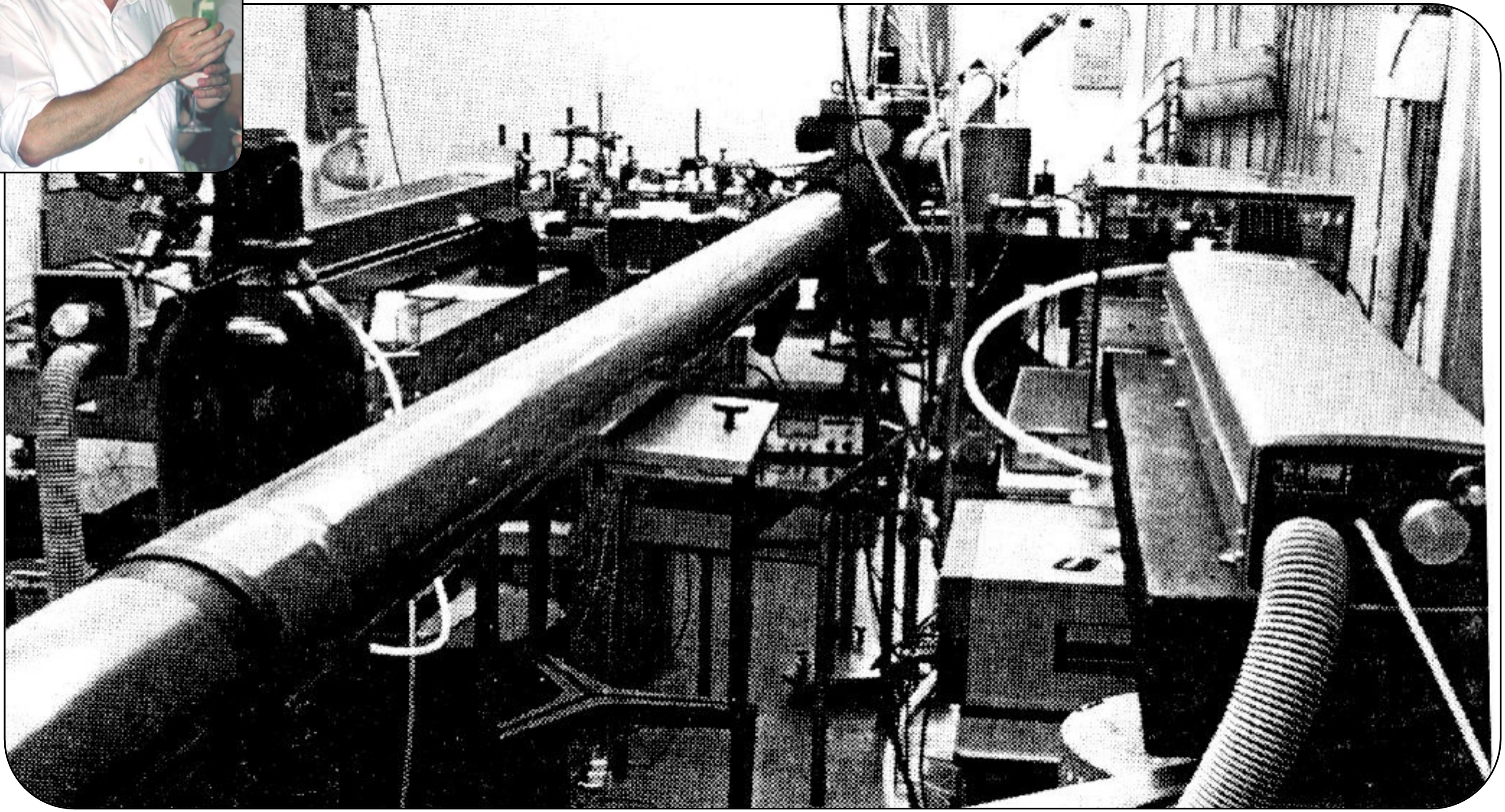
John Clauser – postdocs have ideas…

Berkeley (1972**)**

Alain Aspect and his quantum magic

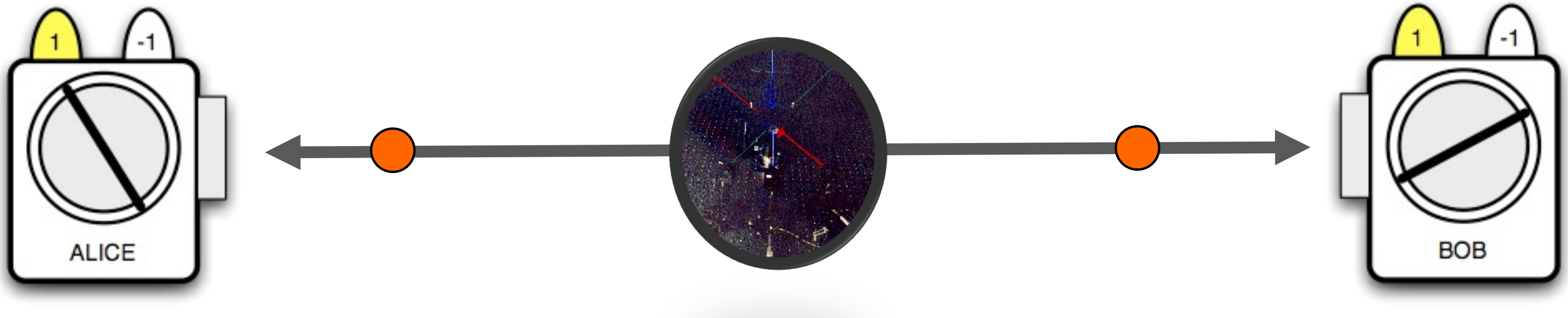
$S > 2$

Et voilà!



Institut d'Optique d'Orsay (1982)

Less reality more security



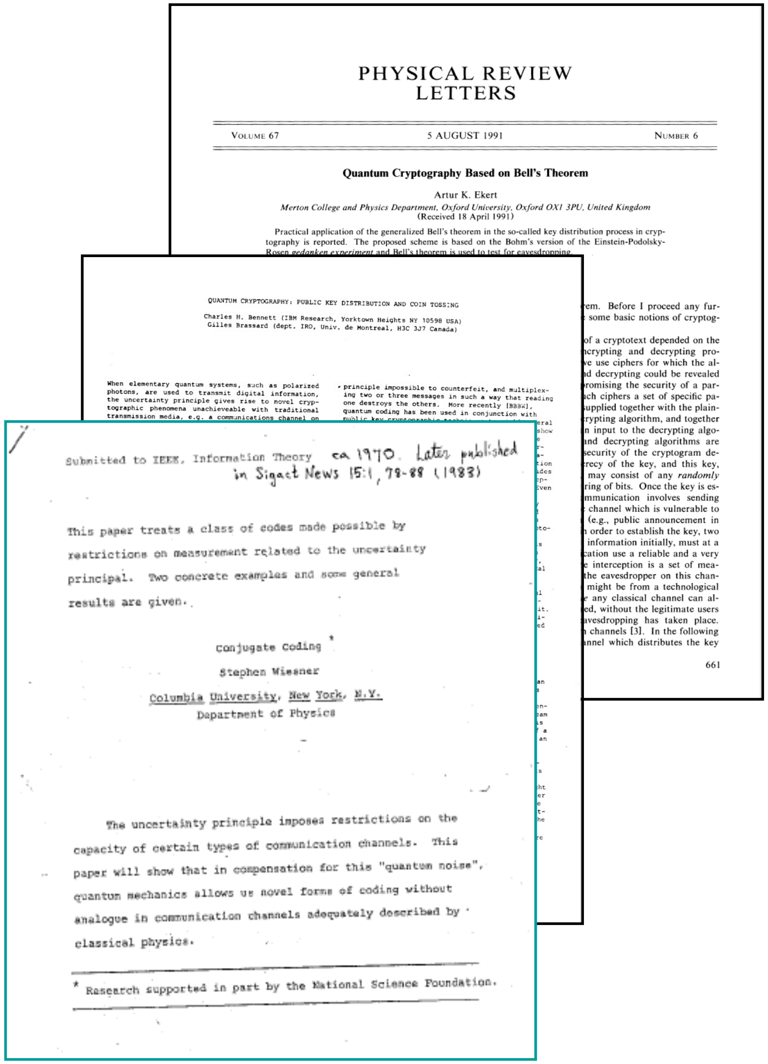
PHOTONS DO NOT CARRY PREDETERMINED VALUES OF POLARIZATIONS

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

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.

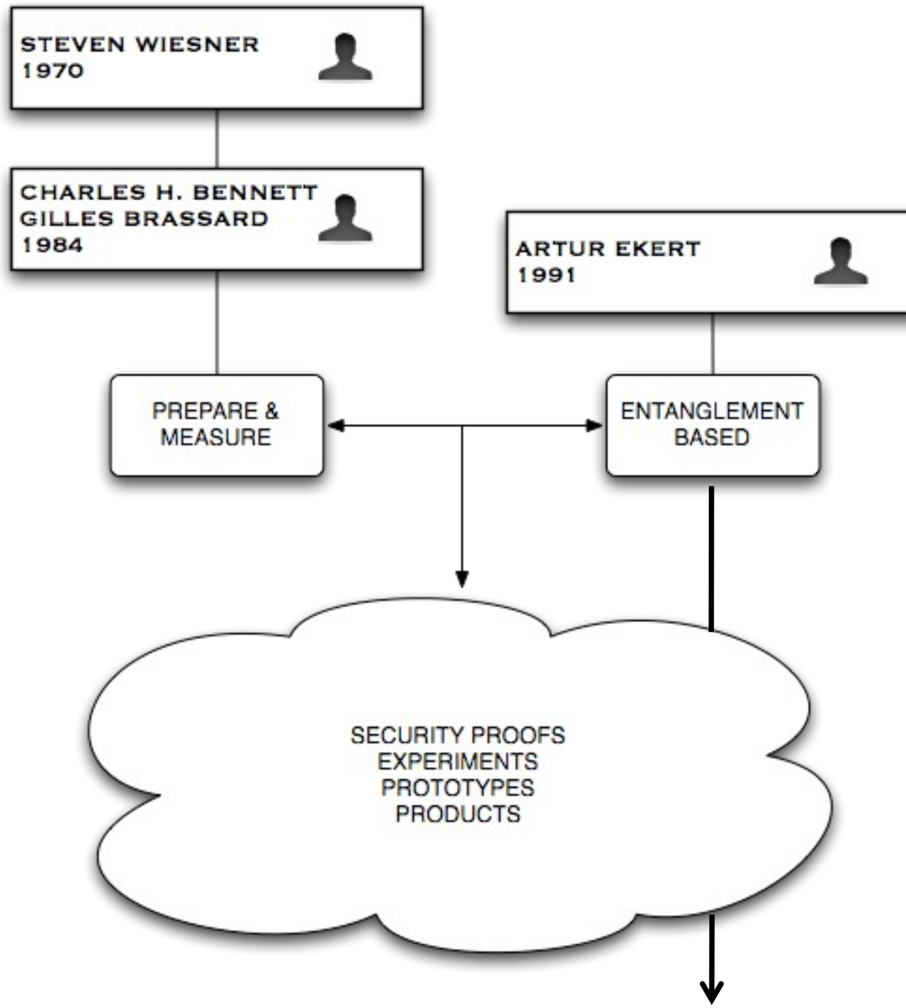
Conjugate Coding*

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.

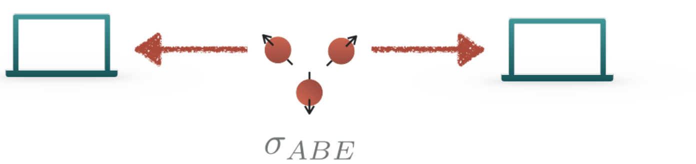
* Research supported in part by the National Science Foundation.



Device independence etc

You need some mathematical gymnastics

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

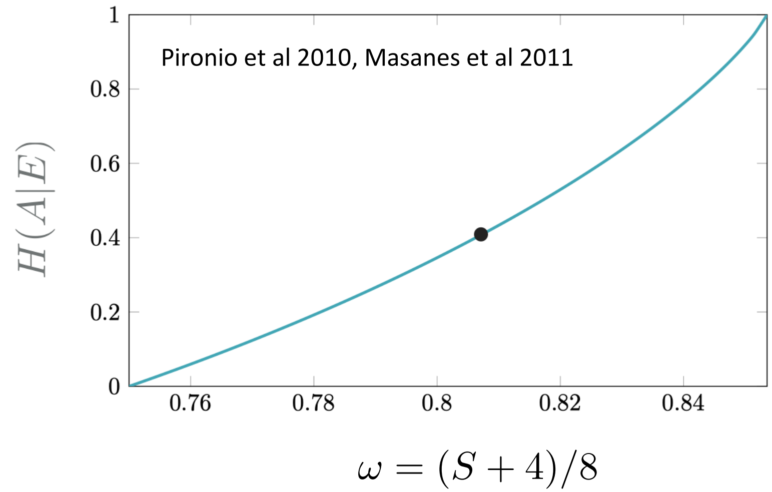


S

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

Extractors

Secret key



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

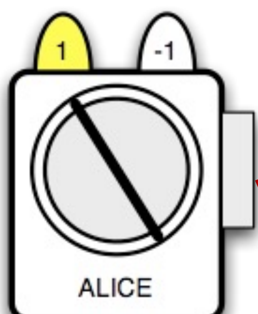
Eve distributes the key!

And all this can be demonstrated…

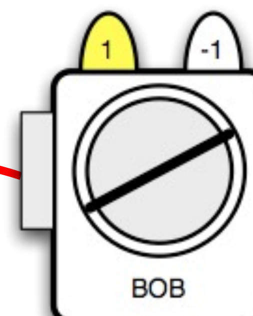
Parametric down conversion

Entangled photons

Optical fibers



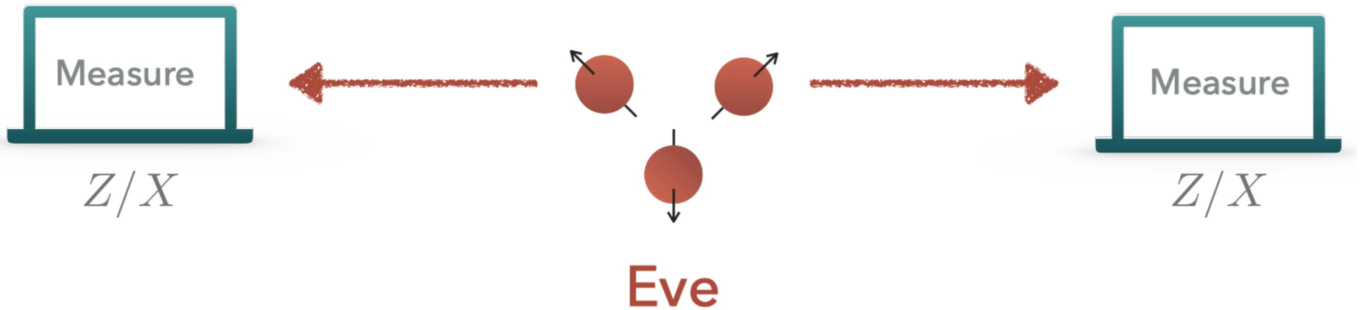
Polarizing filters & photodetectors



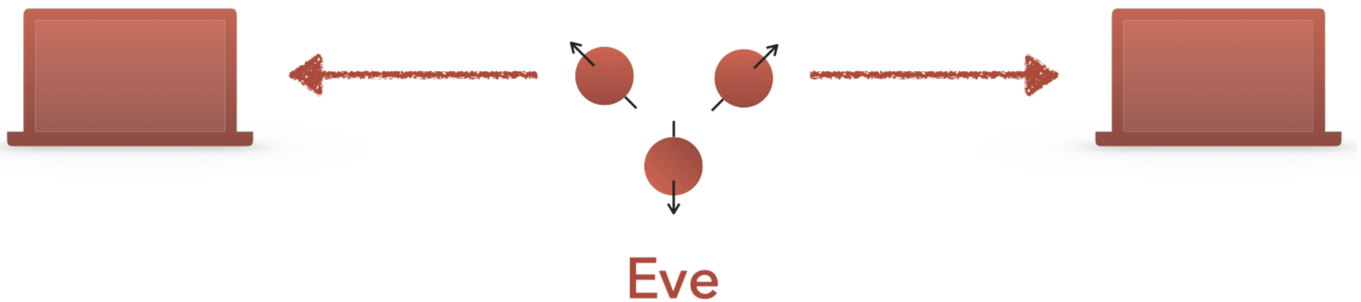
Polarizing filters & photodetectors

At the mercy of Eve

Ekert 91



Device-independent



Courtesy Rotem Arnon-Friedman

Towards device-independent crypto

A. Acin, N. Brunner, N. Gisin, S. Massar, V. Scarani

[Ekert, 91] →
[Mayers & Yao, 98]
Main ideas

[Barrett, Hardy & Kent, 05] →
Proof of concept

[Pironio *et al.*, 09]
IID + asymptotic:
tight rates & noise tolerance

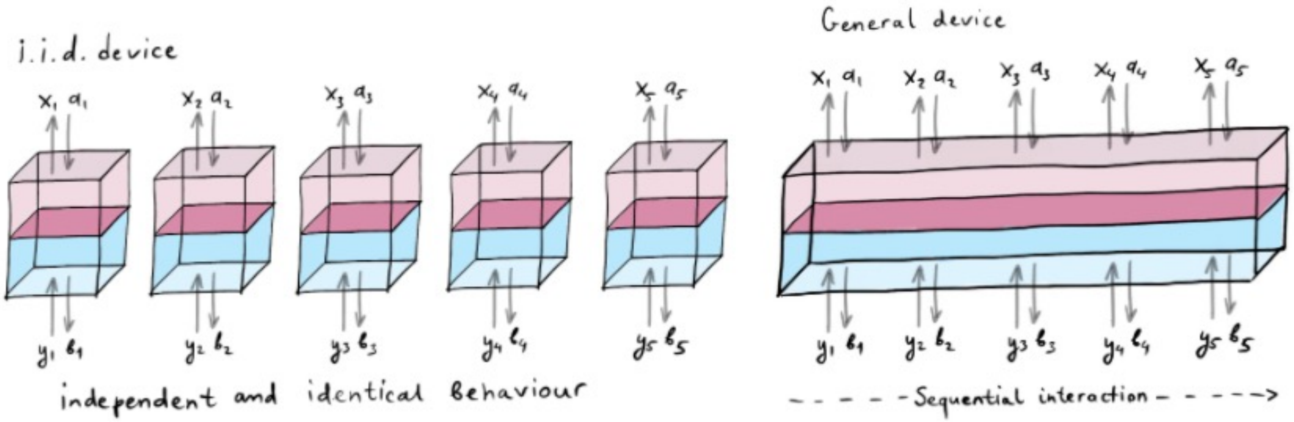
[Reichardt, Unger & Vazirani, 13]
[Vazirani & Vidick, 14]
[Miller & Shi, 14]
General security

← [AF, Renner & Vidick, 16]
General security:
tight rates & noise tolerance

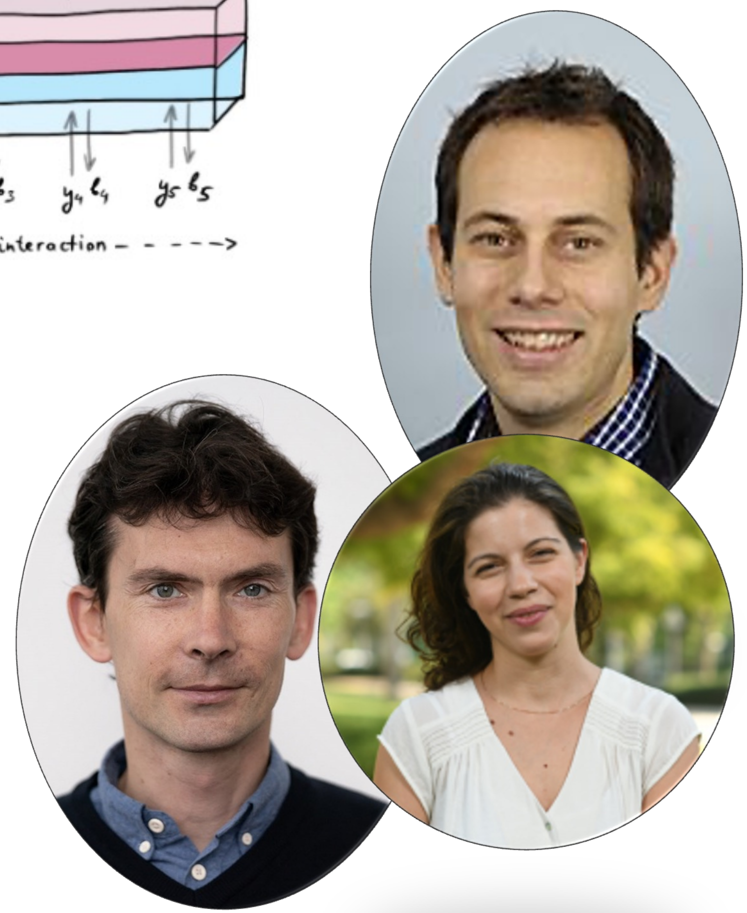
[Dupuis, Fawzi & Renner, 16]
[Dupuis & Fawzi, 18]
Entropy accumulation theorem

Courtesy Rotem Arnon-Friedman

EAT…



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

You can have your key and EAT it

1. **Winning a non-local game** $$H(A|E) \geq f(\text{win prob.})$$

$$\downarrow$$

2. Entropy accumulation (Reduction to IID) $$H_{\min}^{\varepsilon}(\mathbf{A}|\mathbf{E})_{\rho} \geq nH(A|E)_{\sigma} - c_{\varepsilon}\sqrt{n}$$

$$\downarrow$$

3. Quantum-proof extractors $$\left\|\rho_{\mathrm{Ext}(A,S)SE} - \rho_{U_\ell} \otimes \rho_{SE}\right\| \leq \varepsilon$$

$$\downarrow$$

4. Secrecy $$(1 - \Pr(\text{abort}))\left\|\rho_{K_A E} - \rho_{U_\ell} \otimes \rho_E\right\| \leq \varepsilon_{\text{sec}}$$

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
Published online: 27 July 2022
Check for updates

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✉]

Cryptographic key exchange protocols traditionally rely on computational

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, Jian-Wei Pan

Phys. Rev. Lett. **129**, 050502 – Published 27 J

Physics See Research News: Hiding Secrets Usin

Article

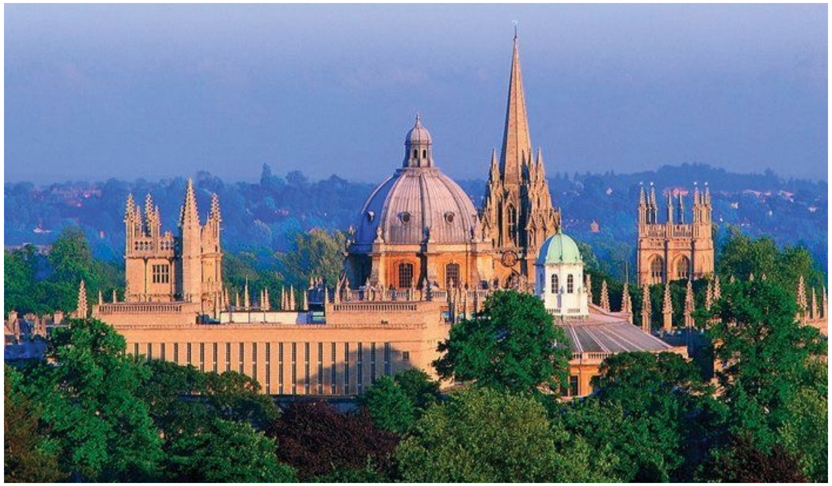
A device-independent quantum key distribution system for distant users

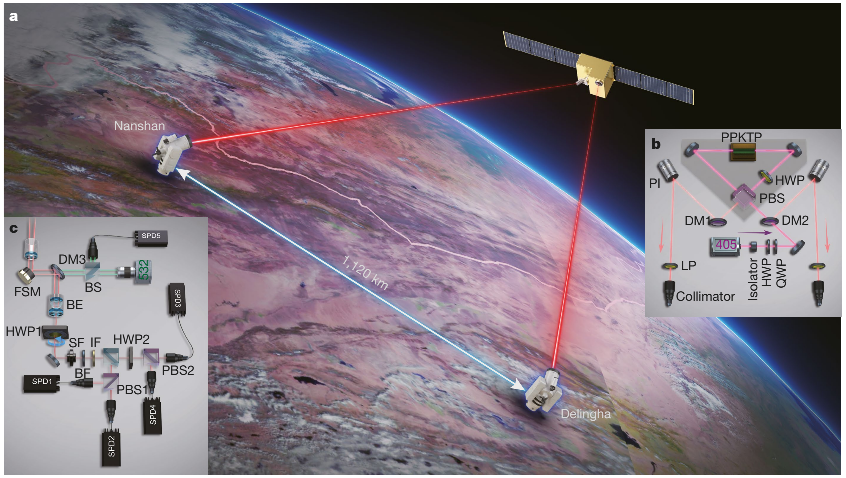
https://doi.org/10.1038/s41586-022-04891-y
Received: 8 October 2021
Accepted: 20 May 2022
Published online: 27 July 2022
Open access
Check for updates

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

Thirty years ago…





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

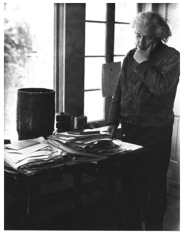
Accepted: 13 May 2020

Published online: 15 June 2020

Check for updates

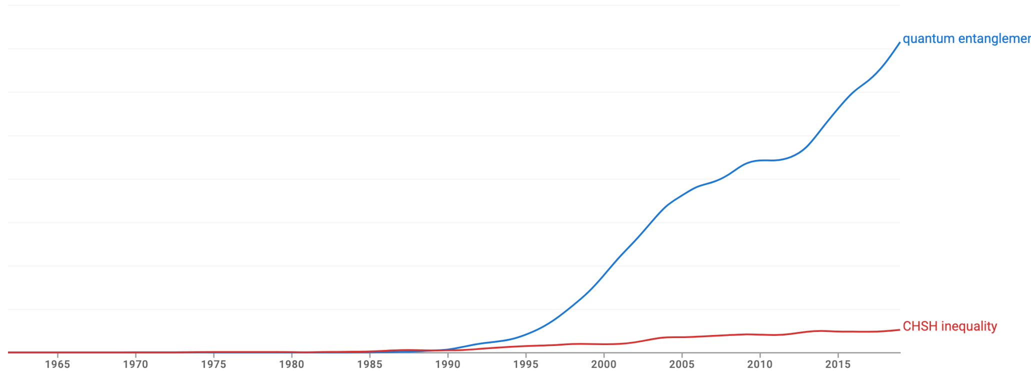
Juan Yin[1,2,3], Yu-Huai Li[1,2,3], Sheng-Kai Liao[1,2,3], Meng Yang[1,2,3], Yuan Cao[1,2,3], Liang Zhang[2,3,4], Ji-Gang Ren[1,2,3], Wen-Qi Cai[1,2,3], Wei-Yue Liu[1,2,3], Shuang-Lin Li[1,2,3], Rong Shu[2,3,4], Yong-Mei Huang[5], Lei Deng[6], Li Li[1,2,3], Qiang Zhang[1,2,3], Nai-Le Liu[1,2,3], Yu-Ao 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] ✉

Crypto helps quantum foundations



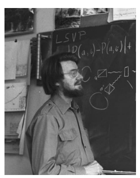
1935

1972

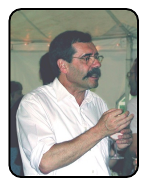


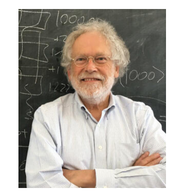
curiosity

1964



1982



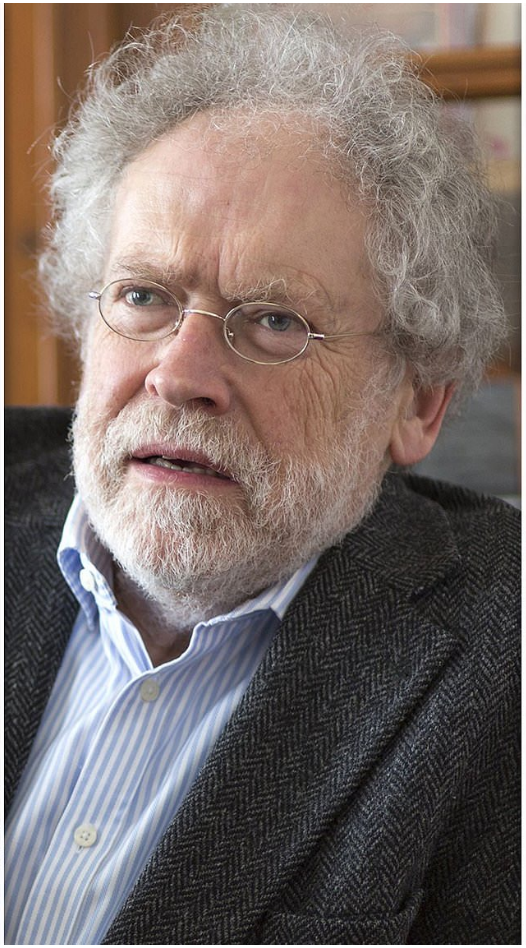
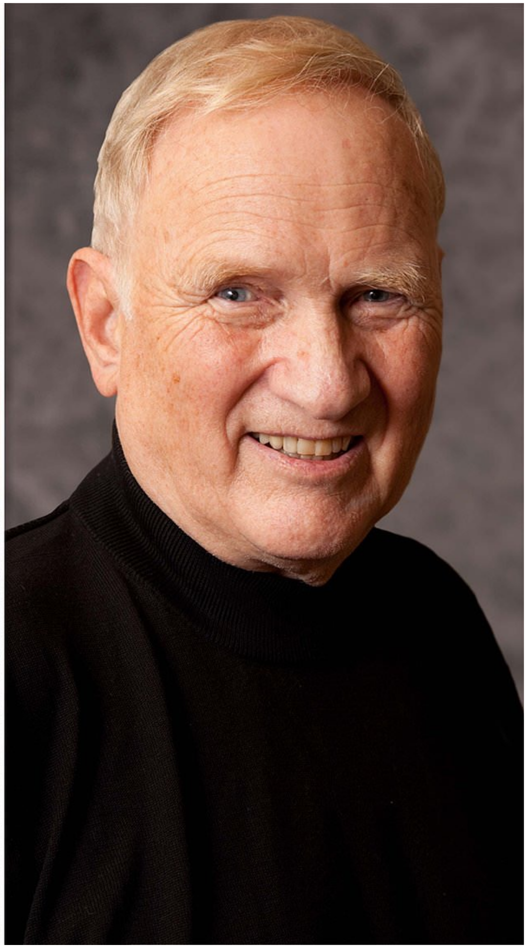


E91

security

BB84

Nobel 2022

End of worries?

You need perfect randomness, right ?