The ultimate limits of privacy and randomness…

…for the paranoid ones

Artur Ekert

Outline

- Is there a perfect cipher?
- Key distribution – the holy grail of cryptography
- Quantum physics comes to the rescue
- Less reality more security

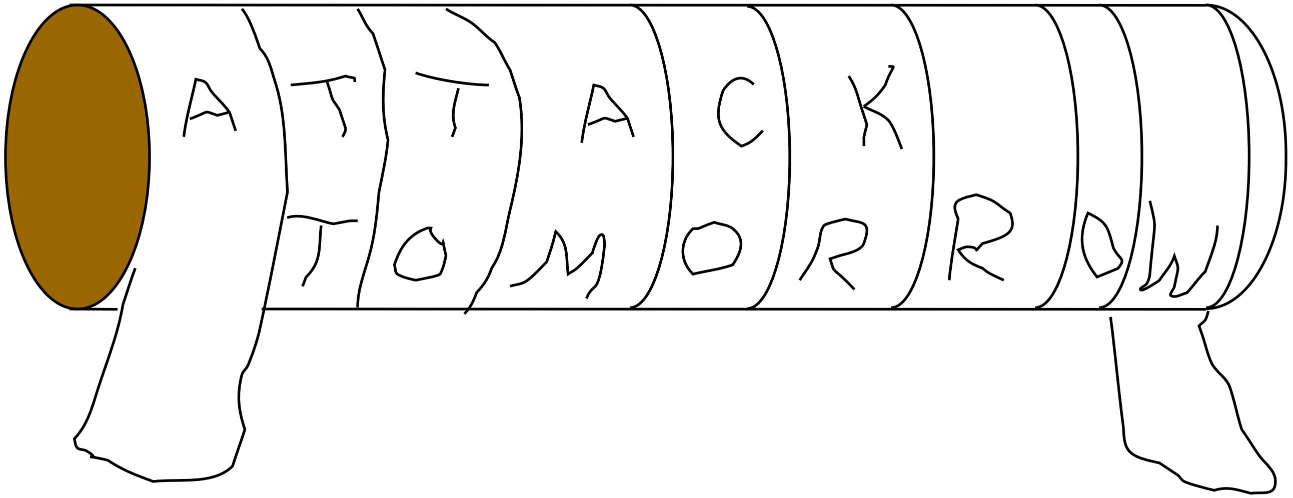
Basic techniques

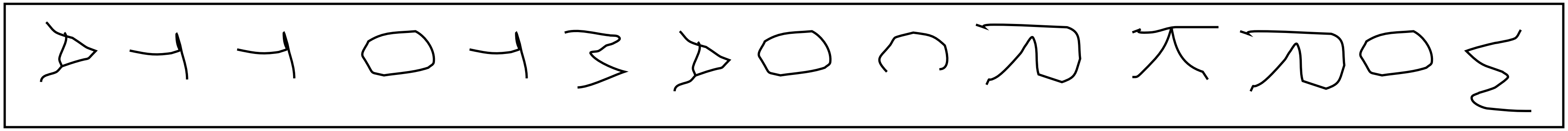
- PERMUTATIONS
  - SCYTALE (400 BC)
- SUBSTITUTIONS
  - CAESAR SIPHER (50 BC)
- PERMUTATIONS + SUBSTITUTIONS

Scytale

400 BC

SPARTA





Permutation of characters

Caesar ciphers

50 BC
ROME

ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ

ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC

ATTACK TOMORROW
DWWDFN WRPRUURZ

Code-makers versus code-breakers

Julius Caesar
(100-44 BC)

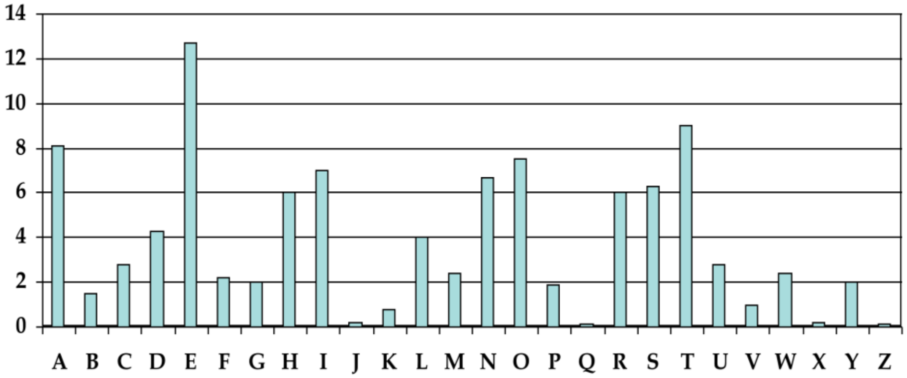
ABCDEFGHIJKLMNOPQRSTUVWXYZ

⇓

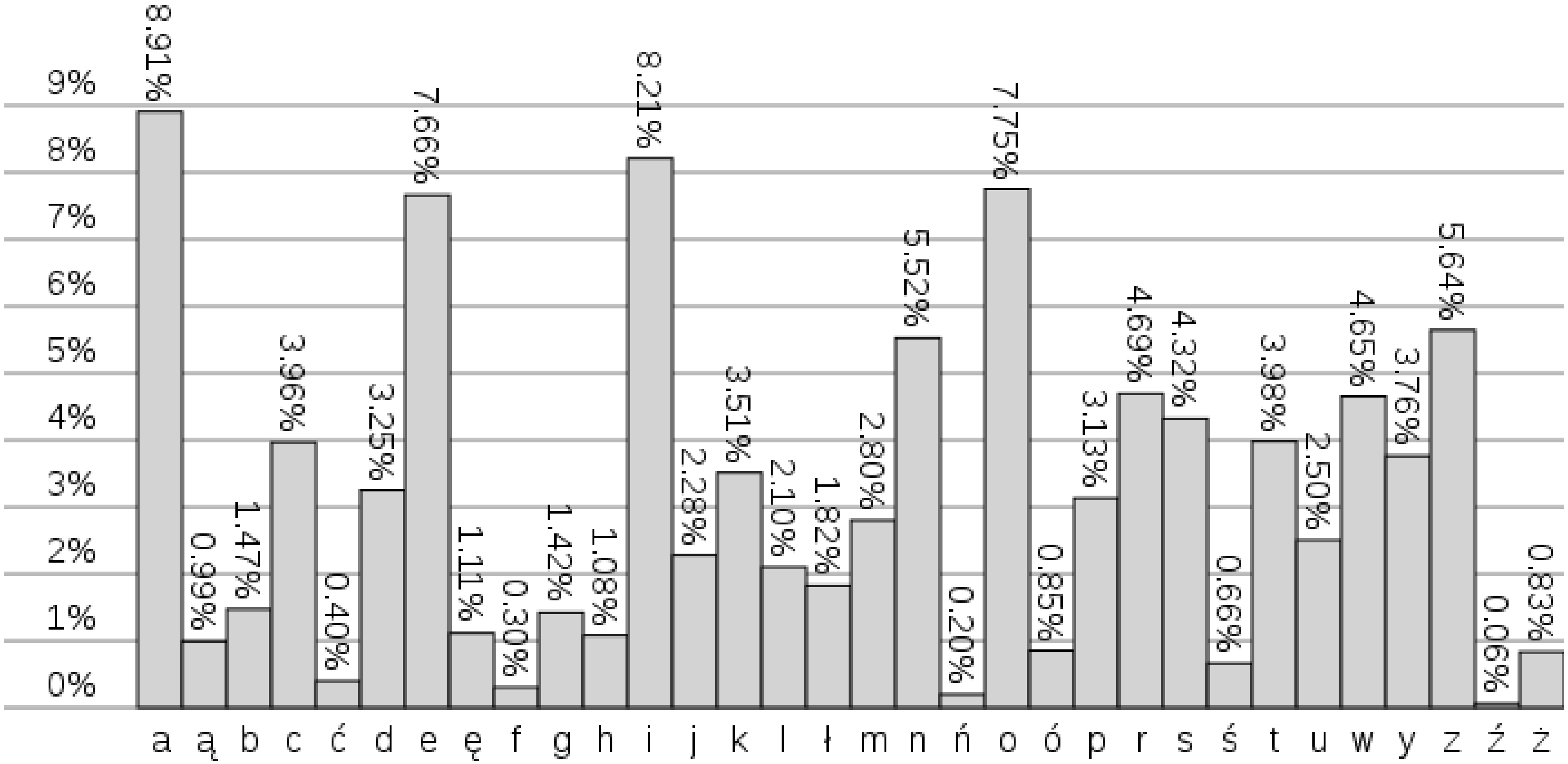
NWDEAPYFGTIJUKLMOZQRSBVCXH

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

Al Kindi
(800-873)



Frequency of letters in Polish



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…

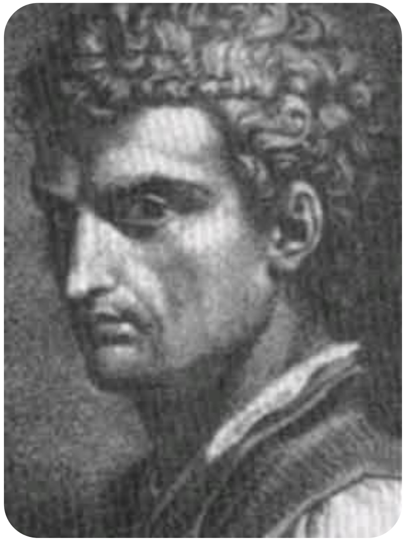
Lipograms in Polish

Najbardziej znany polski lipogram został stworzony przez Juliana Tuwima i zamieszczony w tomie "Pegaz dęba". W utworze tym ani razu nie pojawia się litera "r", co widać w przytoczonym fragmencie:

"Słońce tego dnia wstało jakieś dziwnie leniwe, matowe, bez blasku. Około południa na powleczone niezwykłą bladością niebo wypełzły zwały skłębionych żółtych obłoków i w jednej chwili świat zasnuł się ciemnością".

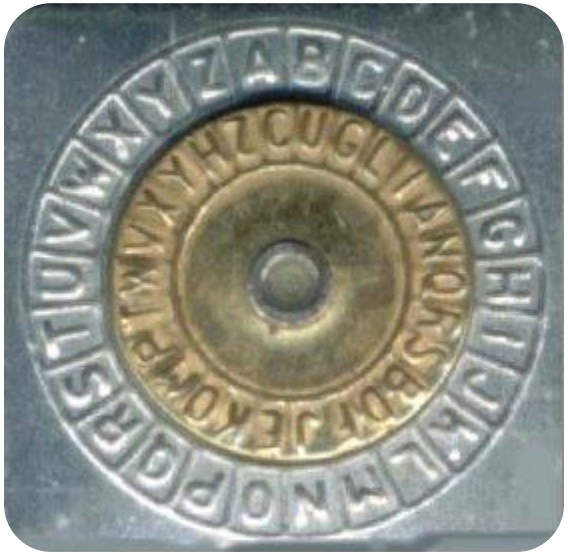
Polyalphabetic ciphers

CODEMAKERS



Leone Battista Alberti
(1404-1472)

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



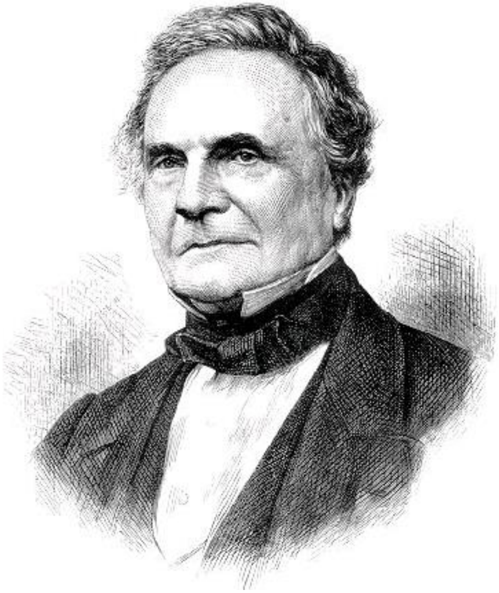
Alberti's encryption disk

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

Plaintext: **S E L L**

Cryptogram: **Z S E S**

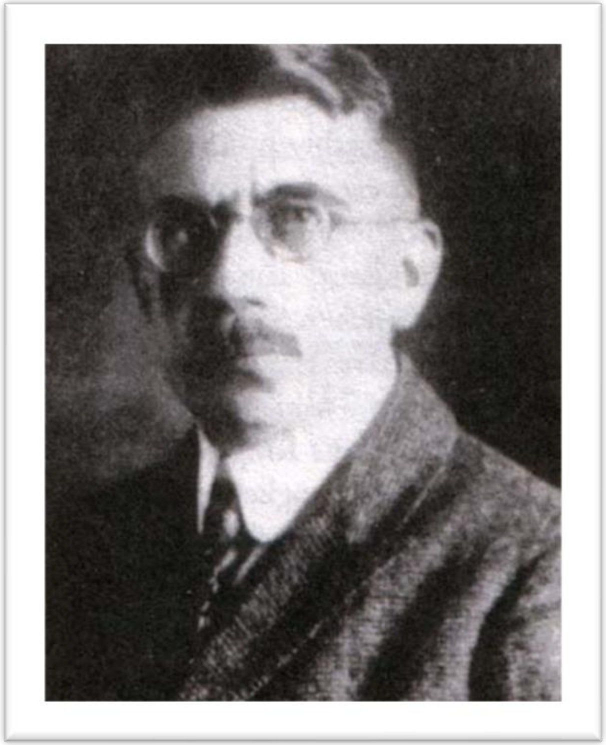
CODEBREAKERS



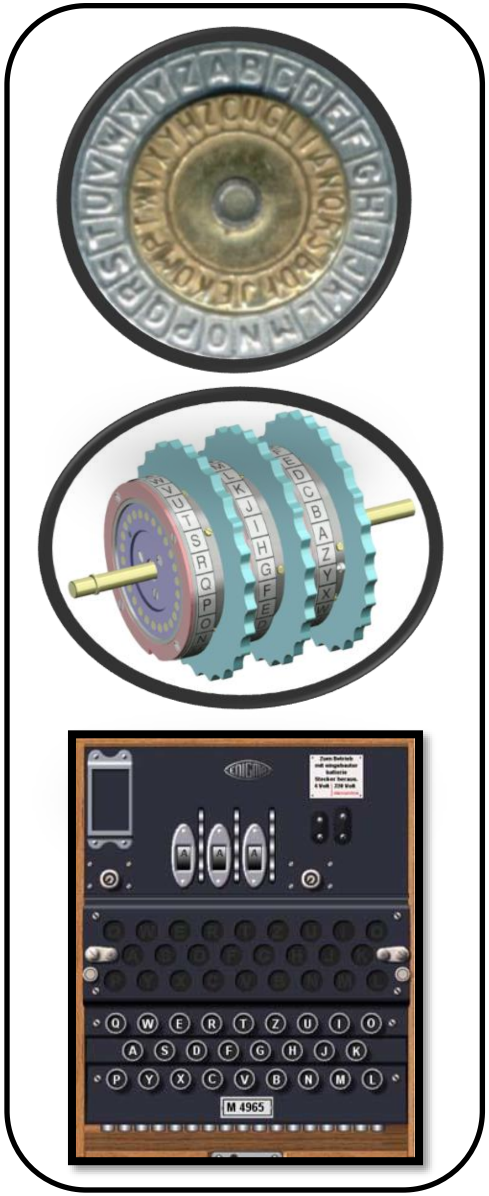
Charles Babbage
(1791-1871)

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)

Henryk Zygalski.

Jerzy Różycki

Marian Rejewski

Maksymilian Ciężki

Gwido Langer

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

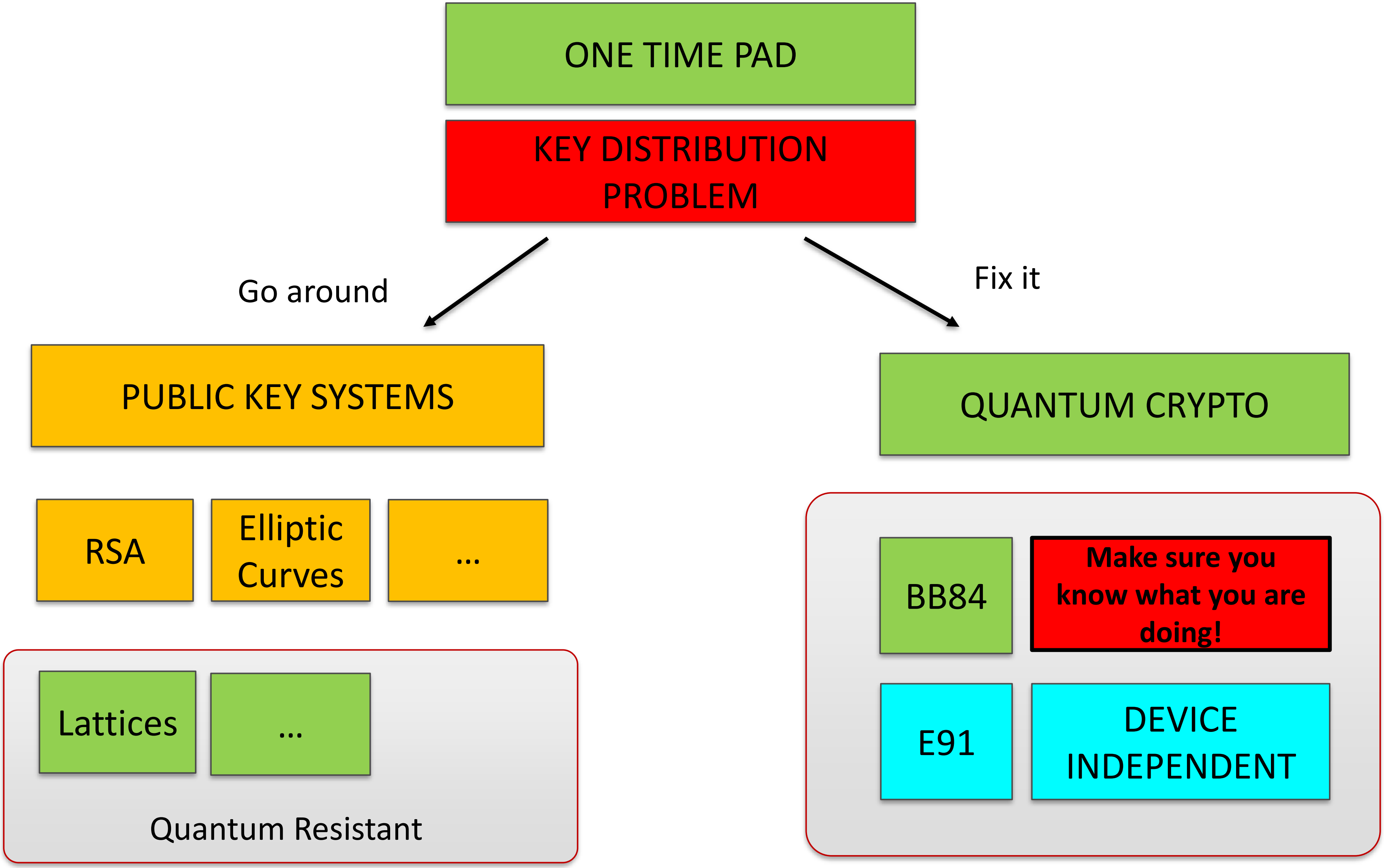
→

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

Quest for perfect secrecy



ONE TIME PAD

KEY DISTRIBUTION PROBLEM

Go around

Fix it

PUBLIC KEY SYSTEMS

RSA

Elliptic Curves

…

Lattices

…

Quantum Resistant

QUANTUM CRYPTO

BB84

Make sure you know what you are doing!

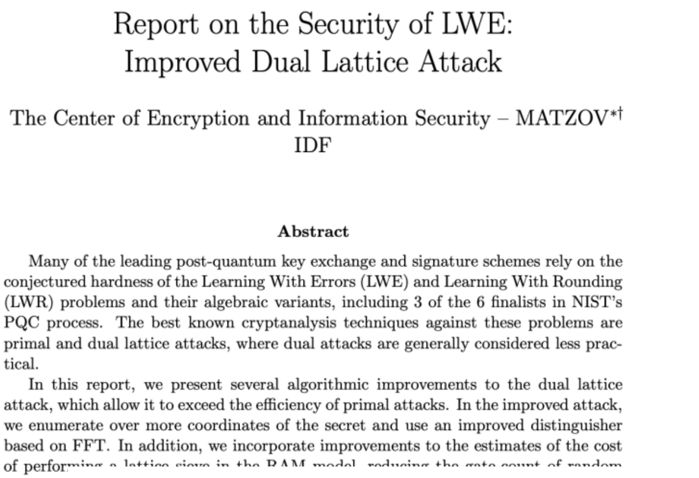
E91

DEVICE INDEPENDENT

Look it up - your homework 😃

- Public key cryptosystems: RSA, elliptic curves and lattice based

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.

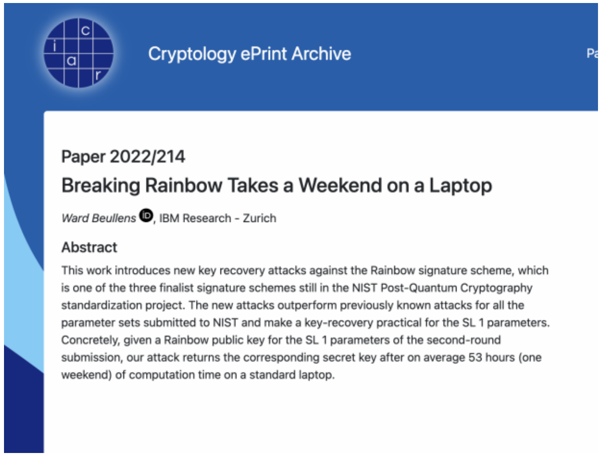
In this report, we present several algorithmic improvements to the dual lattice attack, which allow it to exceed the efficiency of primal attacks. In the improved attack, we enumerate over more coordinates of the secret and use an improved distinguisher based on FFT. In addition, we incorporate improvements 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



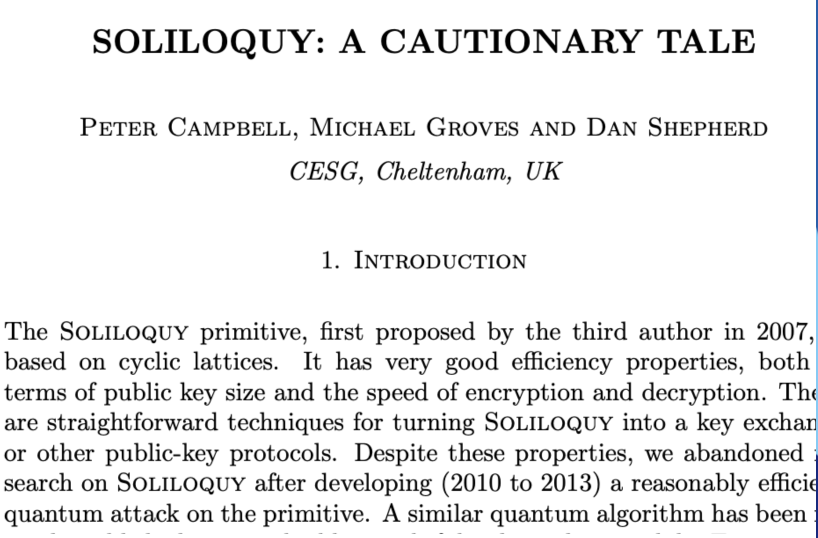
Paper 2022/214

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.

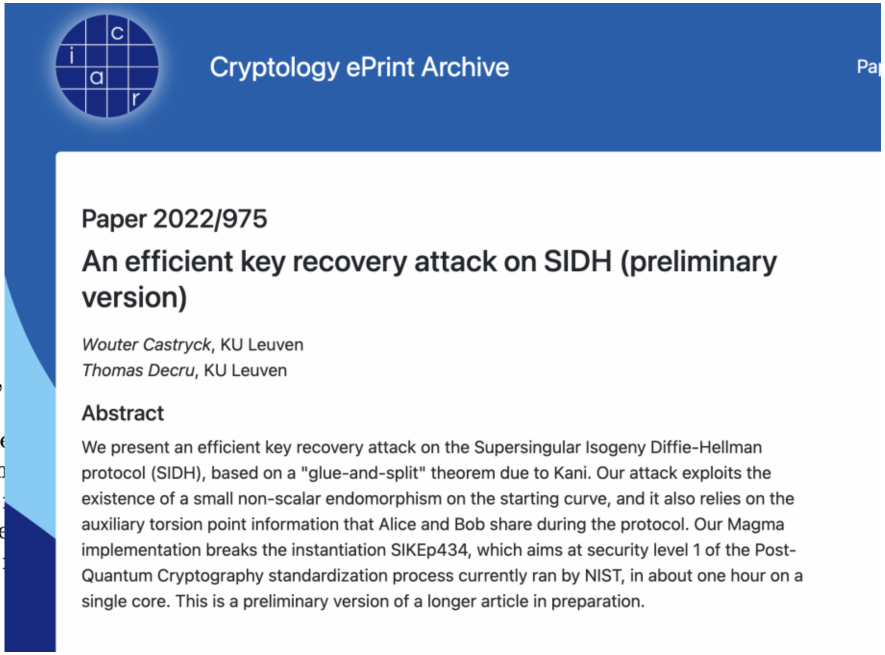


SOLILOQUY: A CAUTIONARY TALE

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 efficie quantum attack on the primitive. A similar quantum algorithm has been



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

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

BASIC IDEA

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

$$X_1 X_2 \leftrightarrow Z = X_1 \oplus X_2$$

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

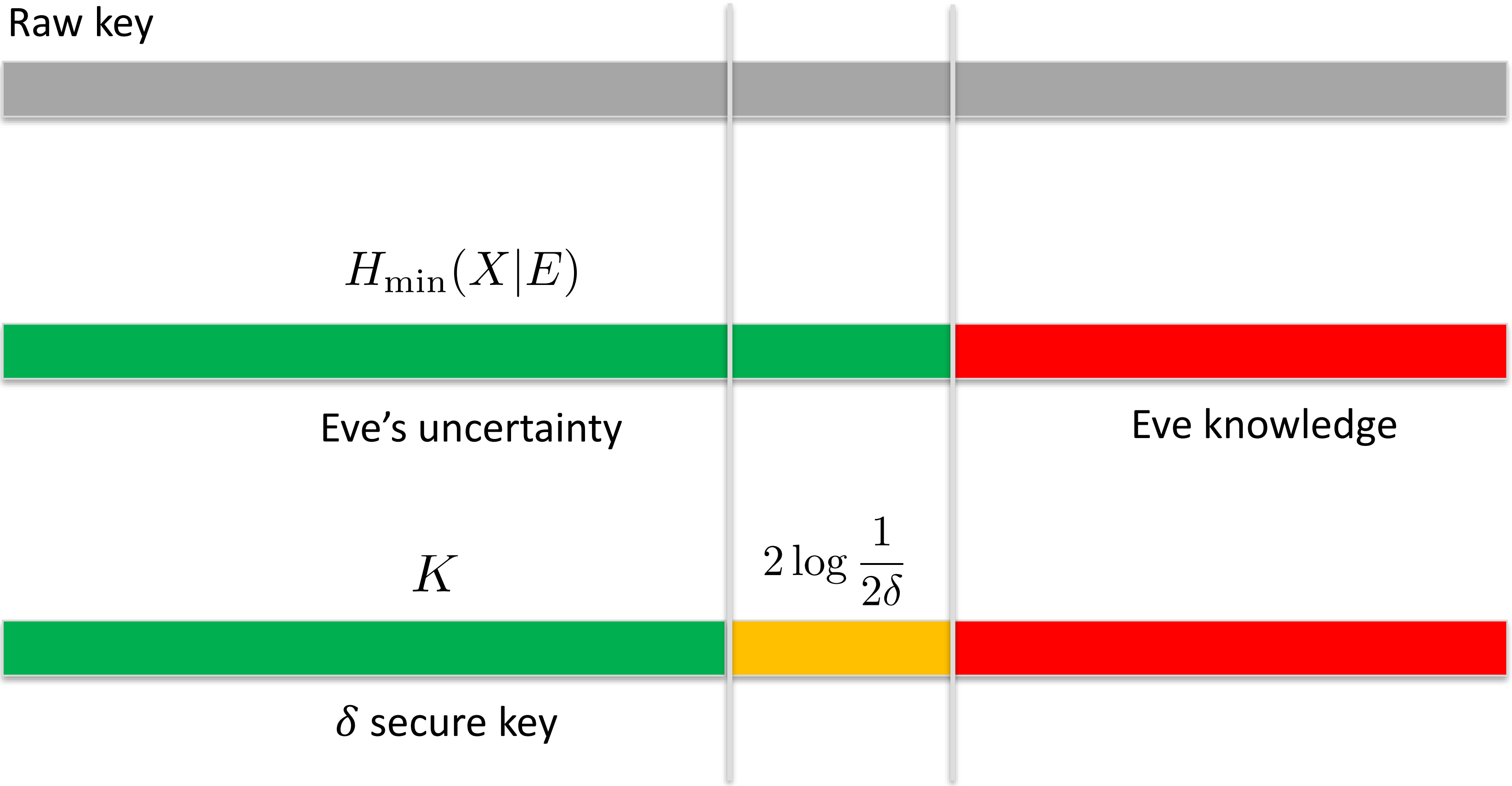
0	1	0	1	1	1	0	0	1	0

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

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

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

The Leftover Hash Lemma



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

Look it up - your homework 😃

- Public key cryptosystems: RSA, elliptic curves and lattice based
- Randomness extractors and privacy amplification
- Why cryptographers use min-entropy rather than Shannon entropy?
- Define security using Kolmogorov / trace distance between probability distributions

How to find out how much Eve knows?

0	1	0	1	1	1	0	0	1	0

X

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

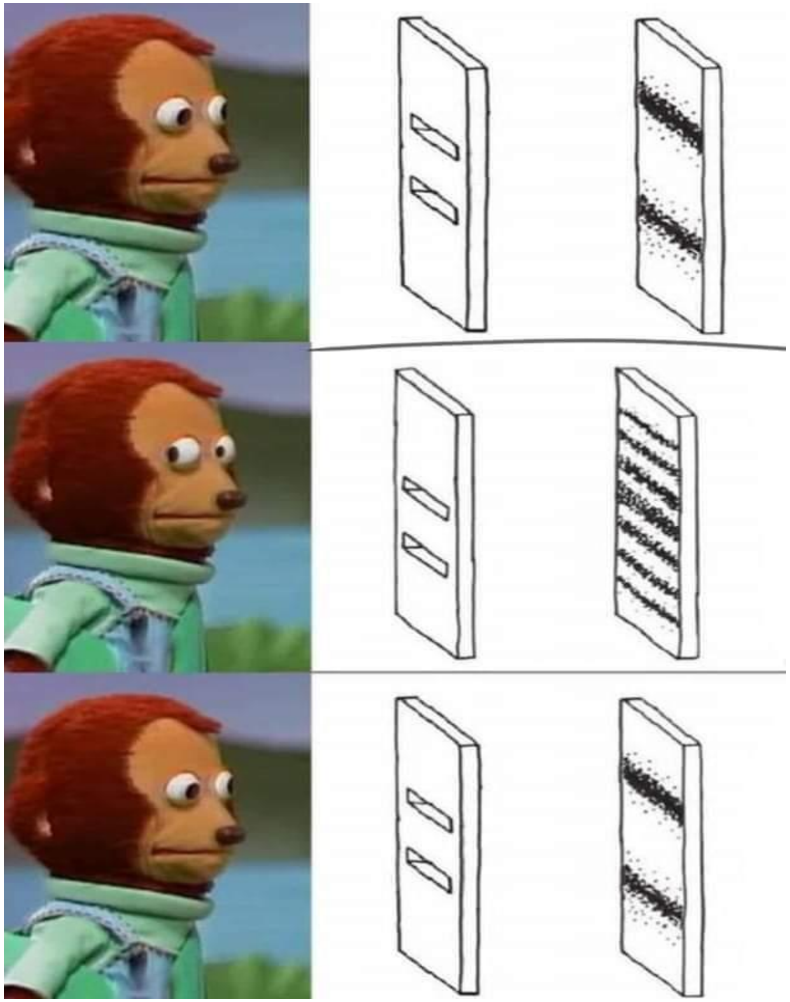
0	1	0	1	1	1	0	0	1	0

X

0	?	?	1	?	0	0	?	?	?

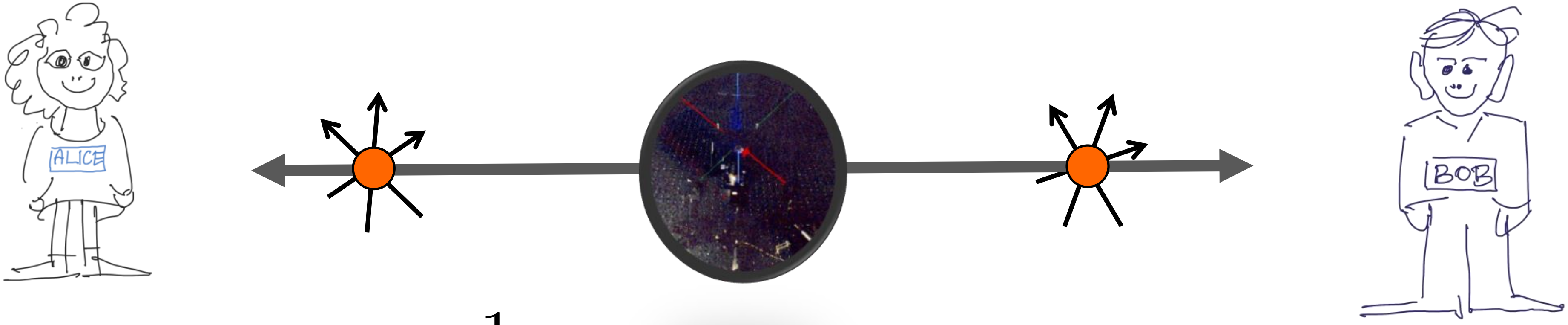
E

Why quantum in cryptography?



“Watching” does make a difference

Use entanglement!



$$\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$$

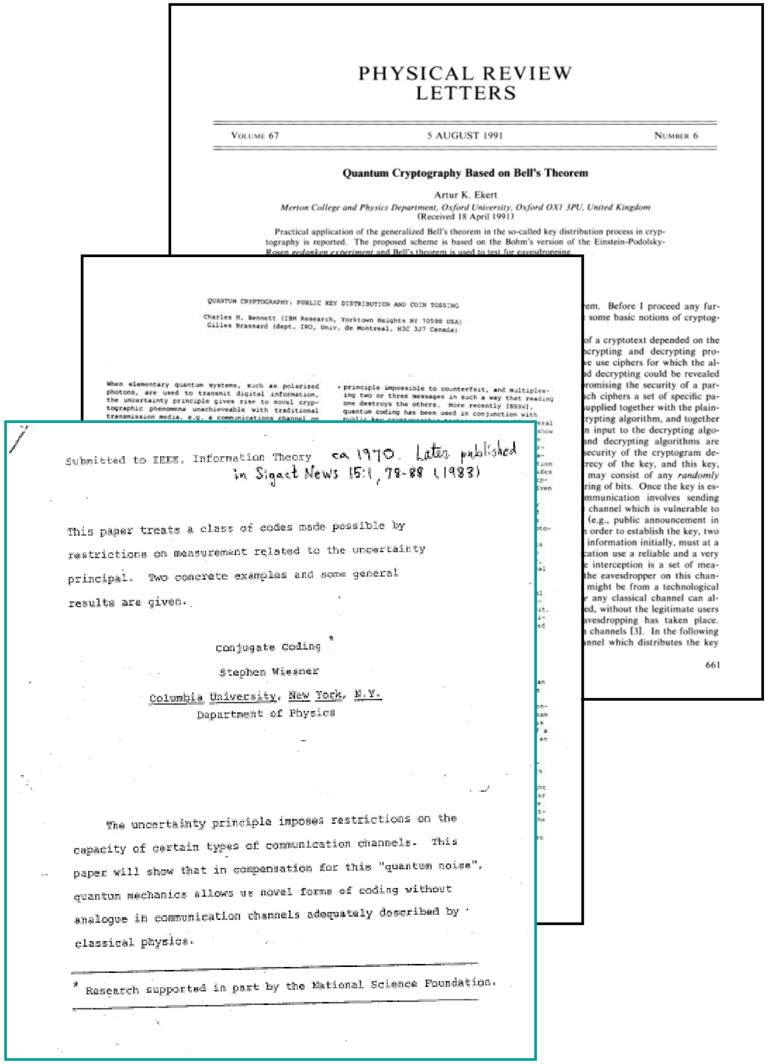
$$\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) \otimes |e\rangle$$

$$\frac{1}{\sqrt{2}}(|0\rangle|0\rangle \otimes |e_0\rangle + |1\rangle|1\rangle \otimes |e_1\rangle)$$

Look it up - your homework 😀

- Public key cryptosystems: RSA, elliptic curves and lattice based
- Randomness extractors and privacy amplification
- Why cryptographers use min-entropy rather than Shannon entropy?
- Define security using Kolmogorov / trace distance between probability distributions
- Quantum entanglement

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.

em. Before I proceed any fur-
some basic notions of cryptog-

of a cryptotext depended on the
ncrypting and decrypting pro-
ve use ciphers for which the al-
d decrypting could be revealed
romising the security of a par-
ch ciphers a set of specific pa-
upplied together with the plain-
rypting algorithm, and together
n input to the decrypting algo-
and decrypting algorithms are
security of the cryptogram de-
recy of the key, and this key,
may consist of any *randomly*
ring of bits. Once the key is es-
mmunication involves sending
channel which is vulnerable to
(e.g., public announcement in
n order to establish the key, two
information initially, must at a
cation use a reliable and a very
e interception is a set of mea-
the eavesdropper on this chan-
might be from a technological
e any classical channel can al-
ed, without the legitimate users
avesdropping has taken place.
n channels [3]. In the following
nnel which distributes the key

661

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)

When elementary quantum systems, such as polarized photons, are used to transmit digital information, the uncertainty principle gives rise to novel cryptographic phenomena unachieveable with traditional transmission media, e.g. a communications channel on

principle impossible to counterfeit, and multiplexing two or three messages in such a way that reading one destroys the others. More recently [BBBW], quantum coding has been used in conjunction with

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.

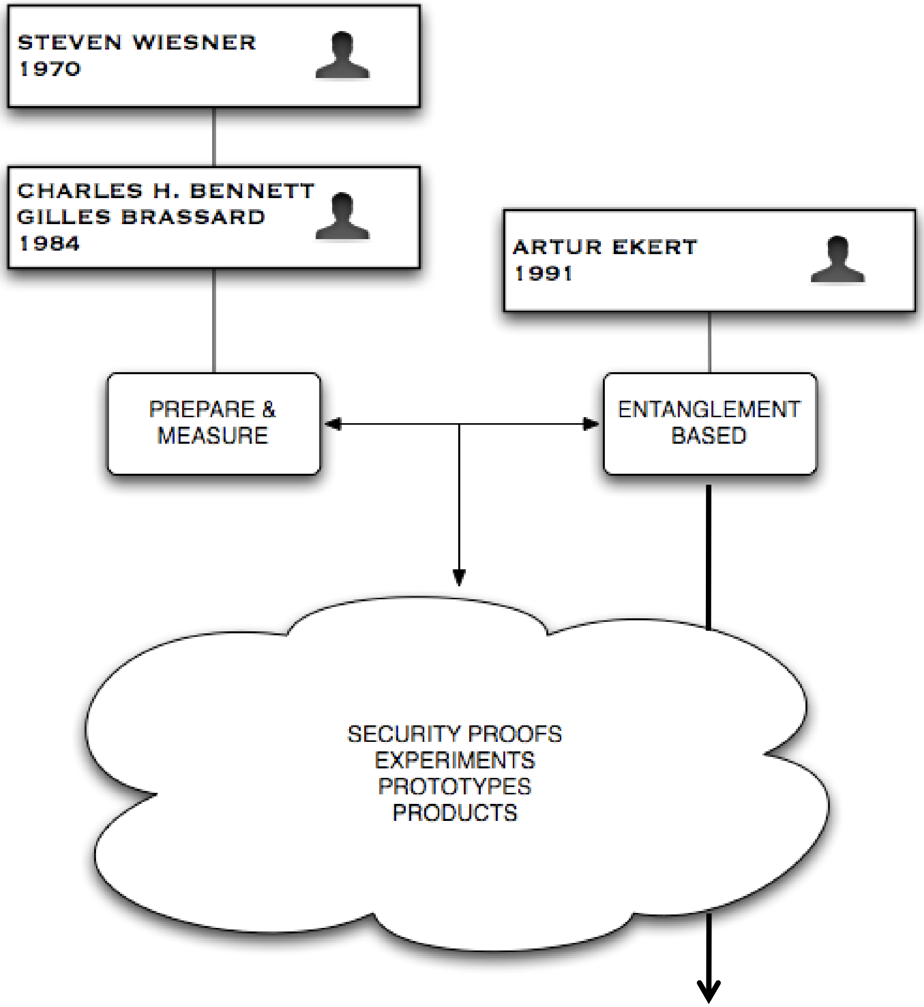
Conjugate Coding *

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.



STEVEN WIESNER
1970

CHARLES H. BENNETT
GILLES BRASSARD
1984

ARTUR EKERT
1991

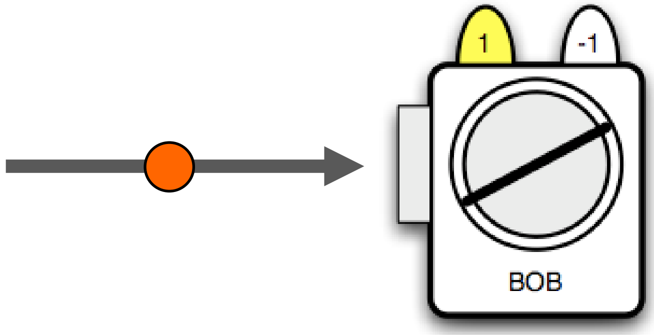
PREPARE & MEASURE

ENTANGLEMENT BASED

SECURITY PROOFS
EXPERIMENTS
PROTOTYPES
PRODUCTS

Device independence etc

Polarization

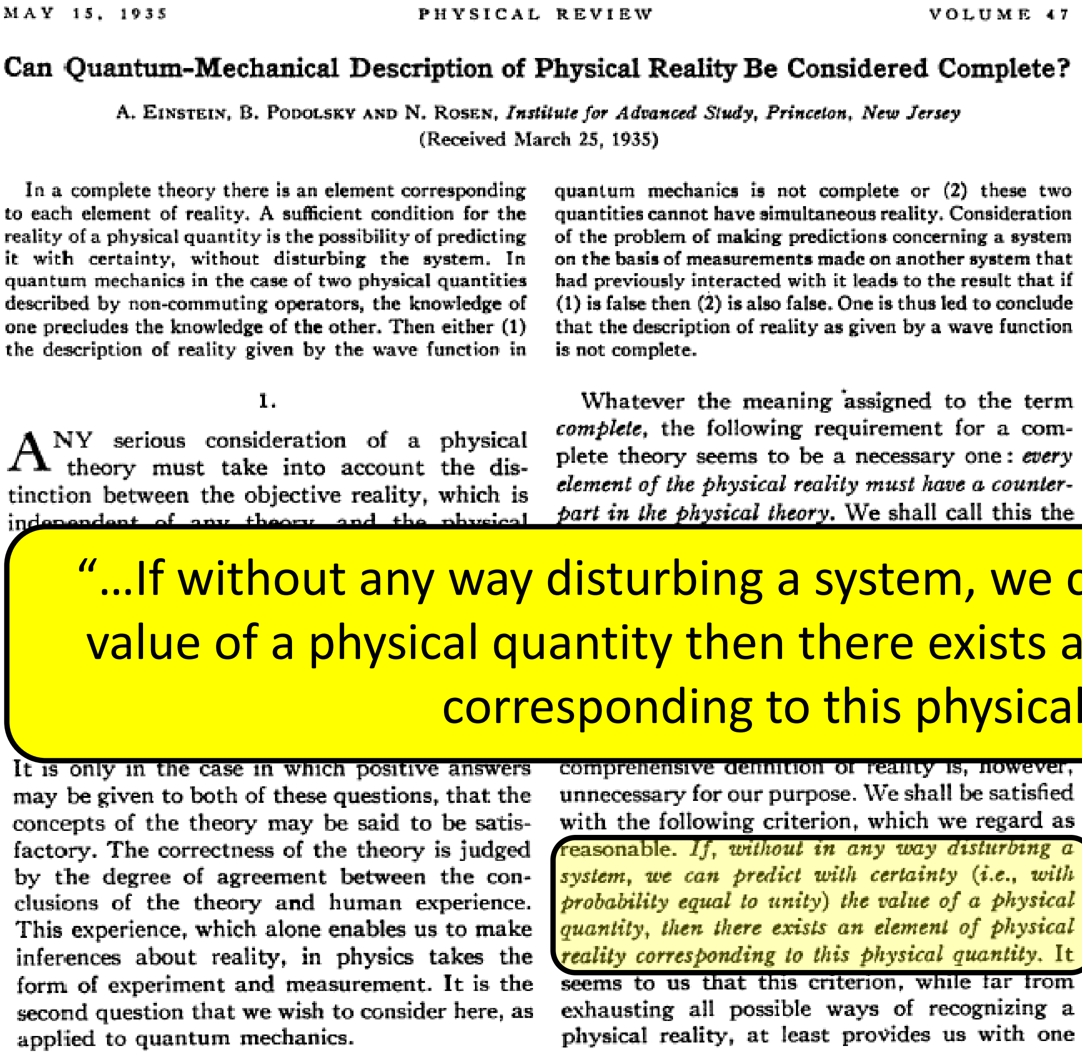


POLARIZATION IS AN INTRINSIC PROPERTY OF A PHOTON

WE CANNOT JUST “MEASURE POLARIZATION” - WE CAN ONLY MEASURE POLARIZATION WITH RESPECT TO SOME SPECIFIED DIRECTION

IN ANY MEASUREMENT WE CAN GET ONLY TWO RESULTS: +1 OR -1

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.

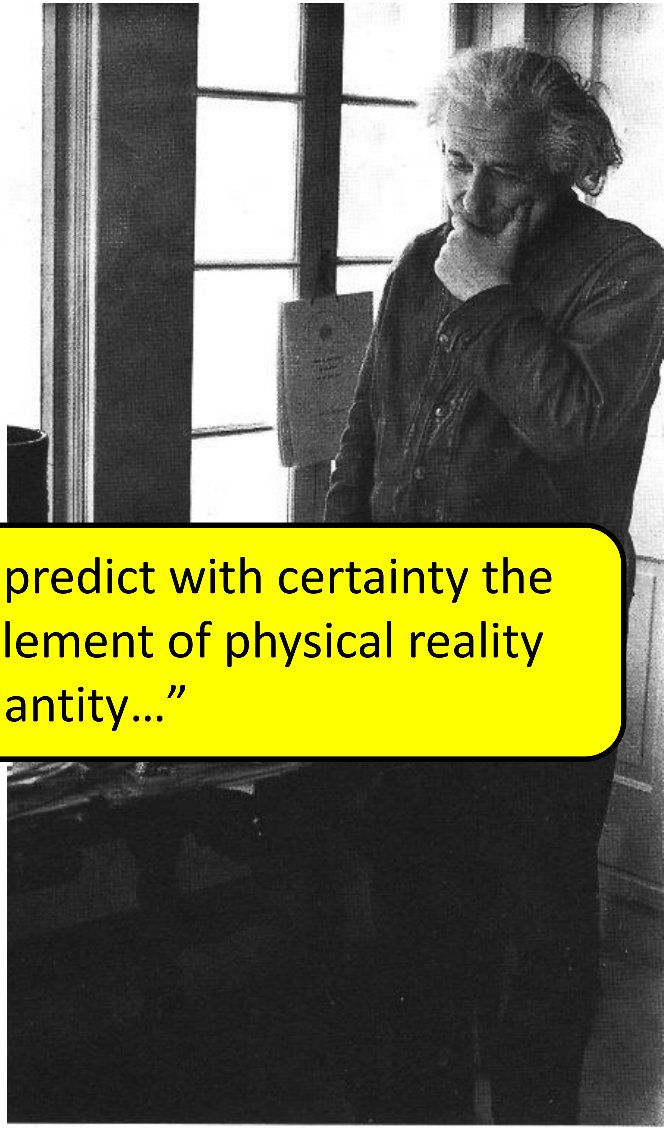
ANY serious consideration of a physical theory must take into account the distinction between the objective reality, which is independent of any theory, and the physical

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

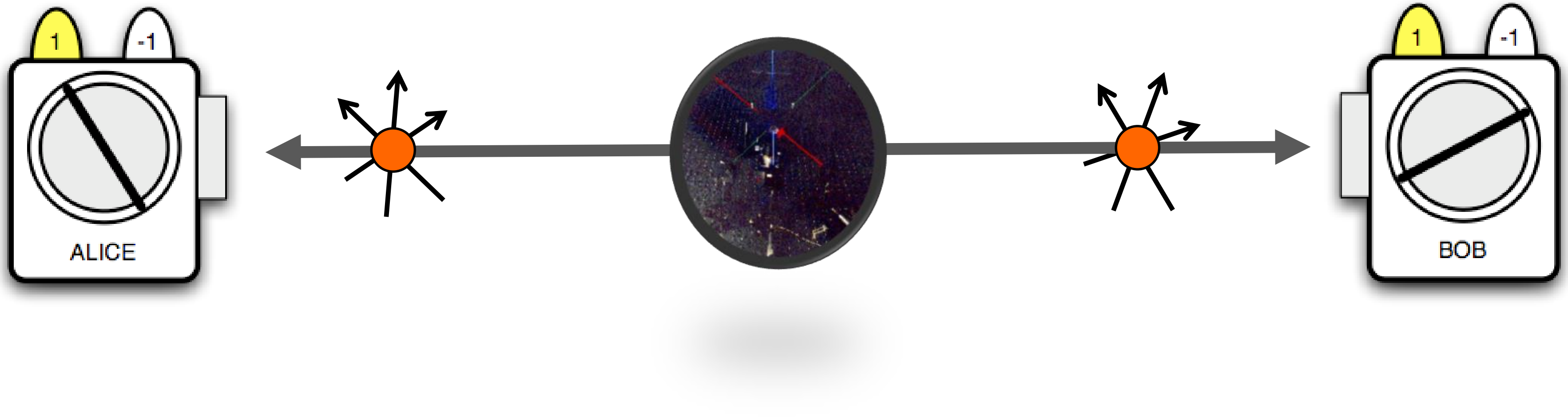
comprehensive definition of reality is, however, unnecessary for our purpose. We shall be satisfied with the following criterion, which we regard as reasonable. *If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity,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



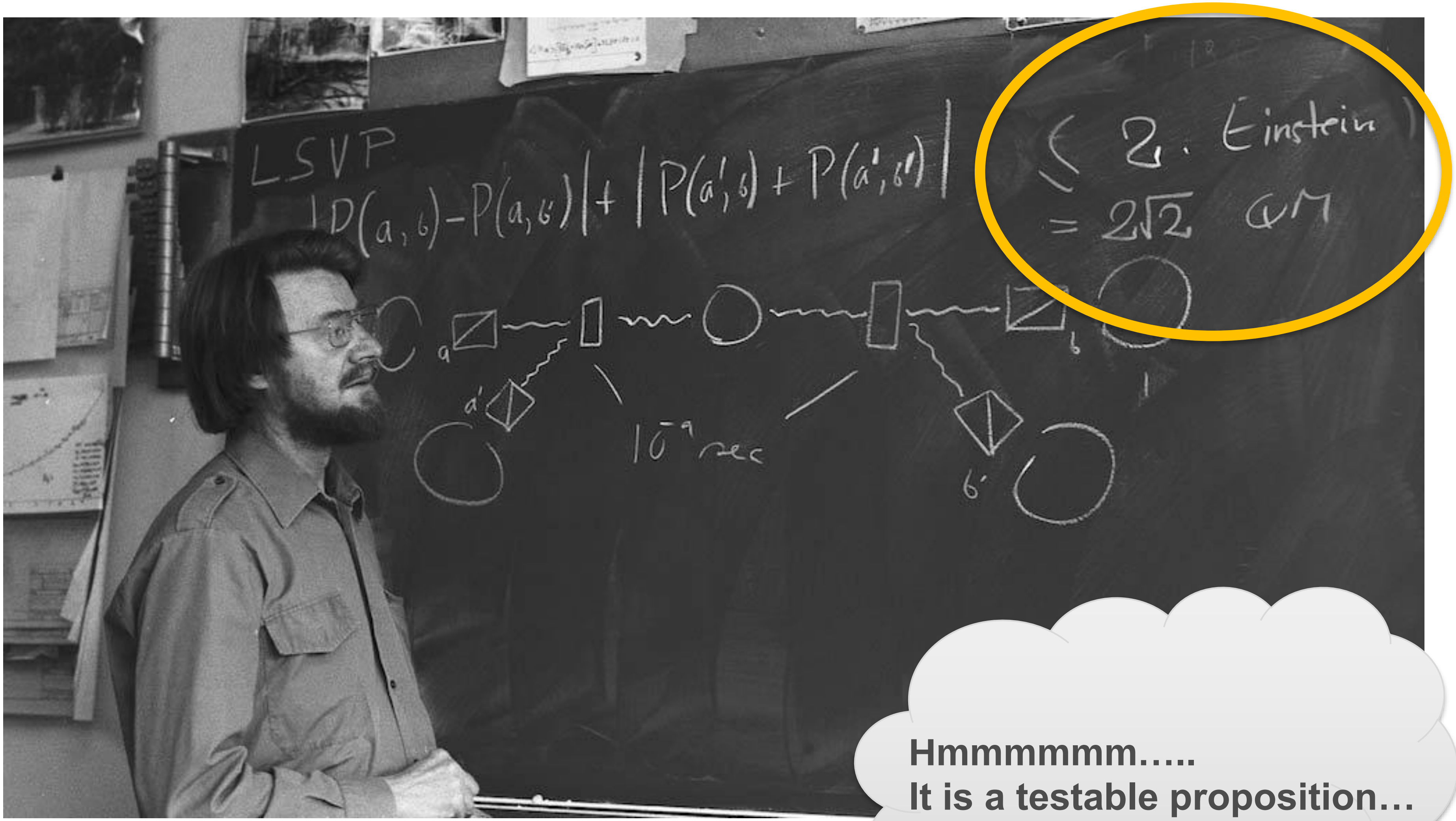
DEFINITION OF EAVESDROPPING

Predetermined or not?



Do photons have predetermined values of polarizations?

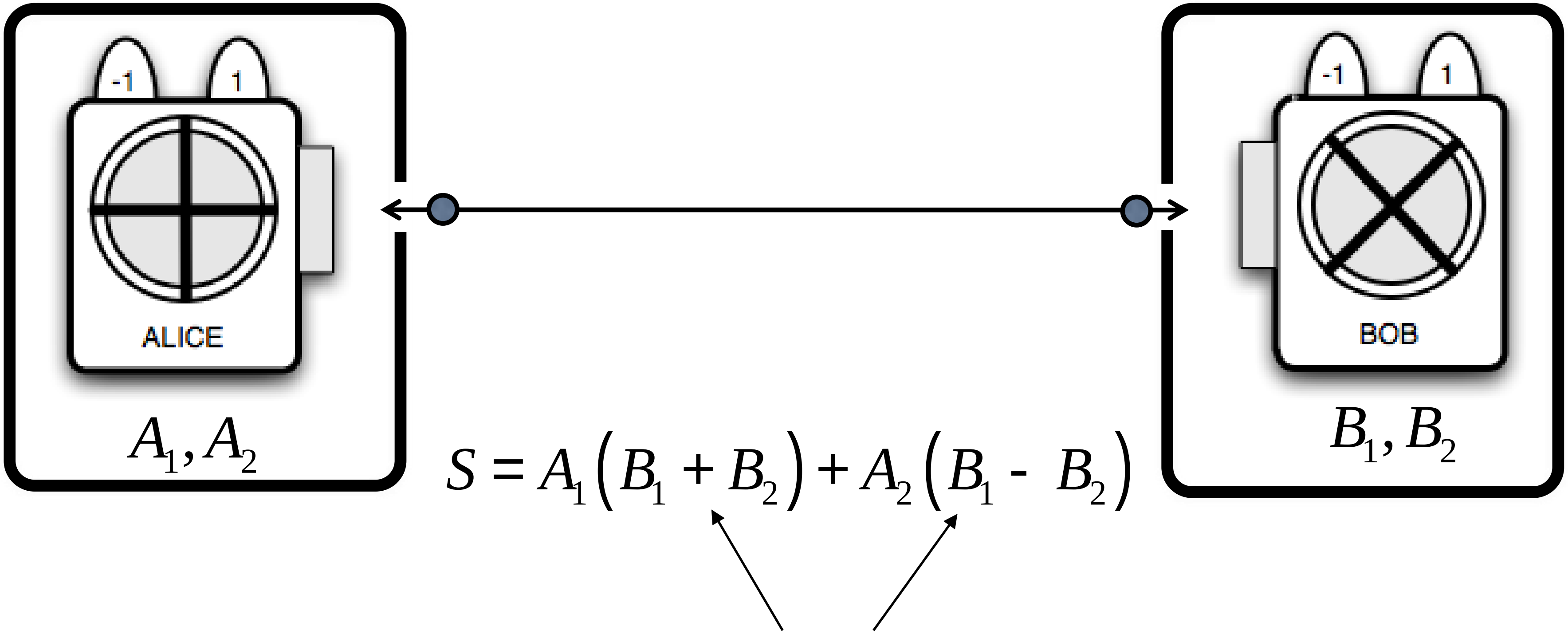
Enter John Bell



Hmmmmmm…..
It is a testable proposition…

year 1964

Bell’s inequalities…

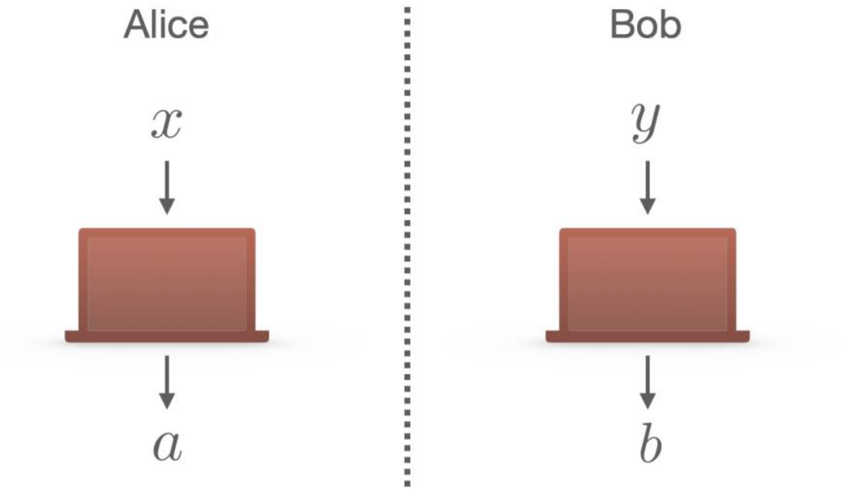


$$S = A_1\left(B_1 + B_2\right) + A_2\left(B_1 - B_2\right)$$

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

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

More recent take on Bell’s inequalities



CHSH Game:

Alice:	Input	$x \in \{0,1\}$
	Output	$a \in \{0,1\}$
Bob:	Input	$y \in \{0,1\}$
	Output	$b \in \{0,1\}$
Win:	$a \oplus b = x \cdot y$	

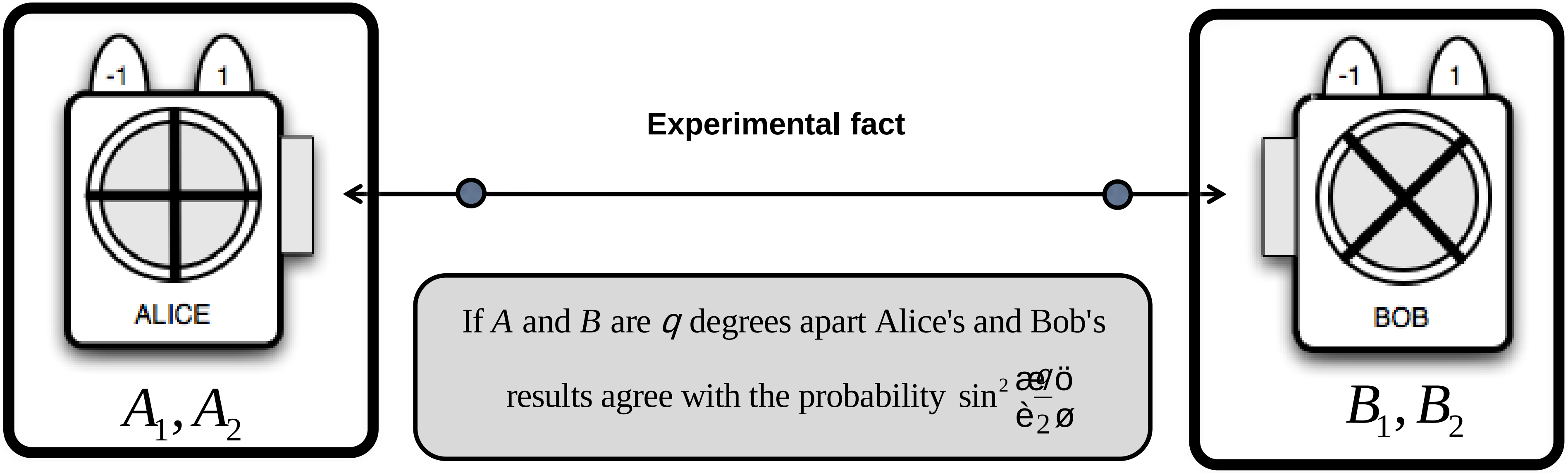
Shared randomness

- Best classical strategy: 75% winning probability $p(ab|xy) = \sum_{\lambda} p(\lambda) p(a|x\lambda) p(b|y\lambda)$
- Best quantum strategy: ~85% winning probability $|\Phi^{+}\rangle_{AB}$

Look it up - your homework 😀

- Public key cryptosystems: RSA, elliptic curves and lattice based
- Randomness extractors and privacy amplification
- Why cryptographers use min-entropy rather than Shannon entropy?
- Define security using Kolmogorov / trace distance between probability distributions
- Quantum entanglement
- CHSH non-local game

Local realism can be refuted…



If A and B are q degrees apart Alice's and Bob's results agree with the probability $\sin^2$ æ$\frac{q}{2}$ö è ø

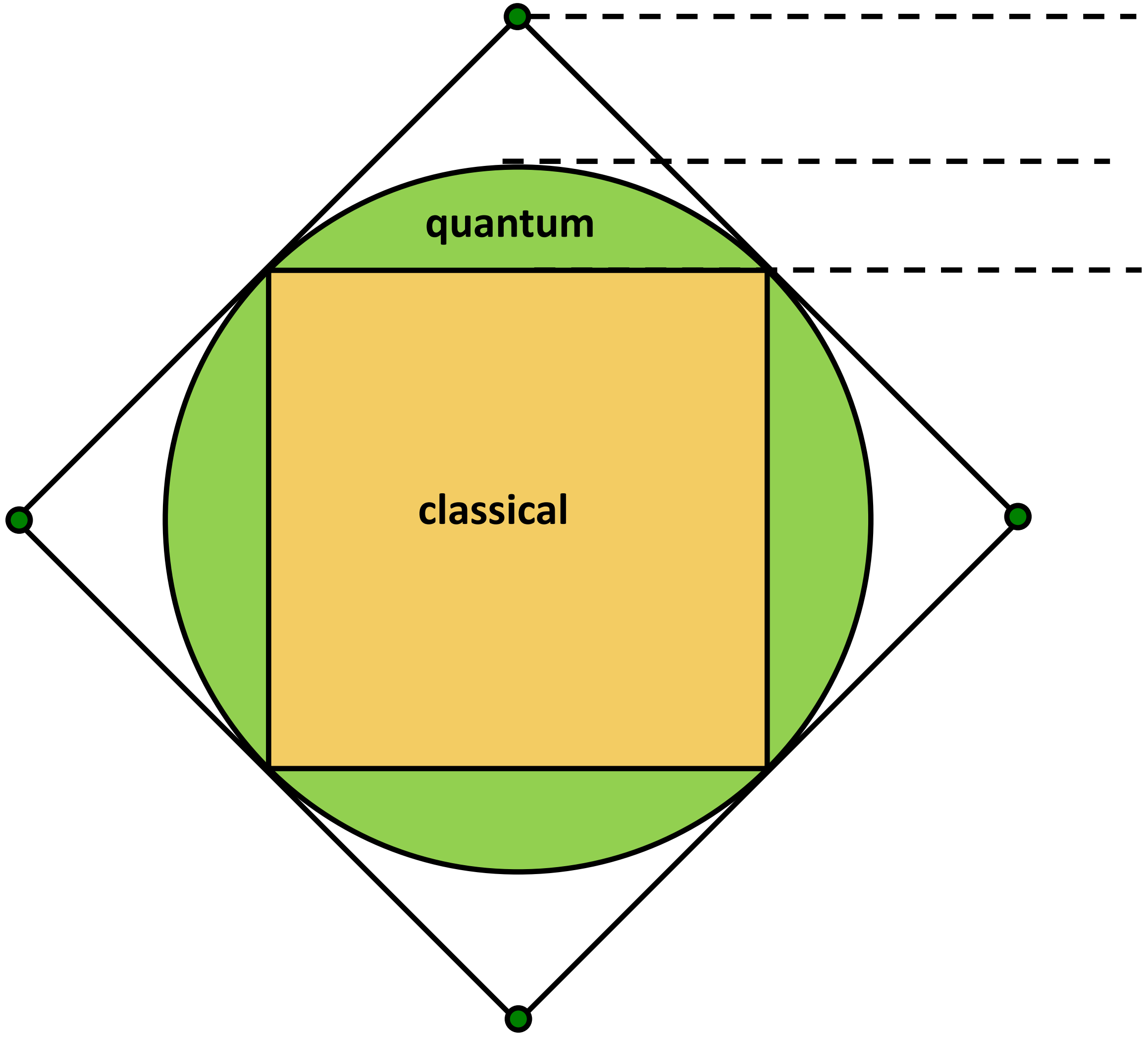
Results agree: $AB = 1$

Results disagree: $AB = -1$

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

$$- 2\sqrt{2} \text{ £ } \langle A_1B_1\rangle - \langle A_1B_2\rangle + \langle A_2B_1\rangle + \langle A_2B_2\rangle \text{ £ } 2\sqrt{2}$$

Correlations galore



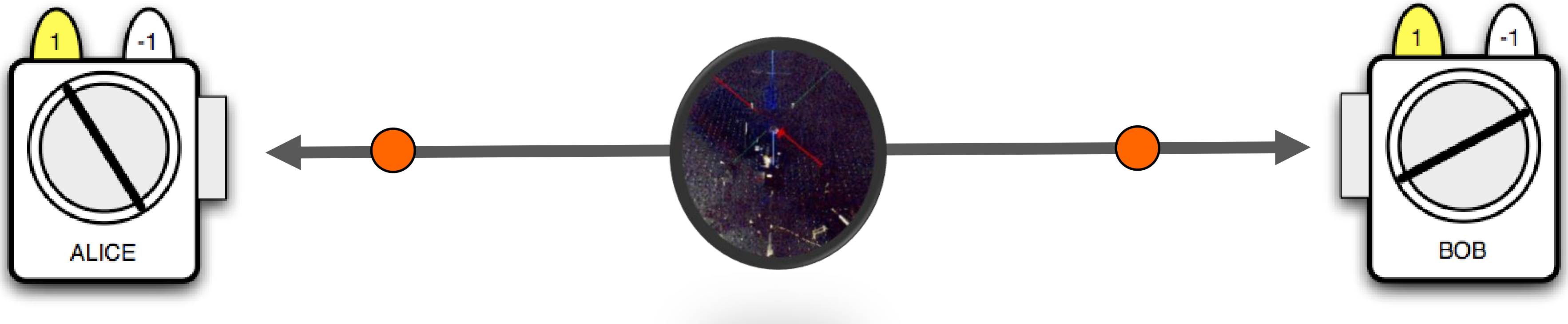
$$|\langle S\rangle| = 4$$

$$|\langle S\rangle| = 2\sqrt{2}$$

$$|\langle S\rangle| = 2$$

Polytope of non-signaling correlations

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

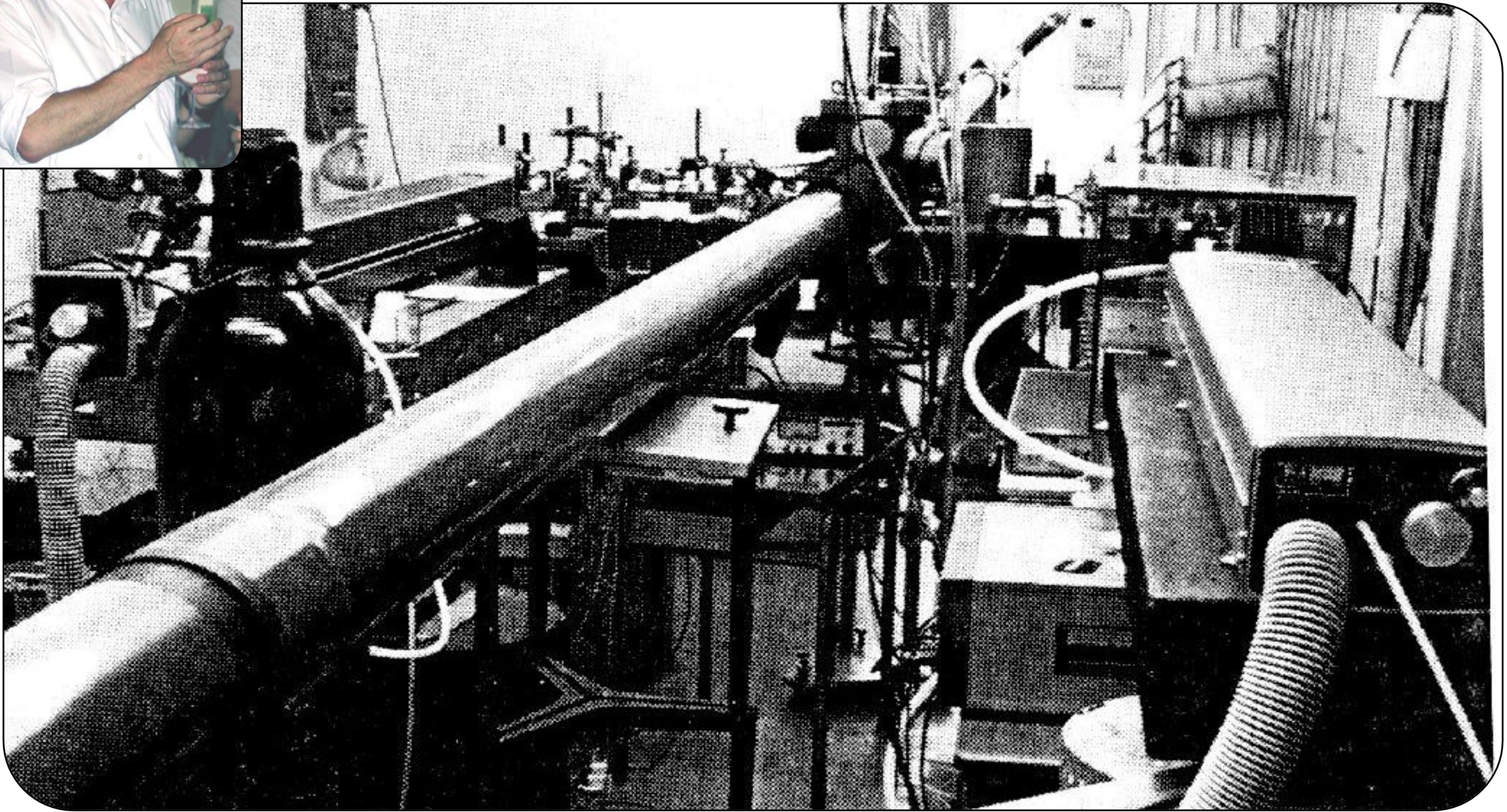
TESTING FOR THE VIOLATION OF BELL'S INEQUALITIES = TESTING FOR EAVESDROPPING

A. Ekert 1991

Alain Aspect and his quantum magic

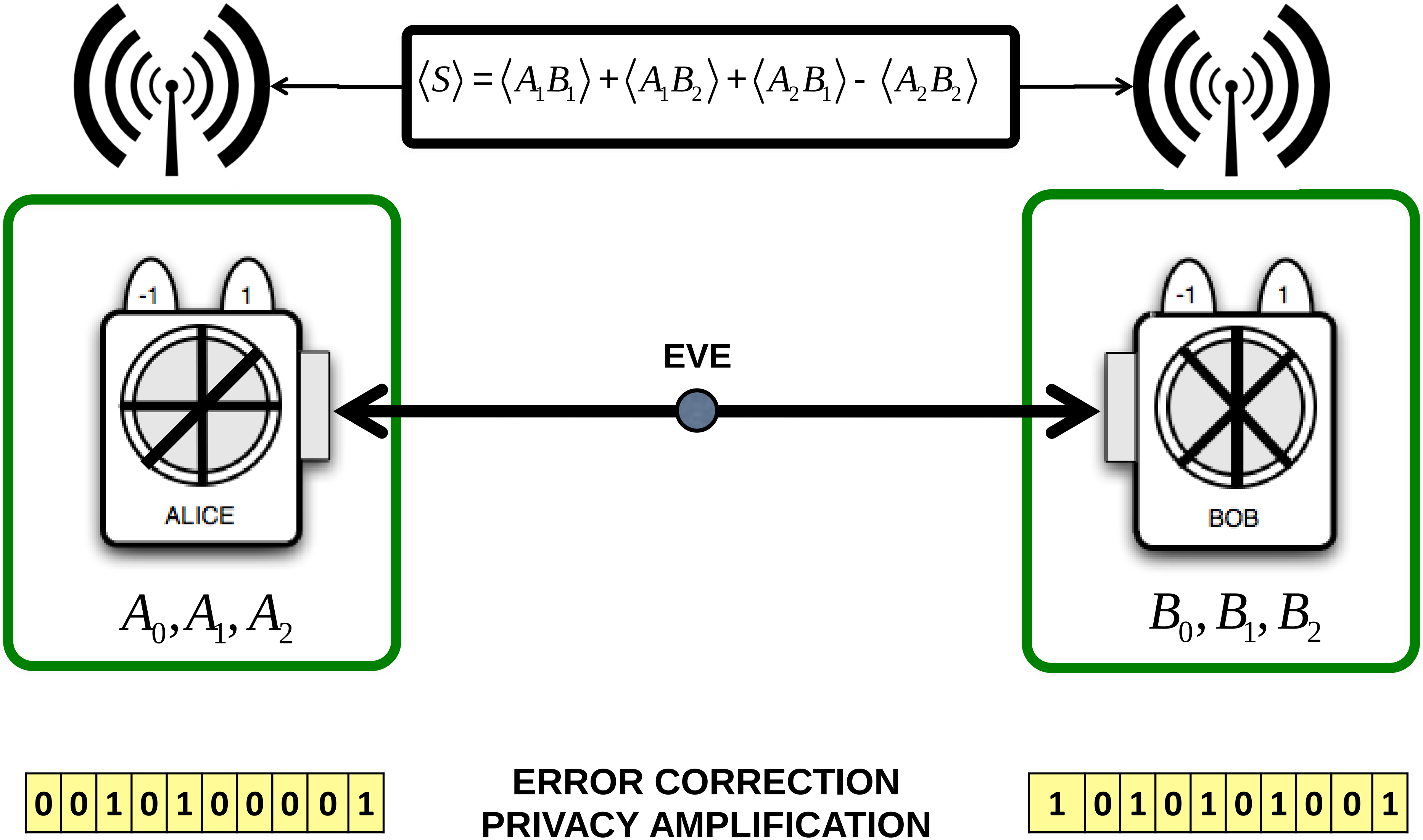
$S > 2$

Et voilà!



Institut d'Optique d'Orsay (1982)

Bell inequalities and security

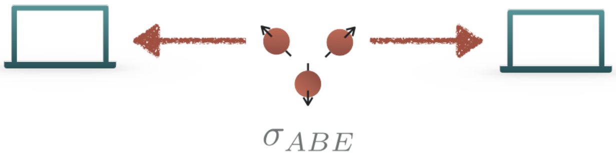


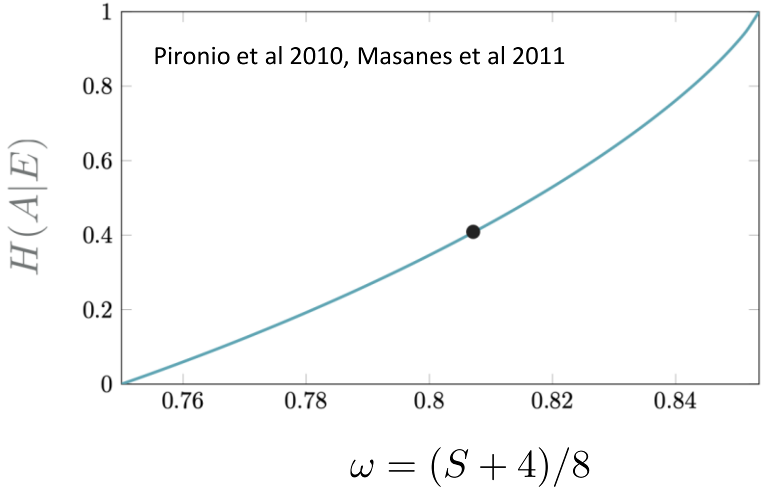
$$\langle S\rangle = \langle A_1 B_1\rangle + \langle A_1 B_2\rangle + \langle A_2 B_1\rangle - \langle A_2 B_2\rangle$$

ERROR CORRECTION
PRIVACY AMPLIFICATION

You need some mathematical gymnastics

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





Pironio et al 2010, Masanes et al 2011

S

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

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

Extractors

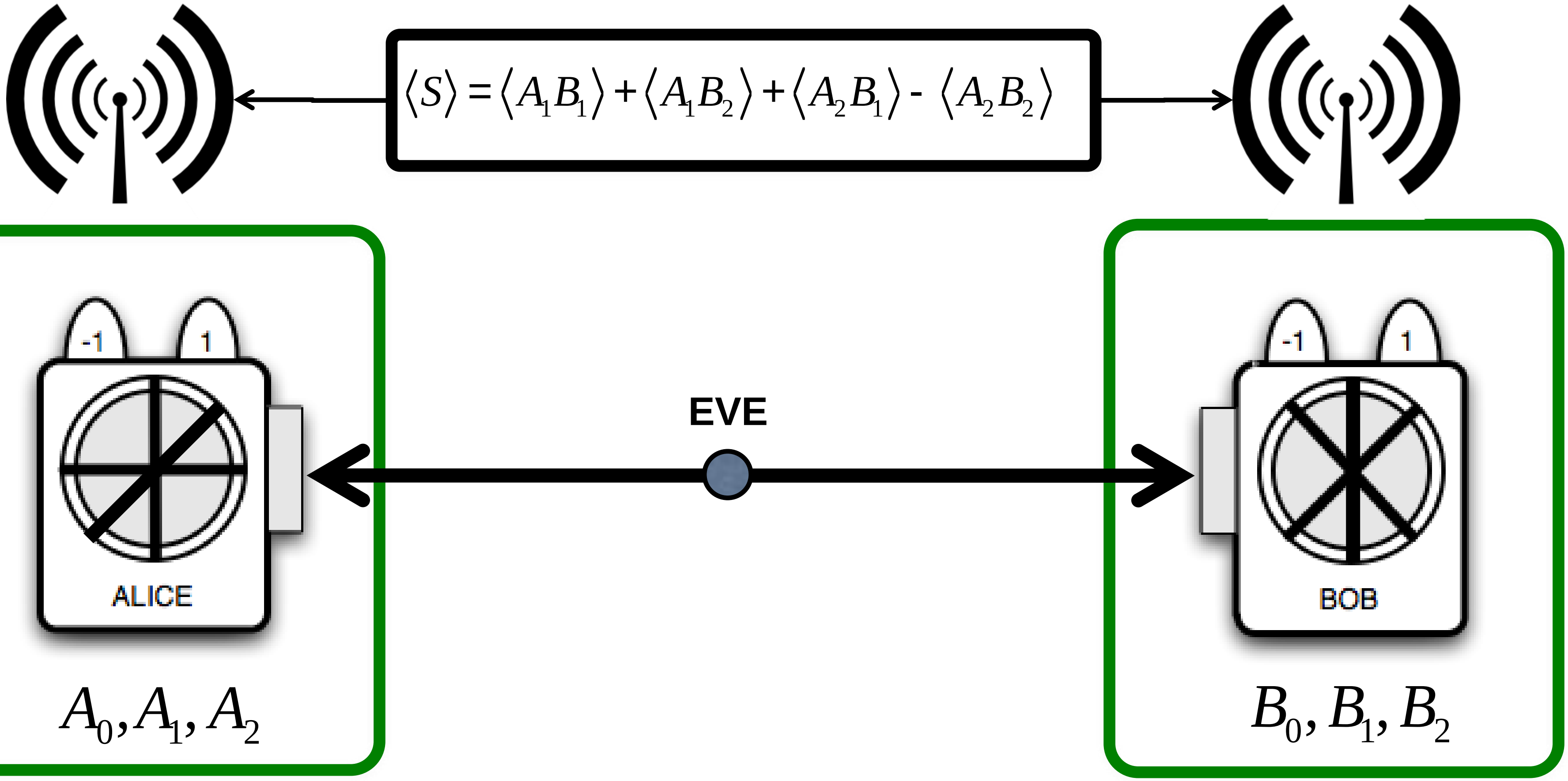
Secret key

Eve distributes the key!

Look it up - your homework 😀

- Public key cryptosystems: RSA, elliptic curves and lattice based
- Randomness extractors and privacy amplification
- Why cryptographers use min-entropy rather than Shannon entropy?
- Define security using Kolmogorov / trace distance between probability distributions
- Quantum entanglement
- CHSH non-local game
- Quantum Asymptotic Equipartition Property for entropy

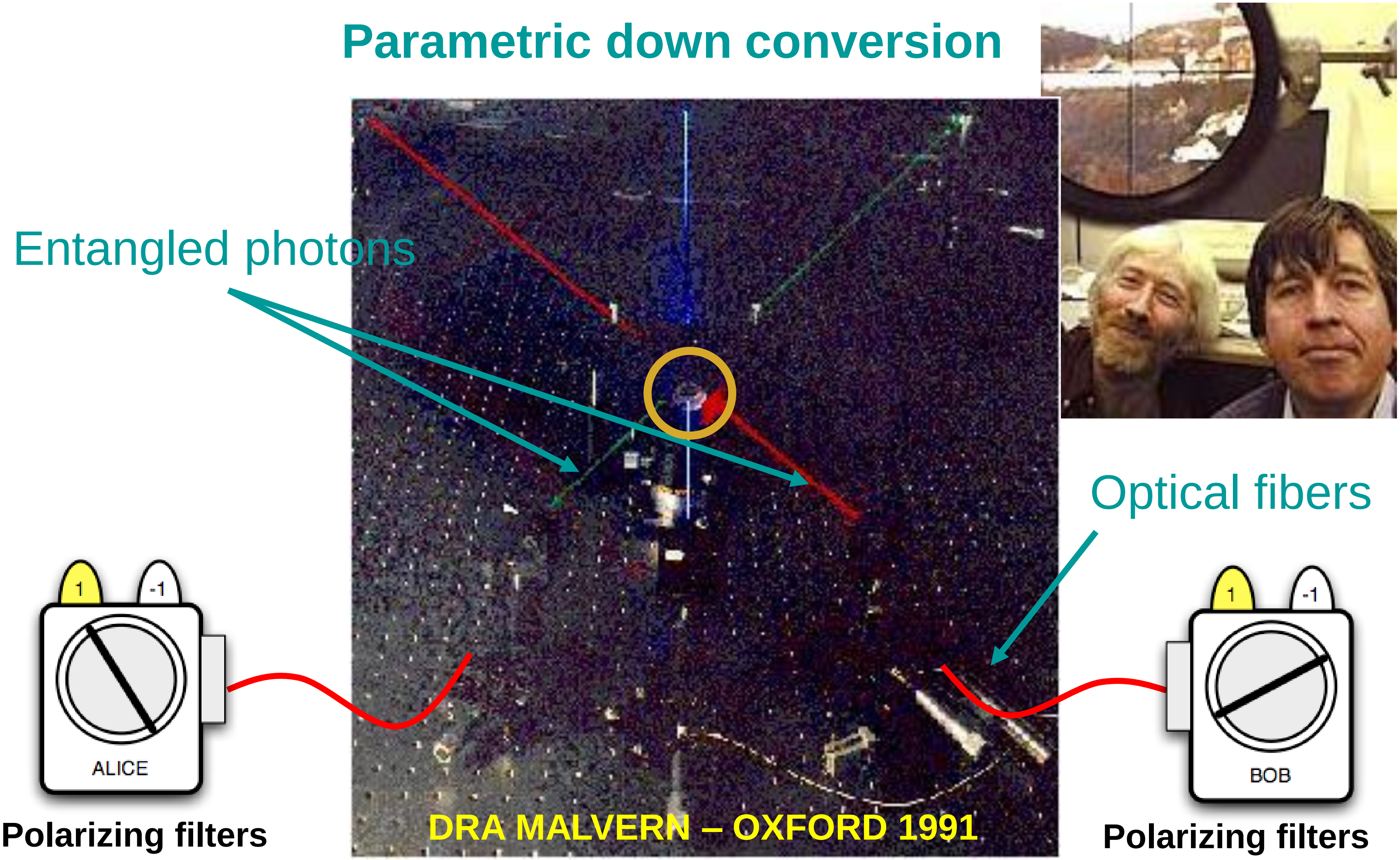
Secure as long as...



$$\langle S\rangle = \langle A_1B_1\rangle + \langle A_1B_2\rangle + \langle A_2B_1\rangle - \langle A_2B_2\rangle$$

- 🟢 **Alice's and Bob's labs are secure - no information leaks**
- 🟡 **Alice and Bob control and trust devices in their labs**
- 🔴 **Alice and Bob have free will and can choose their observables**

And all this can be demonstrated…



Parametric down conversion

Entangled photons

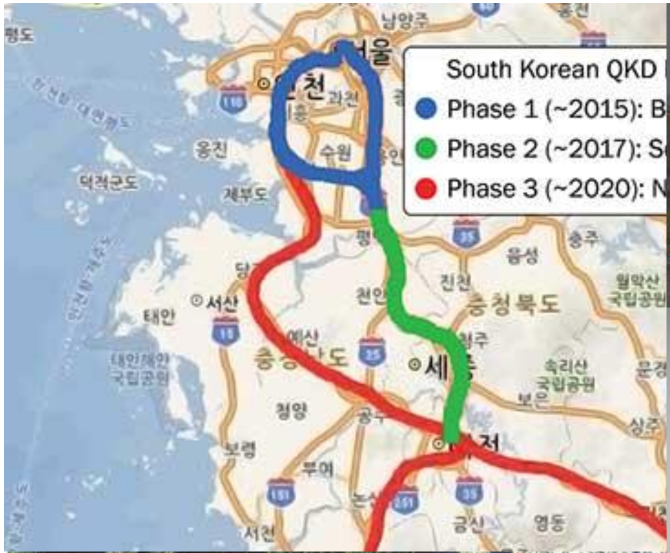
Optical fibers

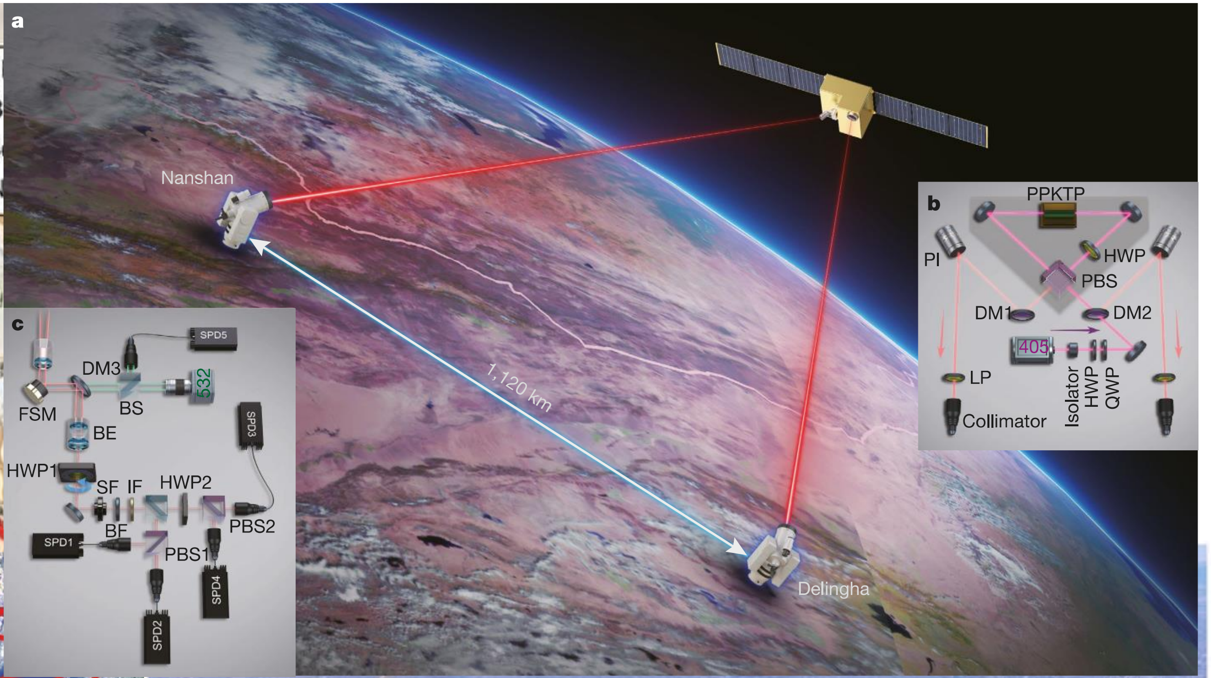
DRA MALVERN – OXFORD 1991

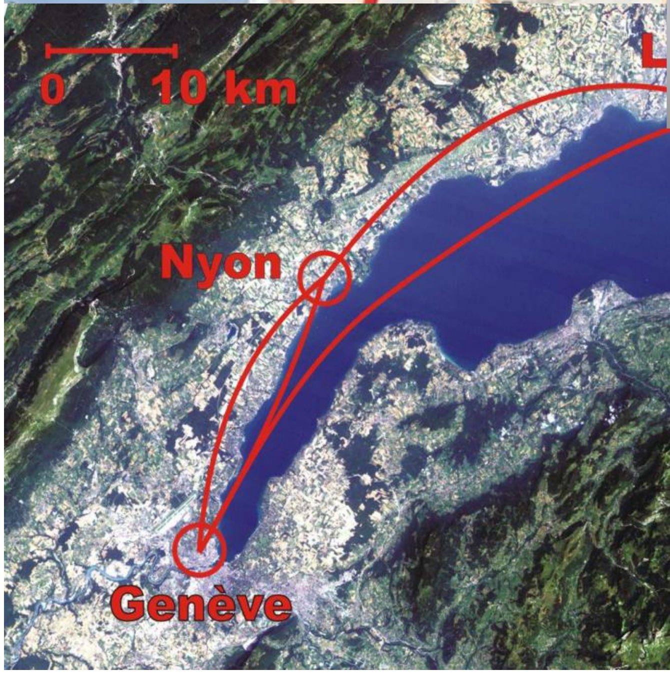
Polarizing filters & photodetectors

Polarizing filters & photodetectors

…and implemented

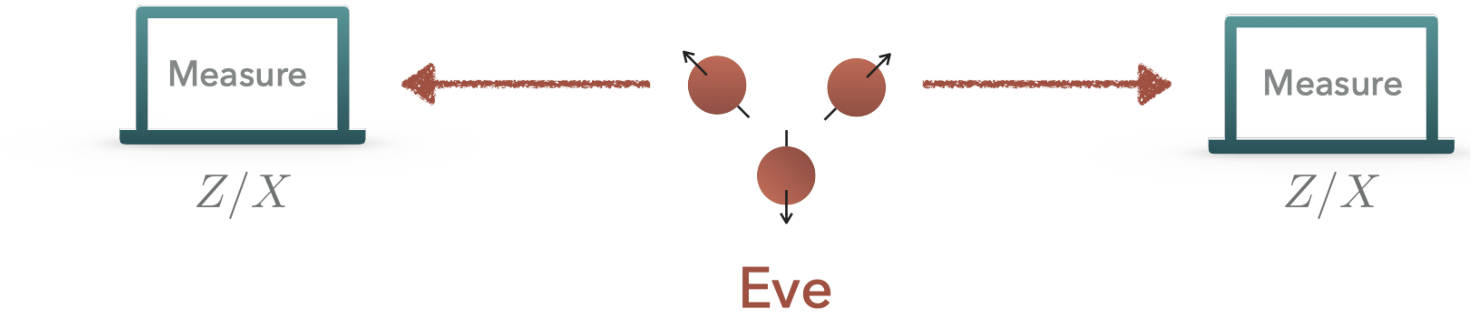




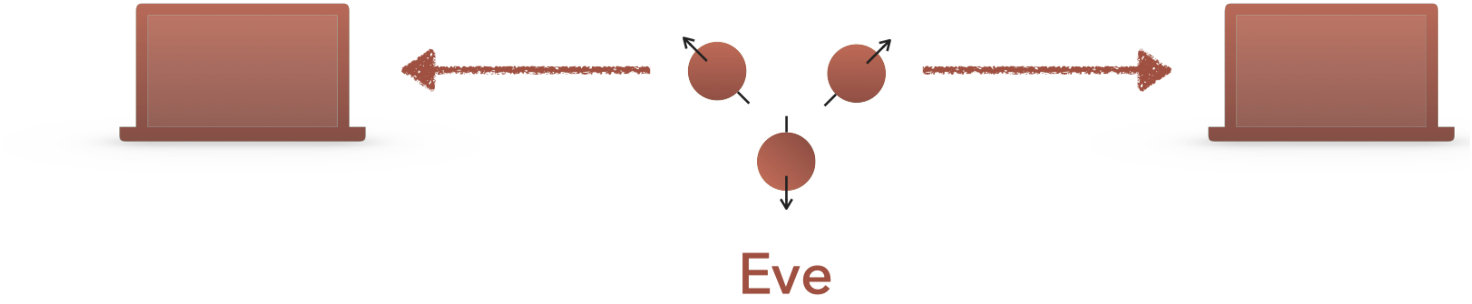


At the mercy of Eve

Ekert 91

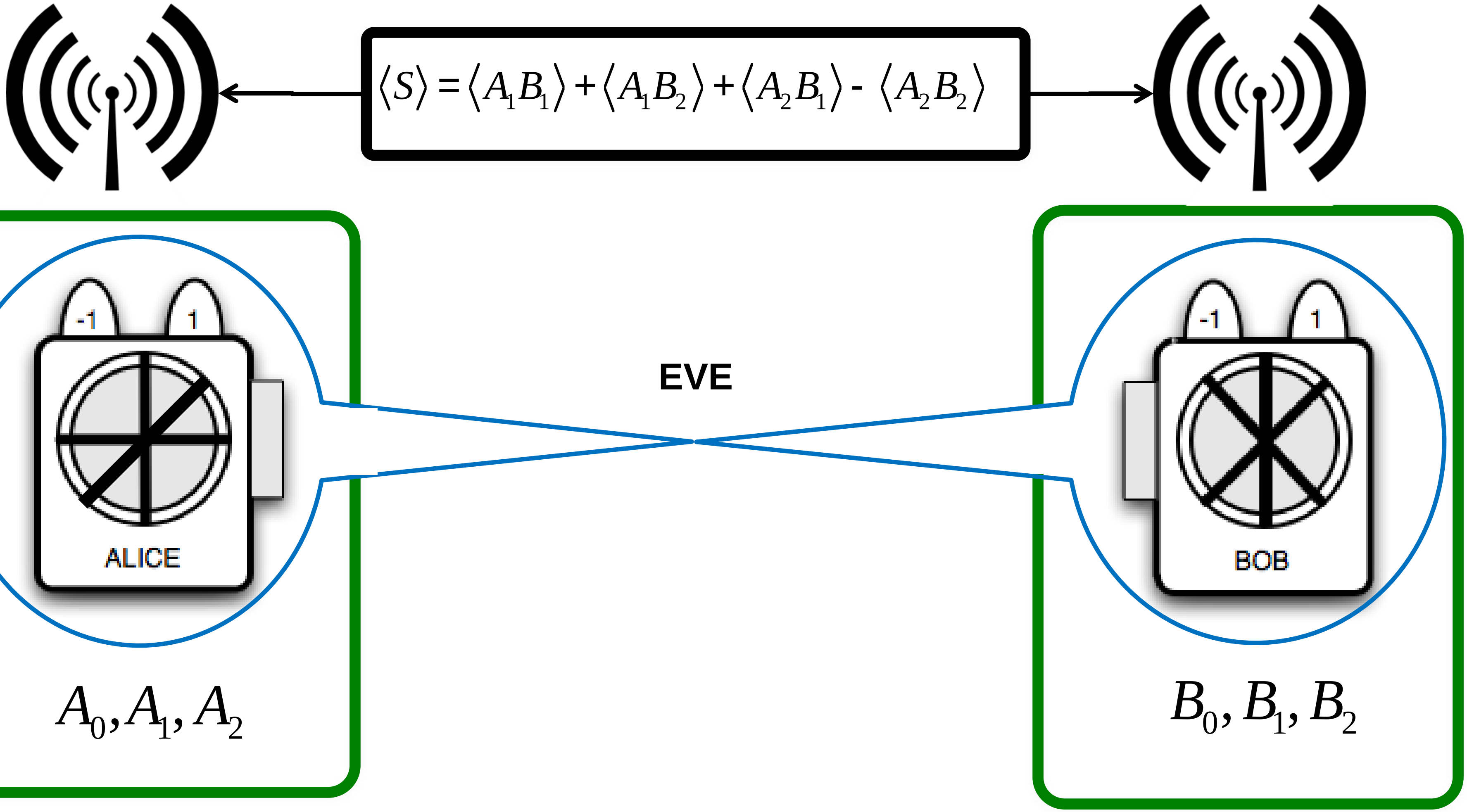


Device-independent



Courtesy Rotem Arnon-Friedman

Device independent



$$\langle S\rangle = \langle A_1B_1\rangle + \langle A_1B_2\rangle + \langle A_2B_1\rangle - \langle A_2B_2\rangle$$

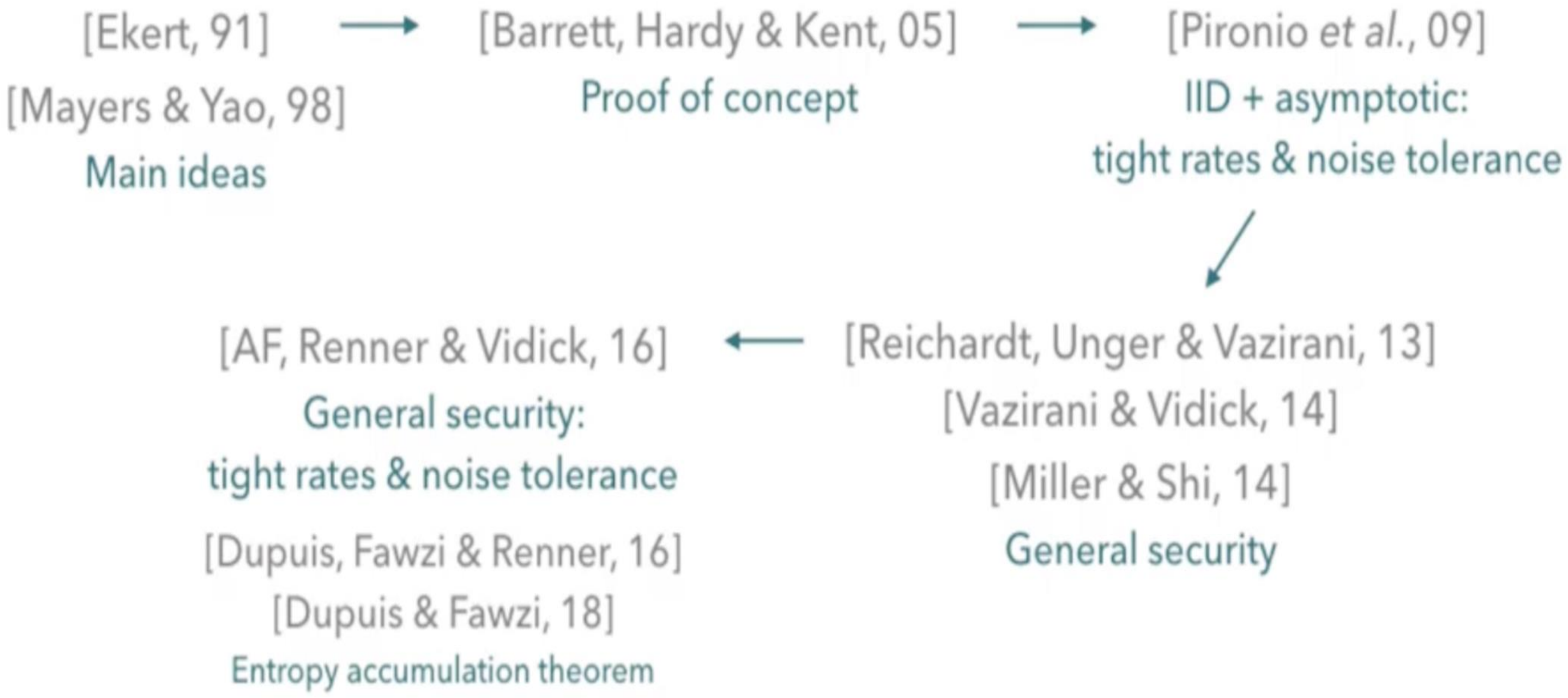
A_0, A_1, A_2

B_0, B_1, B_2

- 🟢 Alice’s and Bob’s labs are secure - no information leaks
- 🟢 Alice and Bob control and trust devices in their labs
- 🔴 Alice and Bob have free will and can choose their observables

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

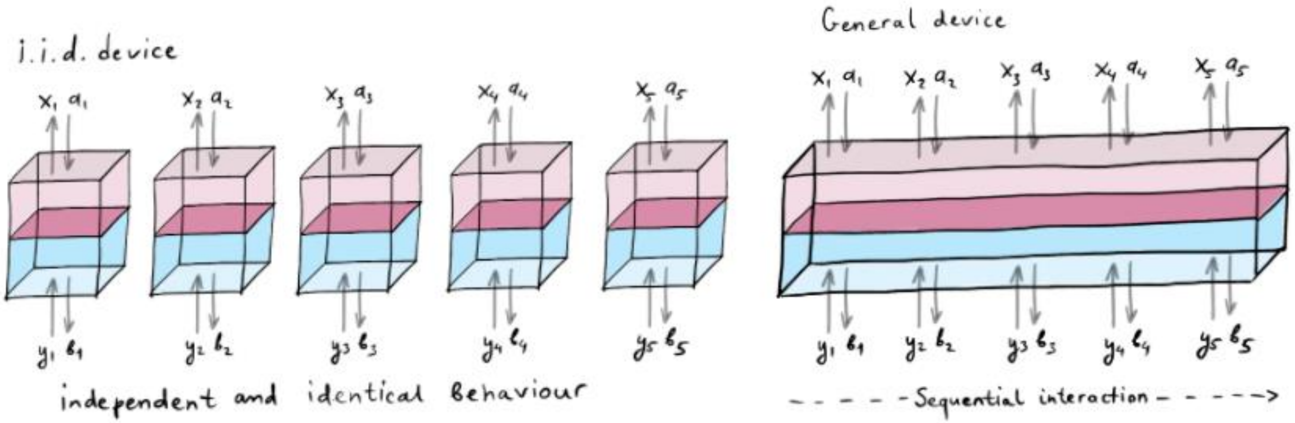
[Dupuis, Fawzi & Renner, 16]

[Dupuis & Fawzi, 18]

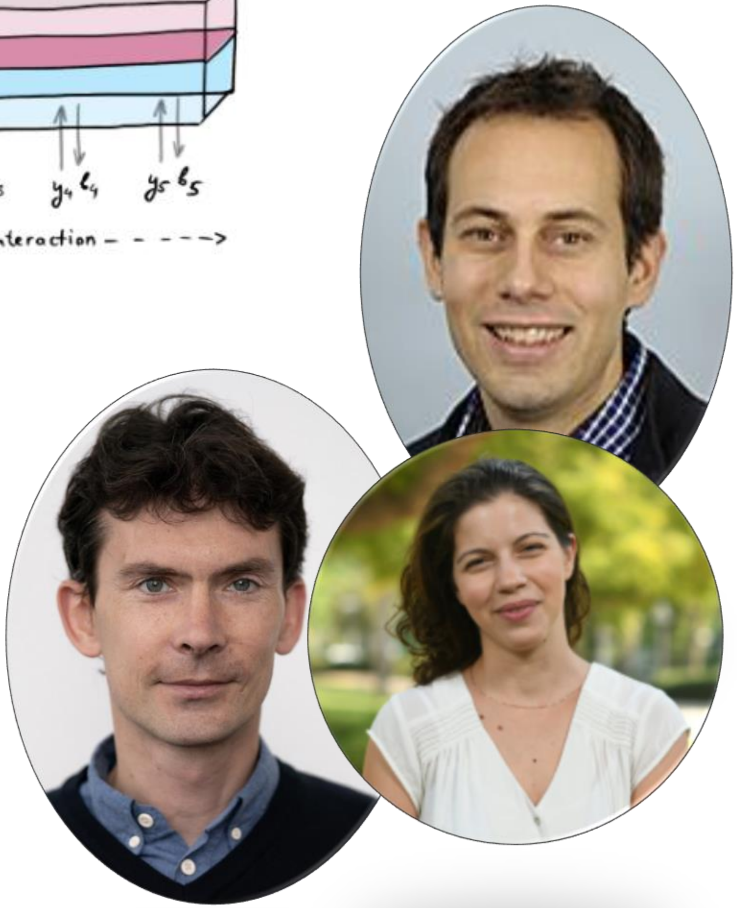
Entropy accumulation theorem

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)

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

$$\downarrow$$

3. Quantum-proof extractors

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

$$\downarrow$$

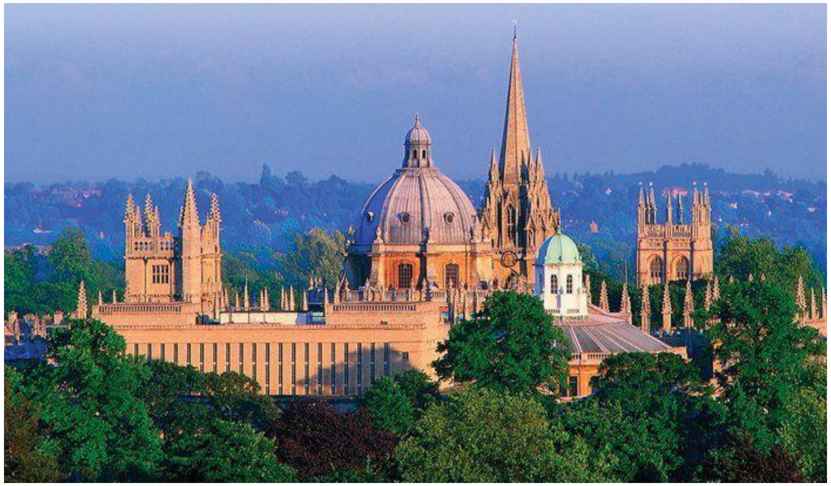
4. Secrecy

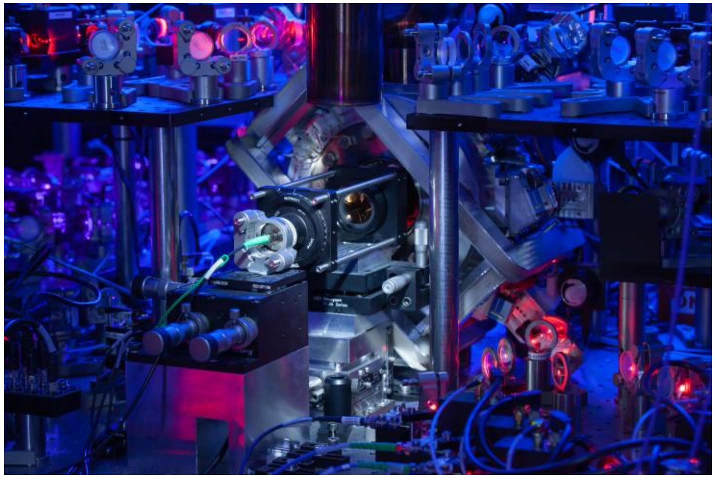
$$(1 - \Pr(\text{abort}))\left\|\rho_{K_A E} - \rho_{U_{\ell}} \otimes \rho_{E}\right\| \leq \varepsilon_{\text{sec}}$$

Look it up - your homework 😃

- Public key cryptosystems: RSA, elliptic curves and lattice based
- Randomness extractors and privacy amplification
- Why cryptographers use min-entropy rather than Shannon entropy?
- Define security using Kolmogorov / trace distance between probability distributions
- Quantum entanglement
- CHSH non-local game
- Quantum Asymptotic Equipartition Property for entropy
- Entropy Accumulation Theorem (EAT) – a real challenge ☺

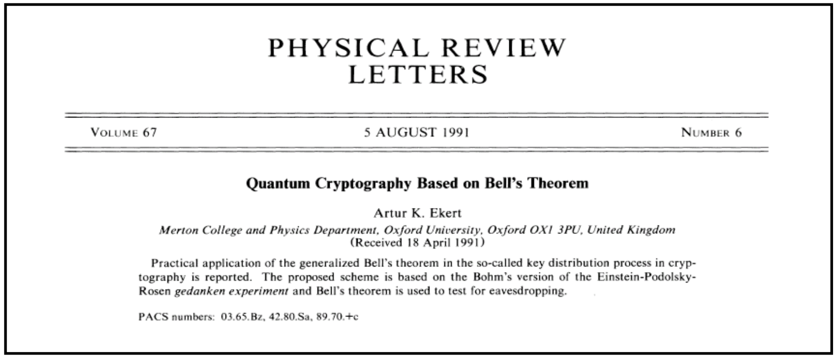
It is not true that nothing changes in Oxford





From Oxford in 1991…

…to Oxford 2021



PHYSICAL REVIEW
LETTERS

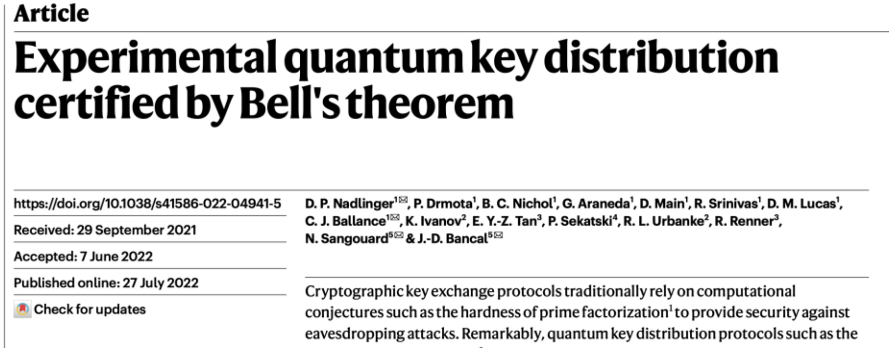
VOLUME 67 5 AUGUST 1991 NUMBER 6

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

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

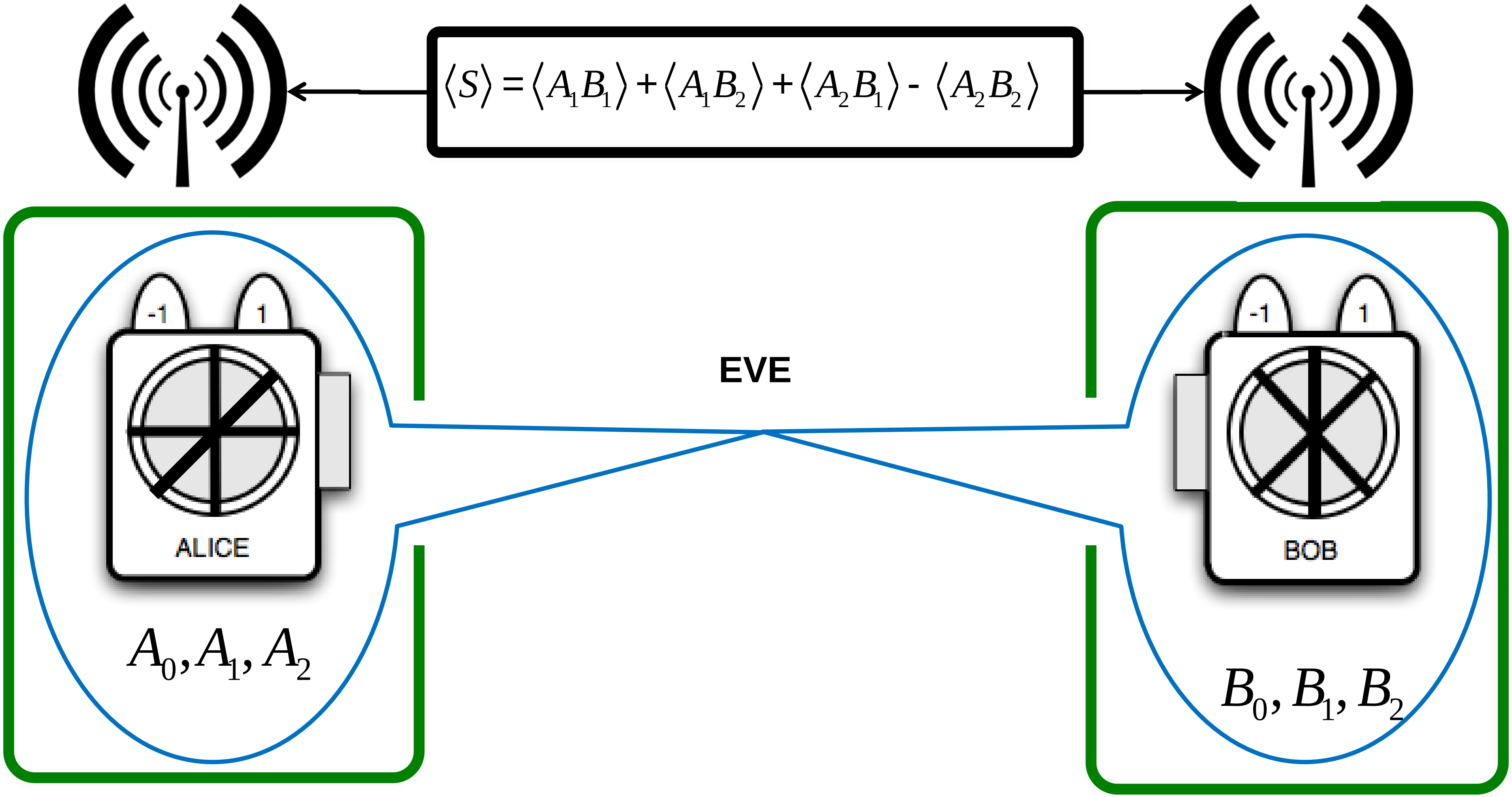
D. P. Nadlinger[1]✉, P. Drmota[1], B. C. Nichol[1], G. Araneda[1], D. Main[1], R. Srinivas[1], D. M. Lucas[1], C. J. Ballance[1]✉, K. Ivanov[2], E. Y.-Z. Tan[3], P. Sekatski[4], R. L. Urbanke[2], R. Renner[3], N. Sangouard[5]✉ & J.-D. Bancal[5]✉

Cryptographic key exchange protocols traditionally rely on computational conjectures such as the hardness of prime factorization[1] to provide security against eavesdropping attacks. Remarkably, quantum key distribution protocols such as the

End of worries?

You need perfect randomness, right ?

Device independent & “partial free will”



$$\langle S\rangle = \langle A_1B_1\rangle + \langle A_1B_2\rangle + \langle A_2B_1\rangle - \langle A_2B_2\rangle$$

- 🟢 Alice’s and Bob’s labs are secure - no information leaks
- 🟢 Alice and Bob control and trust devices in their labs
- 🟡 Alice and Bob have free will and can **choose** their observables

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

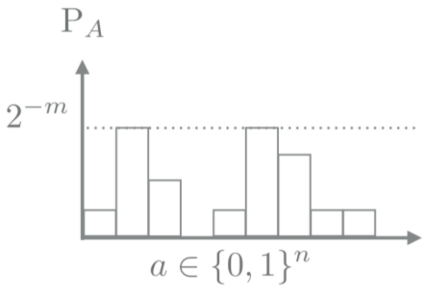
Vol. 507, No. 7493

Look it up - your homework 😃

- Public key cryptosystems: RSA, elliptic curves and lattice based
- Randomness extractors and privacy amplification
- Why cryptographers use min-entropy rather than Shannon entropy?
- Define security using Kolmogorov / trace distance between probability distributions
- Quantum entanglement
- CHSH non-local game
- Quantum Asymptotic Equipartition Property for entropy
- Entropy Accumulation Theorem (EAT) – a real challenge ☺
- Can we do DIQKD with partially secret randomness – your research project ☺
- …

How to quantify what we do not know?

Weak source of randomness



Min-entropy:

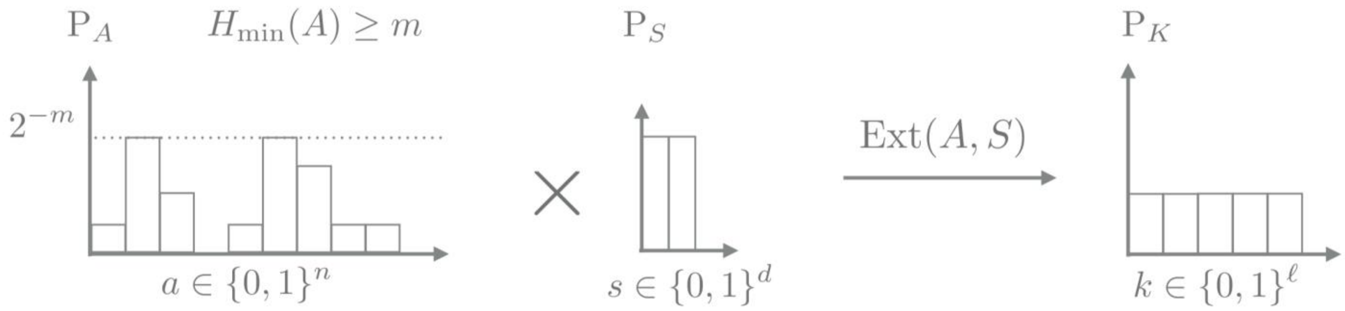
$$H_{\min}(A) = -\log\left(\overset{p_{\text{guess}}(A)}{\max_a \Pr[a]}\right)$$

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

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

Weak source of randomness

Uniform distribution



P_A
$H_{\min}(A) \geq m$
2^{-m}
$a \in \{0,1\}^n$
×
P_S
$s \in \{0,1\}^d$
$\mathrm{Ext}(A,S)$
P_K
$k \in \{0,1\}^\ell$