# Big Brother in a Quantum World

Gilles Brassard

Université de Montréal

CIFAR
CANADIAN INSTITUTE FOR ADVANCED RESEARCH

ChaumFest, CWI, Amsterdam, 22 November 2019

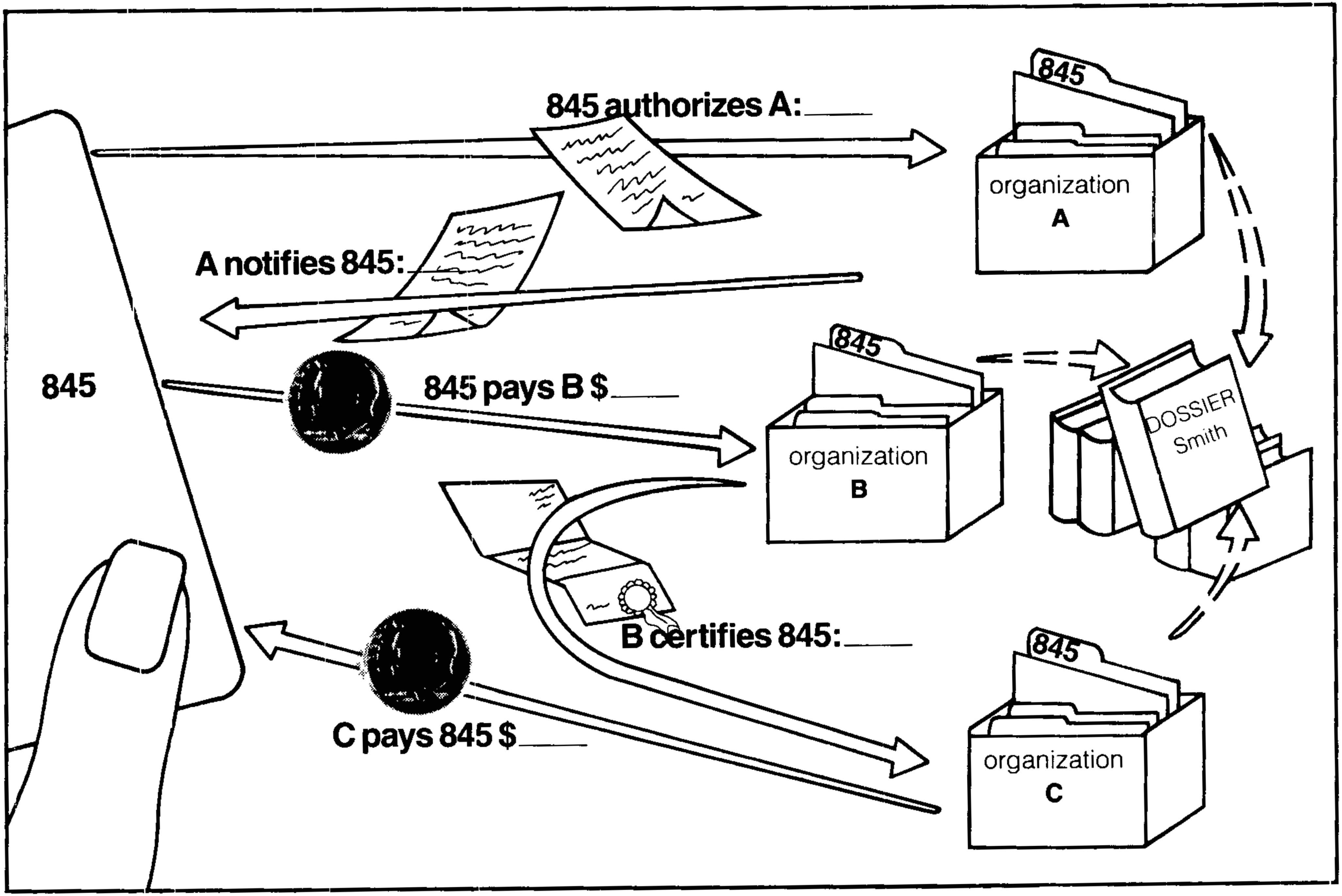
# SECURITY WITHOUT IDENTIFICATION: TRANSACTION SYSTEMS TO MAKE BIG BROTHER OBSOLETE

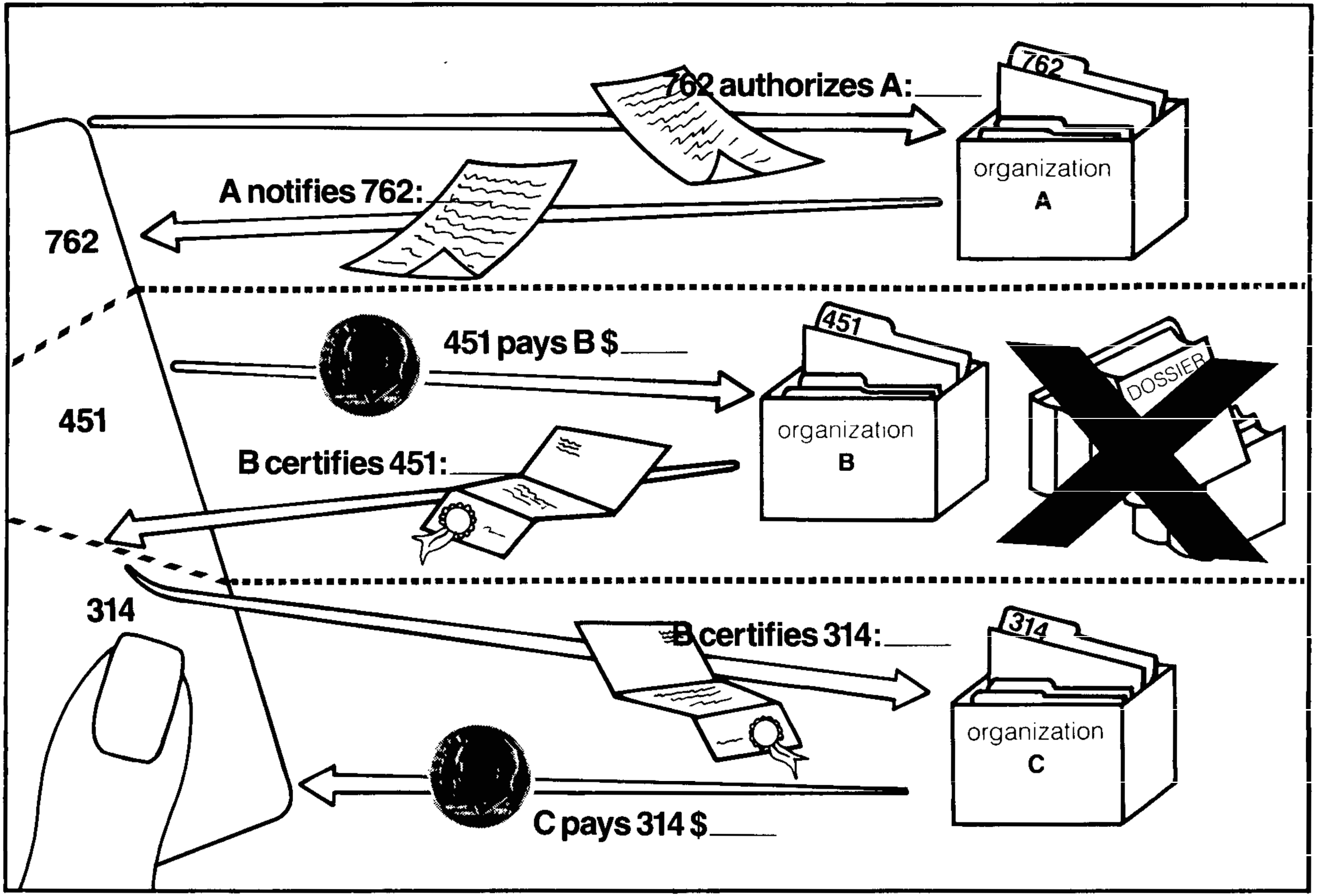
*The large-scale automated transaction systems of the near future can be designed to protect the privacy and maintain the security of both individuals and organizations.*

DAVID CHAUM


**October 1985**

Vol. 28 No. 10


845 authorizes A: ____
A notifies 845: ____
845
845 pays B $ ____
B certifies 845: ____
C pays 845 $ ____
845
organization
A
845
organization
B
845
organization
C
DOSSIER
Smith


762 authorizes A:
762
organization
A
A notifies 762:
762
451 pays B $
451
organization
B
DOSSIER
B certifies 451:
451
314
B certifies 314:
314
organization
C
C pays 314 $

COMMUNICATIONS OF THE ACM

# Security without identification: transaction systems to make big brother obsolete

By David Chaum

Communications of the ACM, October 1985, Vol. 28 No. 10, Pages 1030-1044
10.1145/4372.4373



The large-scale automated transaction systems of the near future can be designed to protect the privacy and maintain the security of both individuals and organizations.

# Crypto 81 Proceedings

[illegible] 81 was published as a UCSB Tech Report. These papers were not refereed, and this predates the existence of IACR. The front matter with preface and table of contents is available here. The cover sheet is also available.

## Session A: Theory & Implementation

### Ron Rivest, MIT, Chairman



## Session B: Algorithms, Techniques, & Funding

### Ralph Merkle, ELXSI Int'l, Chairman



## Session C Computers, Networks, Key Management

### Steve Kent, BBN, Chairman



## Session D Applications and Issues

### Steve Weinstein, American Express, Chairman



## Rump Session

### Paul S. Henry, Bell Labs, Chairman



## Panel Discussion

# Crypto 81 proceedings

The proceedings of Crypto 81 was published as a UCSB Tech Report. These papers were not refereed, and this predates the existence of IACR. The front matter with preface and table of contents is available here. The cover sheet is also available.

## Session A: Theory & Implementation

### Ron Rivest, MIT, Chairman

- The Generation or Cryptographically Strong Pseudo-Random Sequences, Adi Shamir, Weitzmann Institute (Israel) (Metadata)
- On the Necessity or Exhaustive Search for System-Invariant Cryptanalysis, Martin E. Hellman, Ehud Karnin, and Justin Reyneri, Stanford Univ. (Metadata)
- Time-Memory-Processor Tradeoffs, Hamid Amirazizi and Martin E. Hellman, Stanford Univ. (Metadata)
- Primality Testing, Leonard Adleman, USC (Metadata)
- Coin Flipping by Telephone, Manuel Blum, UC Berkeley (Metadata)
- High-Speed Hardware Implementation of the Knapsack Cipher, Paul S. Henry and R. D. Nash, Bell Labs (Metadata)
- A Polynomial Time Solution for Compact Knapsacks, Hamid Amirazizi, Ehud Karnin, and Justin Reyneri, Stanford Univ. (Metadata)
- Some Comments on the Knapsack Problem, Ingemar Ingemarsson, Univ. of Linkoping (Sweden) (Metadata)
- Variant ot a Public Key Cryptosystem based on Goppa codes, John P. Jordan, Bell Labs (Metadata)

## Session B: Algorithms, Techniques, & Funding

### Ralph Merkle, ELXSI Int'l, Chairman

- A System for Point-of-Sale or Access User Authentication and Identification, Gus Simmons, Sandia Corp. (Metadata)
- One-way Sequence for Transaction Verification, Alan G. Konheim, Univ. Calif.,Santa Barbara (Metadata)
- DES '81l: An Update, Miles E. Smid, NBS (Metadata)
- Some Regular Properties of the DES, Donald W. Davies, National Physical Lab (England) (Metadata)
- Subtractive Encryptors - Alternatives to the DES, Don R. Morrison, Univ. New Mexico (Metadata)
- Towards a Design Procedure for Cryptosecure Substitution Boxes, J. A. Gordon, Hatfield Polytechnic (England) (Metadata)
- An Optimally Secure Relativized Cryptosystem Gilles Brassard, Univ. de Montreal (Metadata)
- Scrambling and Randomization, Subhash C. Kak, Louisiana State Univ. (Metadata)
- A Discussion ot NSA Program OCREAE, Larry Hatch, NSA

# Session D Applications and Issues

## Steve Weinstein, American Express, Chairman

- Cryptography, the Next Two Decades, Whitfield Diffie, BNR (Metadata)
- Security Mechanisms in Electronic Cards Stephen B. Weinstein, American Express (Metadata)
- Current Market: Products, Costs, Trends, J. Michael Nye, Marketing Consultants Int'l (Metadata)
- Results on Sampling-based Scrambling for Secure Speech Cummunication, Lin-Shan Lee and , Ger-chih Chow, National Taiwan Univ. (Metadata)
- Some Tnoughts on Speech Encryption A. D. Wyner, Bell Labs (Metadata)
- Nonlinear Feedback Shift Register Sequences H. J. Beker, Racal-Milgo (England) (Metadata)
- Evaluating Relative Security of Commercial ComSec Devices, Albert L. Lang and Janet T. Vasek, Booz, Allen & Hamilton (Metadata)
- Limitations on the Use of Encryption to Enforce Mandatory Security, Morrie Gasser, Mitre (Metadata)
- The Import/Export Dilemma, J. Michael Nye, (Marketing Consultants Int'l (Metadata)

# Rump Session

## Paul S. Henry, Bell Labs, Chairman

- Verification by Anonymous Monitors, David Chaum, Univ. California. Santa Barbara (Metadata)
- Progress in Public Key Cryptography in Great Britain, Martin Kochanski, Telesecurity Ltd. (no paper)
- A General Public Key System Ernst Henze, Univ. Braunschweig (Ww. Germany) (Metadata)
- Discussion ot Adleman's Subexponential Algorithm for Computing Discrete Logarithms, Tore Herlestam, Univ. Lund (Sweden) (Metadata)
- Theorem concerning Pseudo-Random Sequences, Adi Shamir (no paper)
- Protocol for Signing Contracts, Shimon Even, Technion (Israel) (Metadata)
- Ill-Formed Tuoughts Concerning Oblivious Transfer, Ron Rivest, MIT (no paper)

# Panel Discussion

National Security and Commercial Security: Division of Responsibility,
Whitfield Diffie, BNR (Moderator),
Melville Klein, NSA,
Michael L. Dertouzos, MIT,
Andrew Gleason, Harvard
Dean Smith
(Metadata)

International Association for Cryptologic Research

# Crypto 81 proceedings

The proceedings of Crypto 81 was published as a UCSB Tech Report. These papers were not refereed, and this predates the existence of IACR. The front matter with preface and table of contents is available here. The cover sheet is also available.

## Session A: Theory & Implementation

### Ron Rivest, MIT, Chairman

- The Generation or Cryptographically Strong Pseudo-Random Sequences, Adi Shamir, Weitzmann Institute (Israel) (Metadata)
- On the Necessity or Exhaustive Search for System-Invariant Cryptanalysis, Martin E. Hellman, Ehud Karnin, and Justin Reyneri, Stanford Univ. (Metadata)
- Time-Memory-Processor Tradeoffs, Hamid Amirazizi and Martin E. Hellman, Stanford Univ. (Metadata)
- Primality Testing, Leonard Adleman, USC (Metadata)
- Coin Flipping by Telephone, Manuel Blum, UC Berkeley (Metadata)
- High-Speed Hardware Implementation of the Knapsack Cipher, Paul S. Henry and R. D. Nash, Bell Labs (Metadata)
- A Polynomial Time Solution for Compact Knapsacks, Hamid Amirazizi, Ehud Karnin, and Justin Reyneri, Stanford Univ. (Metadata)
- Some Comments on the Knapsack Problem, Ingemar Ingemarsson, Univ. of Linkoping (Sweden) (Metadata)
- Variant ot a Public Key Cryptosystem based on Goppa codes, John P. Jordan, Bell Labs (Metadata)

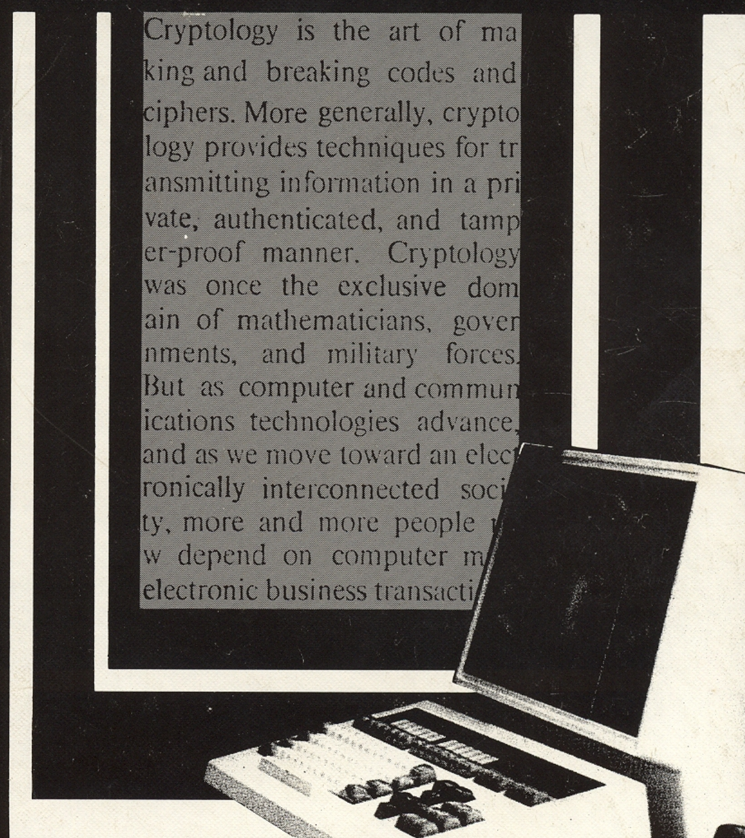
## Session B: Algorithms, Techniques, & Funding

### Ralph Merkle, ELXSI Int'l, Chairman

- A System for Point-of-Sale or Access User Authentication and Identification, Gus Simmons, Sandia Corp. (Metadata)
- One-way Sequence for Transaction Verification, Alan G. Konheim, Univ. Calif.,Santa Barbara (Metadata)
- DES '81l: An Update, Miles E. Smid, NBS (Metadata)
- Some Regular Properties of the DES, Donald W. Davies, National Physical Lab (England) (Metadata)
- Subtractive Encryptors - Alternatives to the DES, Don R. Morrison, Univ. New Mexico (Metadata)
- Towards a Design Procedure for Cryptosecure Substitution Boxes, J. A. Gordon, Hatfield Polytechnic (England) (Metadata)
- An Optimally Secure Relativized Cryptosystem Gilles Brassard, Univ. de Montreal (Metadata)
- Scrambling and Randomization, Subhash C. Kak, Louisiana State Univ. (Metadata)
- A Discussion ot NSA Program OCREAE, Larry Hatch, NSA

# ADVANCES IN CRYPTOLOGY

## Proceedings of Crypto 82




Edited by
David Chaum, Ronald L. Rivest, and Alan T. Sherman

# QUANTUM CRYPTOGRAPHY OR

# UNFORGEABLE SUBWAY TOKENS

Charles H. Bennett,[1] Gilles Brassard,[2]
Seth Breidbart[3] and Stephen Wiesner[4]

1. IBM Research, Yorktown Heights, NY 10598
2. Université de Montréal, Département d'I.R.O., C.P. 6128, Succ. "A", Montréal, Québec H3C 3J7
3. P.O. Box 1526, Wall Street Station, New York, NY 10268
4. MIT Research Laboratory of Electronics, MIT, Cambridge, MA 02139

# 4. CRYPTO 1984: Santa Barbara, California, USA

G. R. Blakley, David Chaum (Eds.): Advances in Cryptology, Proceedings of CRYPTO '84, Santa Barbara, California, USA, August 19-22, 1984, Proceedings. Lecture Notes in Computer Science 196 Springer 1985, ISBN 3-540-15658-5

## Public Key Cryptosystems and Signatures

## Cryptosystems and Other Hard Problems

## Randomness And Its Concomitants

## Analysis and Cryptoanalysis

## Protocols and Authentication

## Impromptu Talks

Publication

# AN INTRODUCTION TO MINIMUM DISCLOSURE (1988)

- Main

Save publication

| | |
|---|---|
| **Title** | An introduction to minimum disclosure |
| **Published in** | CWI Quarterly, Vol. 1, No. 1, p.3-18. ISSN 0922-5366. |
| **Author** | G. Brassard (Gilles), D. Chaum (David), C. Crépeau |
| **Date issued** | 1988-03-01 |
| **Access** | Open Access |

JOURNAL OF COMPUTER AND SYSTEM SCIENCES 37, 156–189 (1988)

# Minimum Disclosure Proofs of Knowledge

GILLES BRASSARD*

*Département d'informatique et de R.O., Université de Montréal, C.P. 6128, Succursale "A," Montréal, Québec, Canada H3C 3J7*

DAVID CHAUM

*Centre for Mathematics and Computer Science (CWI), Kruislaan 413, 1098 SJ Amsterdam, The Netherlands*

AND

CLAUDE CRÉPEAU†

*Laboratory for Computer Science, Massachusetts Institute of Technology, 545 Technology Square, Cambridge, Massachusetts 02139*

Received July 3, 1987

Protocols are given for allowing a "prover" to convince a "verifier" that the prover knows some verifiable secret information, without allowing the verifier to learn anything about the secret. The secret can be probabilistically or deterministically verifiable, and only one of the prover or the verifier need have constrained resources. This paper unifies and extends models and techniques previously put forward by the authors, and compares some independent related work. 

# Big Brother in a Quantum World

Gilles Brassard

Université de Montréal

CIFAR
CANADIAN INSTITUTE FOR ADVANCED RESEARCH

ChaumFest, CWI, Amsterdam, 22 November 2019

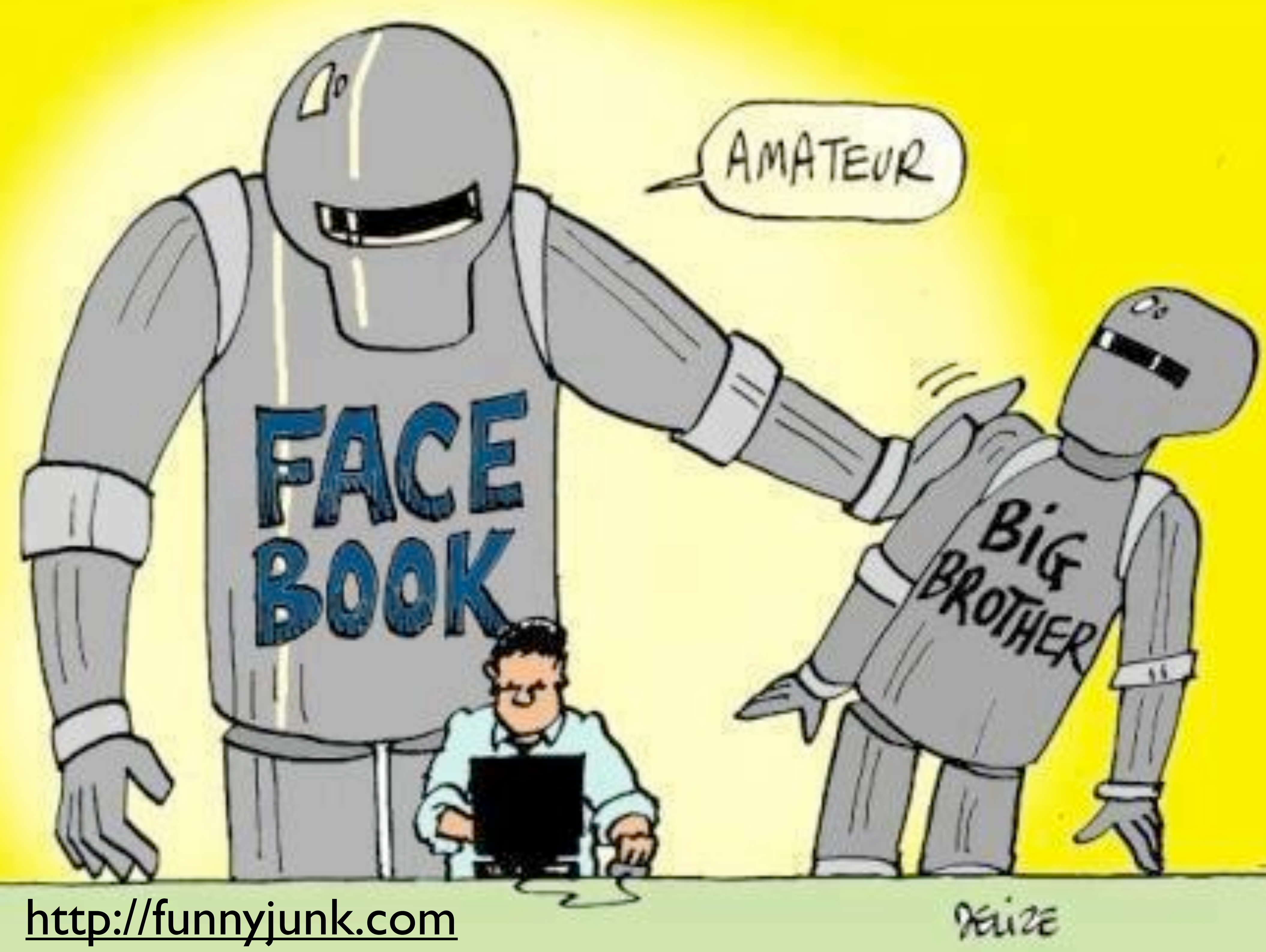
# BIG BROTHER

NATIONAL SECURITY AGENCY

UNITED STATES OF AMERICA

# IS WATCHING YOU


Ajuntament de Barcelona
Zona vigilada
en un radi de 500 m
Pl. George Orwell
PLAÇA
DE
GEORGE ORWELL




http://funnyjunk.com

# Cryptography

Ongoing battle between

Codemakers (cryptographers)

Codebreakers (cryptanalysts)

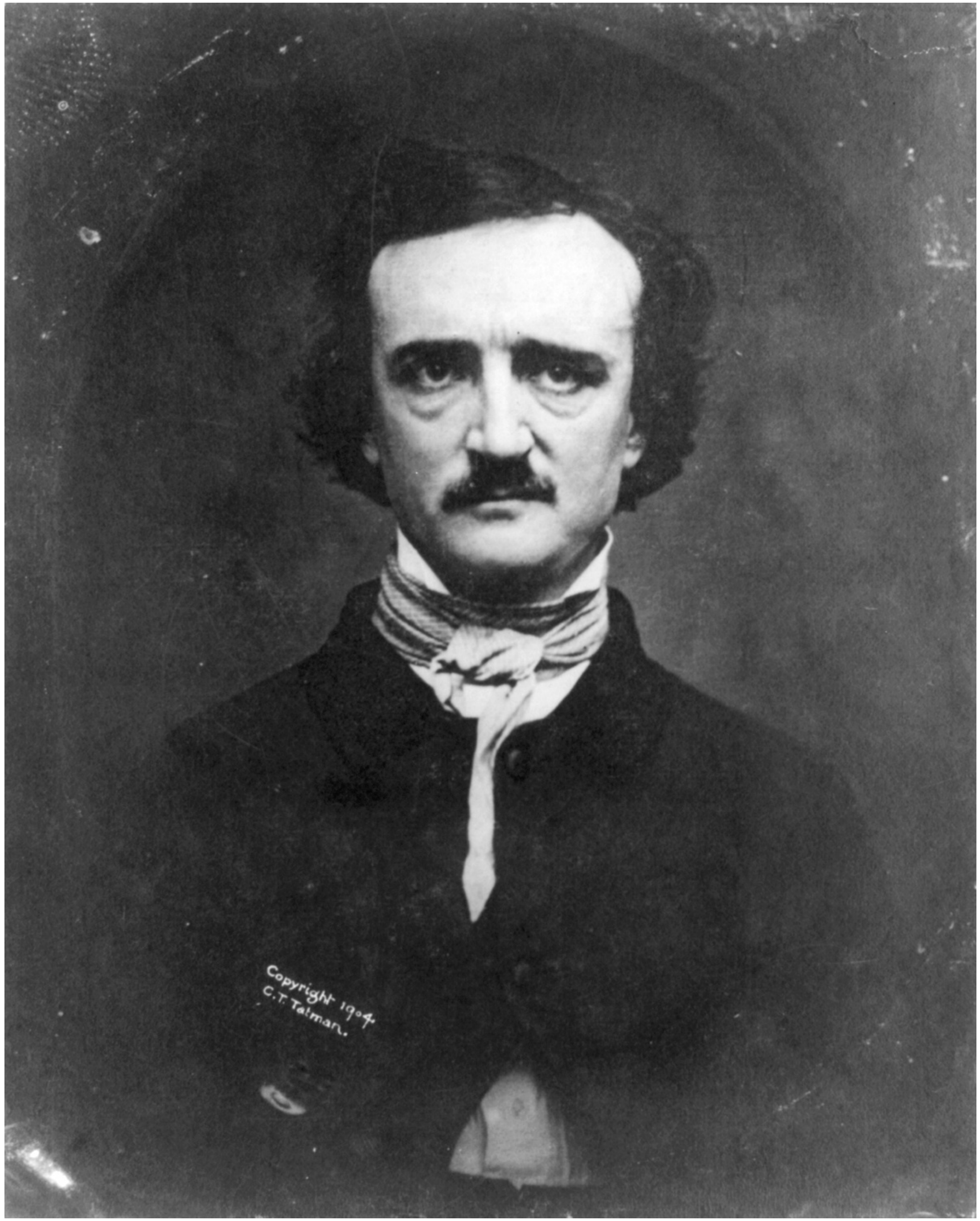
# Who will win?

Codemakers

or

Codebreakers

?




Edgar Allan Poe (1809–1849)

EDGAR
ALLAN POE

# THE GOLD BUG

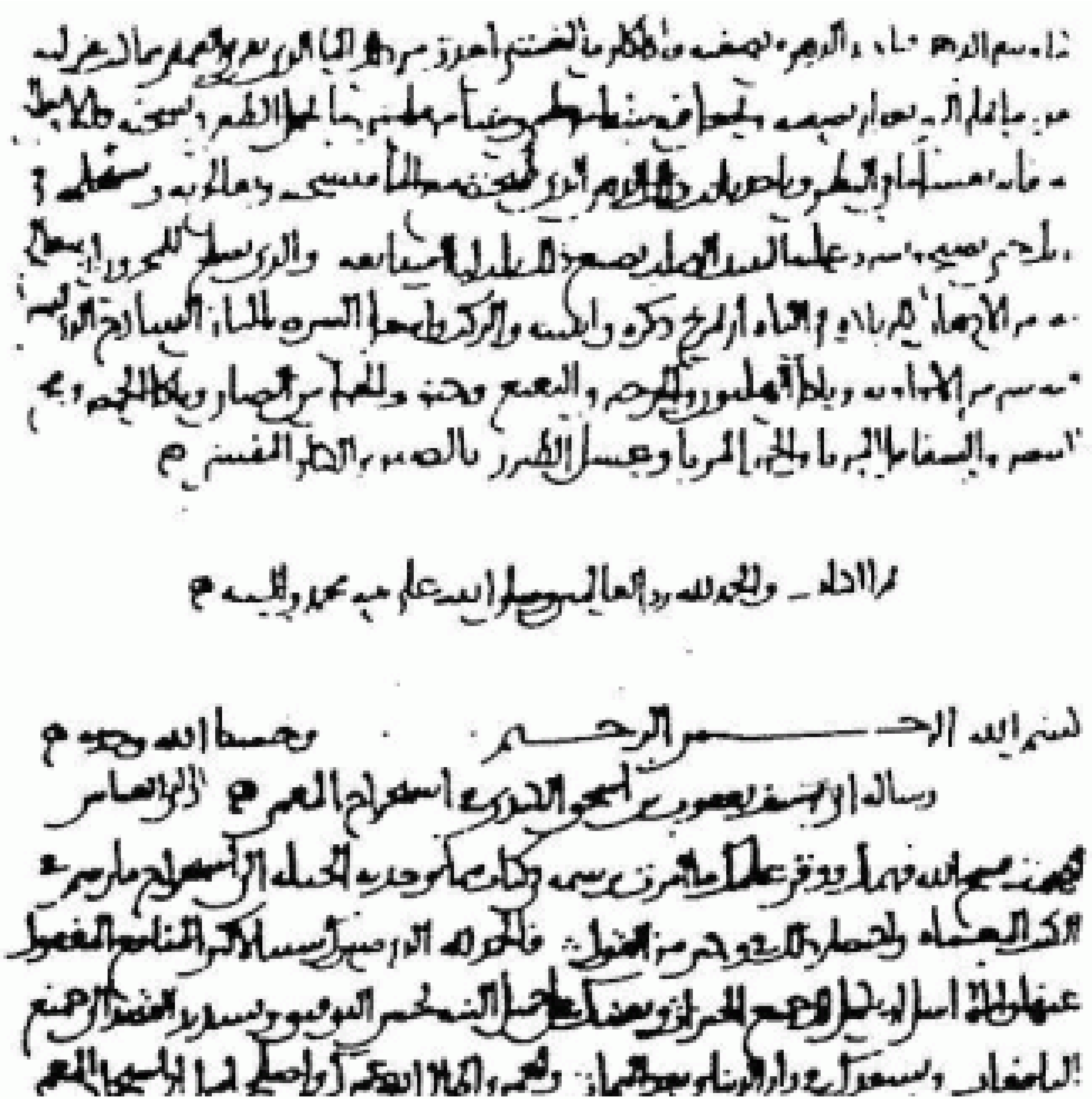
ePubYou

# Al-Kindi

Lived 801-873

Wrote 290 books

Abu Yusuf Ya'qub ibn Is-haq ibn as-Sabbah ibn Oòmran ibn Ismaïl Al-Kindi




Manuscript on Deciphering Cryptographic Messages

Rediscovered in 1987!

# Who will win?

Codemakers

or

Codebreakers

?

# Who will win?

« It may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve »

**Edgar Allan Poe**

(Graham's Lady's and Gentleman's Magazine, July 1841)

Blaise de Vigenère

TRAICTE'

# DES CHIFFRES, OV SECRETES MANIERES D'ESCRIRE:

PAR

*BLAISE DE VIGENERE,*

BOVRBONNOIS.

antes muerto que mudado

A PARIS,

Chez ABEL L'ANGELIER, au premier pillier de la grand' Salle du Palais.

*M. D. LXXXVI.*

1586

AVEC PRIVILEGE DV ROY.

# Who will win?

« It may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve »

**Edgar Allan Poe**

(Graham's Lady's and Gentleman's Magazine, July 1841)

Blaise de Vigenère, 1586
Giovan Battista Belasso, 1553
Charles Babbage, 1854 (1846?)

# Who will win?

« It may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve »

## Was he right?

# Key Establishment

## How can Alice and Bob establish a secret key?

Trusted third party  

Computational security

Quantum physics

# Key Establishment

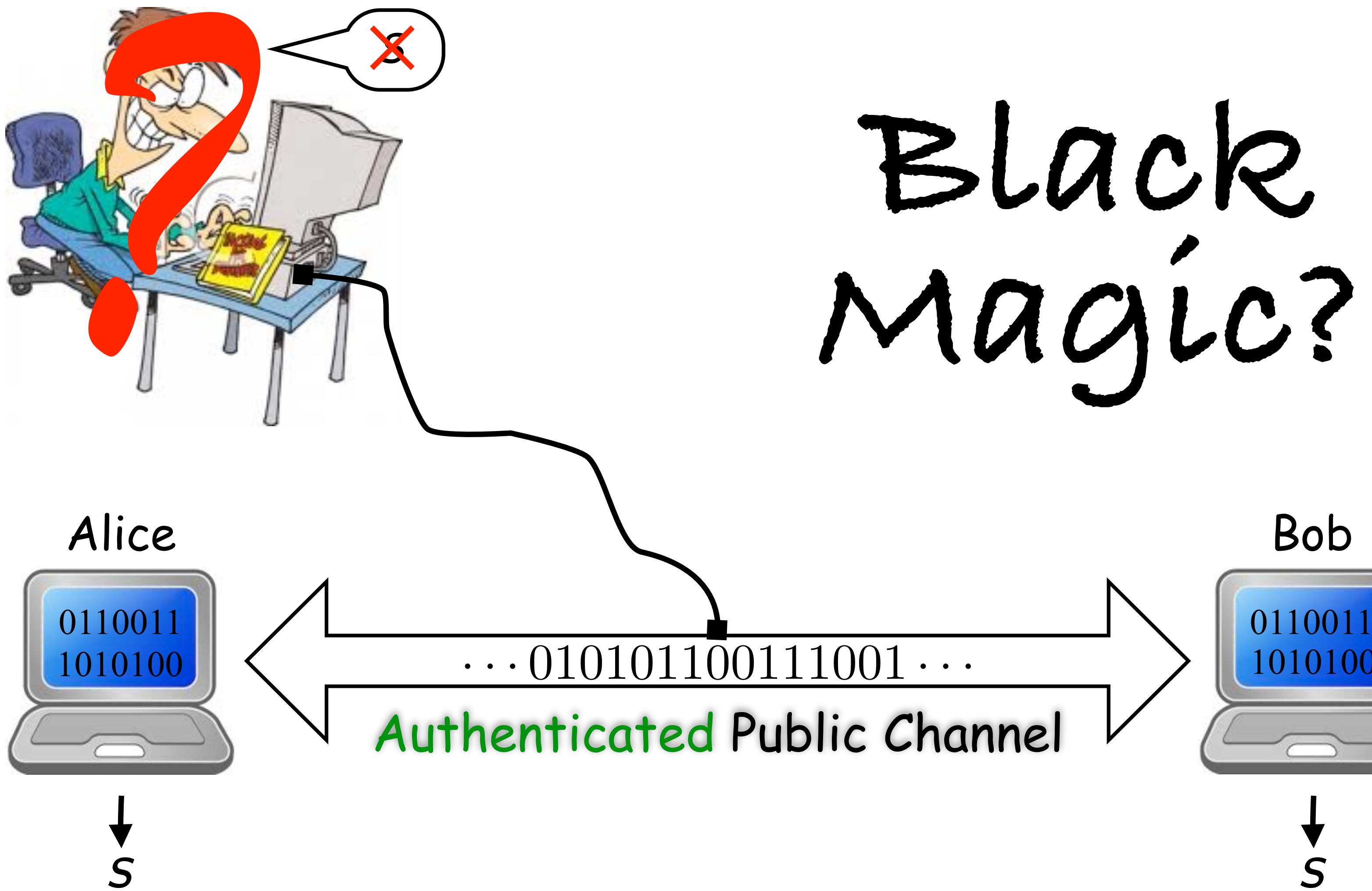
How can Alice and Bob establish a secret key?

Trusted third party  

Computational security

Cannot be unconditionally secure

# Key Establishment Problem



# Computational Security

James Ellis (1970)

Clifford Cocks (1973)

Ralph Merkle (1974)

Diffie et Hellman (1976)

Rivest, Shamir, Adleman (1977)

Robert McEliece (1978)

# The Big Question

We live in a quantum world

Is this a *blessing*

or a **curse**

for codemakers?

# Various Scenarios

## Codemakers

Classical Quantum

## Codebreakers

Classical Quantum

## Communication Channels

Classical Quantum

# Classical Scenario

Codemakers

Classical    Quantum

Codebreakers

Classical    Quantum

Communication Channels

Classical    Quantum

# Key Establishment

James Ellis (1970)

Clifford Cocks (1973)

Ralph Merkle (1974)

Diffie and Hellman (1976)

Rivest, Shamir, Adleman (1977)

Robert McEliece (1978)

# Post-Quantum Crypto

Codemakers

Classical Quantum

Codebreakers

Classical Quantum

Communication Channels

Classical Quantum

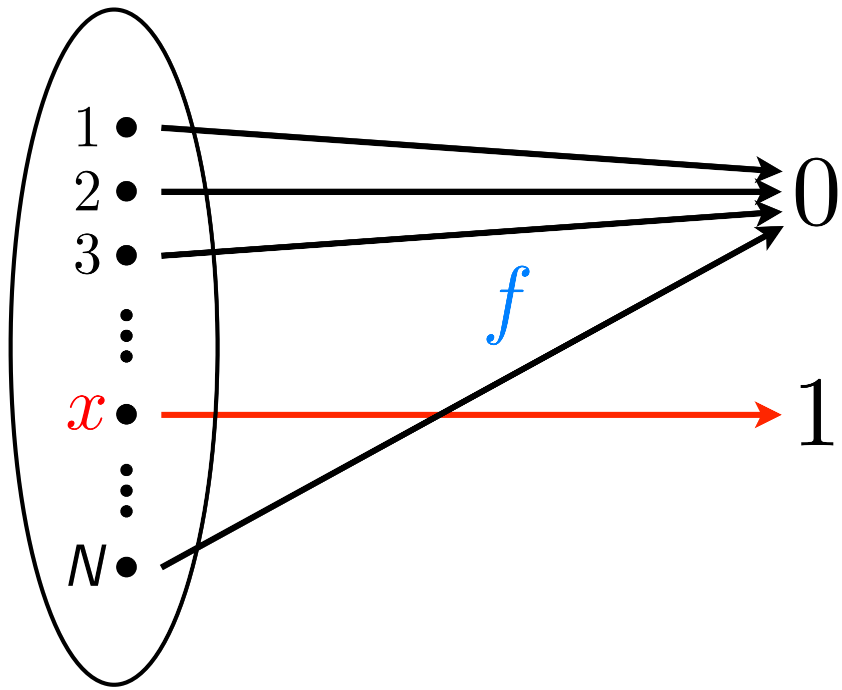
# Shor's algorithm

Can factor large numbers efficiently

Can extract discrete logarithms efficiently
even in elliptic curves

## on a quantum computer

# Grover's Algorithm




Problem: find unique $x$ such that $f(x) = 1$

Classical: requires $N/2$ calls to $f$ on average

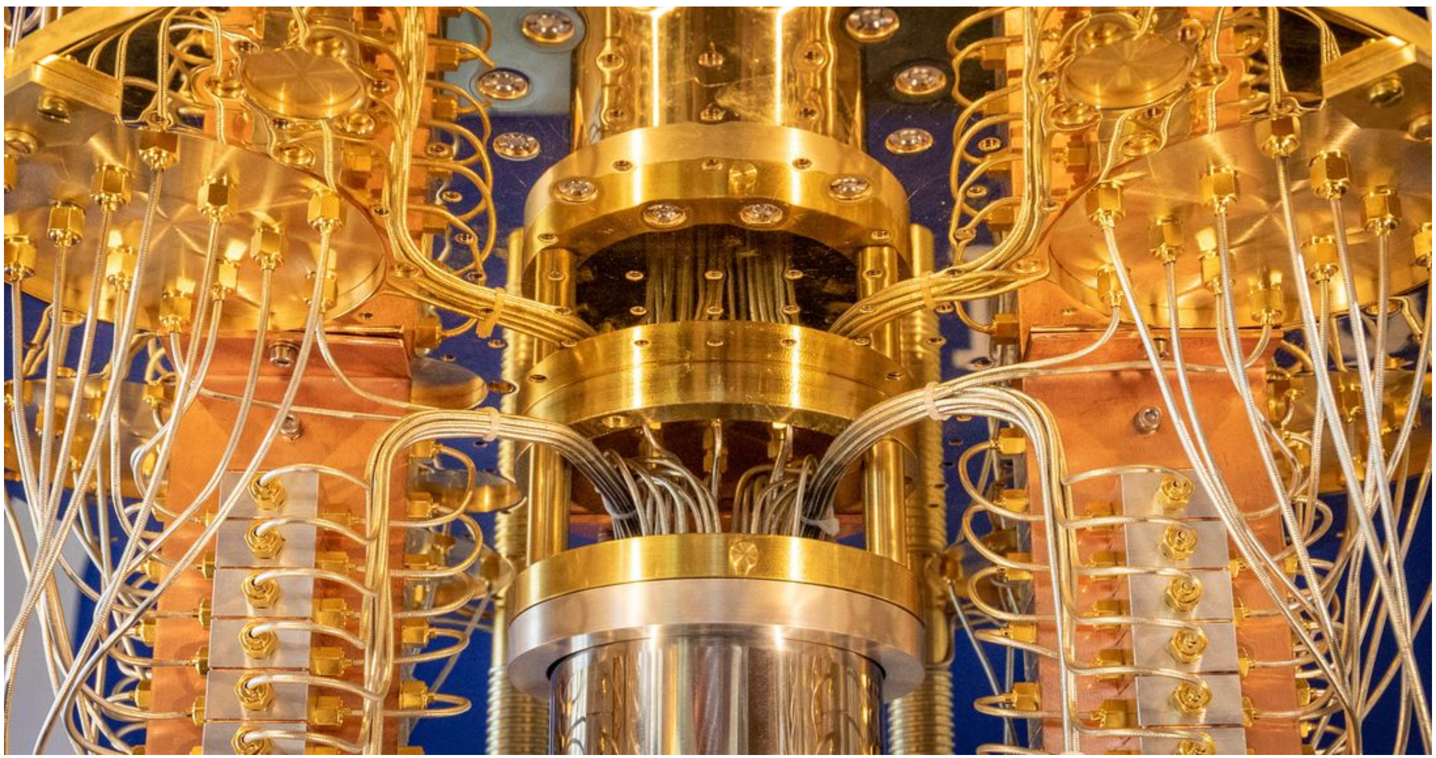
Grover: about $\sqrt{N}$ quantum calls to $f$ suffice!

# IBM's new 53-qubit quantum computer is its biggest yet

The system will go online in October.

**Stephen Shankland** September 18, 2019 5:00 AM PDT





A close-up view of the IBM Q quantum computer. The processor is in the silver-colored cylinder.

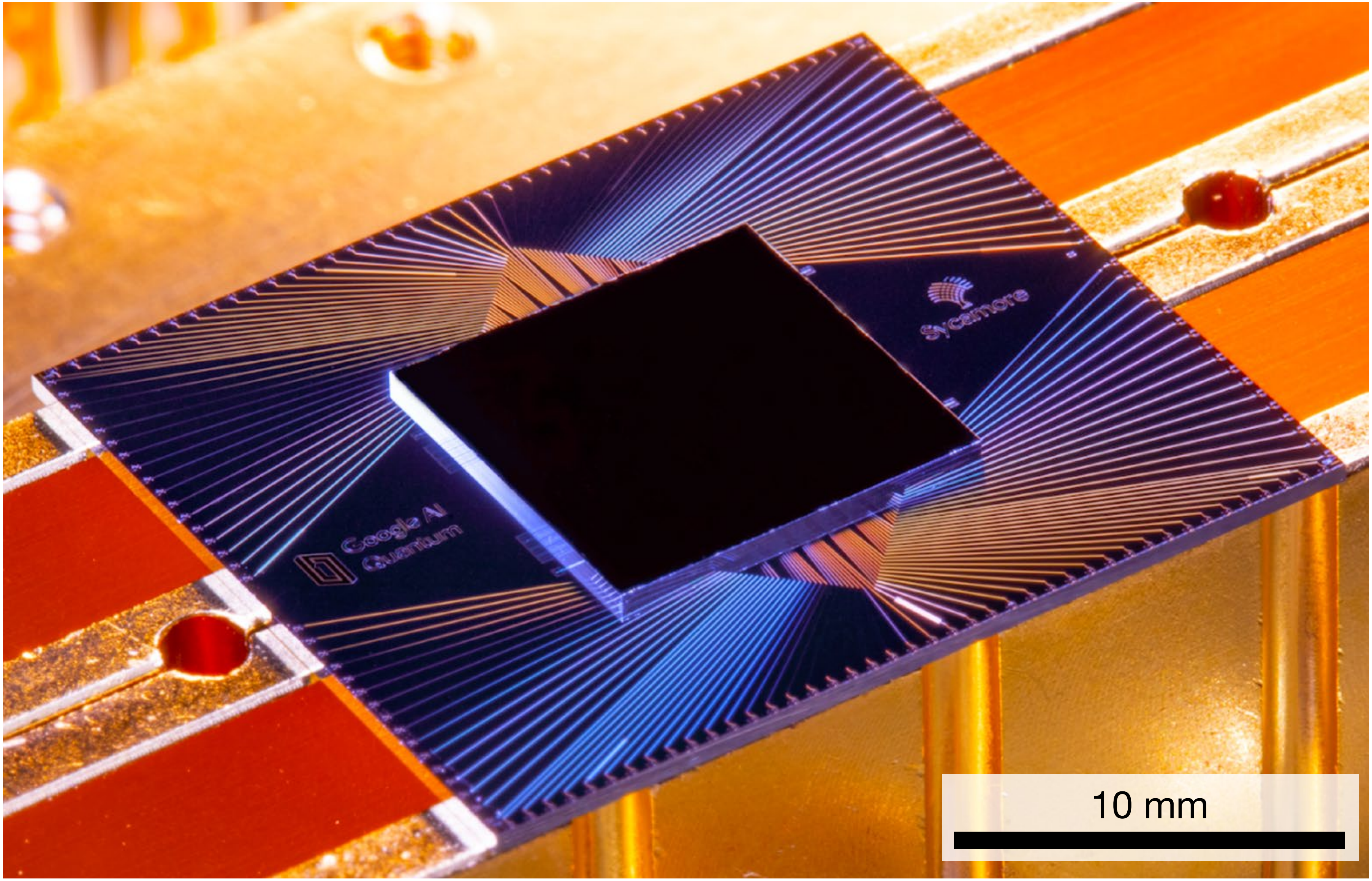
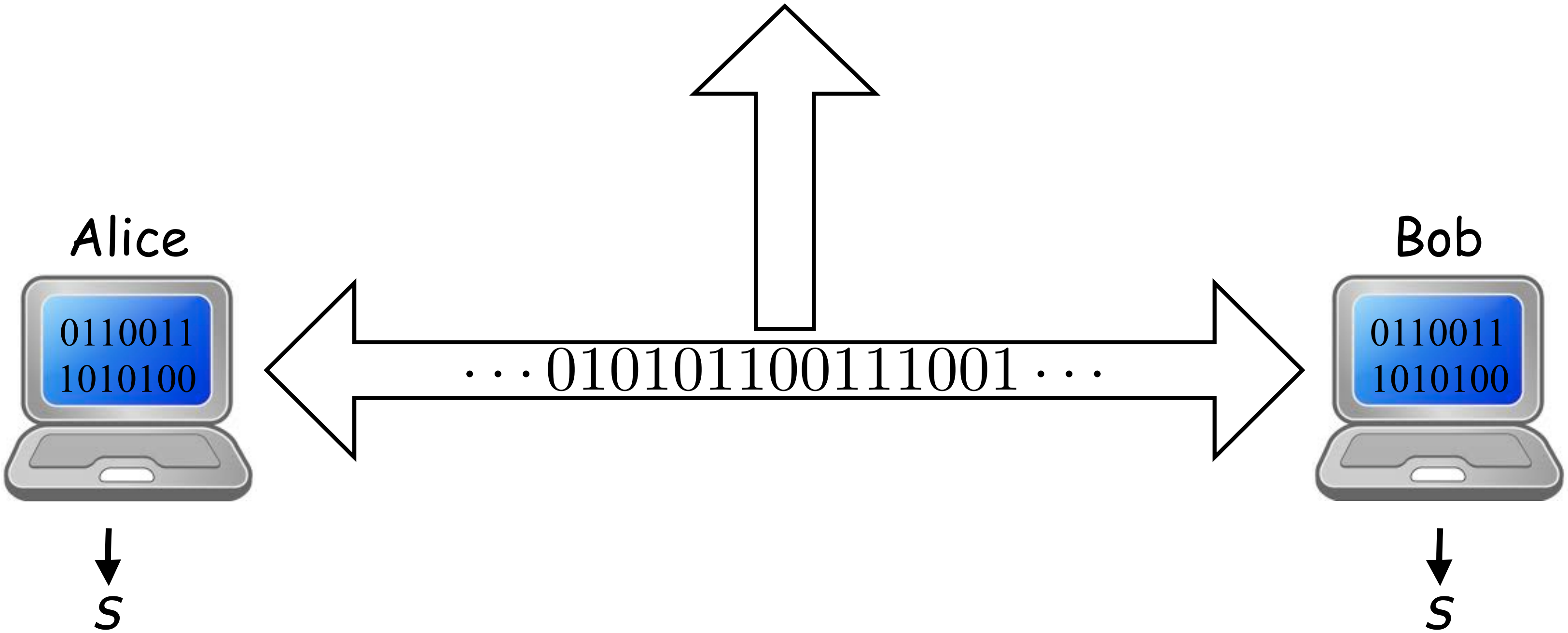



**Fig. 1 | The Sycamore processor. a**, Layout of processor, showing a rectangular array of 54 qubits (grey), each connected to its four nearest neighbours with couplers (blue). The inoperable qubit is outlined. **b**, Photograph of the Sycamore chip.

# Key Establishment in a Quantum World

# Post-Quantum Crypto

James Ellis (1970)

~~Clifford Cocks (1973)~~

~~Ralph Merkle (1974)~~

~~Diffie et Hellman (1976)~~

~~Rivest, Shamir, Adleman (1977)~~

¿ Robert McEliece (1978) ?

# Post-Quantum Crypto

James Ellis (1970)

~~Clifford Cocks (1973)~~

Ralph Merkle (1974)

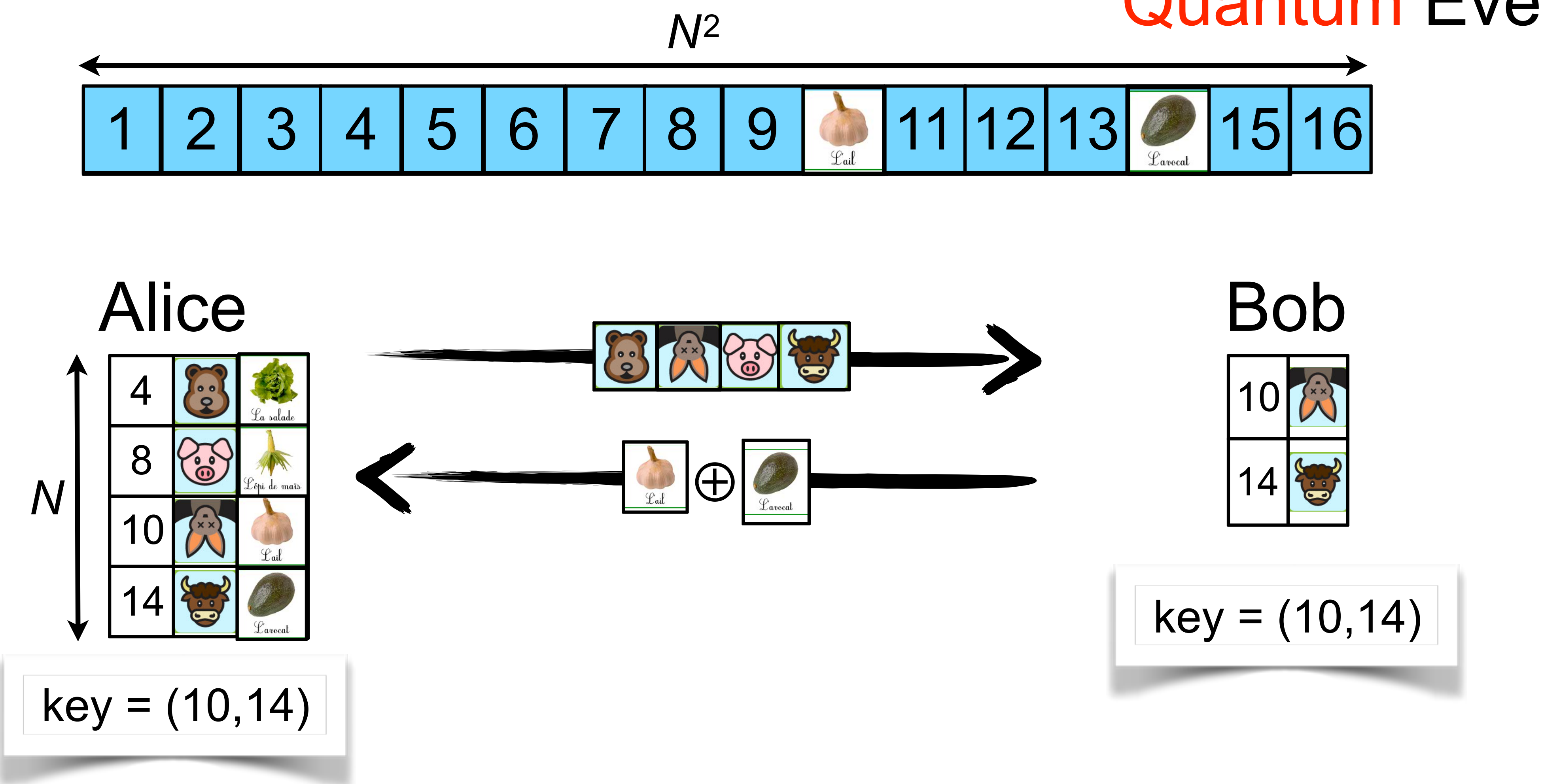
~~Diffie et Hellman (1976)~~

~~Rivest, Shamir, Adleman (1977)~~

¿ Robert McEliece (1978) ?

# Classical Merkle Secure Against Quantum Eve [BHKKLS]

Quantum Eve




Alice needs exactly $N$ calls to each oracle

Bob finds after $2N$+2 expected calls

This requires ~$N^{7/6}$ quantum expected calls!

# Quantum against Quantum

## Codemakers

Classical Quantum

## Codebreakers

Classical Quantum

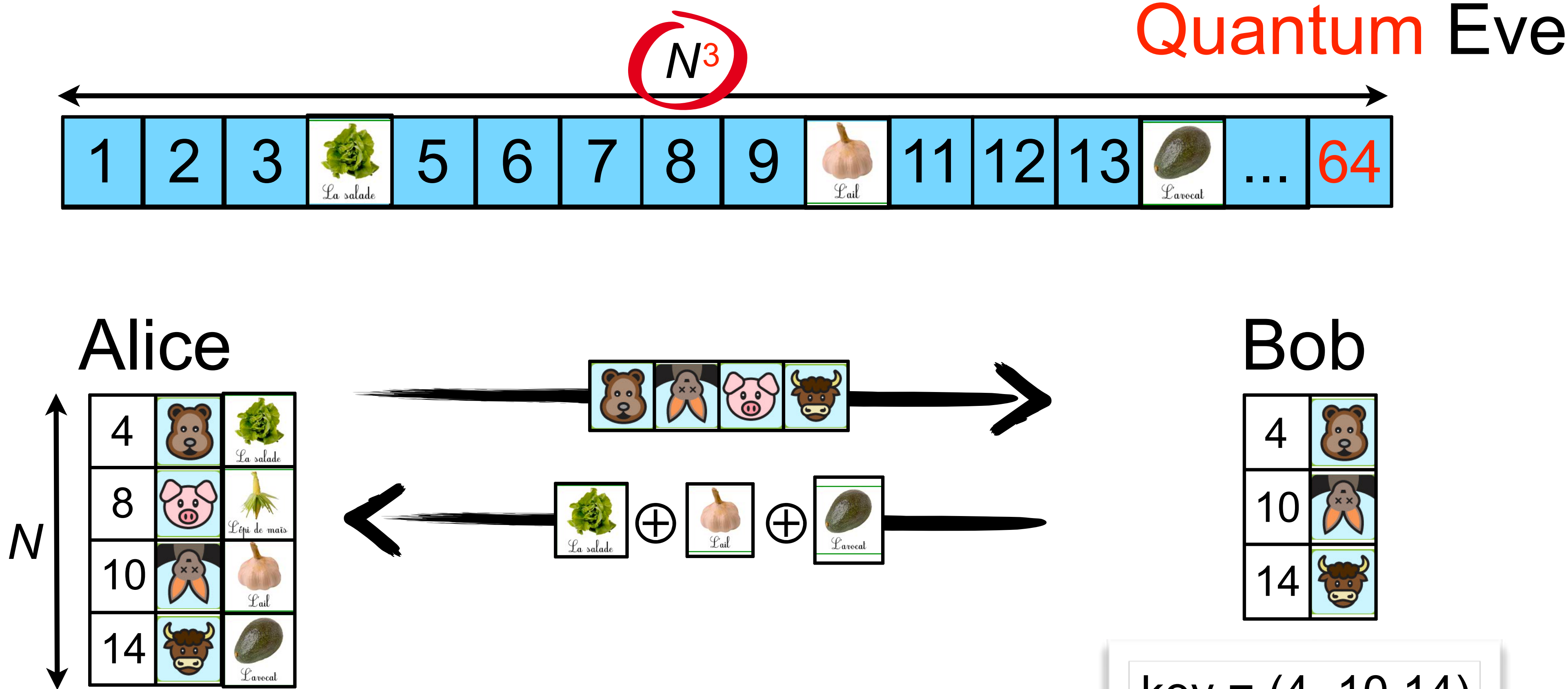
## Channels

Classical Quantum

# Key Establishment in a Quantum World

Quantum Adversary

# All Quantum World [BBHKKLS]




key = (4,10,14)

Alice needs exactly $N$ calls to each oracle

key = (4, 10,14)

Bob finds key after

$$3 \times O\left(\sqrt{\frac{N^3}{N}}\right) = O(N)$$

calls using BBHT

This requires ~$N^{7/4}$ quantum expected calls

# Summary with Classical Channels

UNPROVED security in the computational model

In a classical world, RSA and Diffie-Hellman seem to be secure, but we can't prove it.

In a quantum world, RSA and Diffie-Hellman (even using elliptic curves) are known to be insecure, but McEliece / New Hope / Frodo might be secure.

It seems that Quantum Mechanics is a curse for codemakers!

# Summary with Classical Channels

PROVABLE security in the black box model

When the legitimate parties work in time ~N ...

In a classical world, the eavesdropper must work in time $\sim N^2$ to learn their key.

In a quantum world, the eavesdropper can learn their key in time $\sim N^{7/4}$ against the best scheme discovered so far.

It seems that Quantum Mechanics is again a curse for codemakers!

# Quantum Cryptography

Codemakers

Classical Quantum

Codebreaker

Classical Quantum

Channels

Classical Quantum

# Quantum Cryptography

## Codemakers

(almost) Classical    Quantum

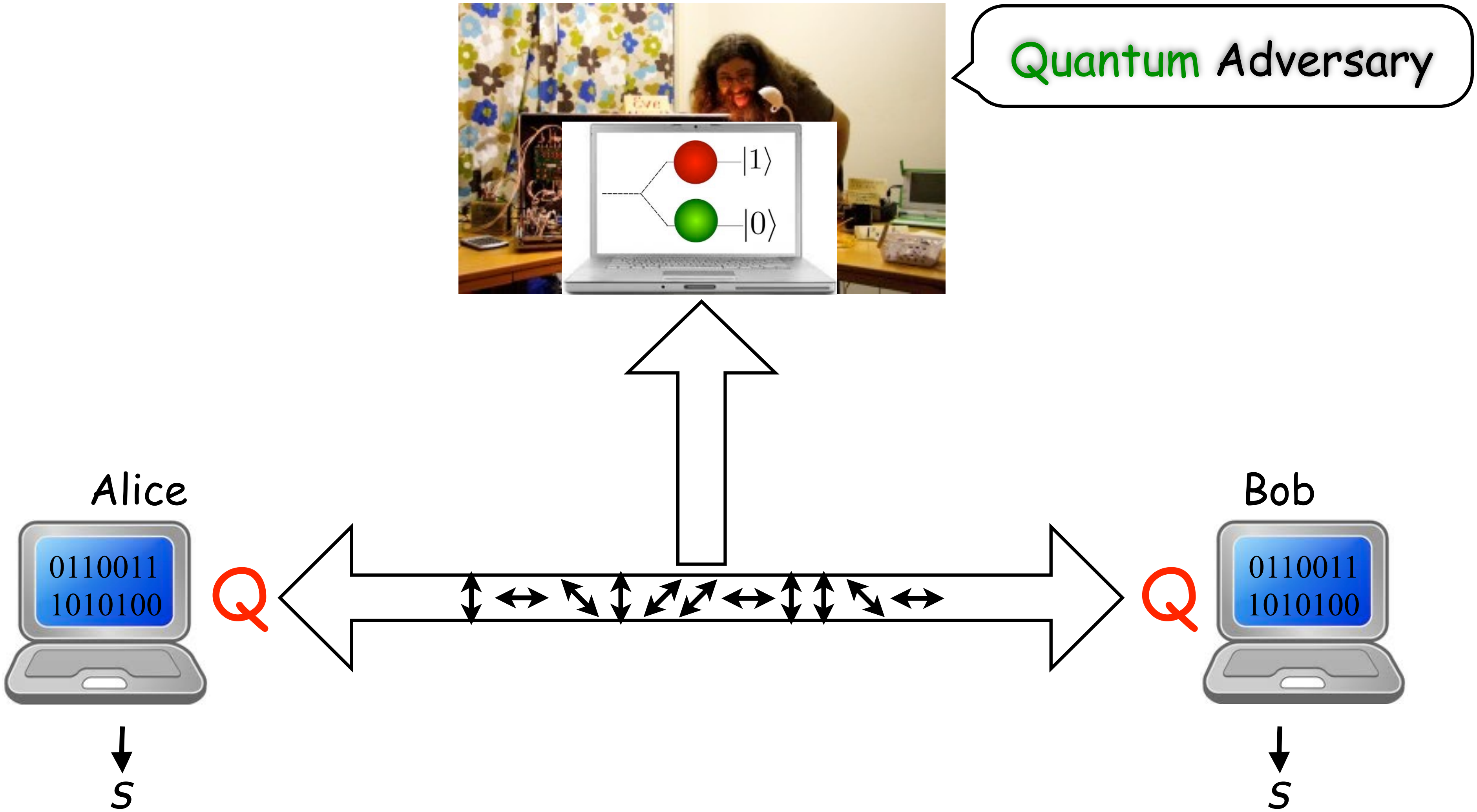
## Codebreaker

Classical    Quantum

## Channels

Classical    Quantum

# Quantum Cryptography



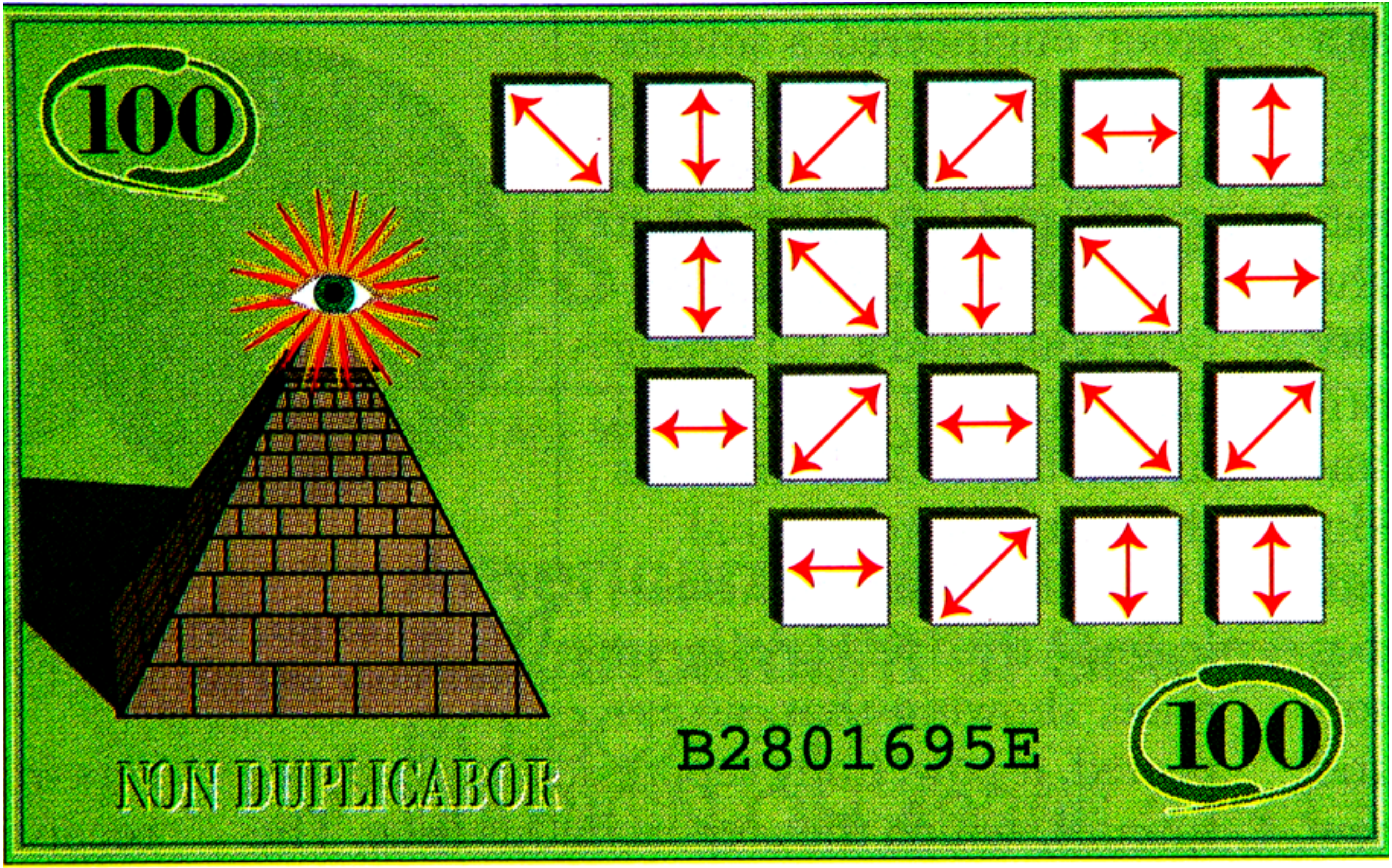

Stephen Wiesner

Conjugate Coding*

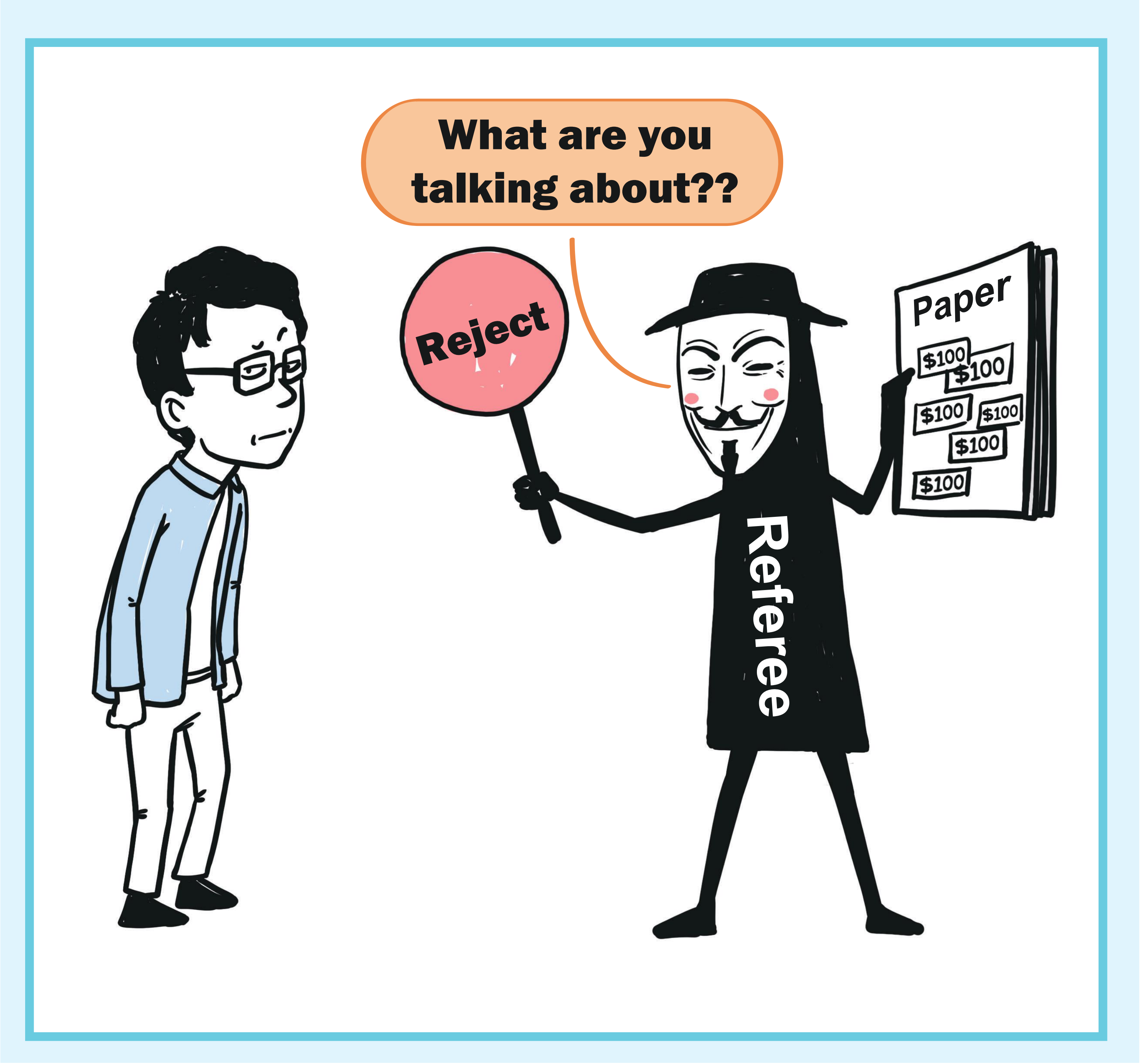
Stephen Wiesner

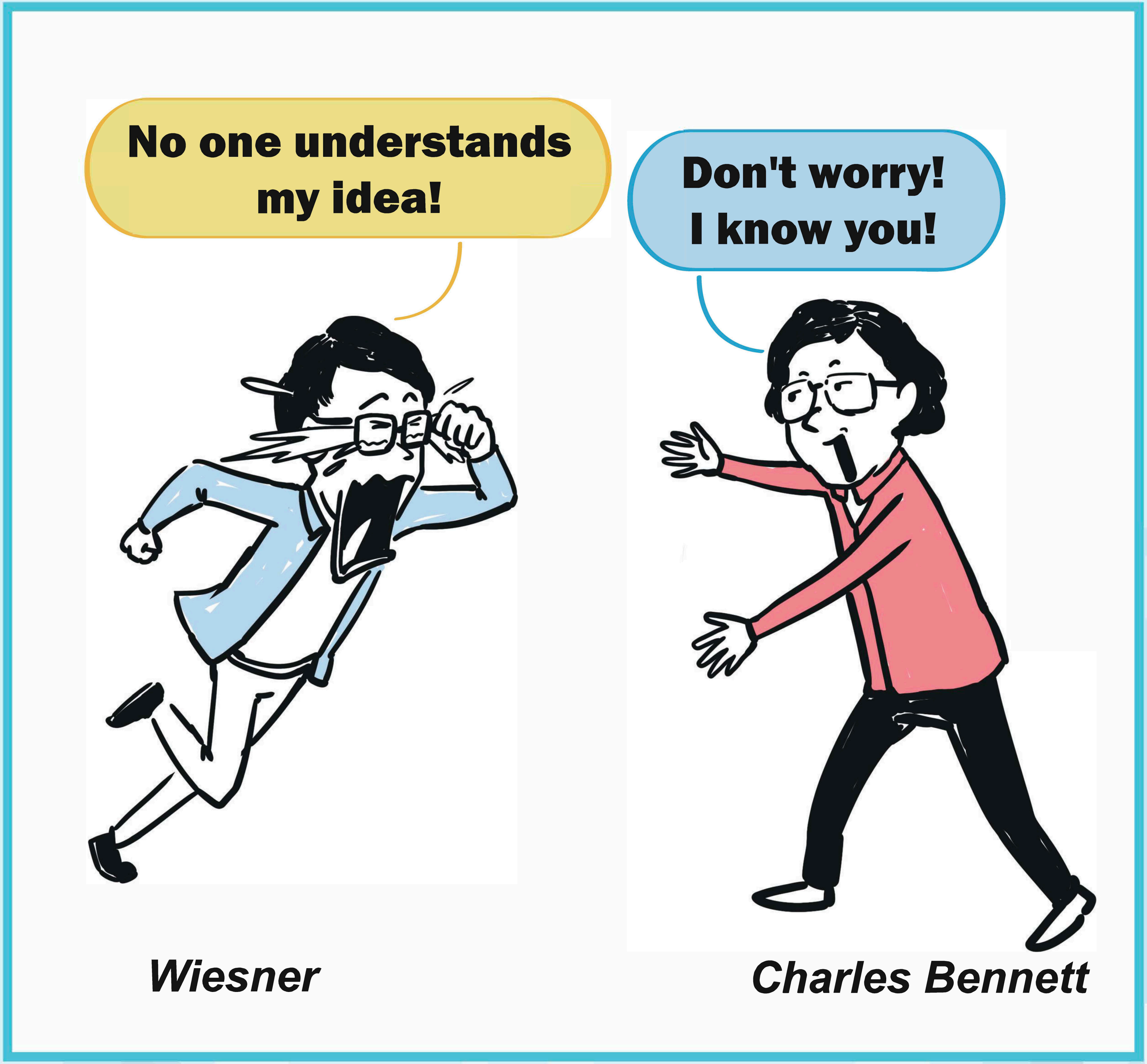
Columbia University, New York, N.Y.
Department of Physics

Written 1968
Published 1983!




**A quantum banknote**, containing particles in a secret set of quantum states, cannot be copied by counterfeiters, who would disturb the particles by attempting to observe them.


What are you talking about??
Reject
Paper
$100
$100
$100
$100
$100
$100
Referee


No one understands my idea!
Don't worry! I know you!
Wiesner
Charles Bennett

2/24/70 | 1

# Quantum Information Theory

False

Conversation w. Steve Wiesner, who told me that:

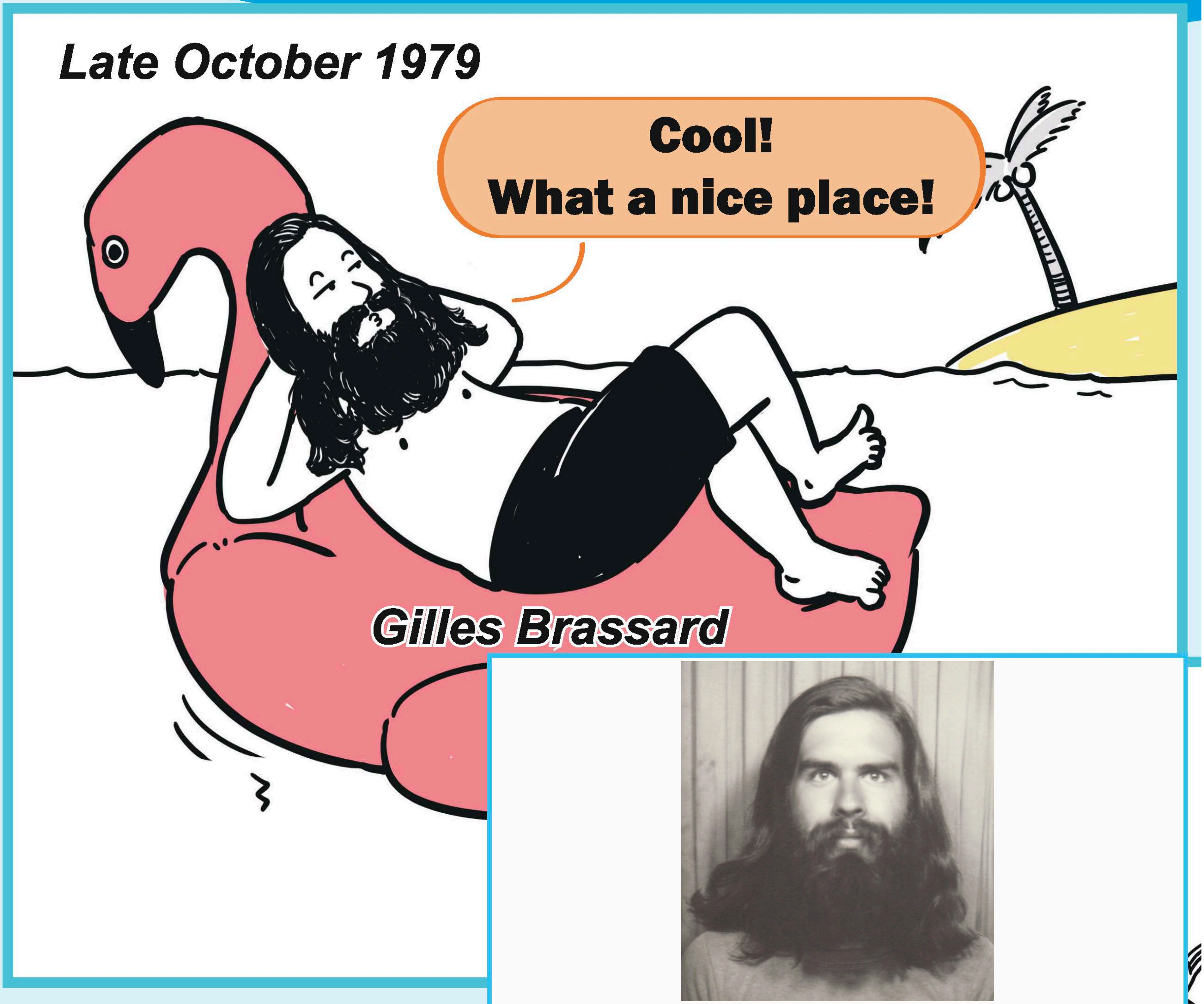
A variation on the Einstein-Rosen-Podolsky Gedankenexperiment can be used to send, through a channel with a nominal capacity of one bit, two bits of information; subject however to the constraint that, ~~that the receiver may at his choice read either~~ whichever bit the ~~[illegible]~~ receiver chooses to read, ~~[illegible]~~ the other bit is destroyed.

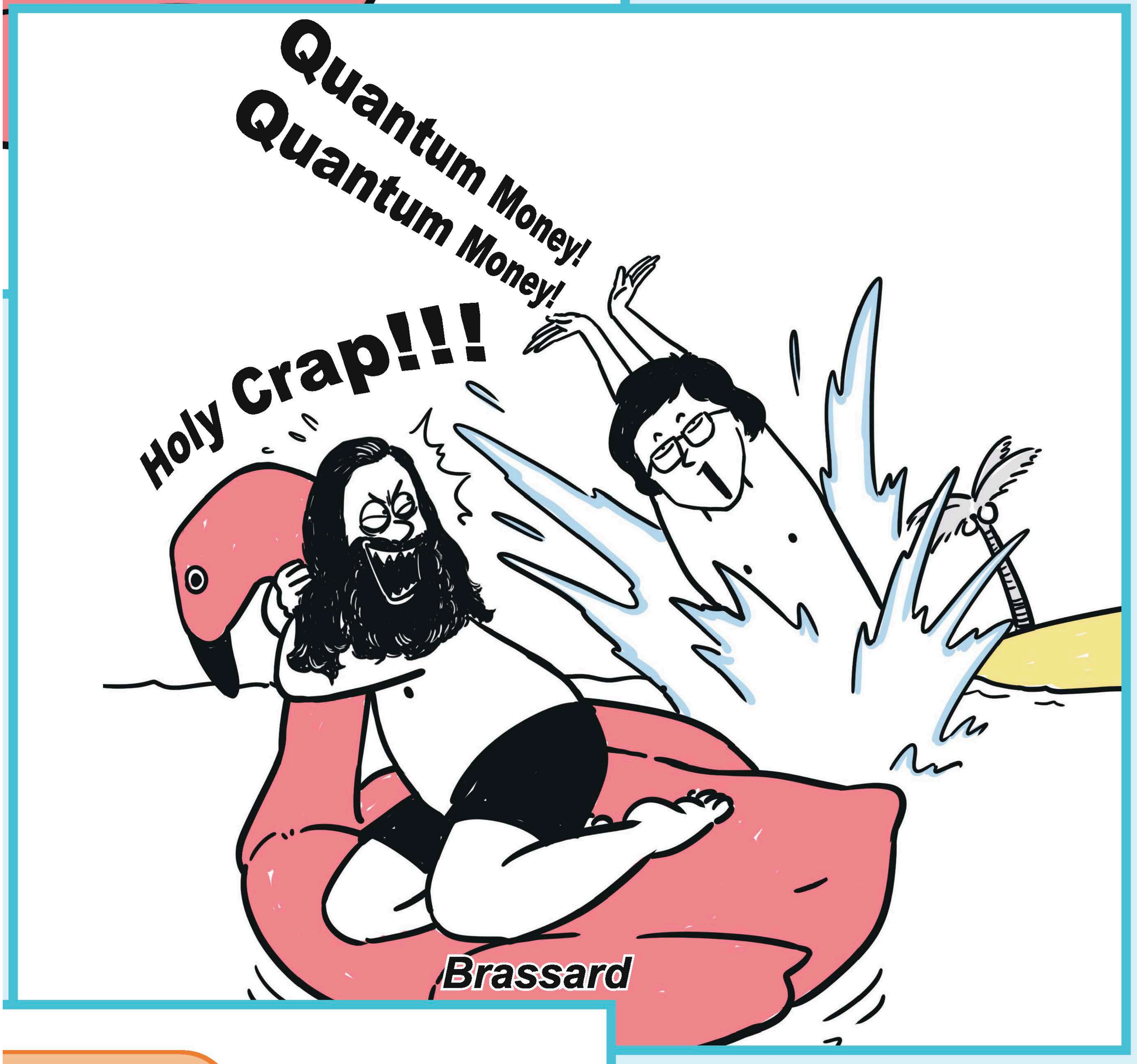
Start with a two-electron system in a singlet state. Separate the electrons and send one of them, A, to the receiver for later use as a sort of code-key. The sending of A does not constitute a message, since the transmitter has exercised no choice in preparing A. Take the other electron, B, and apply to it, at the sender's choice, one of the four operations $I$, $R_x^\pi$, $R_y^\pi$, $R_z^\pi$; where $I$ leaves it unchanged, $R_x^\pi$ rotates it 180° about the x-axis, etc. Now send B to the receiver. The receiver ~~[illegible]~~ is asked ~~[illegible] one of two measurements on both A & B [illegible] to $S_z$ where $S_y$ is~~ to select one spin component, y or z, and measure this same component for both electrons A & B. In either case the receiver recovers one bit of the two bit message encoded into B by the sender's choice of the operators $\{I, R_x, R_y, R_z\}$.

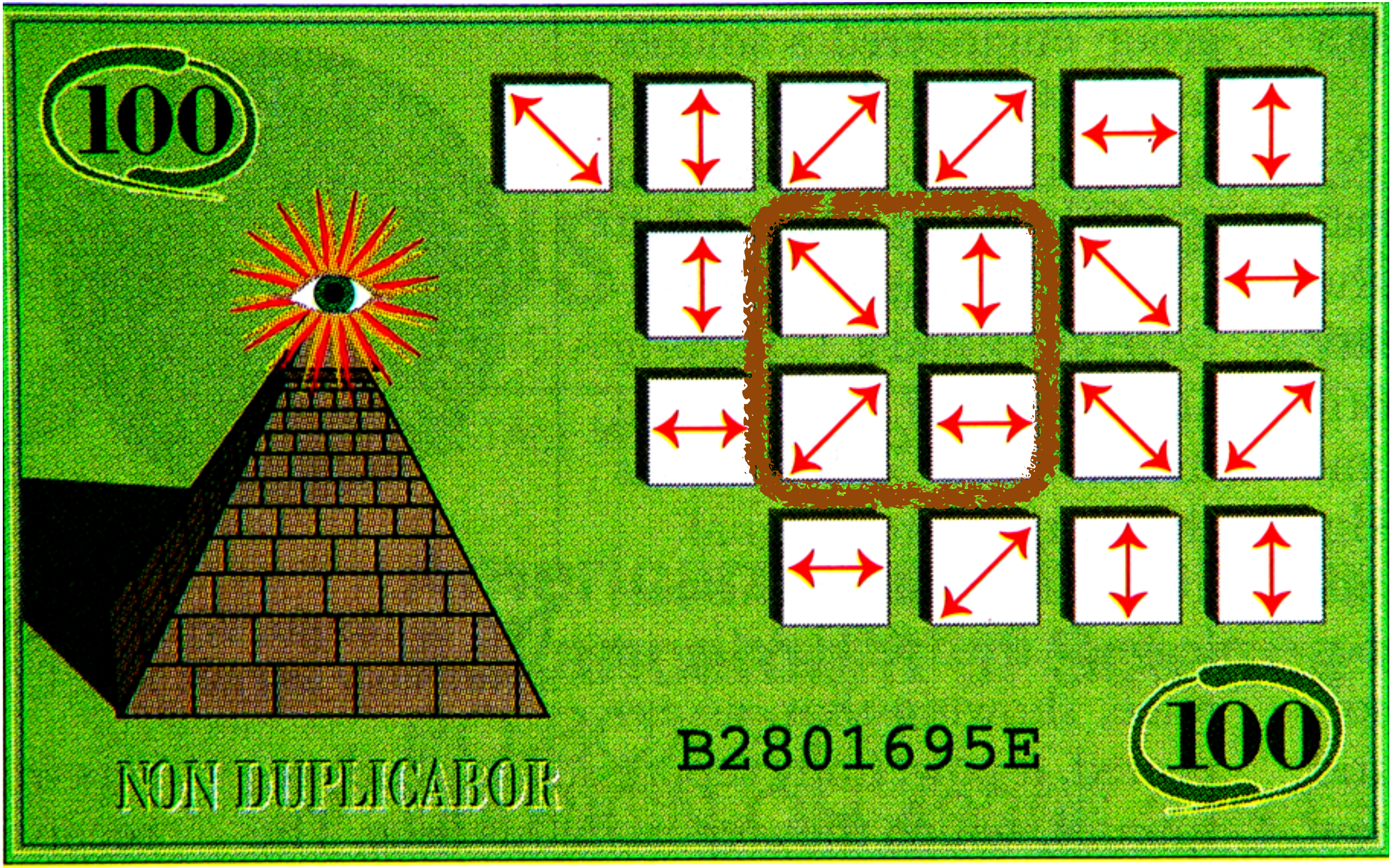
| | Receiver Measures → $S_y$ | $S_z$ |
|---|---|---|
| Sender has applied: $I$ | 0 | 0 |
| $R_x$ | S | S |
| $R_y$ | 0 | S |
| $R_z$ | S | 0 |

S: same spin component

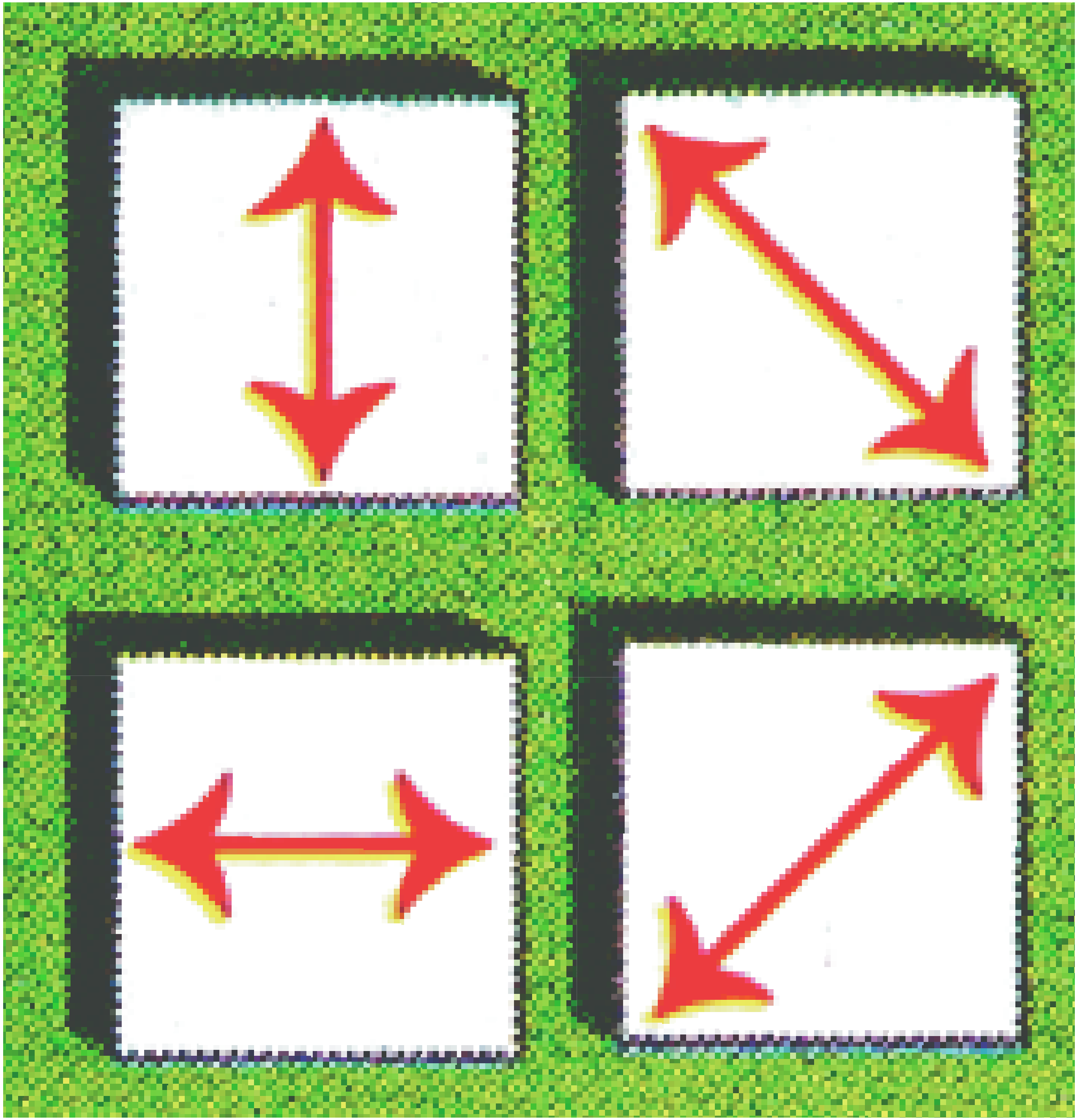
O: A & B have opposite values of the measured spin component.


Late October 1979
Cool!
What a nice place!
Gilles Brassard

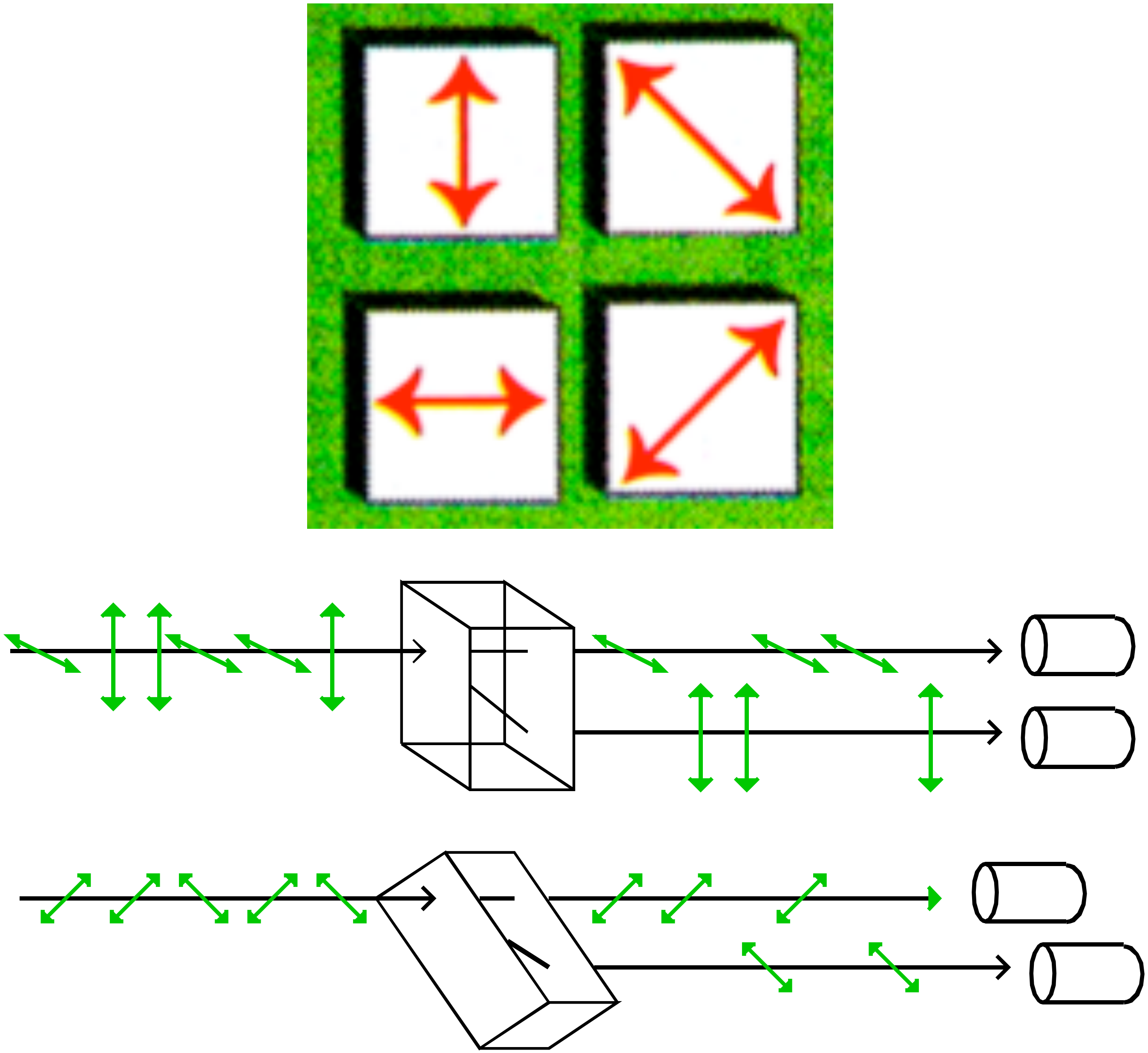

Quantum Money!
Quantum Money!
Holy Crap!!!
Brassard

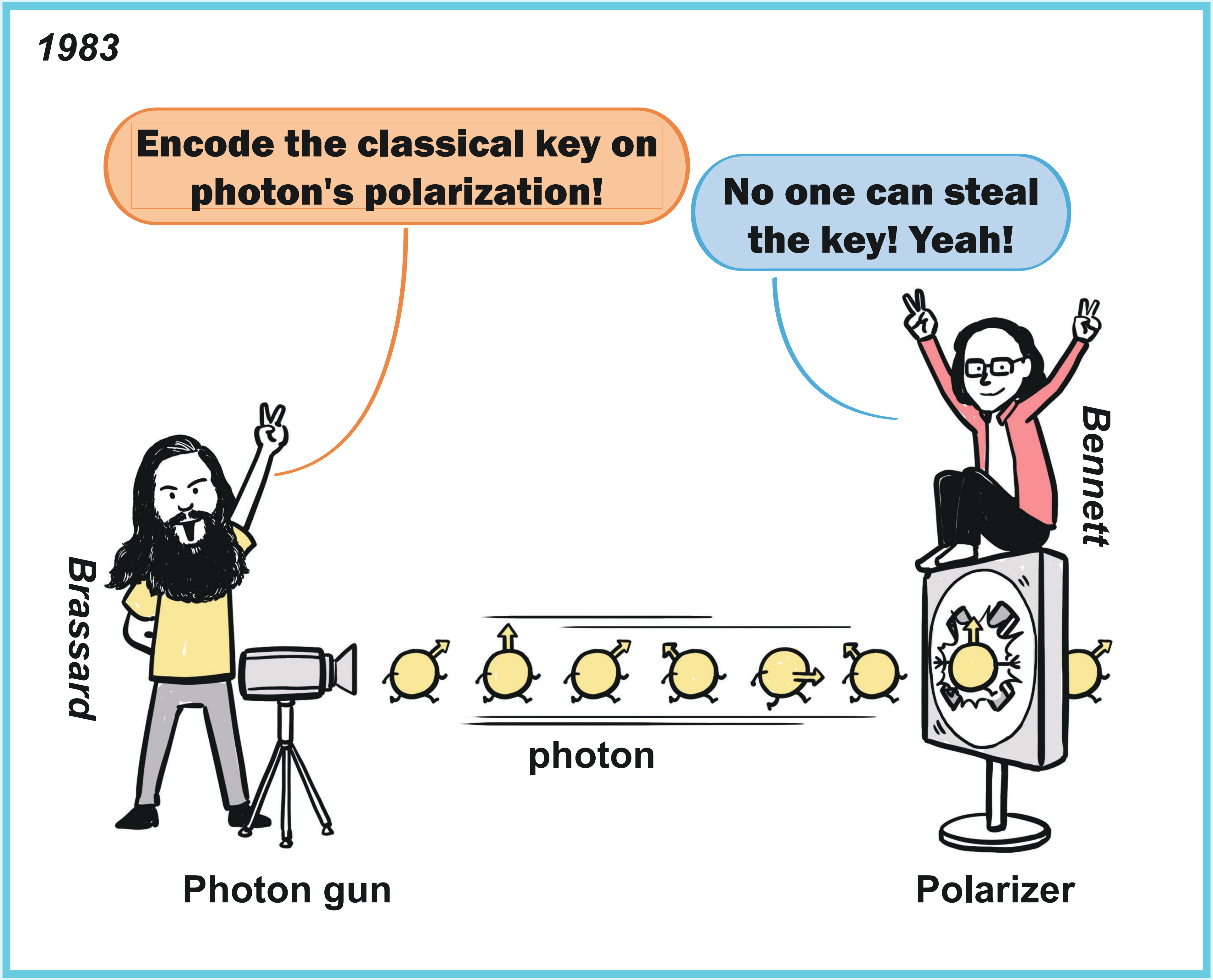



**A quantum banknote**, containing particles in a secret set of quantum states, cannot be copied by counterfeiters, who would disturb the particles by attempting to observe them.



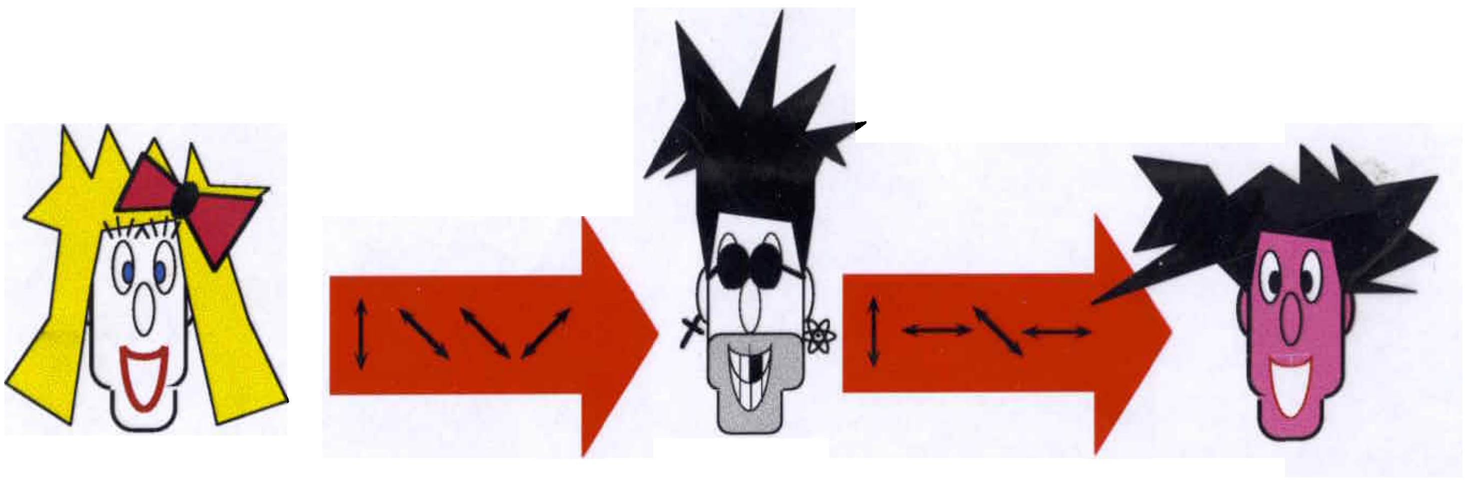
# No measurement can distinguish all four kinds.




1983
Encode the classical key on photon's polarization!
No one can steal the key! Yeah!
Bennett
Brassard
photon
Photon gun
Polarizer

These states cannot be distinguished reliably

Eavesdropping → Errors → Detection



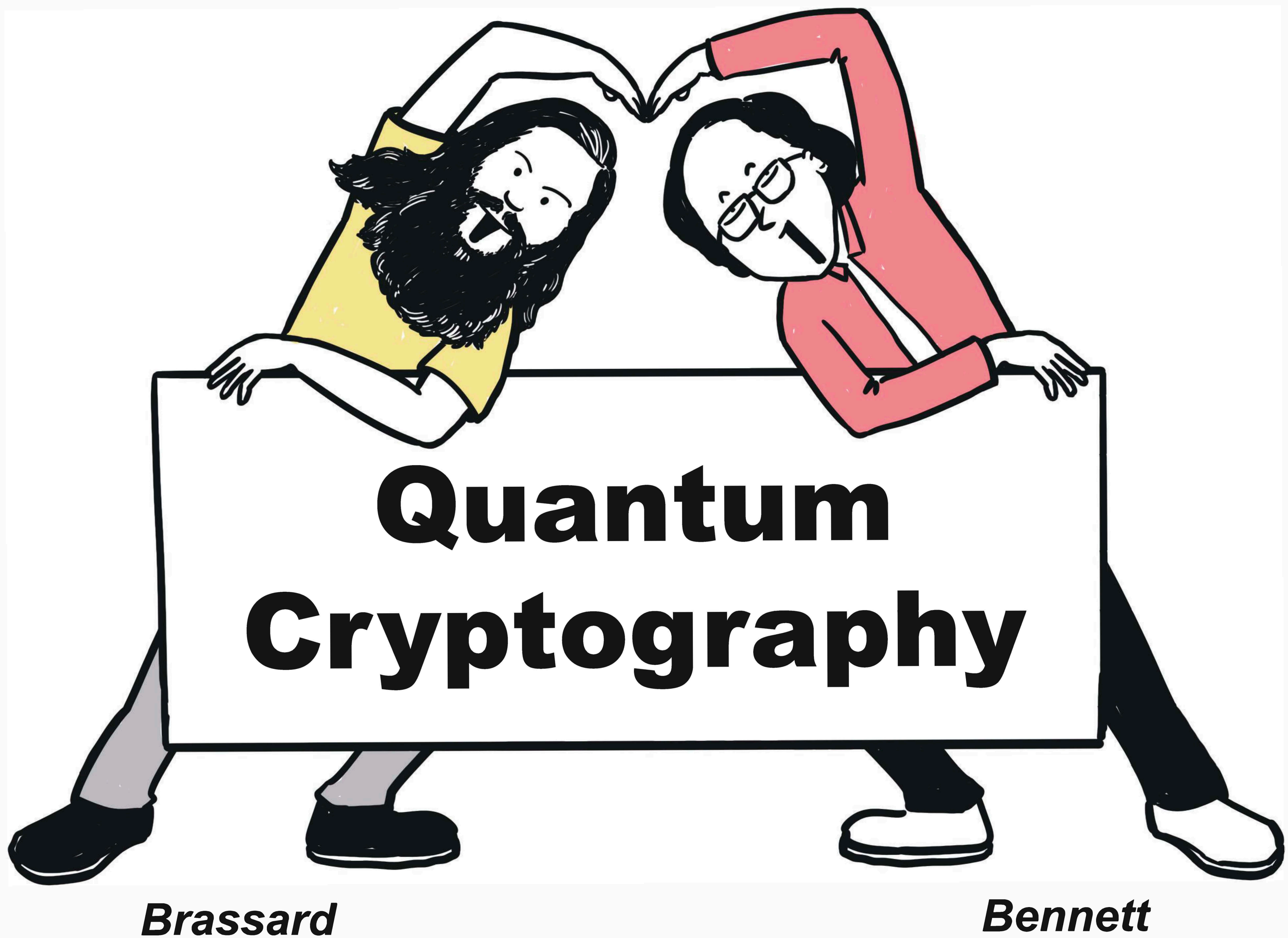
These states cannot be distinguished reliably

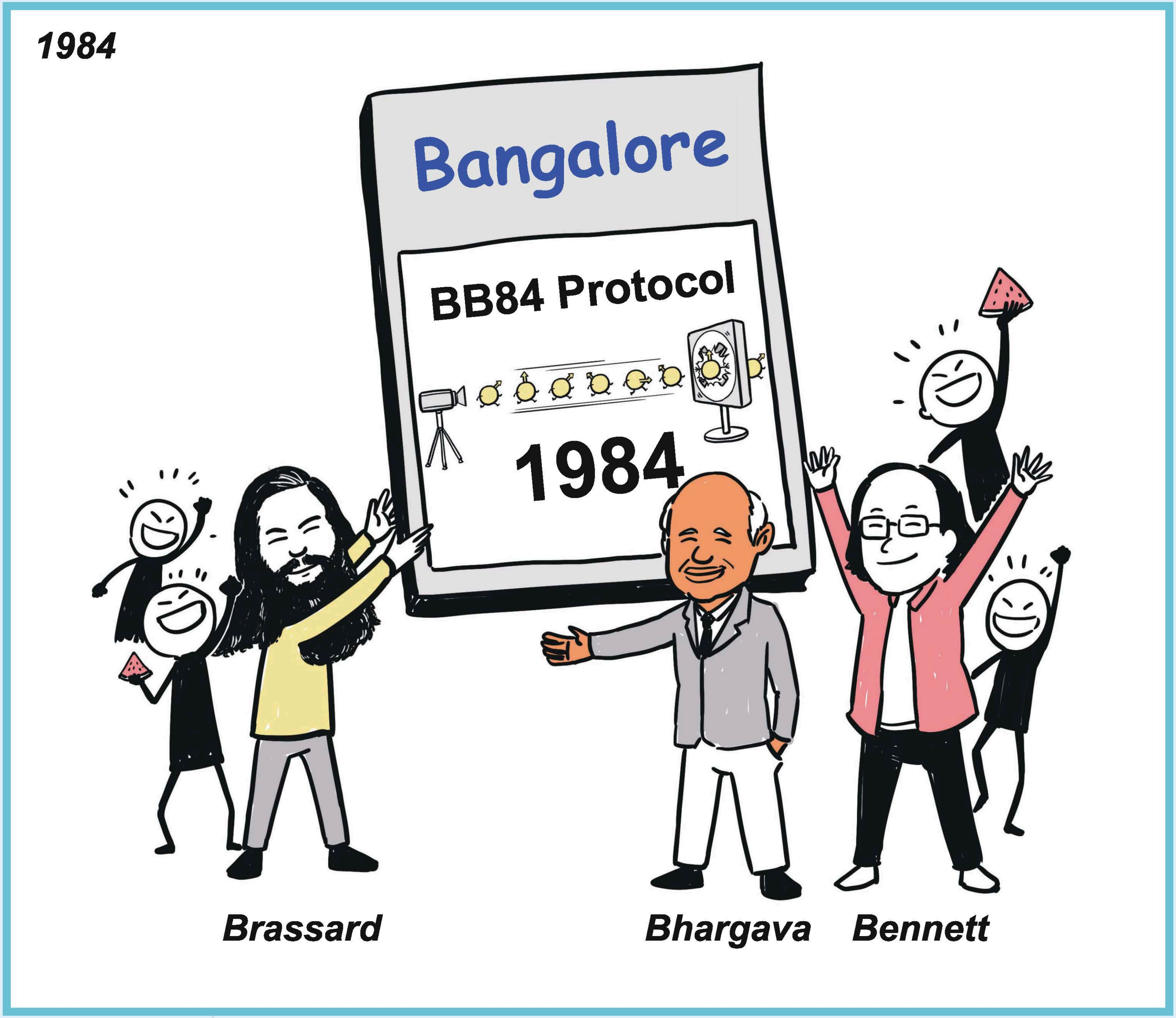
Eavesdropping → Errors → Detection

Use quantum channel to send random key

+ classical one-time-pad to send message

→ eavesdropping prevention


Quantum
Cryptography
Brassard
Bennett




By Sheldon Li

# Quantum Cryptography

## Unconditionally Confidential Transmission of Information

regardless of eavesdropper's technology and computing power

# Who will win?

Codemakers

or

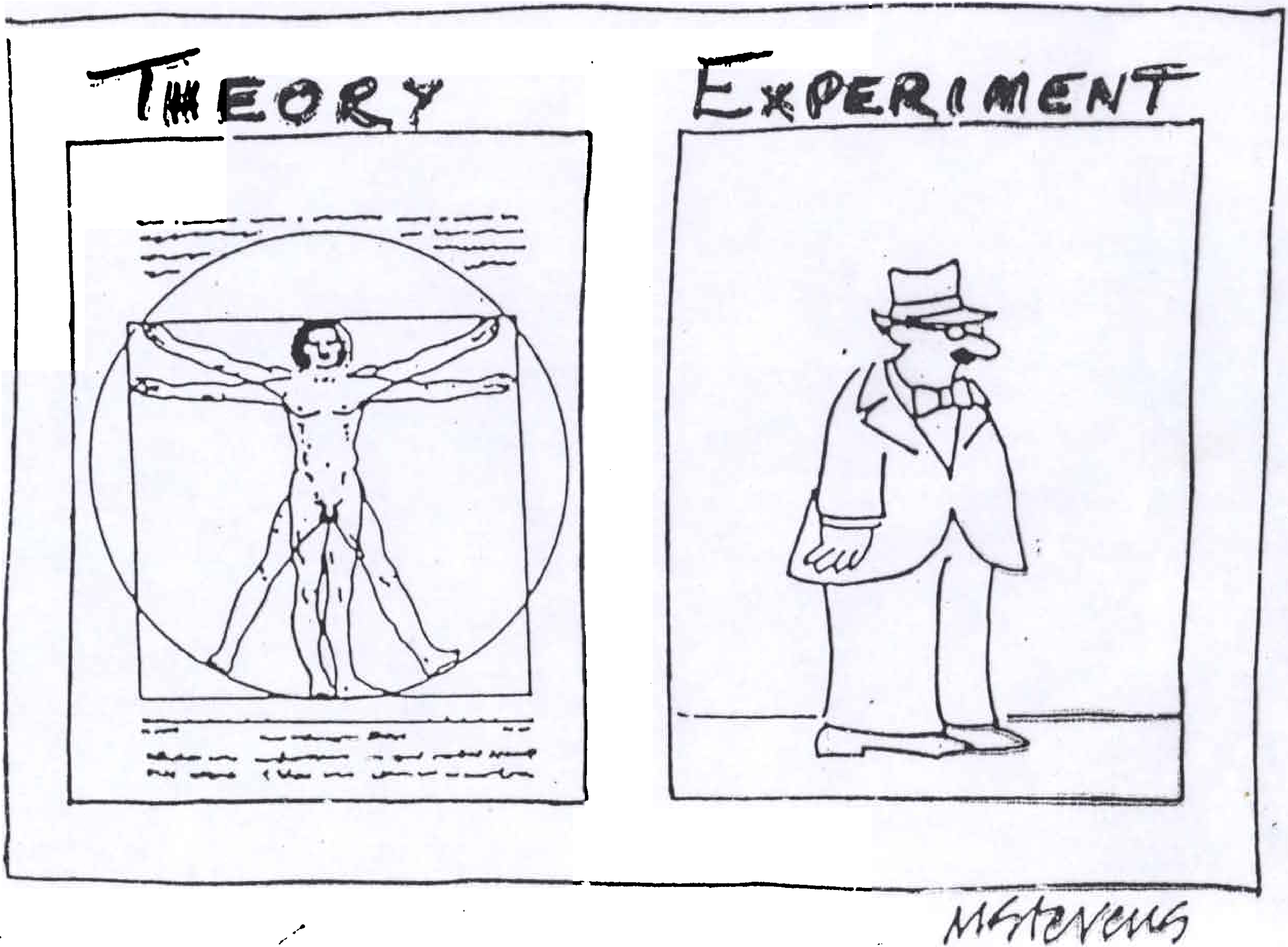
Codebreakers

?

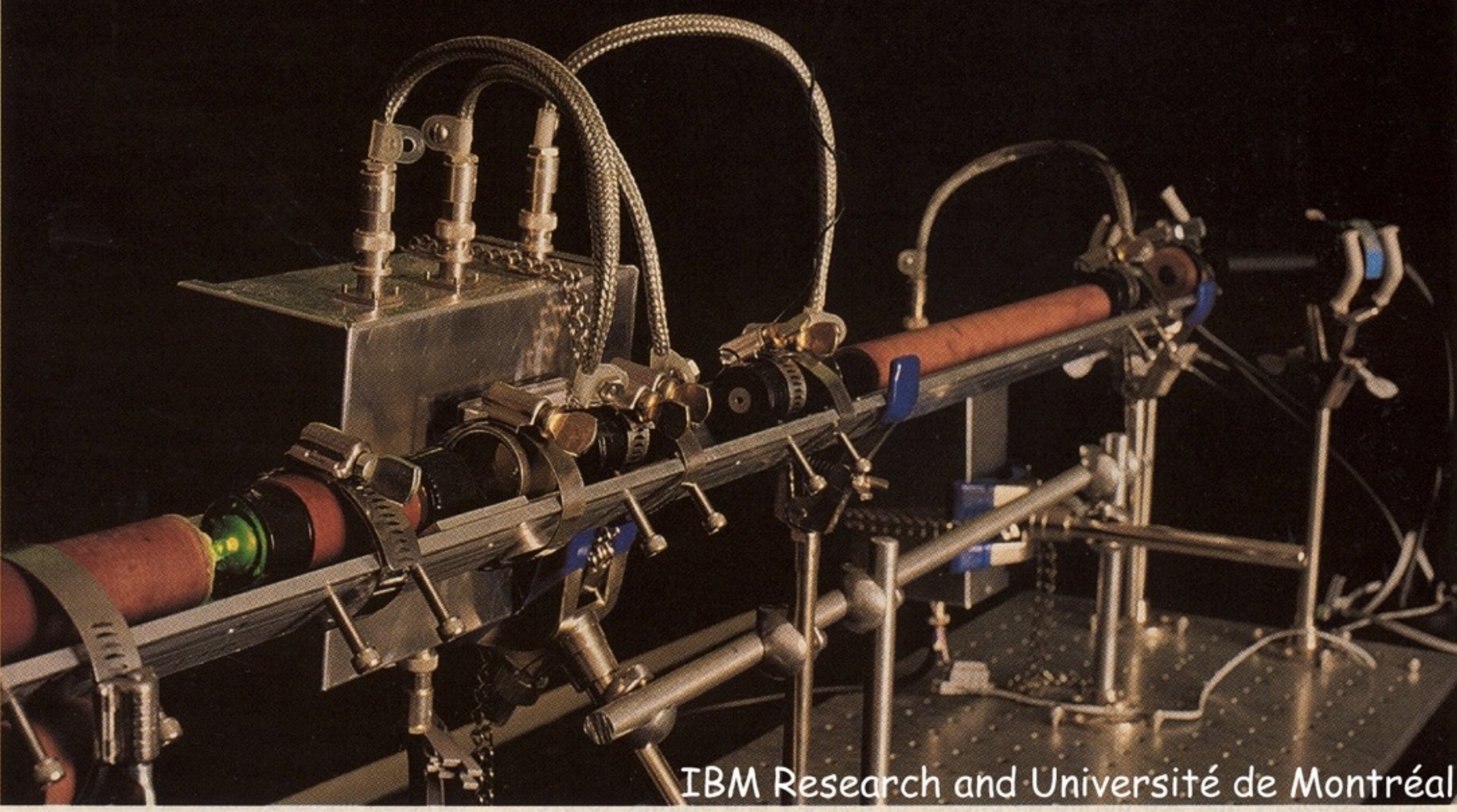
# Who will win?

« It may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve »

Poe was wrong!


THEORY
EXPERIMENT
MStevens

1989: Bennett, Bessette, Brassard, Salvail, Smolin



IBM Research and Université de Montréal

QUANTUM DEVICE generates and measures extremely faint flashes of polarized light, providing a secure way to transmit information [*see illustration on pages 56 and 57*]. On average each flash consists of one tenth of a photon.

Redefining Security!

IDQ is a leading supplier of high-performance multi-protocol NETWORK ENCRYPTION solutions and QUANTUM KEY DISTRIBUTION equipment.



## CENTAURIS CN8000 ENCRYPTOR: SWISS QUANTUM SECURITY

The **Centauris** CN8000 multi-link encryptor is designed to cost-effectively protect traffic on large-scale data networks. It delivers the performance capabilities of ten 10Gbps Centuaris encryptors in one compact chassis, encrypting up to 100Gbps of multiprotocol layer 2 network traffic with no overhead and minimum latency.

The CN8000 is Swiss-manufactured and quantum powered for high security.


Beijing
Jinan
Hefei
Shanghai

# China launches world's 1st quantum satellite

**QUESS satellite designed to establish 'hack-proof' quantum communications**

Thomson Reuters Posted: Aug 16, 2016 9:00 AM ET | Last Updated: Aug 16, 2016 11:56 AM ET

**China launches revolutionary quantum satellite** 0:44

China on Tuesday launched the world's first quantum satellite, which will help it establish "hack-proof" communications between space and the ground, state media said, the latest advance in an ambitious space programme.

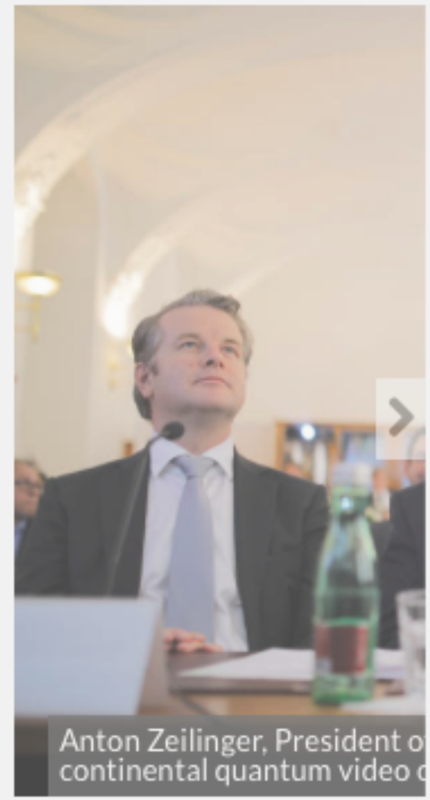
09/29/2017

# AUSTRIAN AND CHINESE ACADEMIES OF SCIENCES SUCCESSFULLY CONDUCTED FIRST INTER-CONTINENTAL QUANTUM VIDEO CALL

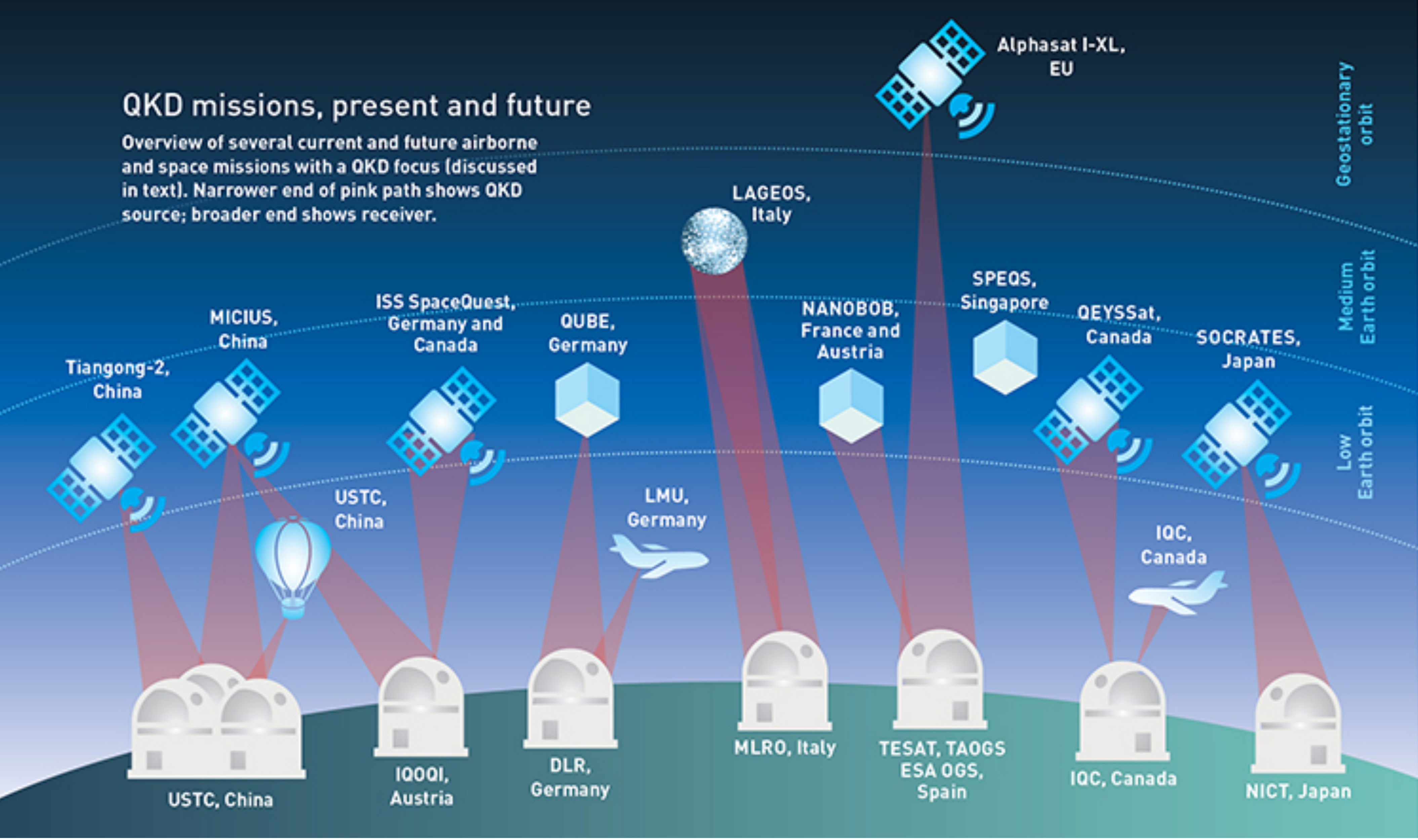
**The two Academy presidents Chunli Bai and Anton Zeilinger tested quantum encrypted communication between Beijing and Vienna in a live-experiment. The quantum key was transmitted via the Chinese quantum satellite Micius.**

cademy of Sciences. © ÖAW

© Johannes Handsteiner/ÖAW



Anton Zeilinger, President o
continental quantum video c


QKD missions, present and future
Overview of several current and future airborne and space missions with a QKD focus (discussed in text). Narrower end of pink path shows QKD source; broader end shows receiver.
Alphasat I-XL, EU
LAGEOS, Italy
Geostationary orbit
Medium Earth orbit
Low Earth orbit
SPEQS, Singapore
NANOBOB, France and Austria
QEYSSat, Canada
SOCRATES, Japan
ISS SpaceQuest, Germany and Canada
QUBE, Germany
MICIUS, China
Tiangong-2, China
USTC, China
LMU, Germany
IQC, Canada
USTC, China
IQOQI, Austria
DLR, Germany
MLRO, Italy
TESAT, TAOGS ESA OGS, Spain
IQC, Canada
NICT, Japan

# Who will win?

« It may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve »

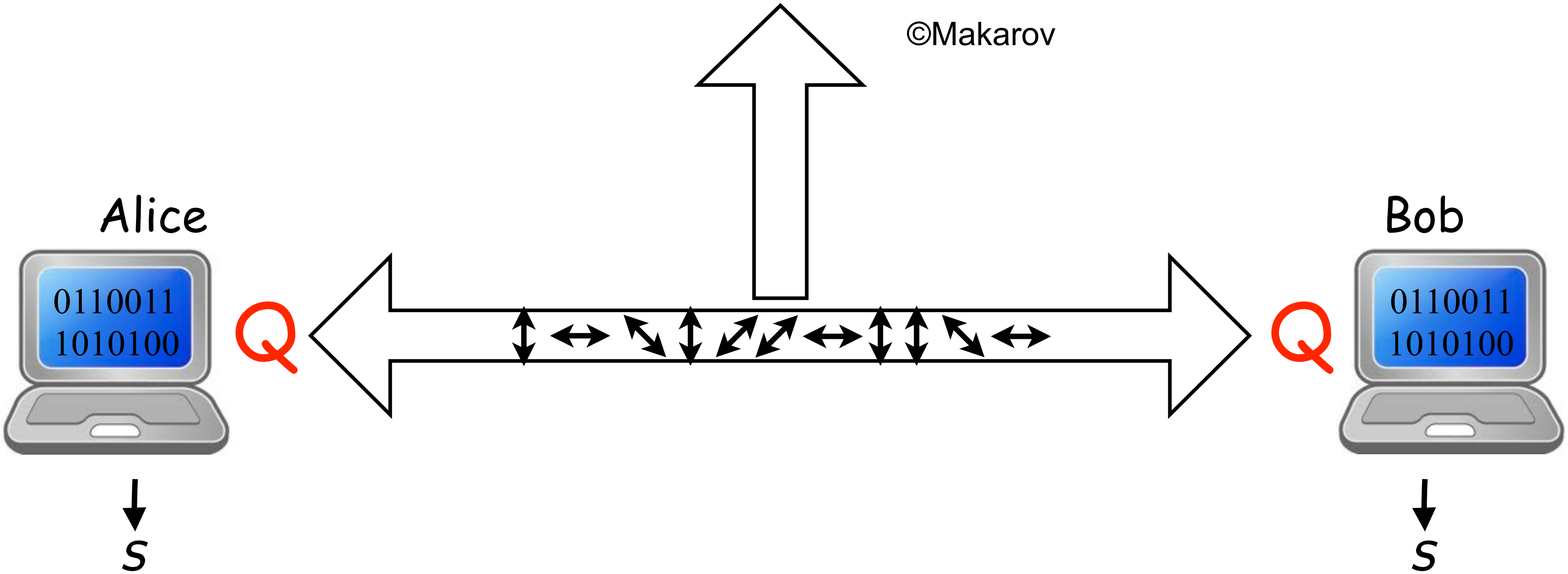
Poe was wrong!

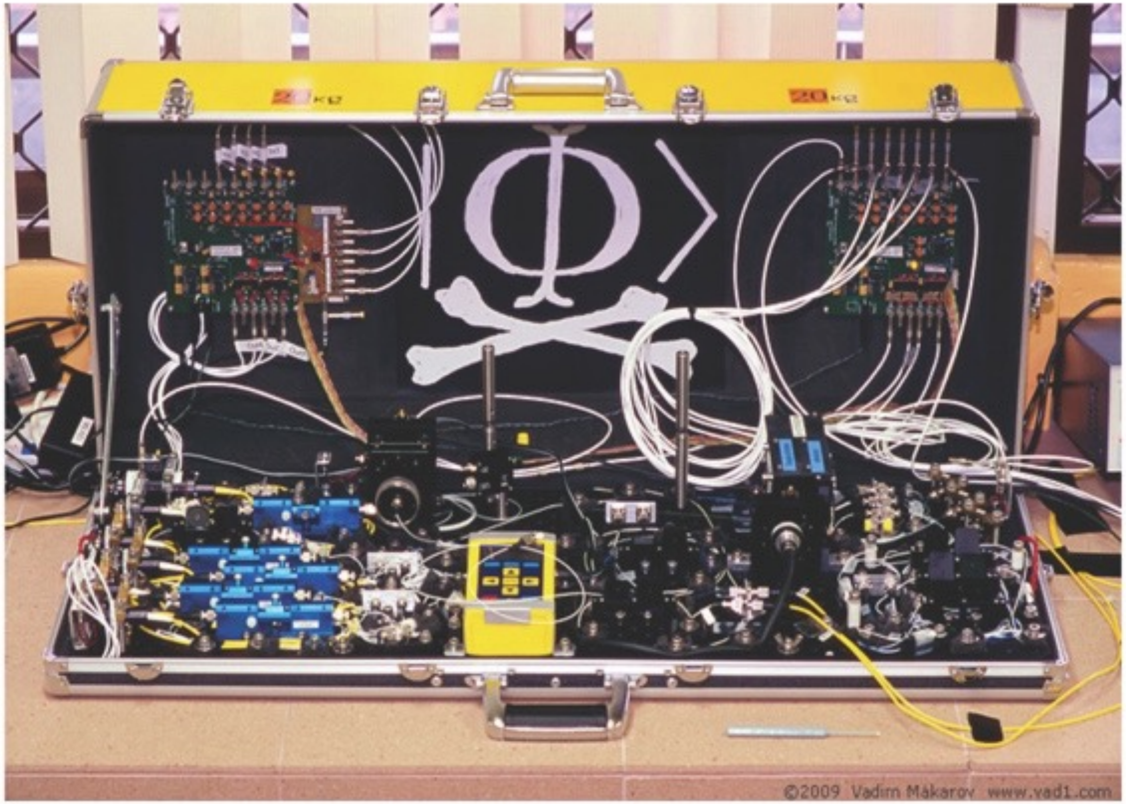

|Φ⟩

# Établissement de clef dans un monde quantique

Adversaire quantique

©Makarov




©2009 Vadim Makarov www.vad1.com

# Who will win?

« It may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve »

Was Poe right after all?

# The Big Question

We live in a quantum world

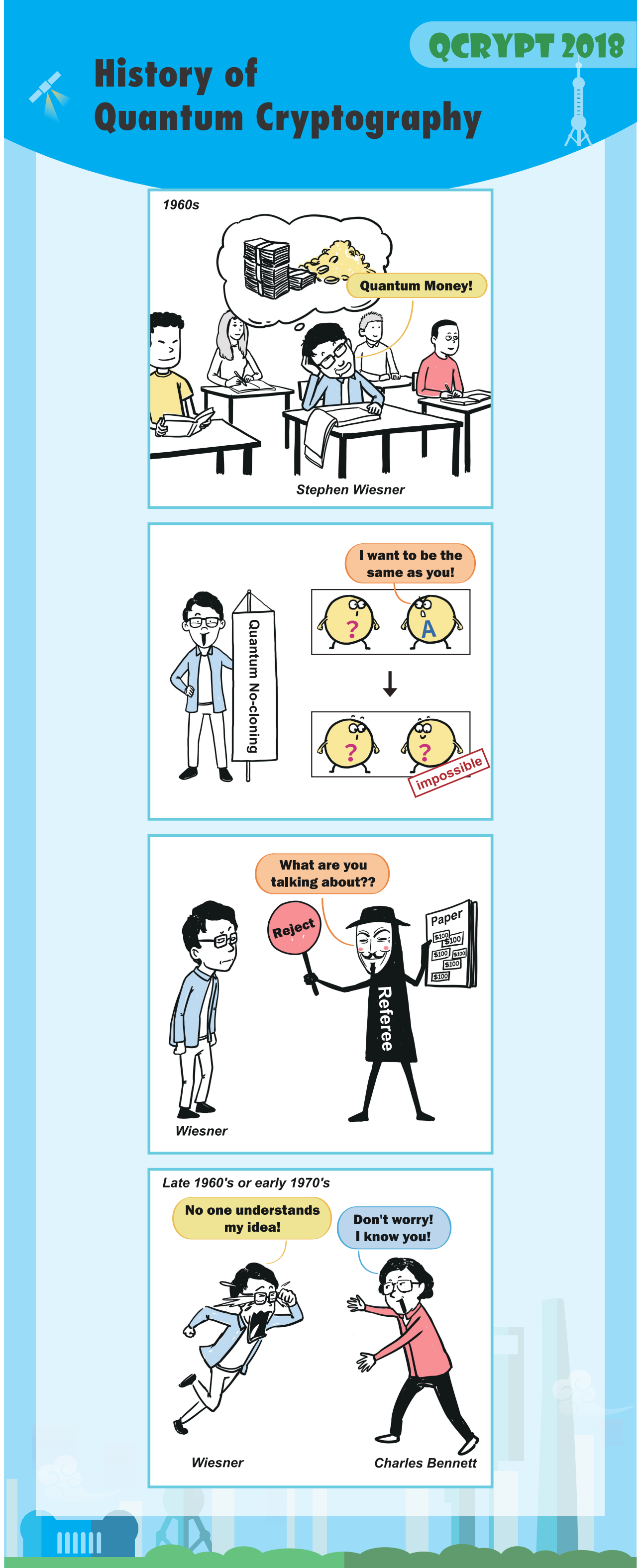
Is this a *blessing*

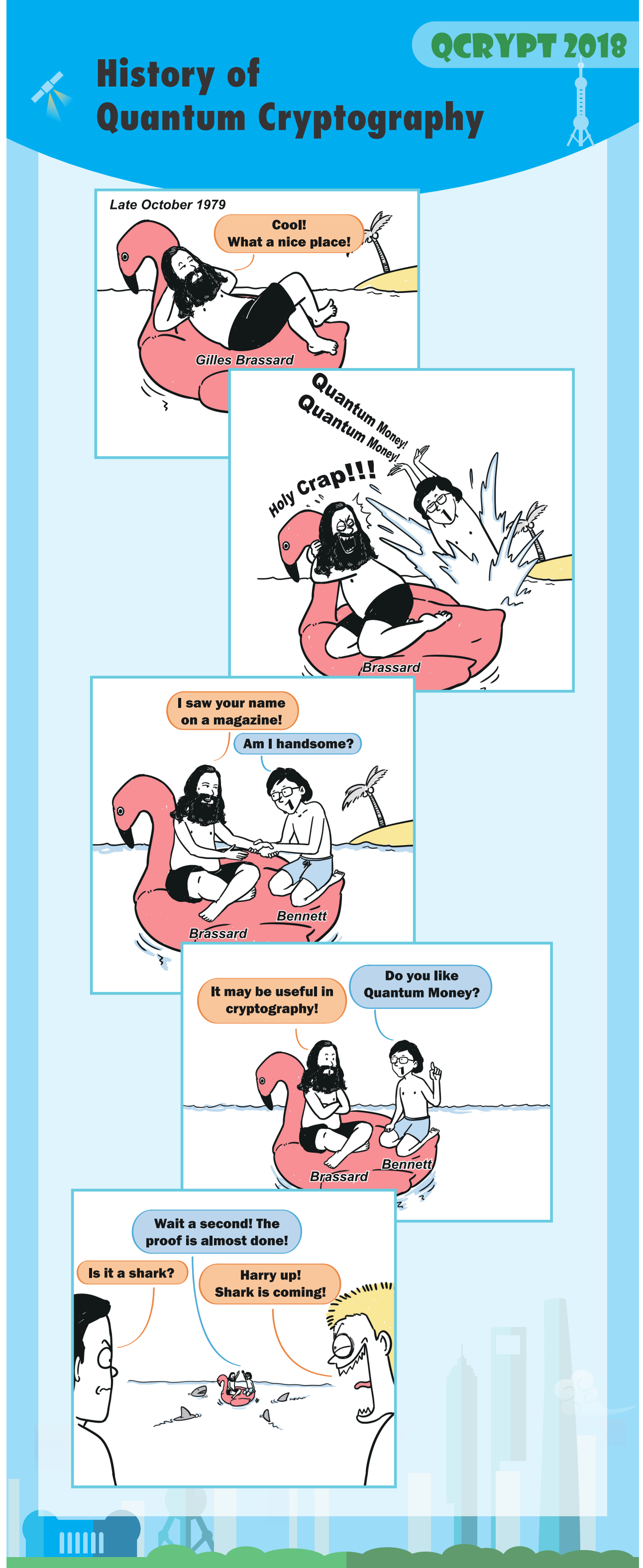
or a **curse**

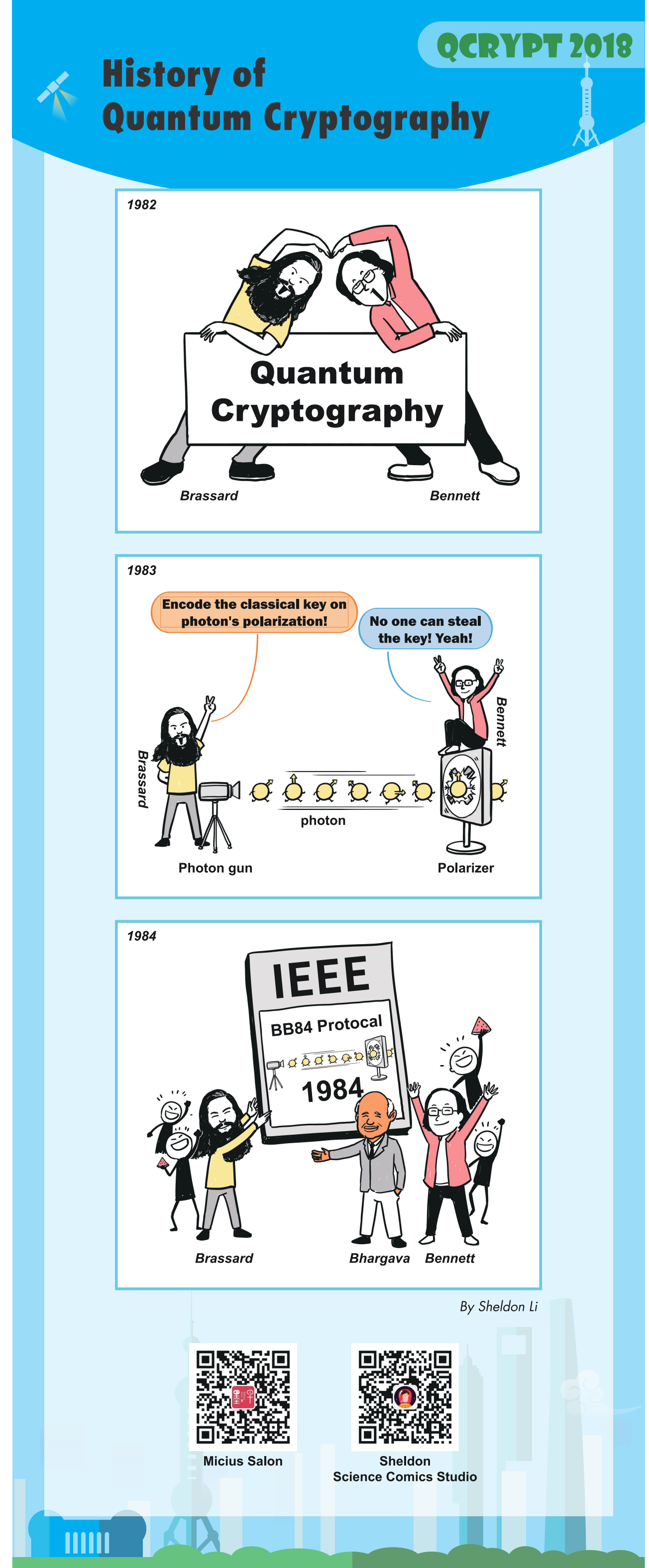
for codemakers?

**The jury is still out!**


*"About your cat, Mr. Schrödinger—I have good news and bad news."*


QCRYPT 2018
History of
Quantum Cryptography
1960s
Quantum Money!
Stephen Wiesner
I want to be the same as you!
Quantum No-cloning
impossible
What are you talking about??
Reject
Paper
Referee
Wiesner
Late 1960's or early 1970's
No one understands my idea!
Don't worry! I know you!
Wiesner
Charles Bennett


QCRYPT 2018
History of
Quantum Cryptography
Late October 1979
Cool! What a nice place!
Gilles Brassard
Quantum Money! Quantum Money!
Holy Crap!!!
Brassard
I saw your name on a magazine!
Am I handsome?
Brassard
Bennett
It may be useful in cryptography!
Do you like Quantum Money?
Brassard
Bennett
Wait a second! The proof is almost done!
Is it a shark?
Harry up! Shark is coming!


QCRYPT 2018
History of
Quantum Cryptography
1982
Quantum Cryptography
Brassard
Bennett
1983
Encode the classical key on photon's polarization!
No one can steal the key! Yeah!
Brassard
Bennett
photon
Photon gun
Polarizer
1984
IEEE
BB84 Protocal
1984
Brassard
Bhargava
Bennett
By Sheldon Li
Micius Salon
Sheldon Science Comics Studio