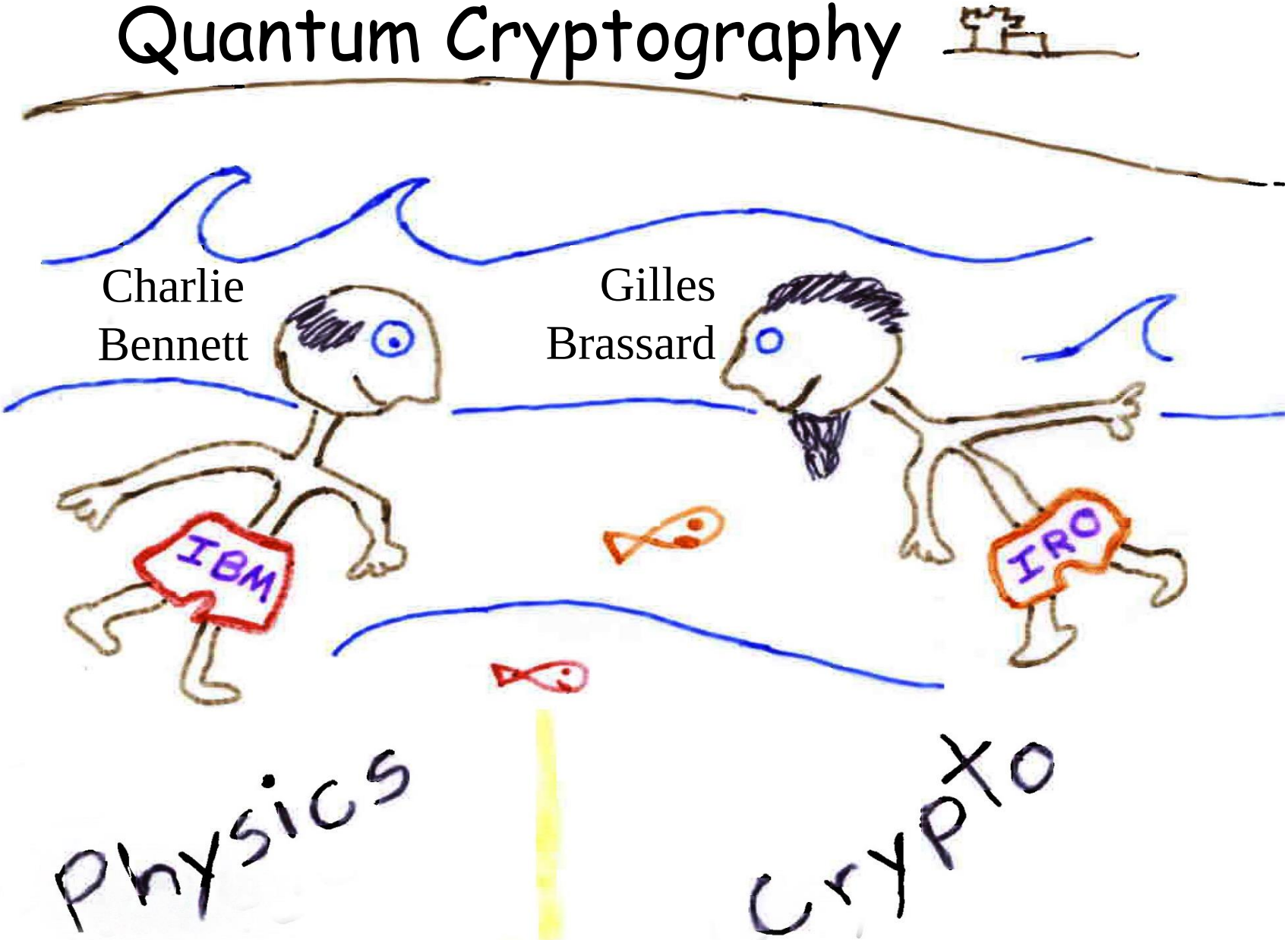
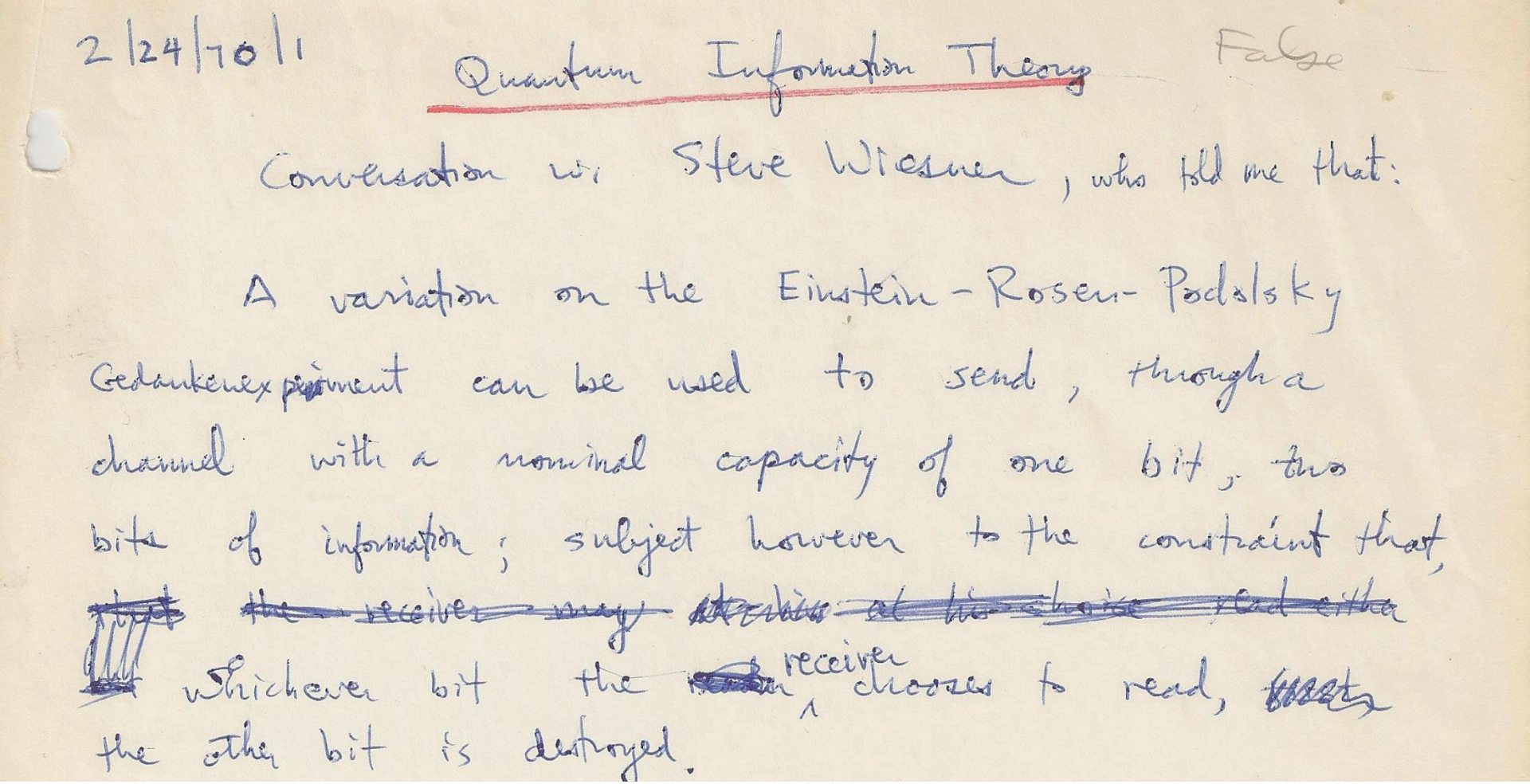
Reminiscences on the beginnings of

Quantum Cryptography



San Juan, Puerto Rico, 1979 drawing courtesy of Chris Fuchs



Bennett's Feb. 1970 notes on Wiesner's ideas, possibly the first mention of "quantum information theory." They describe using an entangled state to multiplex two bits into a signal from which either bit, but not both, can be read. Later Wiesner realized that a joint measurement *would* reveal both (hence the added "false" at upper right), but that fact shows the scheme can achieve another distinctively quantum feat, now called **superdense coding.**

Submitted to IEEE, Information Theory

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.

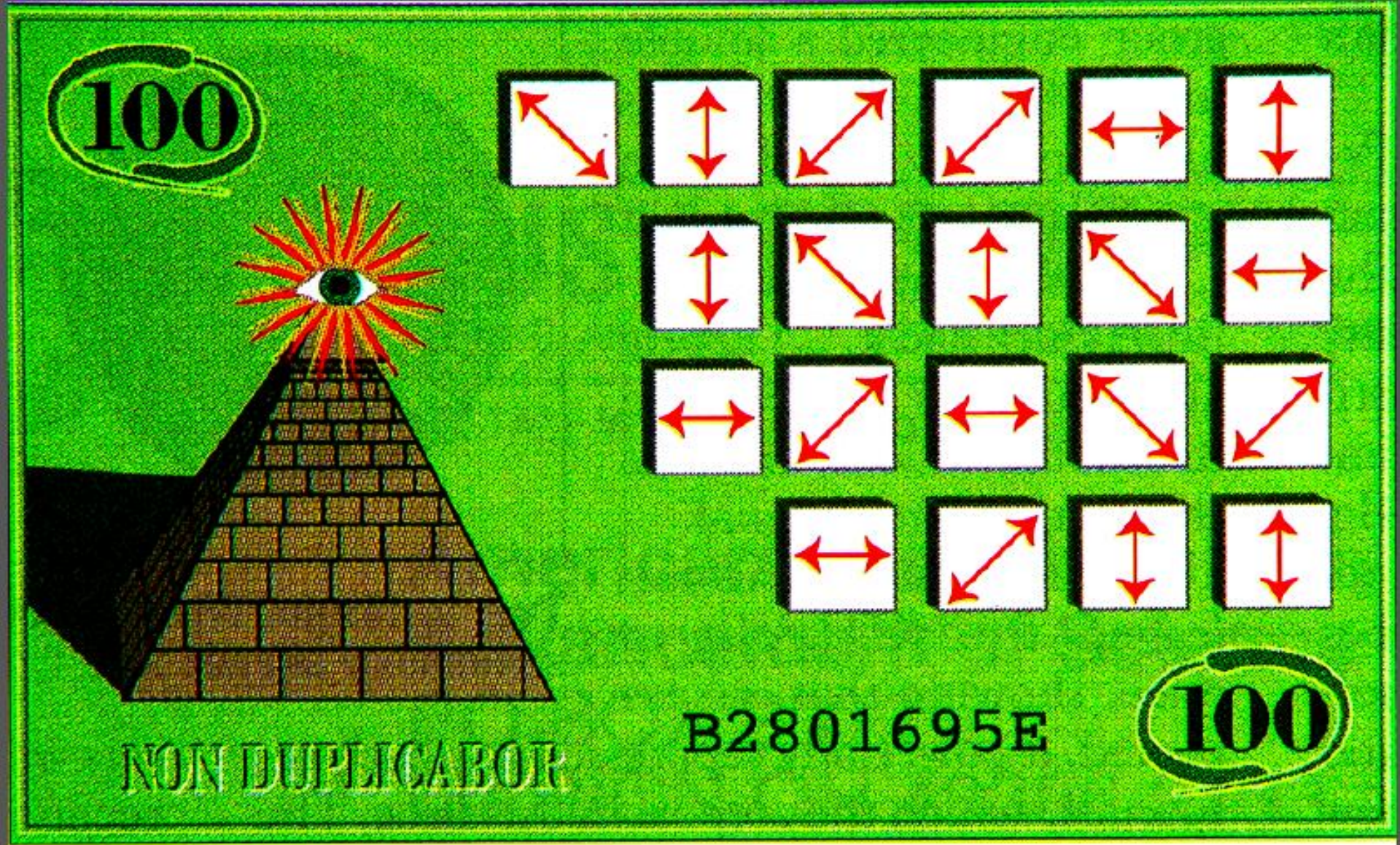
Conjugate Coding *

Stephen Wiesner

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

-

Written in 1968, submitted to IEEE-IT around 1970, circulated in manuscript. Finally published in 1983 (SIGACT News). Introduced **quantum banknotes** (the predecessor of quantum key distribution) and **quantum multiplexing channel** (now called 1 out of 2 oblivious transfer).



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.

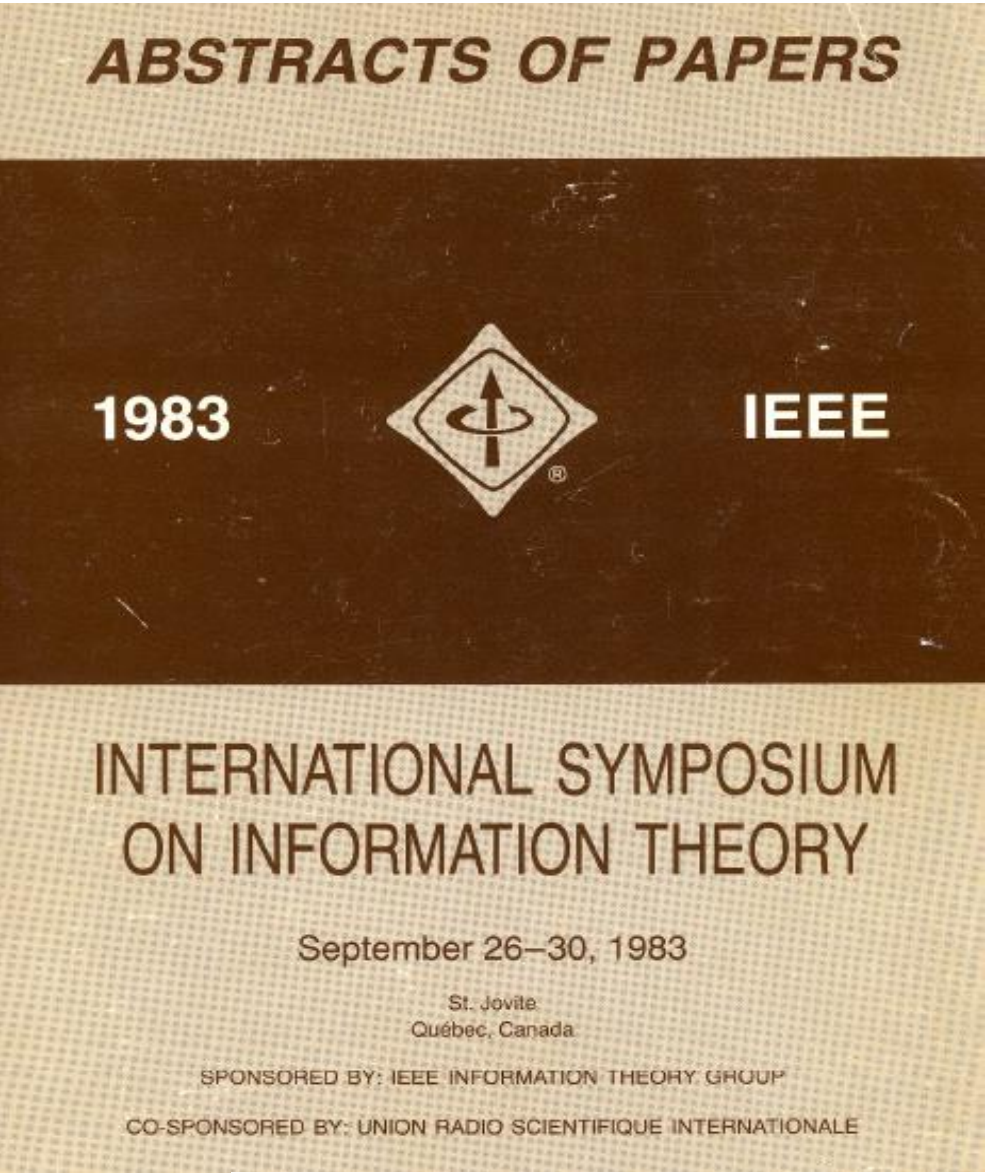
QUANTUM CRYPTOGRAPHY II:
HOW TO RE-USE A ONE-TIME PAD SAFELY EVEN IF P=NP.

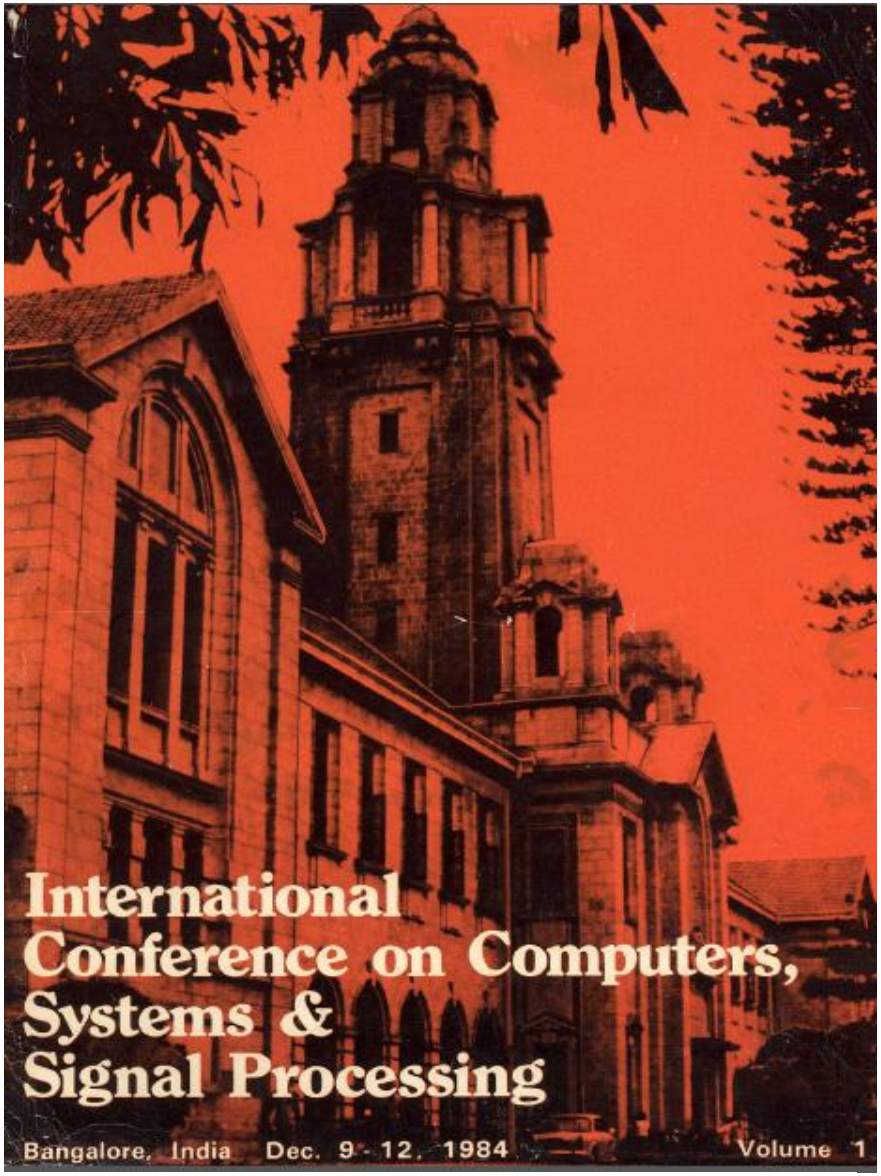
Charles H. Bennett (IBM Yorktown)
Gilles Brassard (Univ. de Montréal)
Seth Breidbart (Box 1526, NY 10268)

November 1982

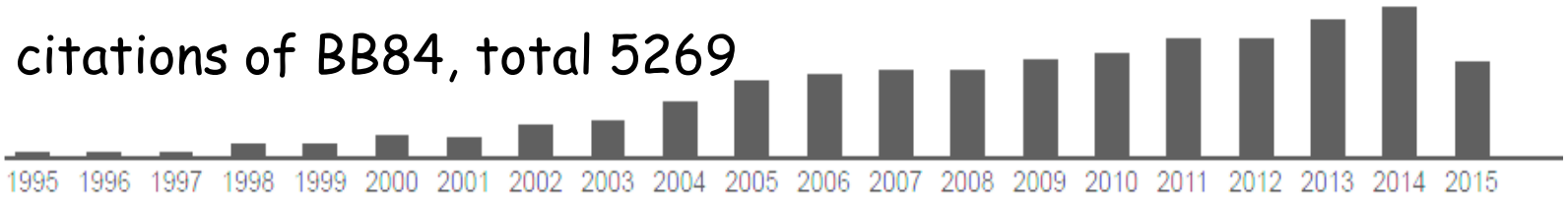
Rejected from STOC in 1982; finally published last year in *Natural Computing*.

This forerunner of BB84 used a one-time pad key in conjunction with an eavesdrop-detecting quantum channel to allow the key to re-used in case no eavesdropping was detected. But by 1983 we had already become more excited by true QKD, which needs no pre-shared key, only an unjammable public channel.





citations of BB84, total 5269



First description of BB84, in abstract of talk by B and B at 1983 St Jovite conference

SESSION D.3

Cryptography I

QUANTUM CRYPTOGRAPHY AND ITS APPLICATION TO PROVABLY SECURE KEY EXPANSION, PUBLIC-KEY DISTRIBUTION, AND COIN-TOSSING, Charles H. Bennett, IBM Research, Yorktown Heights, and Gilles Brassard, Universite de Montreal, departement de'informatique et de recherche operationnelle. When information is encoded in non orthogonal quantum states (such as photons with polarization axes 0°, 45°, 90° and 135°), the uncertainty principle gives rise to novel cryptographic phenomena unachievable with classical transmission media; notably a communication channel whose transmissions cannot be read or copied reliably by an eavesdropper ignorant of certain key information used in creating the transmission. The eavesdropper cannot even gain partial information about the transmission without altering in a random and uncontrollable way, likely to be detected by the channel's legitimate users. The essential manifestation of the uncertainty principle here is that attempting to measure the "rectilinear" (0° or 90°) polarization of a diagonal (45° or 135°) photon or vice versa causes the photon to behave randomly and loose all its stored information.

Such a quantum channel, in conjunction with ordinary insecure classical channels, can be used to achieve many of the advantages of traditional DES-type cryptography and public-key cryptography but with the additional benefit of being provably secure, even against an opponent with superior technology and unlimited computing power. Specifically, Quantum Cryptography makes possible secure transmission of a large volume of messages between users who share initially only a small secret key; and secure communication over a "public" channel

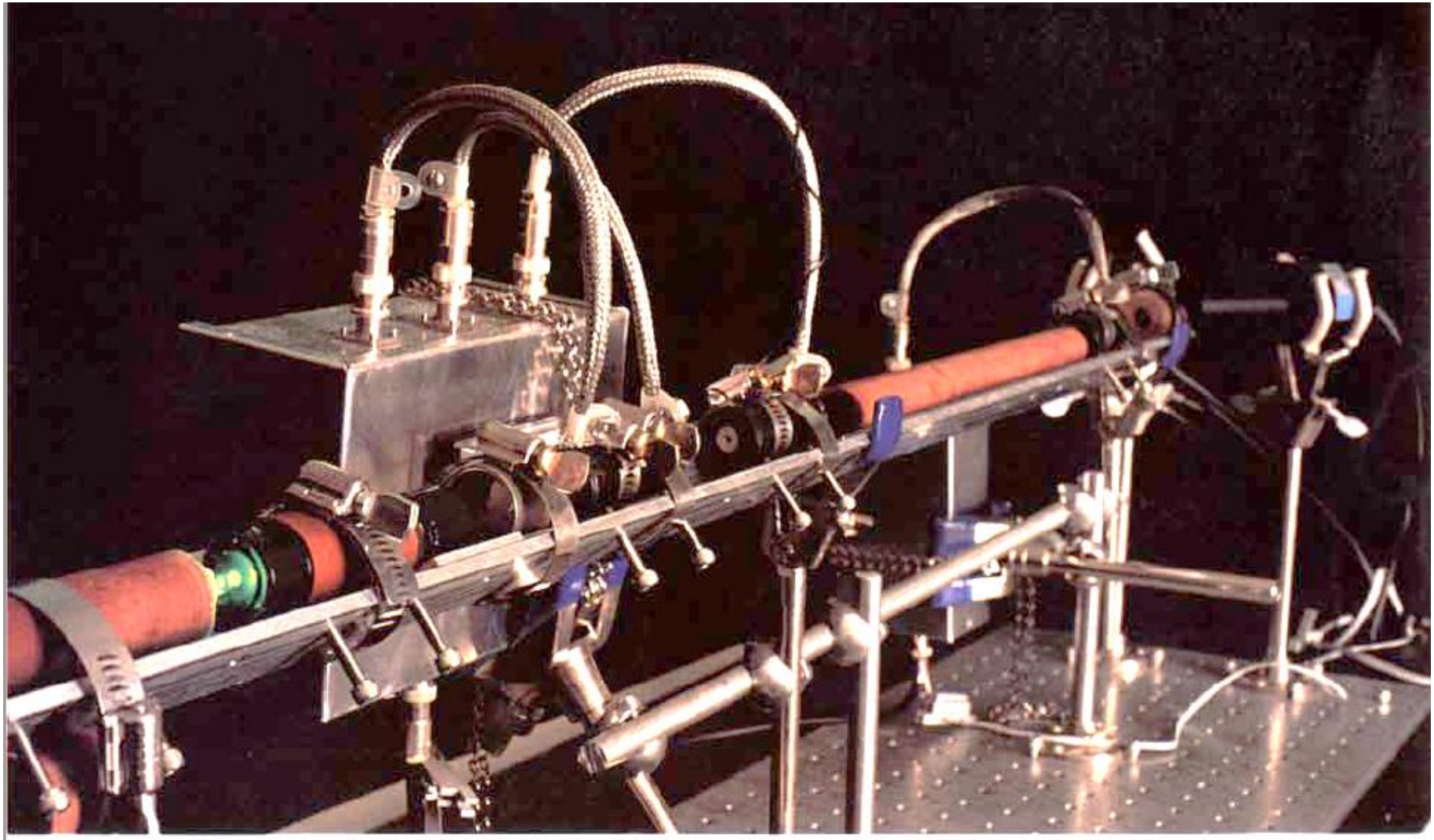
A lesser-known part of BB83 and BB84

now called bit commitment

We also present a protocol for coin-tossing by exchange of quantum messages. Using this protocol, two distrustful parties, communicating at a distance without the help of a third party, can come to agree on a "winner" and a "loser" in such a way that each party has exactly 50% chance of winning. An attempt by either party to bias the outcome would almost certainly be detected by the other party as cheating. Previous protocols for this problem are based on unproven assumptions in the theory of computational complexity, and they offer at least an exponentially small advantage to one of the opponents. By contrast, our protocol is secure against traditional kinds of cheating, even by an opponent with unlimited computing power. Ironically, however, it can be subverted by use of a still subtler quantum phenomenon, the so-called Einstein-Podolsky-Rosen paradox, which in effect allows the initiating party to toss the coin after the responding party has announced his guess of the outcome.

possibly the first conscious use of entanglement in information processing

Homemade apparatus implemented BB84 over a distance of 30 cm



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.

David Deutsch's seminal 1985 paper on quantum computation also contained what may be the first published allusion to the idea of entanglement-based quantum key distribution, later developed by Ekert.

Quantum theory, the Church-Turing principle and the universal quantum computer

DAVID DEUTSCH*

Appeared in *Proceedings of the Royal Society of London A* **400**, pp. 97–117 (1985)†

• • •

However, in some applications, such correlations are precisely what is required. The state of slots 2 and a after the execution of (3.1) is the 'non-separable' (d'Espagnat 1976) state

$$\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle). \tag{3.3}$$

Consider a pair of programs that swap these slots into an output region of the tape, *one at a time*. That is, if the output is at first blank,

• • •

The two bits in (3.3) can also be used as 'keys' for performing 'quantum cryptography' (Bennett *et al.* 1983).

Quantum cryptography really began to be noticed following Ekert's paper connecting it to violations of Bell's Inequality.

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

Prepare-and-measure and entanglement-based quantum QKD are formally equivalent and both widely practiced, but Bell inequality violation enables stronger kinds of security, e.g. allowing Alice and Bob to buy all their equipment from Eve.