QUANTUM CRYPTOGRAPHY

Gilles Brassard
Université de Montréal

Quantum Cryptography

First

theoretical

(1970, 1979, 1984)

and

experimental

(1989)

instance of

Quantum Information

Processing

ca. 1970

Physics

Crypto

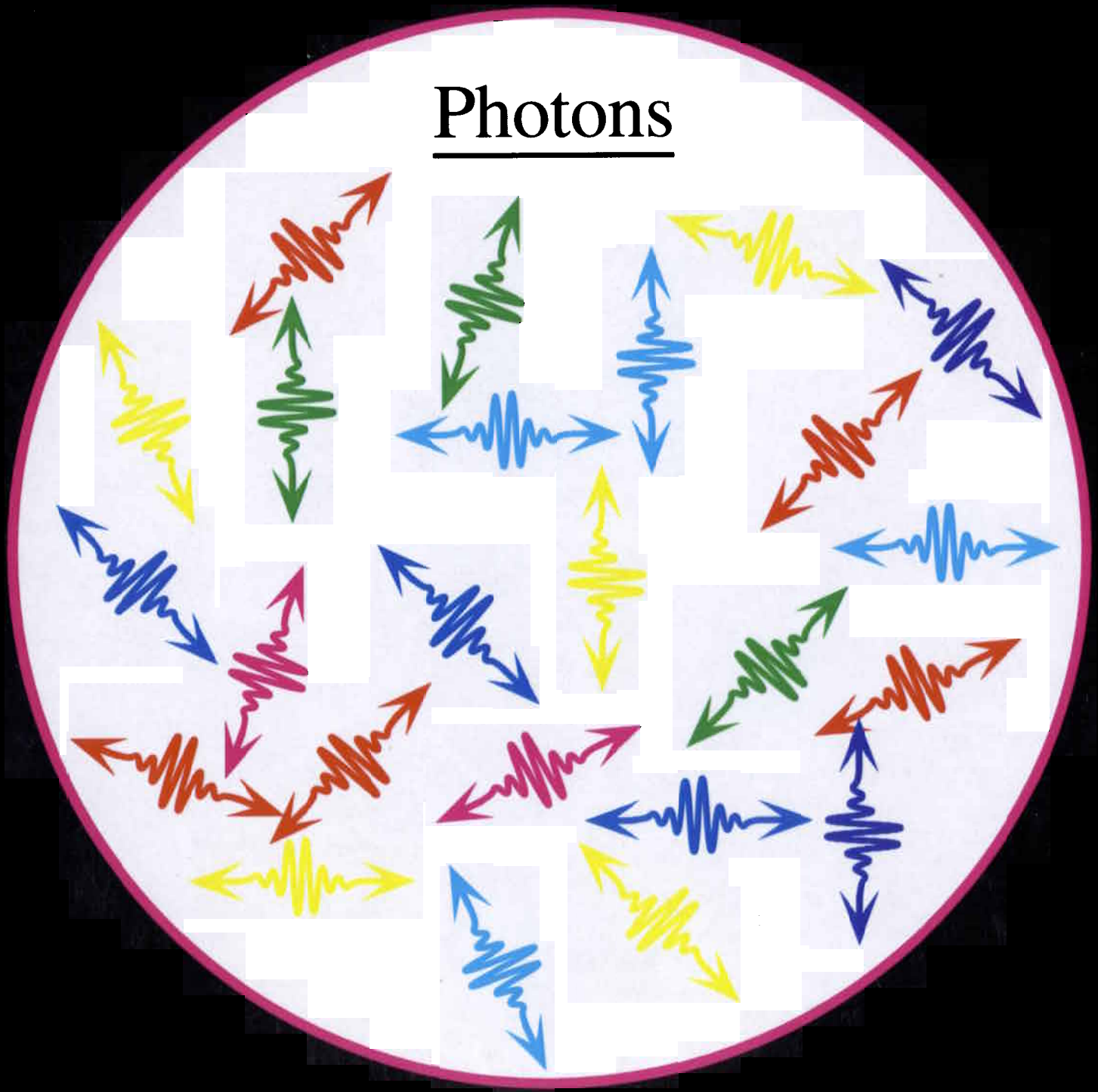
Quantum Information

- Cannot be cloned or copied
- Cannot be broadcast
- Cannot be measured reliably
- Is disturbed by observation
- Sometimes appears to propagate instantaneously
- Can exist in superposition of classical states

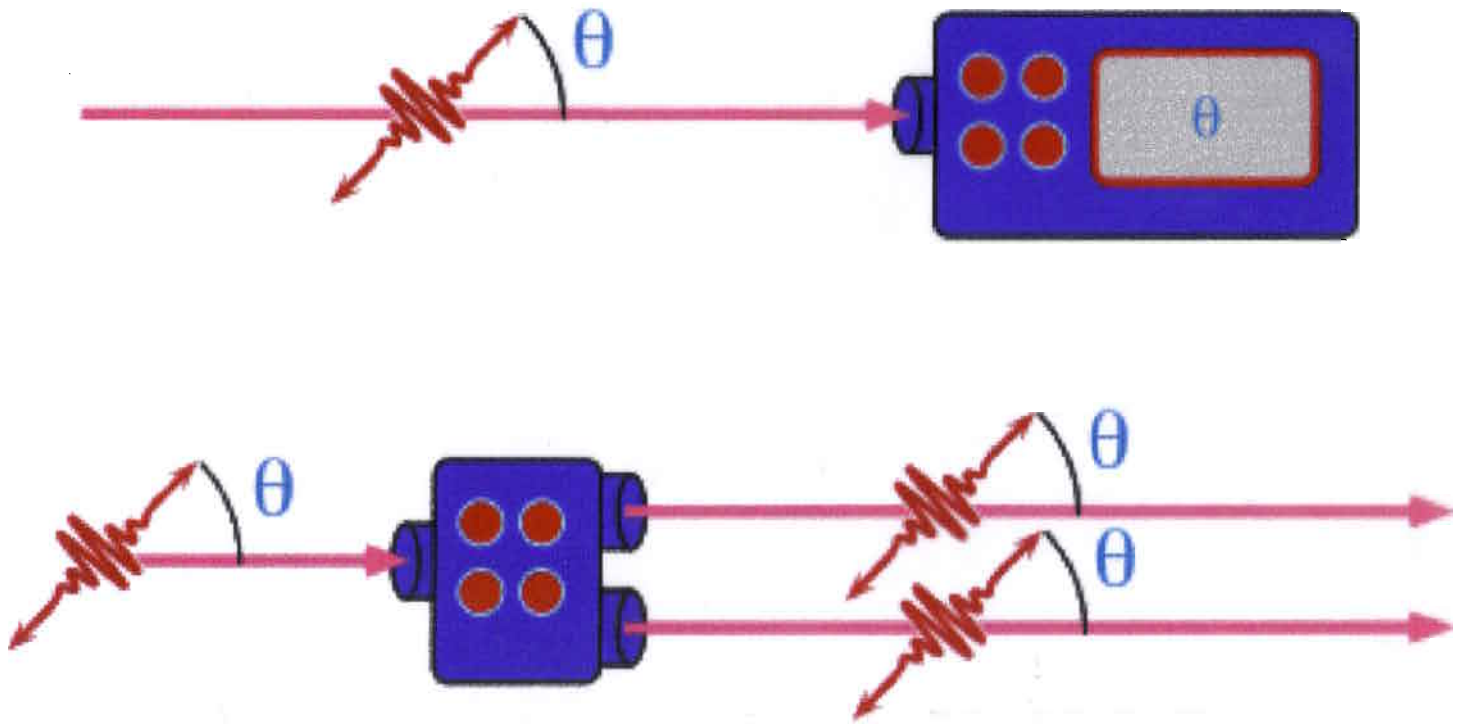
Classical Information

- Can be copied
- Can be broadcast
- Can be measured with arbitrary accuracy
- Is not disturbed by observation
- Cannot travel faster than light

Photons



IMPOSSIBLE!

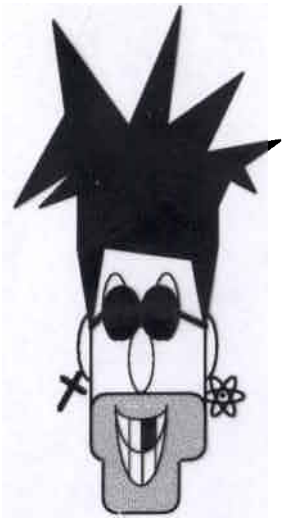


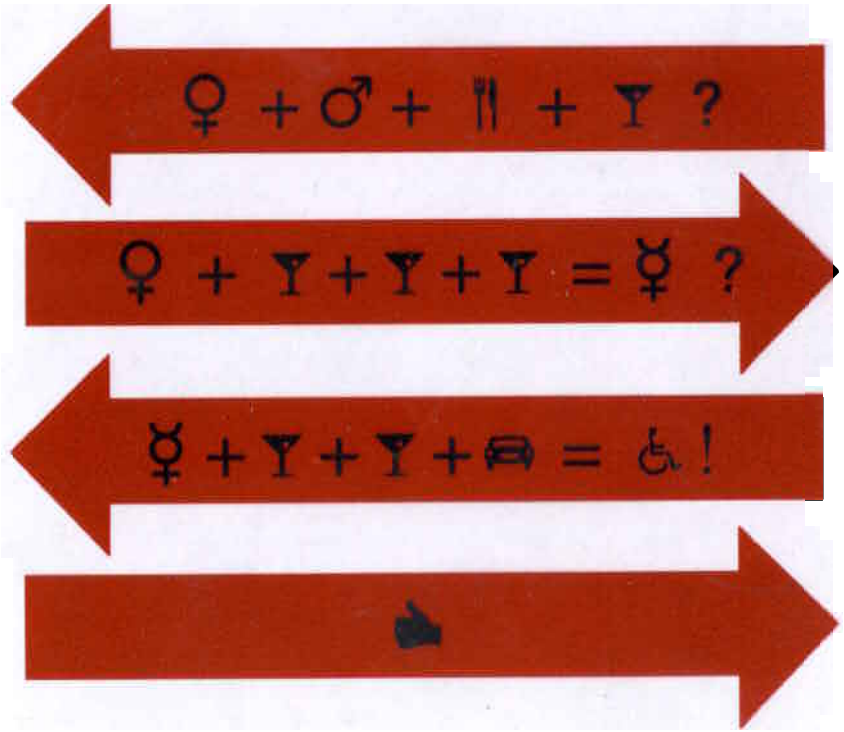
POSSIBLE!

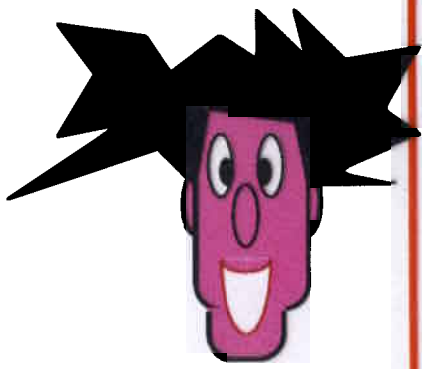
Classical and Quantum information together allow feats that neither could achieve alone

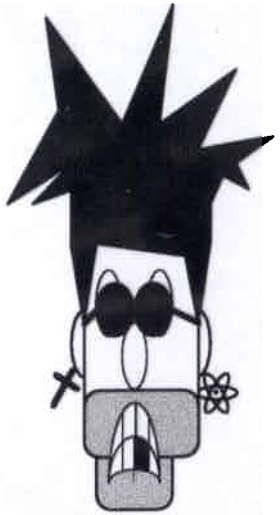
- Quantum Bank Notes
- Quantum Cryptography
- Quantum Computing
- Quantum Teleportation
- Communication Complexity
- Pseudo Telepathy

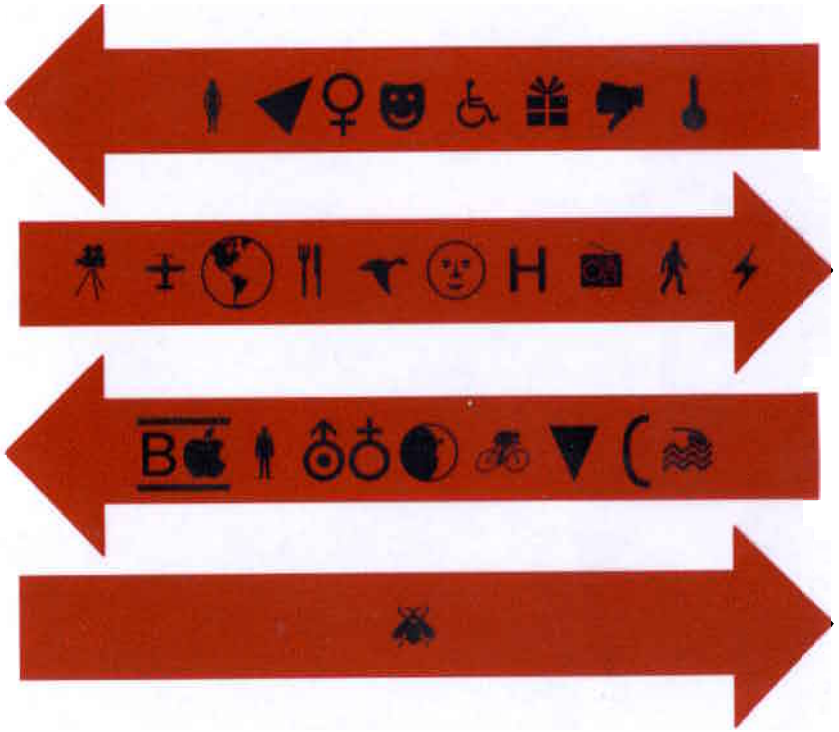

100
NON DUPLICABOR
B2801695E
100

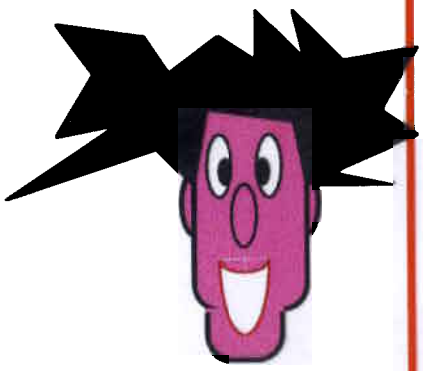






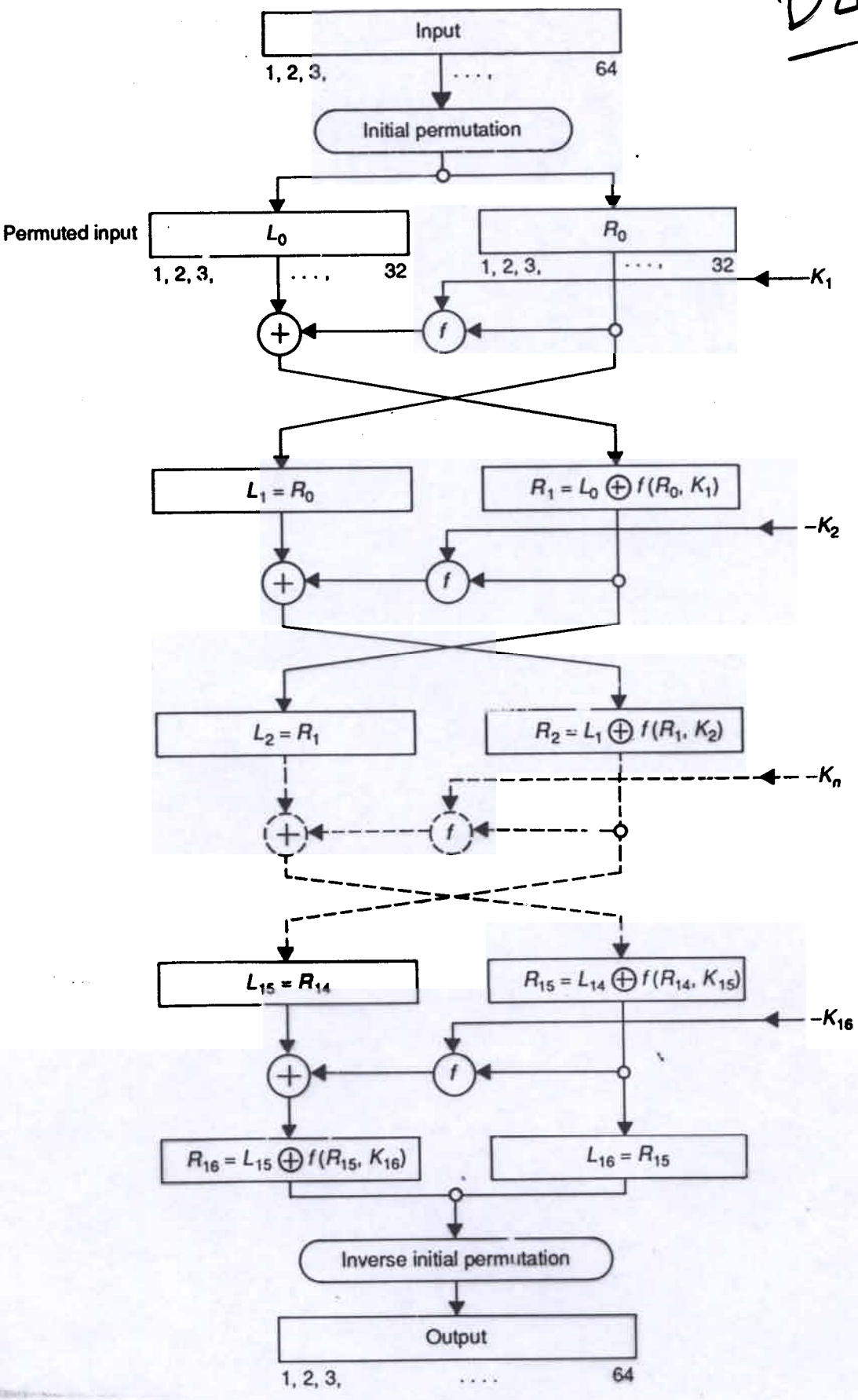







Zur Beachtung!
ENIGMA

DES


Input
1, 2, 3, . . . , 64
Initial permutation
Permuted input
L_0
R_0
1, 2, 3, . . . , 32
1, 2, 3, . . . , 32
K_1
f
$L_1 = R_0$
$R_1 = L_0 \oplus f(R_0, K_1)$
K_2
$L_2 = R_1$
$R_2 = L_1 \oplus f(R_1, K_2)$
K_n
$L_{15} = R_{14}$
$R_{15} = L_{14} \oplus f(R_{14}, K_{15})$
K_{16}
$R_{16} = L_{15} \oplus f(R_{15}, K_{16})$
$L_{16} = R_{15}$
Inverse initial permutation
Output
1, 2, 3, ... 64

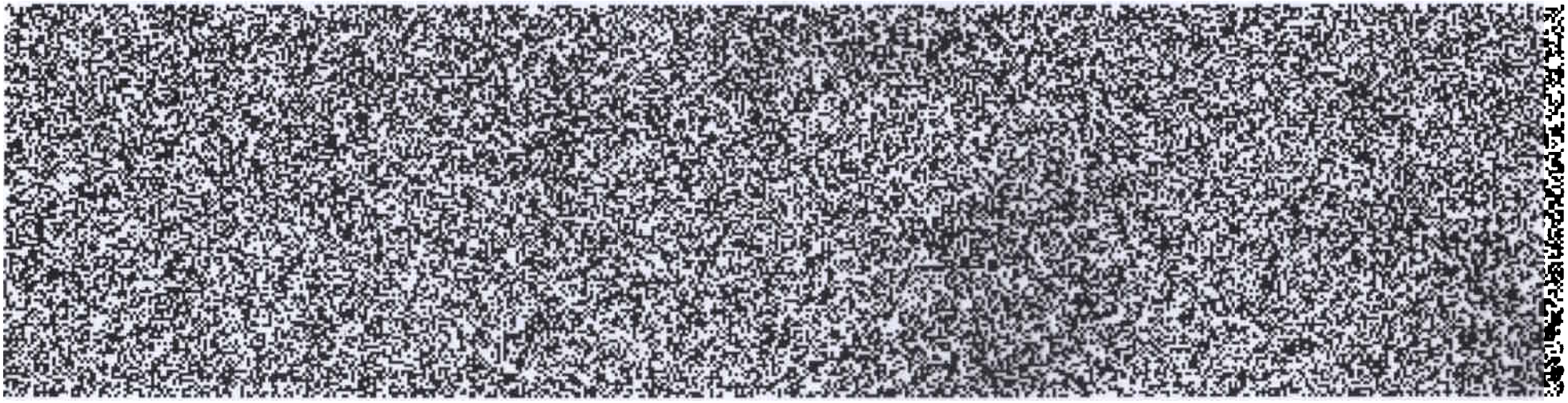
ULTIMATE

Goal:

UNCONDITIONAL

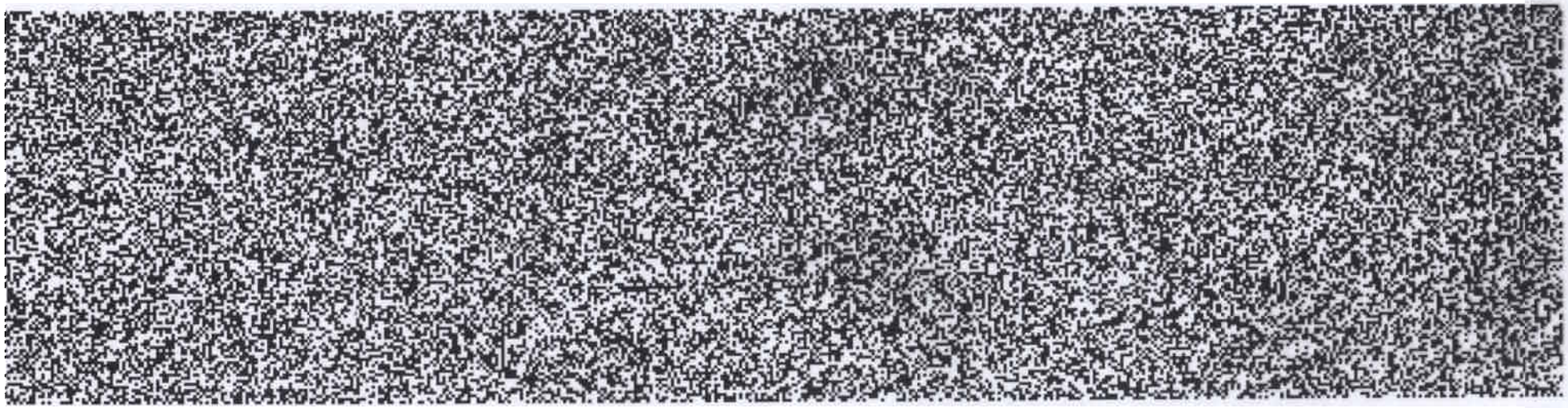
Security

Mask



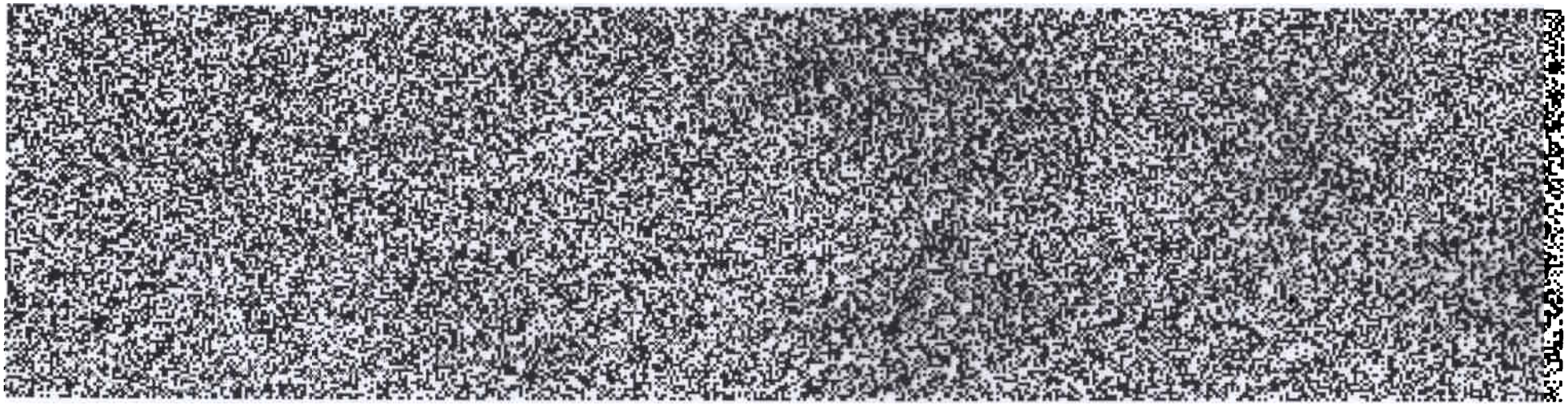
one-time pad

Message 1

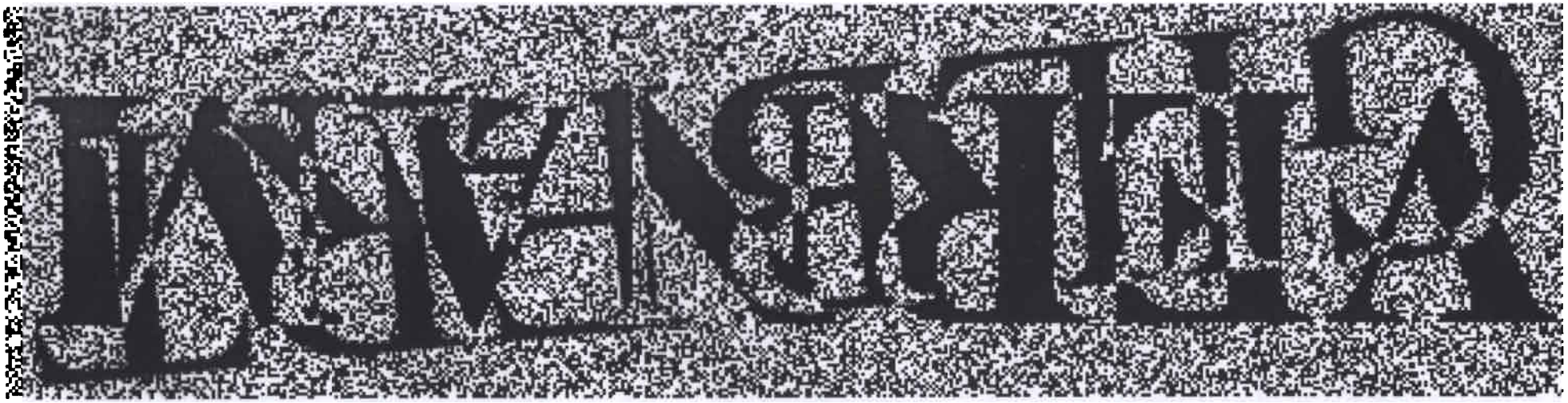


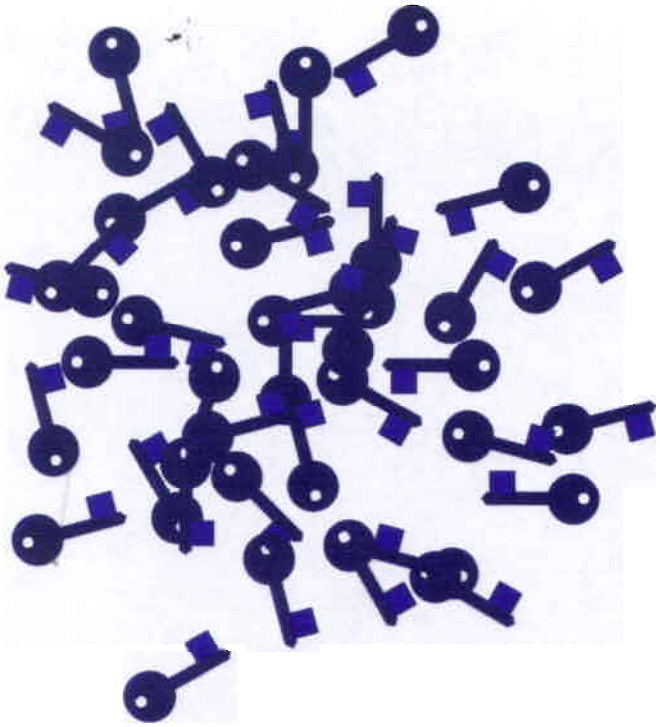
MIND

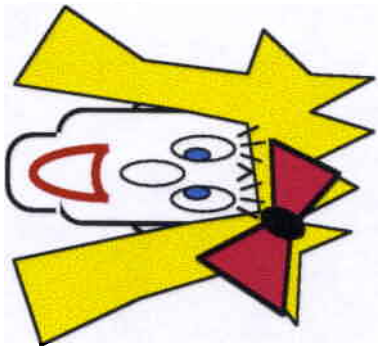
Message 2

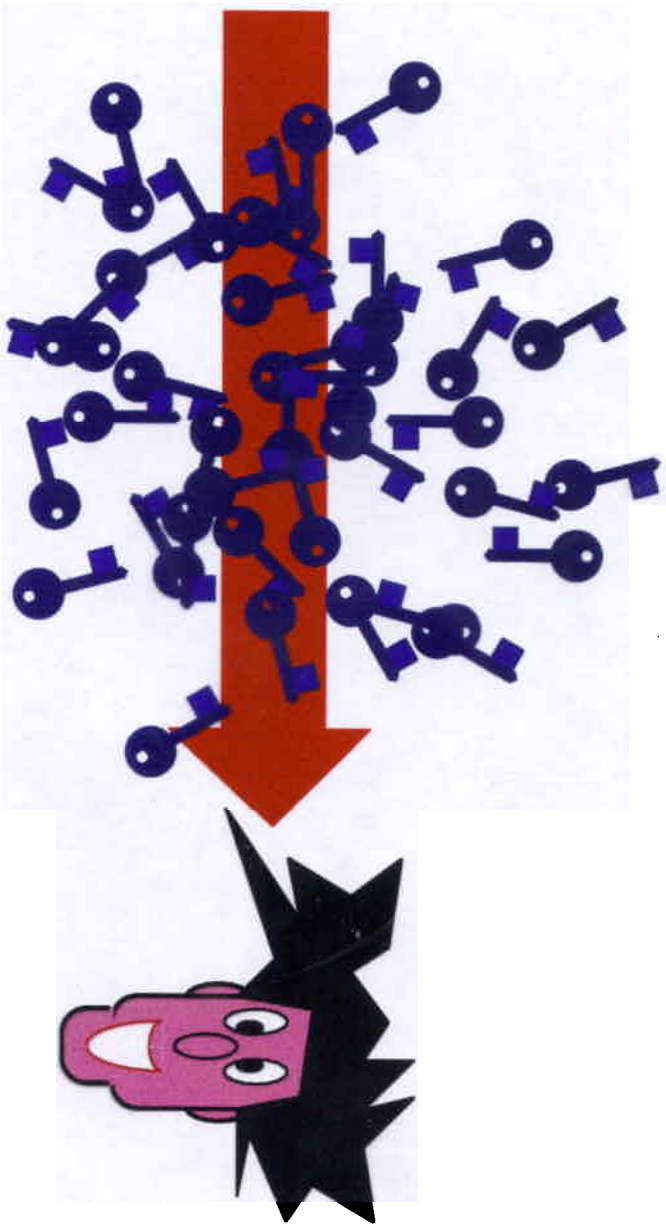


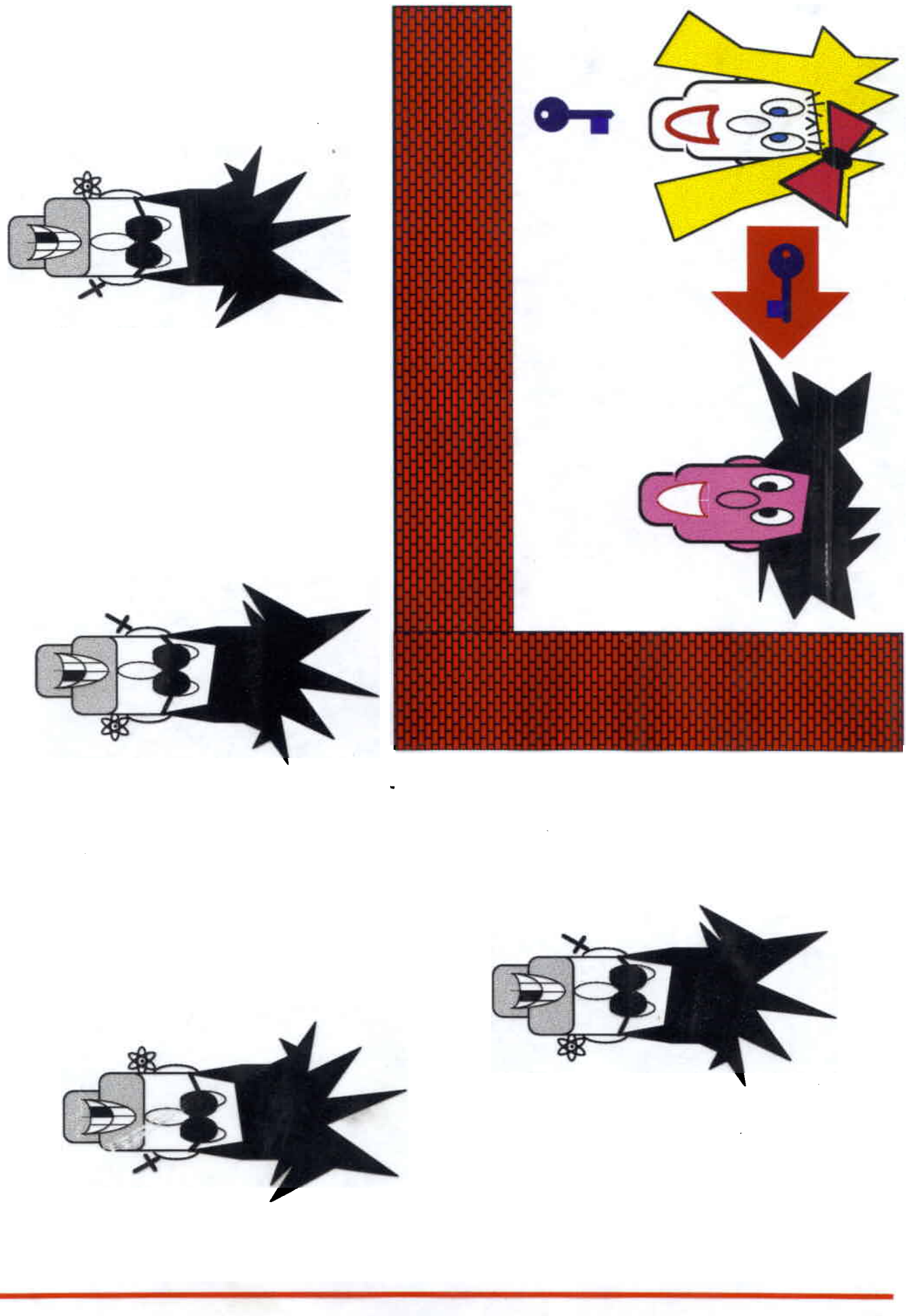
Quilt


DEVASTATION









Quantum Cryptography

0 

1 

These states cannot be distinguished reliably

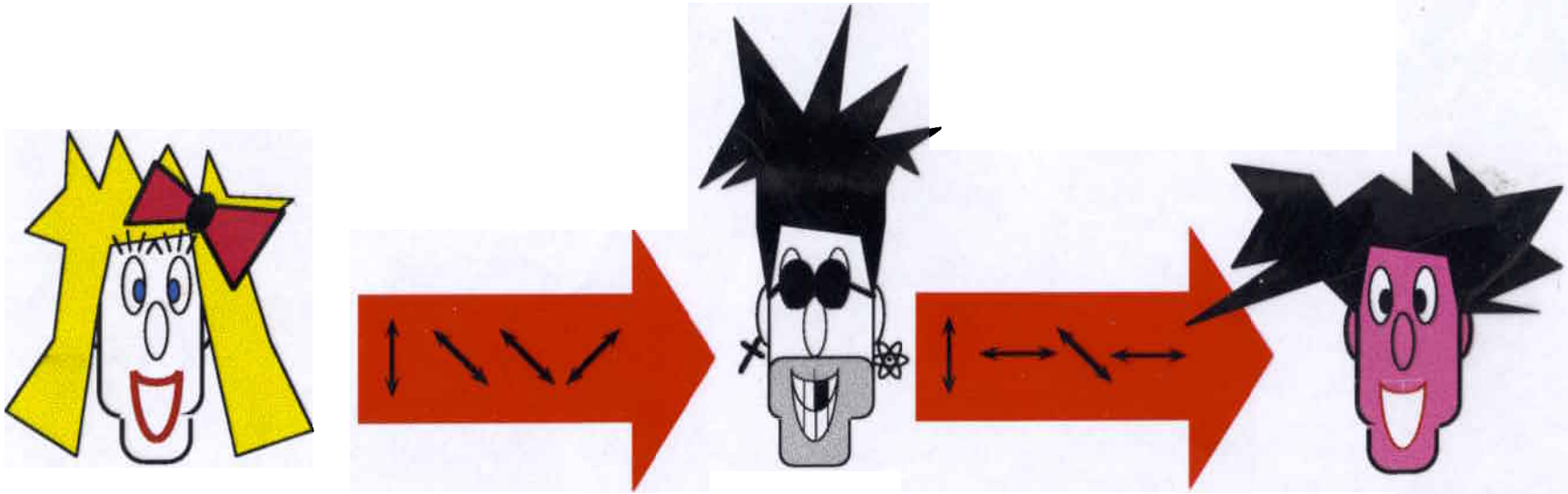
Eavesdropping → Errors → Detection

Use quantum channel to send random key

+ classical one-time-pad to send message

→ eavesdropping prevention

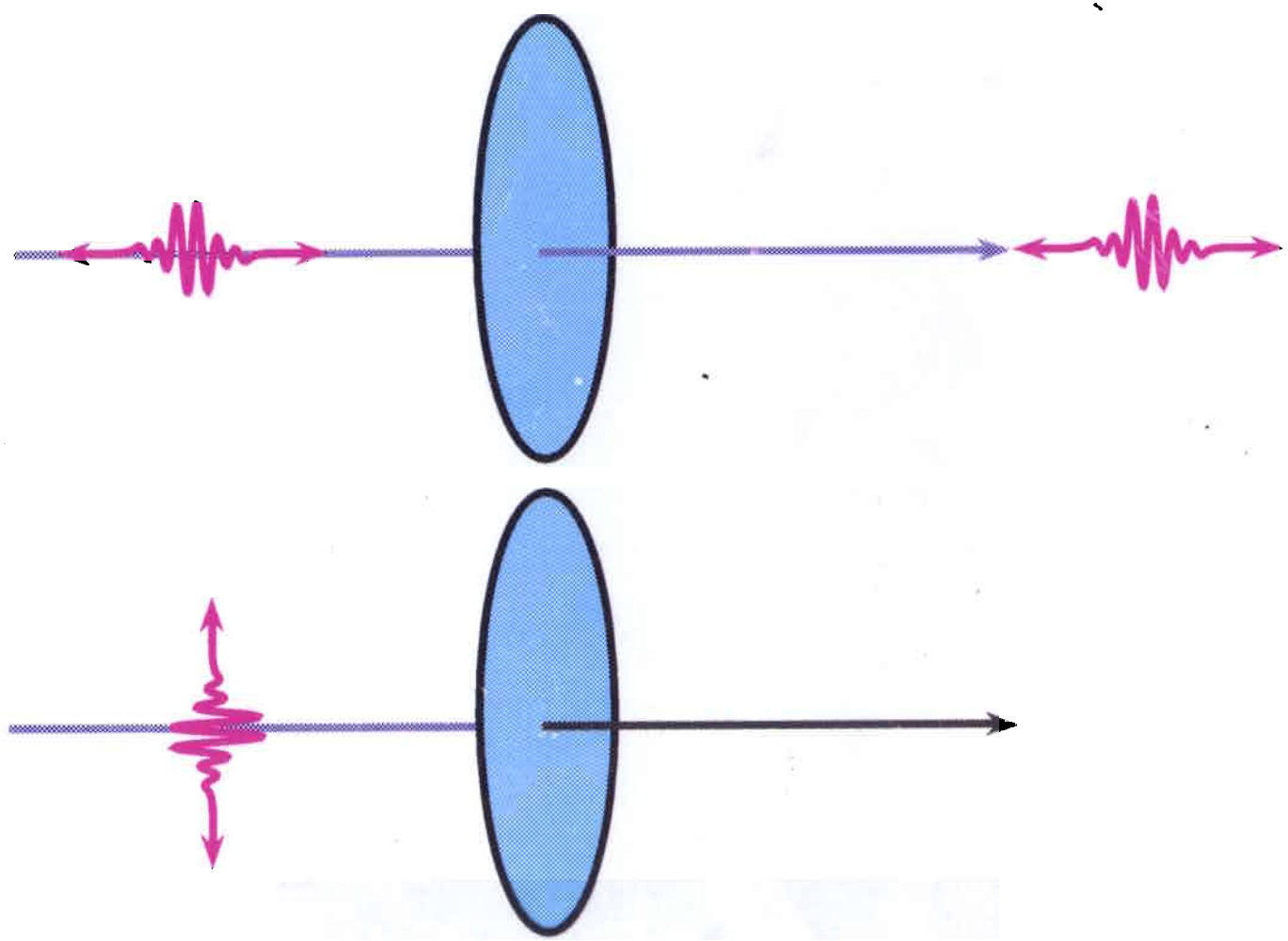
Eavesdropping



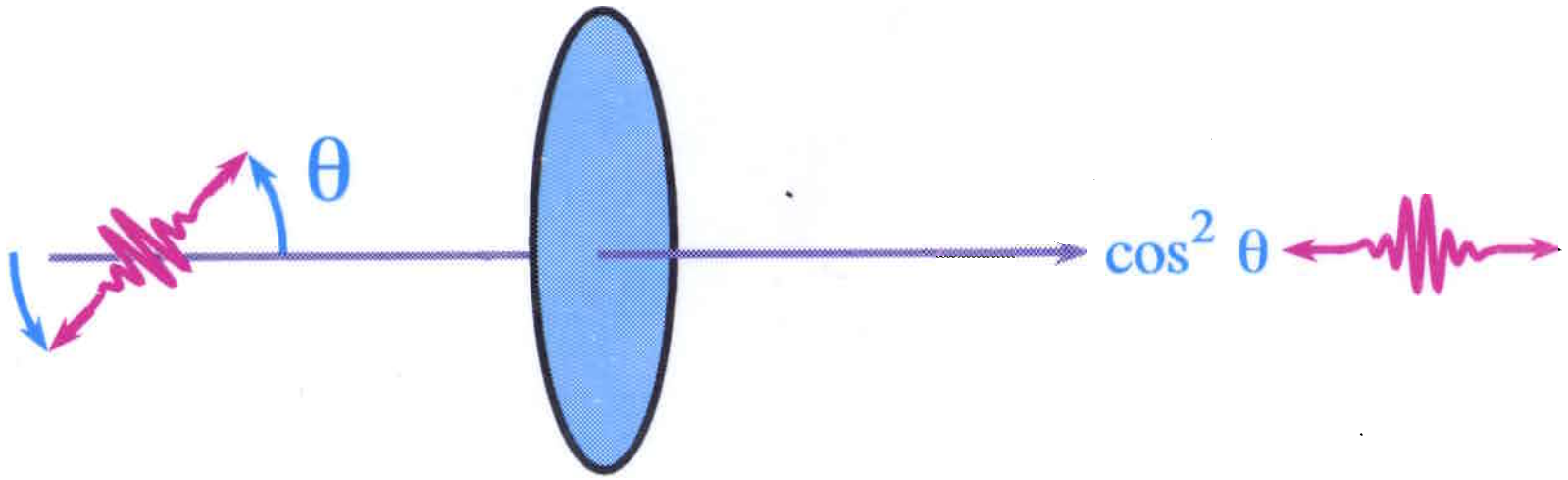
++×+

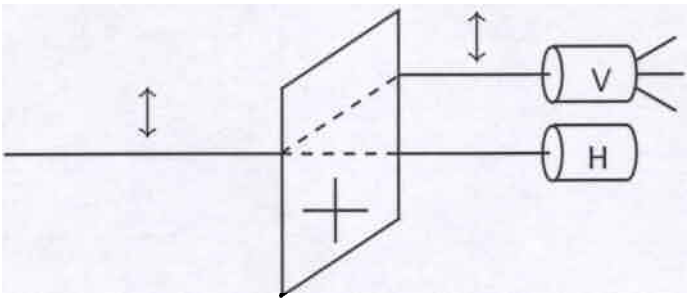
bits eavesdropped ↔ errors

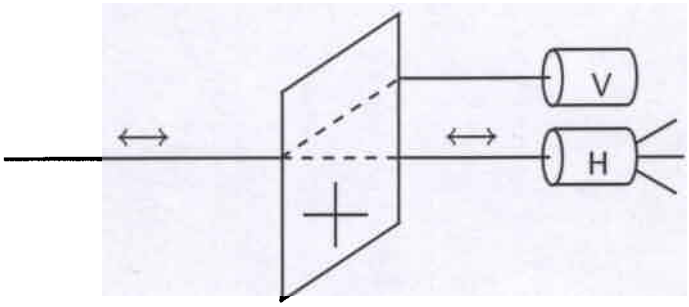
Polarizing Filter

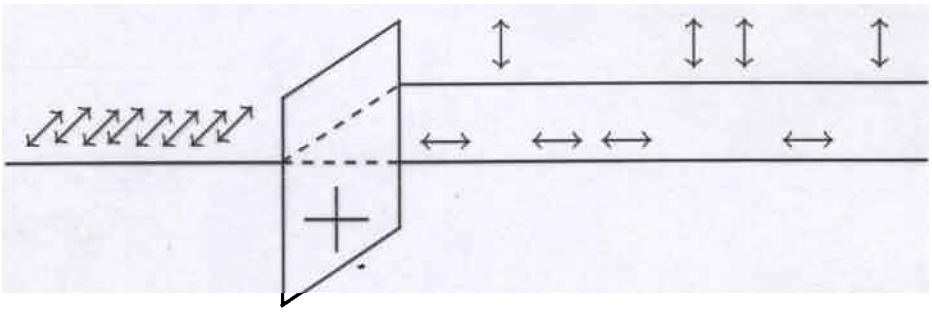


Polarizing Filter



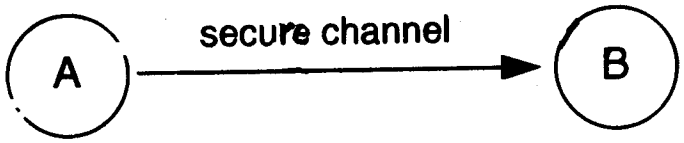

V
H


V
H

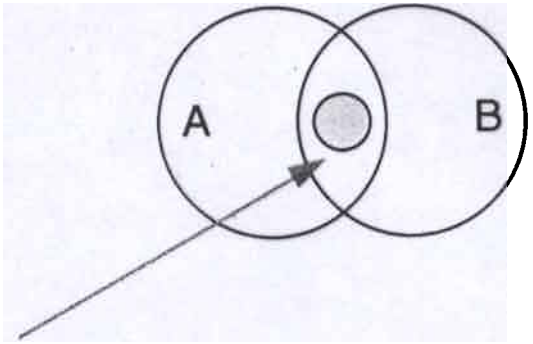


Quantum Cryptography = Quantum Key Distribution (QKD)

- conventional **key distribution:**
  - Alice sends **particular** key data to Bob



- **quantum key distribution:**
  - key **does not exist** before transmission
  - Alice and Bob generate **independent** random number sets
  - **remote comparison,** bit-by-bit, using a **photon state preparation & measurement protocol** identifies a **shared subset**



- **EXAMPLE**: polarized single-photons
  - Alice **prepares** vertical or 45 ° polarized photons
  - Bob **measures** horizontal or - 45 ° polarization
  - QM gives the **probability** that Alice's photon triggers Bob's detector
  - **detected** photons identify **shared bits**

			Alice 0	Alice 1
Bob	1	↔	0	50%
	0	↘↙	50%	0

An example of QKD

Step 1: Alice & Bob generate **independent** random bit sets

Alice	1	0	1	0	...

Bob	0	0	1	1	...

Step 2: Comparison by quantum communication

Alice	1	0	1	0	...
	↕	↕	↕	↕	...
	↕	↕	↔	↔	...
Bob	0	0	1	1	...
result	N	N	Y	N	...

Step 3: Bob sends Alice (publicly) a copy of the results (but not his measurement)

Alice	1	0	**1**	0	...
result	N	N	**Y**	N	...

Bob	0	0	**1**	1	...
result	N	N	**Y**	N	...

retain the "Y" bits: **perfectly correlated subset = key**

Los Alamos

PRL 67(6): 661, 1991

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.

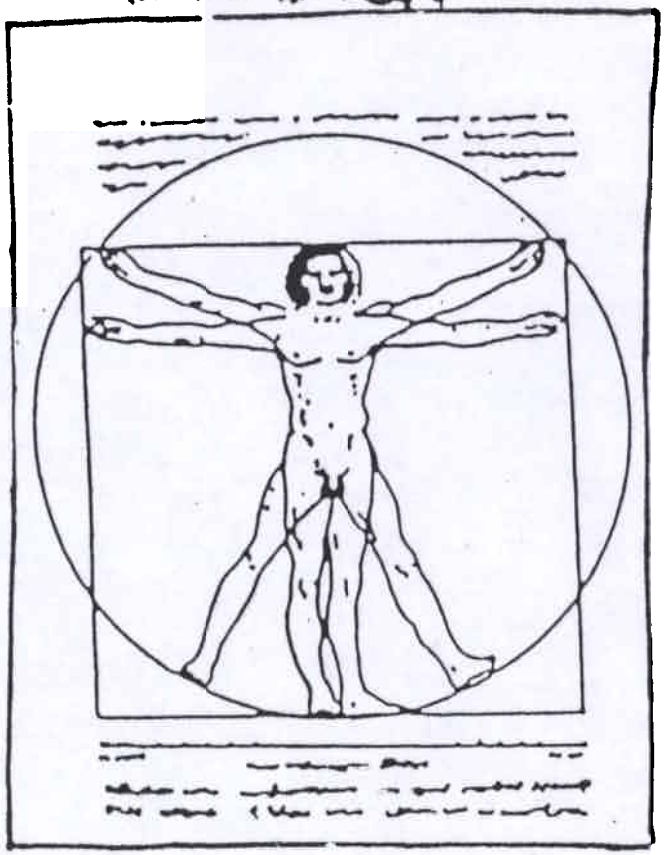
PACS numbers: 03.65.Bz, 42.80.Sa, 89.70.+c

Cryptography, despite a colorful history that goes back to 400 B.C., only became part of mathematics and information theory this century, in the late 1940s, mainly due to the seminal papers of Shannon [1]. Today, one can briefly define cryptography as a mathematical system of transforming information so that it is unintelligible and therefore useless to those who are not meant to have access to it. However, as the computational process associated with transforming the information is always performed by physical means, one cannot separate the mathematical structure from the underlying laws of physics that govern the process of computation [2]. Deutsch has shown that quantum physics enriches our computational possibilities far beyond classical Turing machines [2], and current work in quantum cryptography originated by Bennett and Brassard provides a good example of this fact [3].

In this paper I will present a method in which the security of the so-called key distribution process in cryptography depends on the completeness of quantum mechanics. Here completeness means that quantum description provides maximum possible information about any system under consideration. The proposed scheme is based on the Bohm's well-known version of the Einstein-Podolsky-Rosen *gedanken experiment* [4]; the generalized Bell's theorem (Clauser-Horne-Shimony-Holt inequalities) [5] is used to test for eavesdropping. From a theoretical point of view the scheme provides an interesting and new extension of Bennett and Brassard's original idea, and from an experimental perspective offers a practical realization by a small modification of experiments that were set up to test Bell's theorem. Before I proceed any further let me first introduce some basic notions of cryptography.

Originally the security of a cryptotext depended on the secrecy of the entire encrypting and decrypting procedures; however, today we use ciphers for which the algorithm for encrypting and decrypting could be revealed to anybody without compromising the security of a particular cryptogram. In such ciphers a set of specific parameters, called a *key*, is supplied together with the plaintext as an input to the encrypting algorithm, and together with the cryptogram as an input to the decrypting algorithm. The encrypting and decrypting algorithms are publicly announced; the security of the cryptogram depends entirely on the secrecy of the key, and this key, which is very important, may consist of any *randomly chosen*, sufficiently long string of bits. Once the key is established, subsequent communication involves sending cryptograms over a public channel which is vulnerable to total passive interception (e.g., public announcement in mass media). However, in order to establish the key, two users, who share no secret information initially, must at a certain stage of communication use a reliable and a very secure channel. Since the interception is a set of measurements performed by the eavesdropper on this channel, however difficult this might be from a technological point of view, *in principle* any classical channel can always be passively monitored, without the legitimate users being aware that any eavesdropping has taken place. This is not so for quantum channels [3]. In the following I describe a quantum channel which distributes the key

THEORY



EXPERIMENT

M Stevens

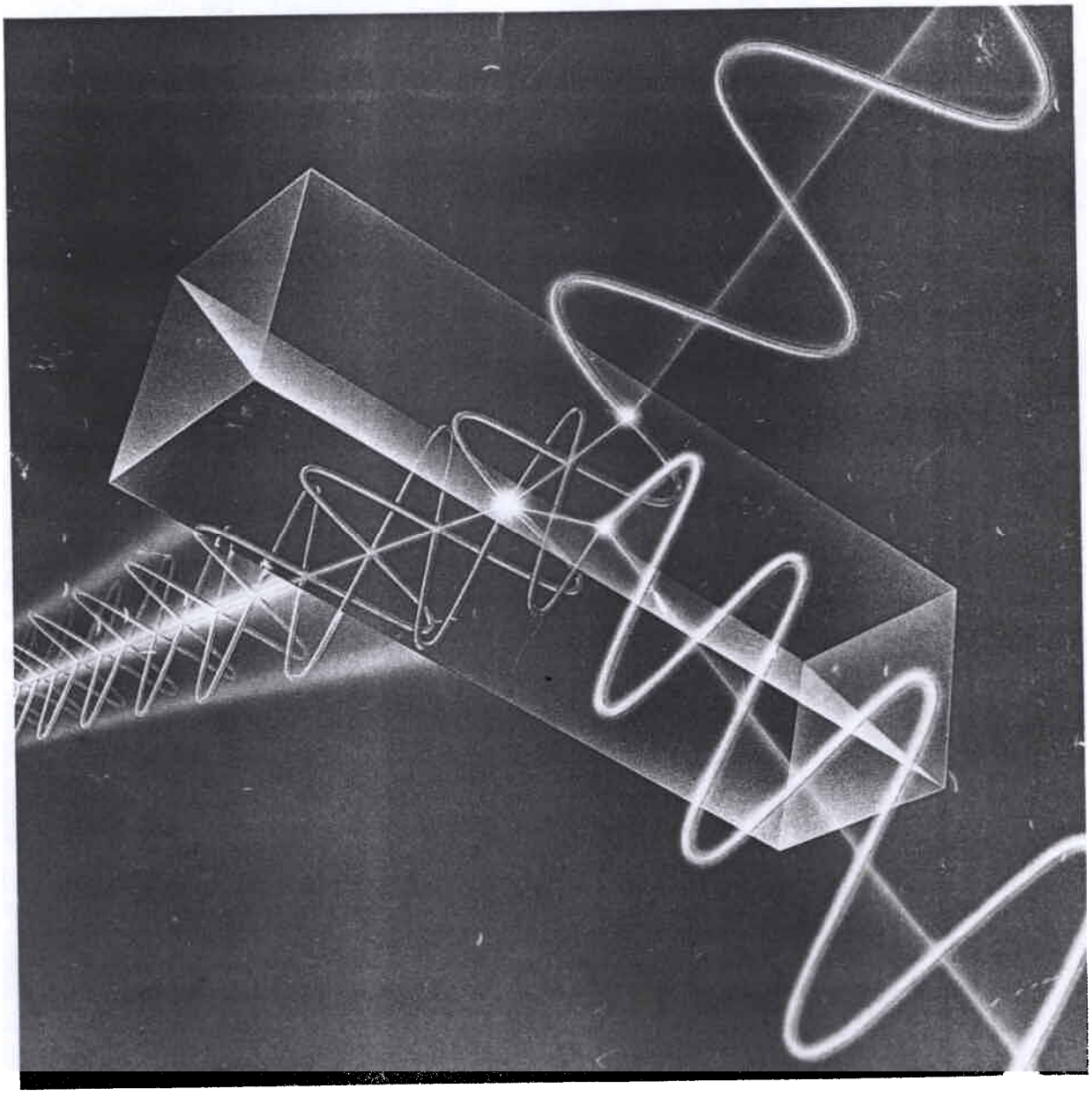
OCTOBER 1992
$3.95

SCIENTIFIC AMERICAN

The promise of diamond semiconductors.

Was early man a heroic hunter—or a scavenger?

Raising the grades in U.S. science education.



***Light signals** split by a simple prism allow messages to be transmitted in absolute secrecy.*

Quantum Cryptography

For ages, mathematicians have searched for a system that would allow two people to exchange messages in absolute secrecy. Quantum mechanics has now joined forces with cryptology to achieve a major step in that direction

by Charles H. Bennett, Gilles Brassard and Artur K. Ekert

In his classic short story "The Gold Bug," published in 1843, Edgar Allan Poe explains the rudiments of code breaking and ventures the opinion that the human mind can break any cipher that human ingenuity could devise. During the subsequent century and a half, the contest between code makers and code breakers has undergone reversals and complications that would have delighted Poe. An unbreakable cipher was invented in 1918, although its unbreakability was not proved until the 1940s. This cipher was rather impractical because it required the sender and receiver to agree beforehand on a key—a large stockpile of secret random digits, some of which were used up each time a secret message was transmitted. More practical ciphers with short, reusable keys, or no secret key at all, were developed in the 1970s, but to this day they remain in a mathematical limbo, having neither been broken nor proved secure.

A recent unexpected development is the use of quantum mechanics to perform cryptographic feats unachievable by mathematics alone. Quantum cryptographic devices typically employ individual photons of light and take advantage of Heisenberg's uncertainty principle, according to which measuring a quantum system in general disturbs it and yields incomplete information about its state before the measurement. Eavesdropping on a quantum communications channel therefore causes an unavoidable disturbance, alerting the legitimate users. Quantum cryptography exploits this effect to allow two parties who have never met and who share no secret information beforehand to communicate in absolute secrecy under the nose of an adversary. Quantum techniques also assist in the achievement of subtler cryptographic goals, important in the post-cold war world, such as enabling two mutually distrustful parties to make joint decisions based on private information, while compromising its confidentiality as little as possible.

CHARLES H. BENNETT, GILLES BRASSARD and ARTUR K. EKERT share a deep interest in the fundamental connections between physics and the theory of computation. Bennett and Brassard have pioneered the field of quantum cryptography. Since 1973 Bennett has been a researcher at the IBM Thomas J. Watson Research Center in Yorktown Heights, N.Y. In 1979 Brassard became a professor of computer science at the Université de Montréal, where he currently holds the E.W.R. Steacie Memorial Fellowship. Ekert, who last year received his doctoral degree from the University of Oxford, is a Junior Research Fellow at Merton College at Oxford. This is Bennett's third article for *Scientific American*.

The art of cryptography began at least 2,500 years ago and has played an important role in history ever since. Perhaps one of the most famous cryptograms, the Zimmermann Note, propelled the U.S. into World War I. When the cryptogram was broken in 1917, Americans learned that Germany had tried to entice Mexico to join its war effort by promising Mexico territories in the U.S.

Around this time Gilbert S. Vernam of American Telephone and Telegraph Company and Major Joseph O. Mauborgne of the U.S. Army Signal Corps developed the first truly unbreakable code called the Vernam cipher [*see box on page 52*]. One distinctive feature of the code is its need for a key that is as long as the message being transmitted and is never reused to send another message. (The Vernam cipher is also known as the one-time pad from the practice of furnishing the key to spies in the form of a tear-off pad, each sheet of which was to be used once and then carefully destroyed.) The discovery of the Vernam cipher did not create much of a stir at the time, probably because the cipher's unbreakability was not definitively proved until later and because its massive key requirements made it impractical for general use.

Because of this limitation, soldiers and diplomats continued to rely on weaker ciphers using shorter keys. Consequently, during World War II, the Allies were able to read most of the secret messages transmitted by the Germans and Japanese. These ciphers, though breakable, were by no means easy to crack. Indeed, the formidable task of breaking increasingly sophisticated ciphers was one of the factors that stimulated the development of electronic computers.

Academic interest in cryptology grew more intense in the mid-1970s, when Whitfield Diffie, Martin E. Hellman and Ralph C. Merkle, then at Stanford University, discovered the principle of public-key cryptography (PKC). Soon afterward, in 1977, Ronald L. Rivest, Adi Shamir and Leonard M. Adleman, then at the Massachusetts Institute of Technology, devised a practical implementation [see "The Mathematics of Public-Key Cryptography," by Martin E. Hellman; SCIENTIFIC AMERICAN, August 1979].

Public-key cryptosystems differ from all previous schemes in that parties wishing to communicate do not need to agree on a secret key beforehand. The idea of PKC is for a user, whom we shall call Alice, to choose randomly a pair of mutually inverse transformations—to be used for encryption and decryption; she then publishes the instructions for performing encryption but not decryption. Another user, Bob, can then use Alice's public-encryption algorithm to prepare a message that only she can decrypt. Similarly, anyone, including Alice, can use Bob's public-encryption algorithm to prepare a message that only he can decrypt. Thus, Alice and Bob can converse secretly even though they share no secret to begin with. Public-key cryptosystems are especially suitable for encrypting electronic mail and commercial transactions, which often occur between parties who, unlike diplomats and spies, have not anticipated their need to communicate secretly.

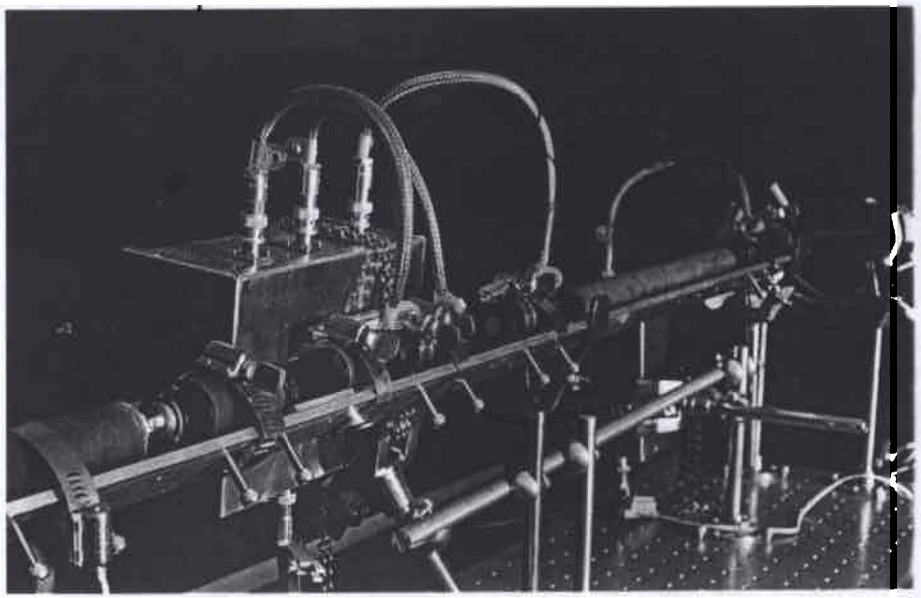
Offsetting this advantage is the fact that public-key systems have not been proven to be secure. Indeed, in 1982 Shamir, now at the Weizmann Institute of Science in Israel, cracked one of the early public-key cryptosystems, the knapsack cipher. Poe could be smiling from the grave, knowing there is a clever method of attack, as yet undiscovered, that could break any of these ciphers in a few minutes.

Several years before the discovery of public-key cryptography, another striking development had quietly taken place: the union of cryptography with quantum mechanics. Around 1970 Stephen J. Wiesner, then at Columbia University, wrote a paper entitled "Conjugate Coding," explaining how quantum physics could be used, at least in principle, to accomplish two tasks that were impossible from the perspective of classical physics. One task was a way to produce bank notes that would be physically impossible to counterfeit. The other was a scheme for combining two classical messages into a single quantum transmission from which the receiver could extract either message but not both. Unfortunately, Wiesner's paper was rejected by the journal to which he sent it, and it went unpublished until 1983. Meanwhile, in 1979, two of us (Bennett and Brassard) who knew of Wiesner's ideas began thinking of how to combine them with public-key cryptography. We soon realized that they could be used as a substitute for PKC: two users, who shared no secret initially, could communicate secretly, but now with absolute and provable security, barring violations of accepted physical laws.

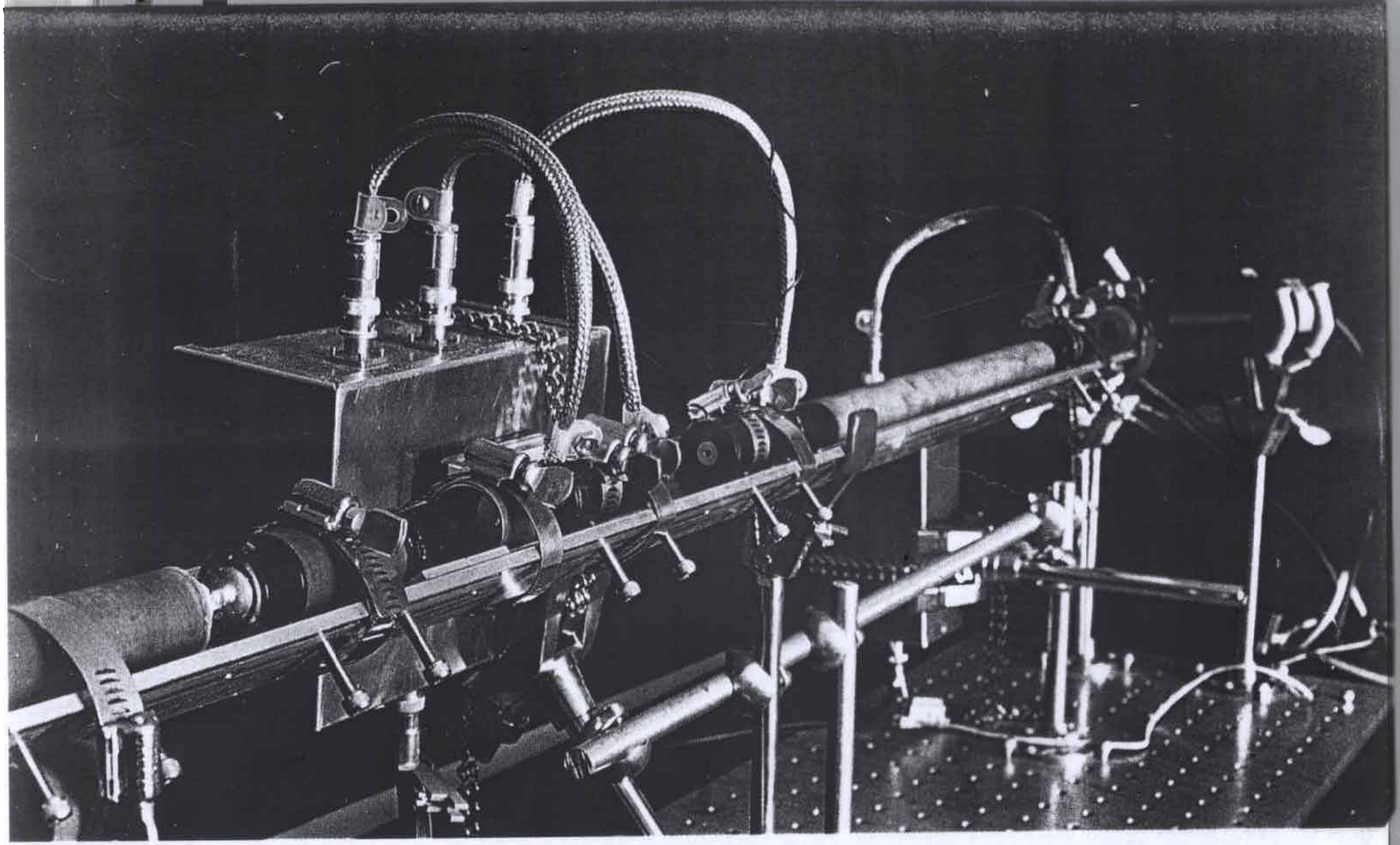
Our early quantum cryptographic schemes, developed between 1982 and 1984, were somewhat impractical, but refinements over the next few years culminated in the building of a fully working prototype at the IBM Thomas J. Watson Research Center in 1989. John Smolin, now at the University of California at Los Angeles, helped to build the electronics and optics for the apparatus, and François Bessette and Louis Salvail of the University of Montreal assisted in writing the software. At about the same time, the theoretical ideas of David Deutsch of the University of Oxford led one of us (Ekert) to conceive of a slightly different cryptosystem based on quantum correlations. In early 1991, utilizing ideas conceived by Massimo Palma of the University of Palermo, John Rarity and Paul Tapster of the British Defence Research Agency started experiments implementing Ekert's cryptosystem.

To explain how such systems work, we need to describe in more detail some aspects of the mathematics of classical cryptography, especially the role of the key. In the early days of crypto the security of a cipher depended secrecy of the entire encryption cryption procedure. Today such dures are usually known publi the key is kept secret. In such the key is used to control and ize the encryption and decrypti cesses in such a way that an ad who has intercepted the cry and knows the general method cryption but not the key will not to infer anything useful about th nal message. Consequently, the gram may be broadcast over a channel such as a radio or print newspaper. The key, however, sent through a very secure priva nel, such as a clandestine meet delivery by a trusted courier. Al the distribution of a key over channels is expensive, it make ble subsequent secret commun over inexpensive public channel

Ultimately, the security of a gram depends on the length of t In two brilliant papers written 1940s, Claude E. Shannon, then Laboratories, showed that if the shorter than the message being e ed, some information about th sage can be inferred from the gram by a sufficiently powerful sary. This leakage of information regardless of how complicated



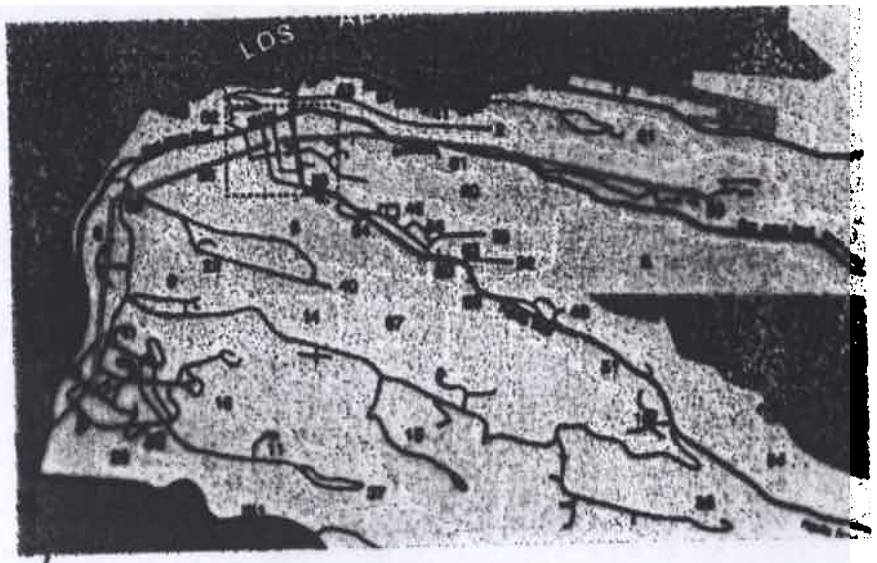
QUANTUM DEVICE generates and measures extremely faint flashes of polarized light, providing a secure way to transmit information [*see illustration on pages 56 and 57*]. On each flash consists of one tenth of a photon.

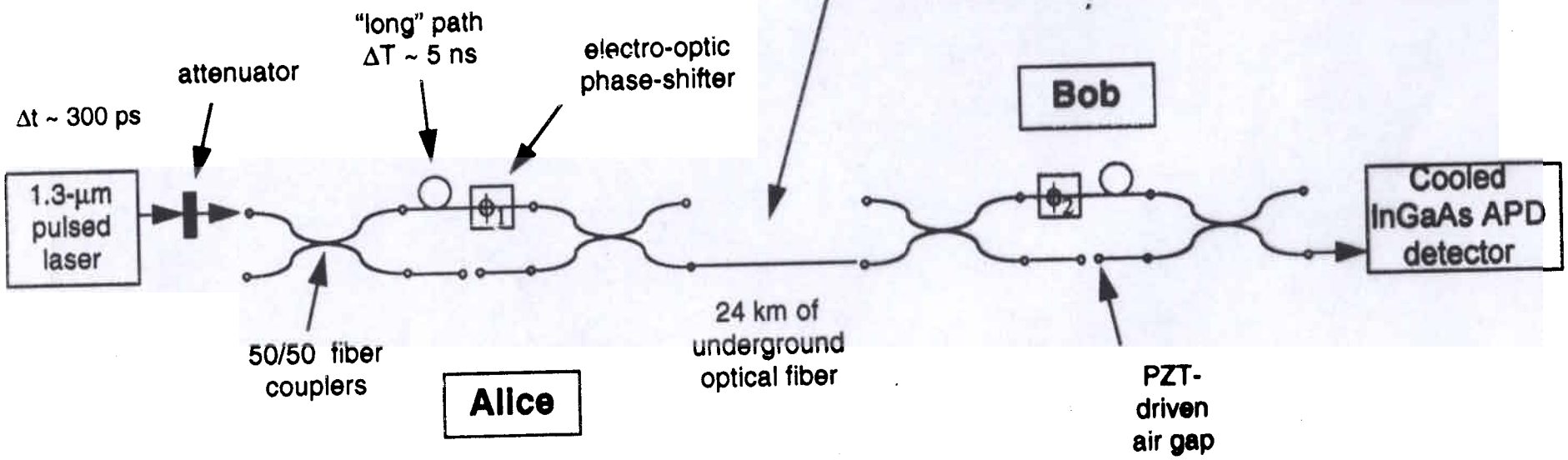


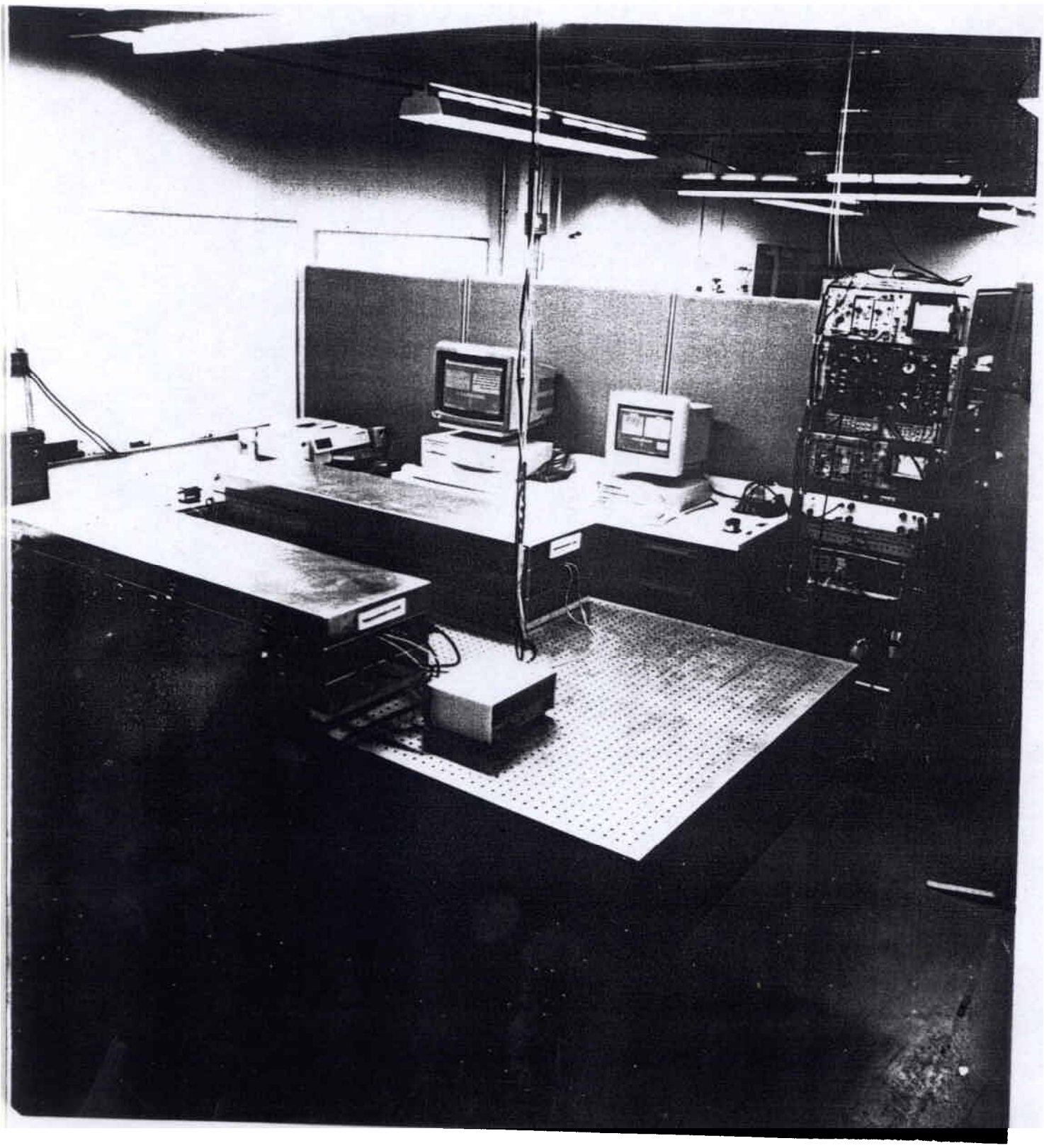
QUANTUM DEVICE generates and measures extremely faint flashes of polarized light, providing a secure way to transmit information [*see illustration on pages 56 and 57*]. On average, each flash consists of one tenth of a photon.

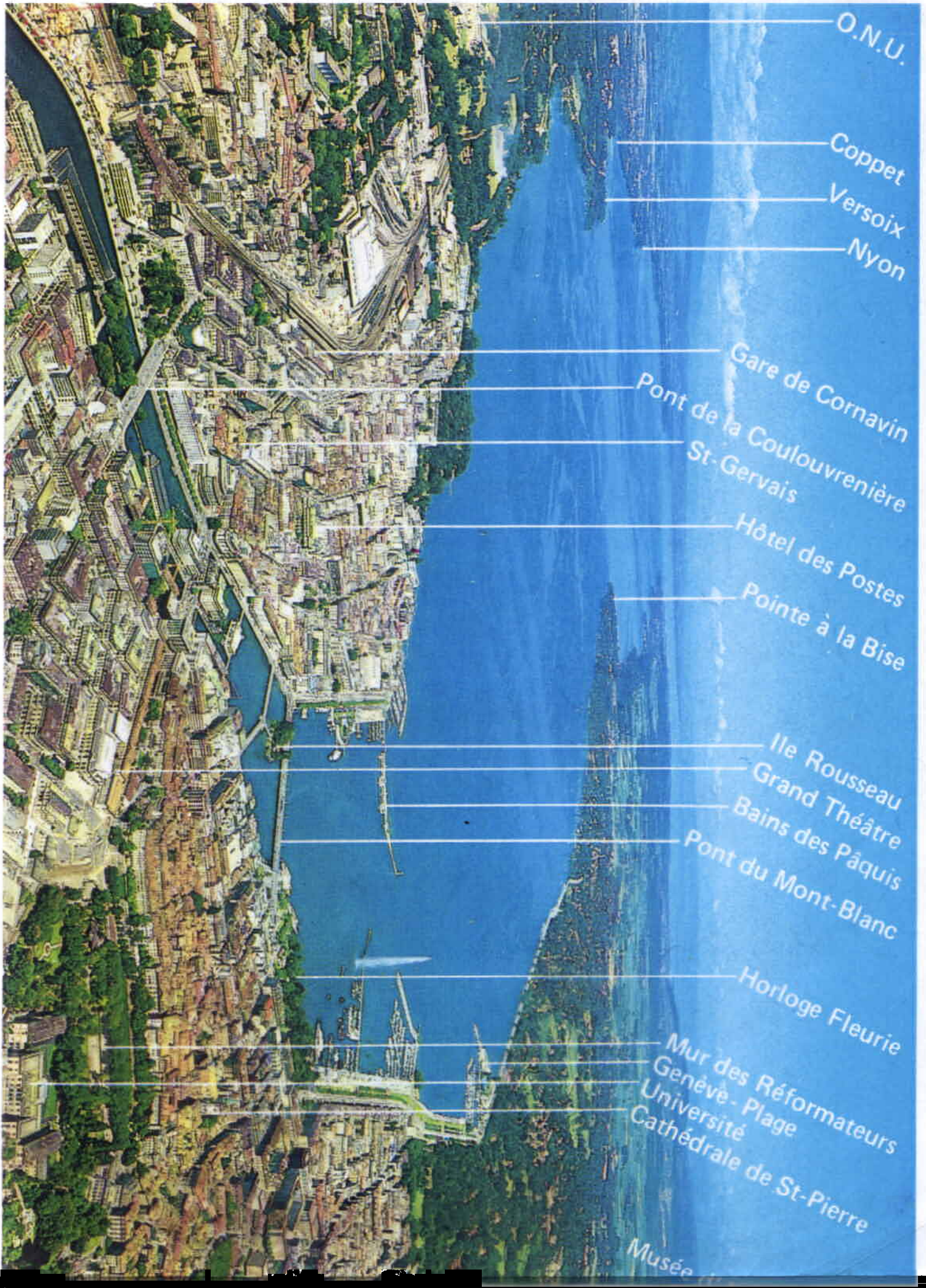
~~48~~ ~~24~~-km QKD experiment at Los Alamos

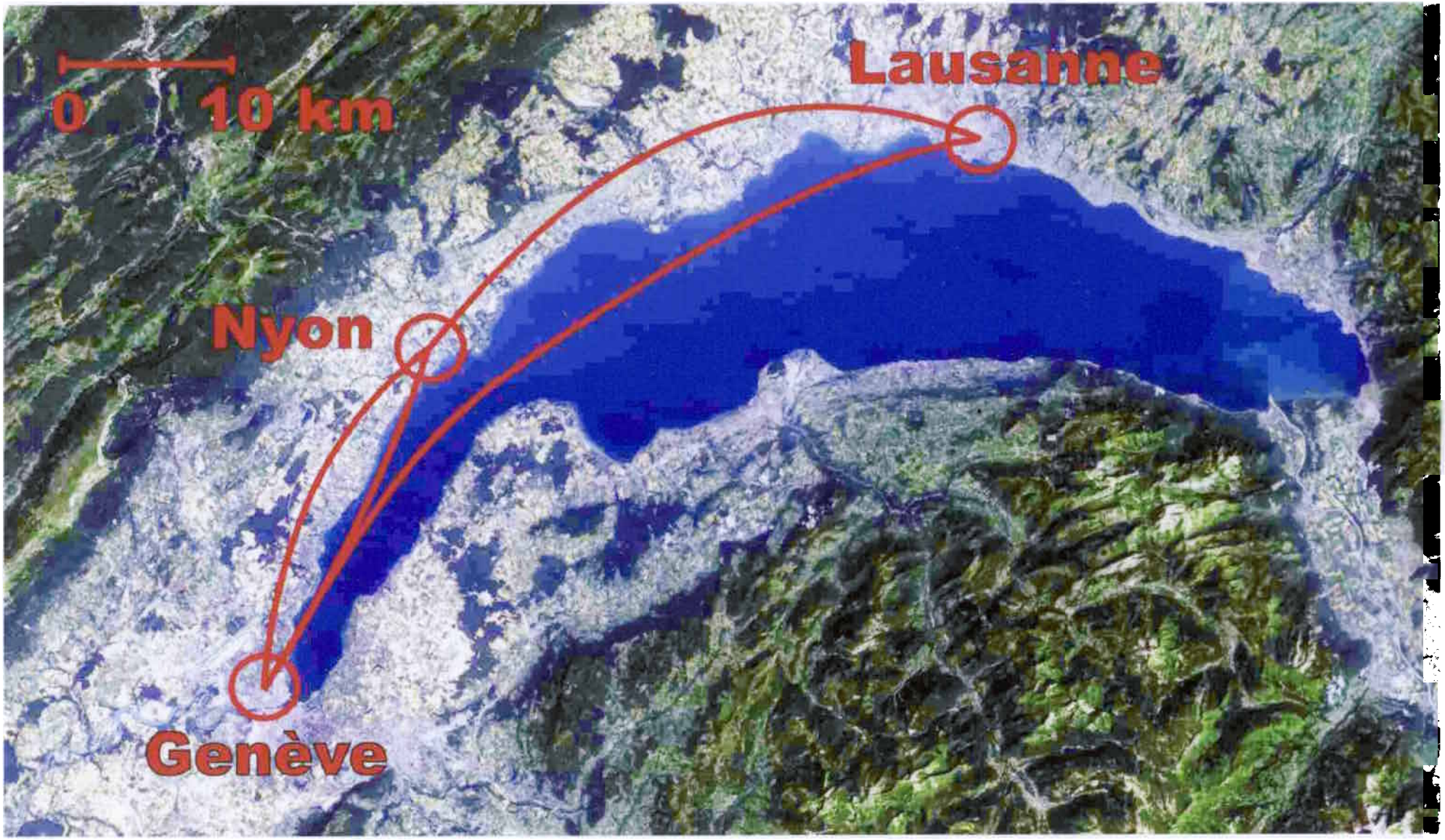
- single-photon interference over 24-km optical paths within **installed, underground** fiber
  - **first demonstration of QKD outside a laboratory**
  - "real-world" environment

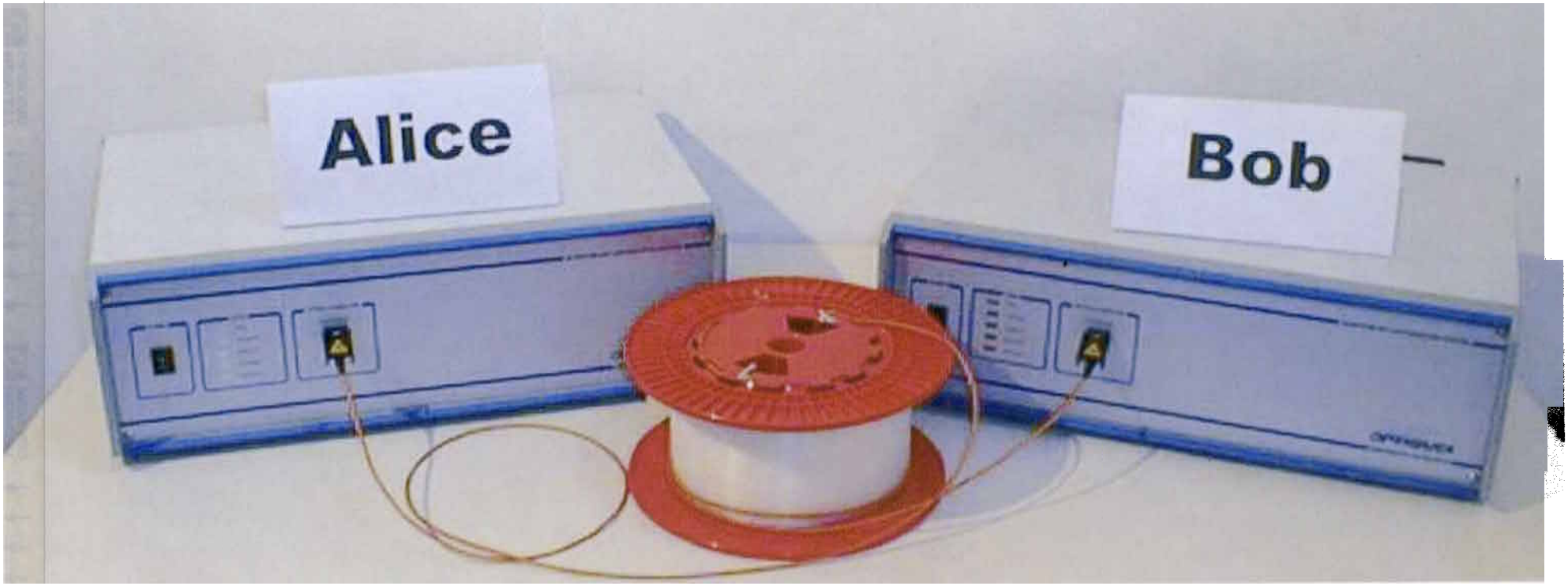







O.N.U.
Coppet
Versoix
Nyon
Gare de Cornavin
Pont de la Coulouvrenière
St-Gervais
Hôtel des Postes
Pointe à la Bise
Ile Rousseau
Grand Théâtre
Bains des Pâquis
Pont du Mont-Blanc
Horloge Fleurie
Mur des Réformateurs
Genève - Plage
Université
Cathédrale de St-Pierre
Musée


0
10 km
Lausanne
Nyon
Genève


Alice
Bob

Quantum Security... at last

Quantum Key Distribution System

Key distribution over optical fiber with absolute security

Main features

- First quantum cryptography system
- Security guaranteed by quantum physics
- Point-to point key distribution
- Standard optical fiber
- Distances up to 70 km
- Key rate up to 1000 bits/s
- Compact and reliable

Key distribution is a central problem in cryptography. Currently, public key cryptography is commonly used to solve it. However, these algorithms are vulnerable to increasing computer power. In addition, their security has never been formally proven.

Quantum cryptography exploits a fundamental principle of quantum physics - observation causes perturbation - to distribute cryptographic keys with absolute security.

id Quantique is introducing the first quantum key distribution system. It consists of an emitter and a receiver, which can be connected to PC's through the USB port.

id Quantique

1, rue Cingria 1205 Geneva Switzerland
Tel: [+41] 022 702 89 29 Fax: [+41] 022 781 39 80
email: info@idquantique.com
web: http://www.idquantique.com

id Quantique

PRL 85 (6) : 1330, 2000

Limitations on Practical Quantum Cryptography

Gilles Brassard,[1] Norbert Lütkenhaus,[2] Tal Mor,[3,4] and Barry C. Sanders[5]

[1]*Département IRO, Université de Montréal, C.P. 6128, succursale centre-ville, Montréal, Québec Canada H3C 3J7*

[2]*Helsinki Institute of Physics, P.O. Box 9, 00014 Helsingin yliopisto, Finland*

[3]*Electrical Engineering, University of California at Los Angeles, Los Angeles, California 90095-1594*

[4]*Electrical Engineering, College of Judea and Samaria, Ariel, Israel*

[5]*Department of Physics, Macquarie University, Sydney, New South Wales 2109, Australia*

(Received 2 February 2000)

We provide limits to practical quantum key distribution, taking into account channel losses, a realistic detection process, and imperfections in the "qubits" sent from the sender to the receiver. As we show, even quantum key distribution with perfect qubits might not be achievable over long distances when the other imperfections are taken into account. Furthermore, existing experimental schemes (based on weak pulses) currently do not offer unconditional security for the reported distances and signal strength. Finally we show that parametric down-conversion offers enhanced performance compared to its weak coherent pulse counterpart.

PACS numbers: 03.67.Dd, 05.40.Ca, 42.50.Dv, 89.80.+h

Quantum information theory suggests the possibility of accomplishing tasks that are beyond the capability of classical computer science, such as information theoretically secure cryptographic key distribution [1,2]. Currently, we lack security proofs for standard (secret and public) key distribution schemes, and the most widely used classical schemes become insecure against potential attacks by quantum computers [3].

Whereas the security of idealized quantum key distribution (QKD) schemes has been reported against very sophisticated collective [4] and joint [5] attacks, we show here that already very simple attacks severely disturb the security of existing experimental schemes, for the chosen transmission length and signal strength. For a different parameter region a positive security proof against individual attacks has been given recently [6] making use of ideas presented here.

In the four-state scheme [1], usually referred to as Bennett-Brassard-84 (BB84), the sender (Alice) and the receiver (Bob) use two conjugate bases (say, the rectilinear basis, +, and the diagonal basis, ×) for the polarization of single photons. In basis + they use the two orthogonal basis states $|0_+\rangle$ and $|1_+\rangle$ to represent "0" and "1," respectively. In basis × they use the two orthogonal basis states $|0_\times\rangle = (|0_+\rangle + |1_+\rangle)/\sqrt{2}$ and $|1_\times\rangle = (|0_+\rangle - |1_+\rangle)/\sqrt{2}$ to represent 0 and 1. The basis is revealed later on via an authenticated classical channel that offers no protection against eavesdropping. The signals where Bob used the same basis as Alice form the *sifted key* on which Bob can decode the bit value. The remaining signals are ignored in the protocol and in this security analysis. Finally, Alice and Bob use error correction and privacy amplification [7,8] to obtain a secure final key [5].

In order to be practical and secure, a QKD scheme must be based on existing—or nearly existing—technology, but its security must be guaranteed against an eavesdropper with unlimited computing power whose technology is limited only by the laws of quantum mechanics. The experiments are usually based on weak coherent pulses (WCP) as signal states with a low probability of containing more than one photon [7,9–11]. Initial security analysis of such weak-pulse schemes was done [7,12], and evidence of some potentially severe security problems (not existing for the idealized schemes) was shown [12,13].

Using a conservative definition of security, we provide several explicit limits on experimental QKD. First, we show that secure QKD to arbitrary distance can be totally impossible for given losses and detector dark counts, even with the assumption of a perfect source. Second, we show that QKD can be totally insecure even with perfect detection, due to losses and multiphoton states. Combining these results we compute a maximal distance beyond which (for any given source and detection units) secure QKD schemes cannot be implemented. Finally, we establish the advantage of a better source, which makes use of parametric down-conversion (PDC).

The effect of losses is that single-photon (SP) signals will arrive only with a probability F at Bob's site where they will lead to a detection in Bob's detectors with a probability η_B (detection efficiency). This leads to an expected probability of detected signals given by $p_{\text{exp}}^{\text{signal}} = F\eta_B$. For optical fibers, as used for most current experiments, the transmission efficiency F is connected to the absorption coefficient β and length ℓ of the fiber and a distance-independent constant loss in optical components c, via the relation

$$F = 10^{-(\beta\ell + c)/10} \tag{1}$$

which, for given β and c, gives a one-to-one relation between distance and transmission efficiency. Also, QKD can be achieved through free space [7,11], in which case

 0031-9007/00/85(6)/1330(4)$15.00

Beyond Key Distribution

- Private quantum channels
- Coin flipping
- Bit commitment
- Oblivious transfer
- Discreet decision making
- Zero-knowledge
- Authentication
- Signature
- etc, etc, etc...

Quantum Multiplexing

Wiesner ≈ 1970

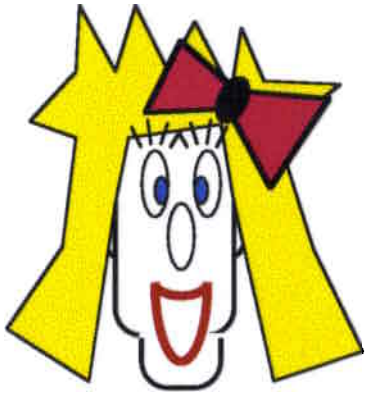
Alice sends Bob two messages.

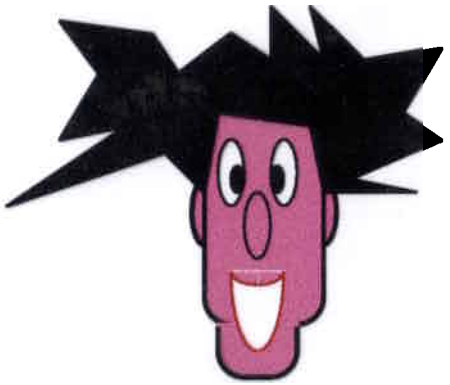
Bob chooses which one to read →

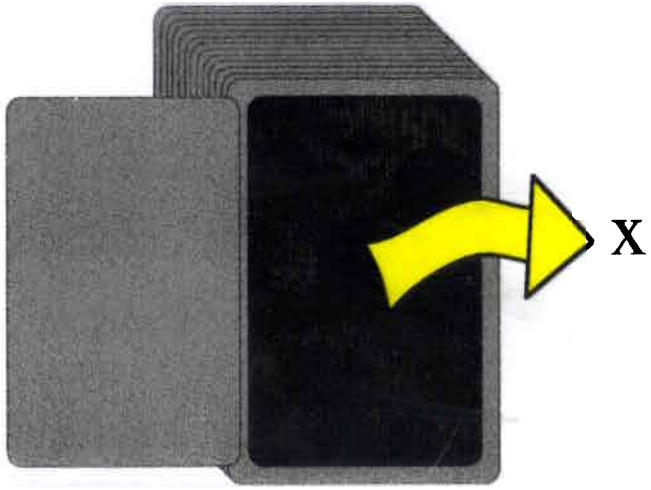
destroys the other

Commit(x)

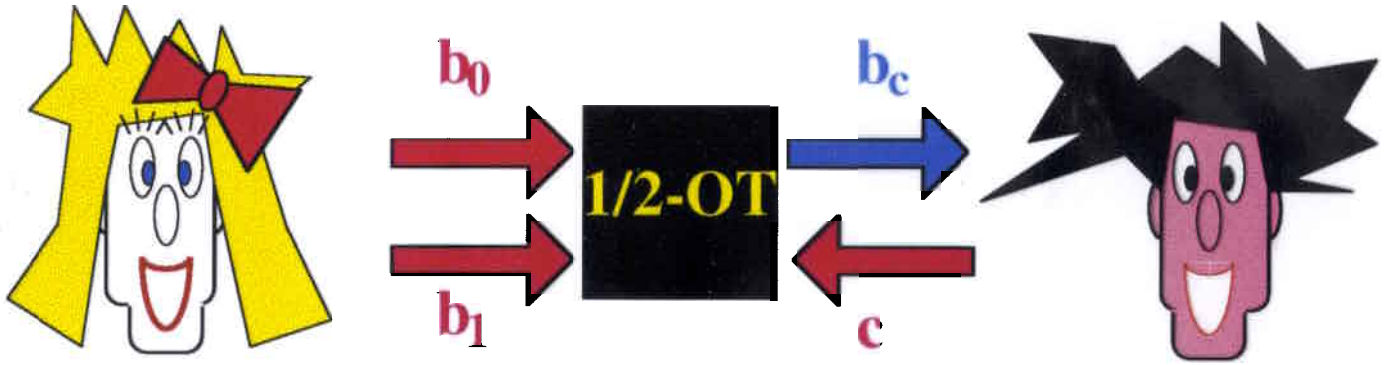
Unveil(x)





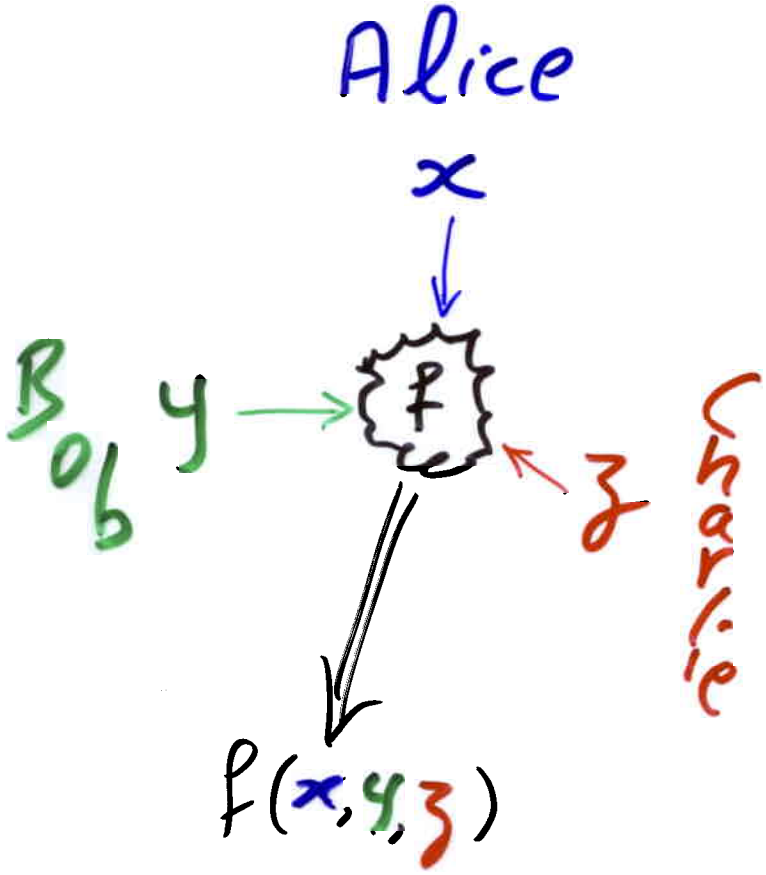


1/2-Oblivious Transfer

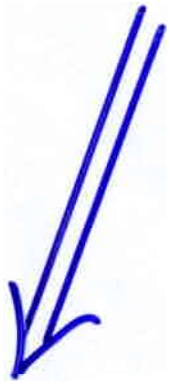


Discreet Decision Making

$$f : X \times Y \times Z \rightarrow \{0, 1\}$$



Bit Commitment



Coin Flipping

Zero-Knowledge

[Identification]

Reduction ?

Bit Commitment

Oblivious Transfer

Probably Not !

(Classically)

Reduction ?

Bit Commitment

oblivious Transfer

YES!

("Quantumly")

UPS and DOWNS of Quantum bit commitments

Gilles Brassard Université de Montréal
Claude Crépeau McGill University
Dominic Mayers Princeton University
Louis Salvail BRICS, Aarhus

BB84 Bit Commitment

(coin tossing)

Fun but known to be insecure from the start!

(1984)

A QUANTUM BIT COMMITMENT SCHEME PROVABLY UNBREAKABLE BY BOTH PARTIES

Gilles Brassard
Claude Crépeau
Richard Jozsa
Denis Langlois

Reprinted from PROCEEDINGS OF THE 34th ANNUAL SYMPOSIUM ON FOUNDATIONS OF COMPUTER SCIENCE, Palo Alto, California, November 3 — 5, 1993

The Trouble with Quantum Bit Commitment

Dominic Mayers

Département IRO, Université de Montréal

C.P. 6128, succursale Centre-Ville,Montréal (Québec), Canada H3C 3J7.

(April 28, 2001)

Abstract

In a recent paper, Lo and Chau explain how to break a family of quantum bit commitment schemes, and they claim that their attack applies to the 1993 protocol of Brassard, Crépeau, Jozsa and Langlois (BCJL). The intuition behind their attack is correct, and indeed they expose a weakness common to all proposals of a certain kind, but the BCJL protocol does not fall in this category. Nevertheless, it is true that the BCJL protocol is insecure, but the required attack and proof are more subtle. Here we provide the first complete proof that the BCJL protocol is insecure.

1994 PACS numbers: 03.65.Bz, 42.50.Dv, 89.70.+c

46

Is Quantum Bit Commitment Really Possible?

Hoi-Kwong Lo* and H. F. Chau†
School of Natural Sciences, Institute for Advanced Study, Olden Lane, Princeton, NJ 08540
(March 23, 2001)

We show that all proposed quantum bit commitment schemes are insecure because the sender, Alice, can almost always cheat successfully by using an Einstein-Podolsky-Rosen type of attack and delaying her measurement until she opens her commitment.

PACS Numbers: 89.70.+c, 03.65.Bz, 89.80.+h

Work on quantum cryptography was started by S. J. Wiesner in a paper written in about 1970, but remained unpublished until 1983 [1]. Recently, there have been lots of renewed activities in the subject. The most well-known application of quantum cryptography is the so-called quantum key distribution (QKD) [2–4], which is useful for making communications between two users totally unintelligible to an eavesdropper. QKD takes advantage of the uncertainty principle of quantum mechanics: Measuring a quantum system in general disturbs it. Therefore, eavesdropping on a quantum communication channel will generally leave unavoidable disturbance in the transmitted signal which can be detected by the legitimate users. Besides QKD, other quantum cryptographic protocols [5] have also been proposed. In particular, it is generally believed [4] that quantum mechanics can protect private information while it is being used for public decision. Suppose Alice has a secret x and Bob a secret y. In a "two-party secure computation" (TPSC), Alice and Bob compute a prescribed function $f(x, y)$ in such a way that nothing about each party's input is disclosed to the other, except for what follows logically from one's private input and the function's output. An example of the TPSC is the millionaires' problem: Two persons would like to know who is richer, but neither wishes the other to know the exact amount of money he/she has.

In classical cryptography, TPSC can be achieved either through trusted intermediaries or by invoking some unproven computational assumptions such as the hardness of factoring large integers. The great expectation is that quantum cryptography can get rid of those requirements and achieve the same goal using the laws of physics alone. At the heart of such optimism has been the widespread belief that *unconditionally* secure quantum bit commitment (QBC) schemes exist [6]. Here we put such optimism into very serious doubt by showing that *all* proposed QBC schemes are insecure: A dishonest party can exploit the non-local Einstein-Podolsky-Rosen (EPR) [18] type correlations in quantum mechanics to cheat successfully. To do so, she generally needs to maintain the coherence of her share of a quantum system by using a quantum computer. We remark that all proposed QBC schemes contain an invalid implicit assumption that some measurements are performed by the two participants. This is why this EPR-type of attack was missed in earlier analysis.

Let us first introduce bit commitment. A bit commitment scheme generally involves two parties, a sender, Alice and a receiver, Bob. Suppose that Alice has a bit ($b = 0$ or 1) in mind, to which she would like to be committed towards Bob. That is, she wishes to provide Bob with a piece of evidence that she has already chosen the bit and that she cannot change it. Meanwhile, Bob should not be able to tell from that evidence what b is. At a later time, however, it must be possible for Alice to *open* the commitment. In other words, Alice must be able to show Bob which bit she has committed to and convince him that this is indeed the genuine bit that she had in mind when she committed.

A concrete example of an implementation of bit commitment is for Alice to write down her bit in a piece of paper, which is then put in a locked box and handed over to Bob. While Alice cannot change the value of the bit that she has written down, without the key to the box Bob cannot learn it himself. At a later time, Alice gives the key to Bob, who opens the box and recovers the value of the committed bit. This illustrative example of implementation is, however, inconvenient and insecure. A locked box may be very heavy and Bob may still try to open it by brute force (e.g. with a hammer).

What do we mean by cheating? As an example, a cheating Alice may choose a particular value of b during the commitment phase and tell Bob *another* value during the opening phase. A bit commitment scheme is secure against a cheating Alice only if such a fake commitment can be discovered by Bob. For concreteness, it is instructive to consider a simple QBC protocol due to Bennett and Brassard [2]. Its procedure goes as follows: Alice and Bob first agree on a security parameter, a positive integer s. The sender, Alice, chooses the value of the committed bit, b. If $b = 0$, she prepares and sends Bob a sequence

*Present Address: BRIMS, Hewlett-Packard Labs, Filton Road, Stoke Gifford, Bristol BS12 6QZ, UK. e-mail: hkl@hplb.hpl.hp.com
†Present Address: Department of Physics, University of Hong Kong, Pokfulam Road, Hong Kong. e-mail: hfchau@hkusua.hku.hk

41

Unconditionally secure quantum bit commitment is impossible

Dominic Mayers
Département IRO, Université de Montréal
C.P. 6128, succursale Centre-Ville,Montréal (Québec), Canada H3C 3J7.
(February 27, 2001)

The claim of quantum cryptography has always been that it can provide protocols that are unconditionally secure, that is, for which the security does not depend on any restriction on the time, space or technology available to the cheaters. We show that this claim does not hold for any quantum bit commitment protocol. Since many cryptographic tasks use bit commitment as a basic primitive, this result implies a severe setback for quantum cryptography. The model used encompasses all reasonable implementations of quantum bit commitment protocols in which the participants have not met before, including those that make use of the theory of special relativity.

1994 PACS numbers: 03.65.Bz, 42.50.Dv, 89.70.+c

a. Introduction. Quantum cryptography is often associated with a cryptographic application called key distribution [1,2] and it has achieved success in this area [5]. However, other applications of quantum mechanics to cryptography have also been considered and a basic cryptographic primitive called bit commitment, the main focus of this letter, was at the basis of most if not all of these other applications [3,6,15,5].

In a concrete example of bit commitment, a party, Alice, writes a bit b on a piece of paper and puts it into a safe. She gives the safe to another party, Bob, but keeps the key. The objective of this scheme, and of bit commitment in general, is that Alice cannot change her mind about the value of the bit b, but meanwhile Bob cannot determine the bit b. At a later time, if Alice wants to unveil b to Bob, she gives the key to Bob.

In 1993, a protocol was proposed to realize bit commitment in the framework of quantum mechanics, and the unconditional security (see sections b and c) of this protocol has been generally accepted for quite some time. However, this result turned out to be wrong. The non security of this protocol, called the BCJL protocol, was realized in the fall of 1995 [12]. After this discovery, Brassard, Crépeau and other researchers have tried to find alternative protocols [4]. Some protocols were based on the theory of special relativity. For additional information about the history of the result see [5]. See also [11].

Here it is shown that an unconditionally secure bit commitment protocol is impossible, unless a computing device, such as a beam splitter, a quantum gate, etc. can be simultaneously trusted by both participants in the protocol. This encompasses any protocol based on the theory of special relativity. A preliminary version of the proof appeared in [13].

b. The model for quantum protocols. It is neither possible in this letter to describe in detail a model for two-party quantum protocols, nor is it is useful for the purpose of this letter. The following description includes all that is necessary for our proof.

In our model, a two-party quantum protocol is executed on a system $H_A \otimes H_B \otimes H_E$ where H_A and H_B correspond to two areas, one on Alice's side and one on Bob's side, and H_E corresponds to the environment. We adopt the "decoherence" point of view in which a mixed state ρ of $H_A \otimes H_B$ is really the reduced state of $H_A \otimes H_B$ entangled with the environment H_E, the total system $H_A \otimes H_B \otimes H_E$ always being in a pure state $|\psi\rangle$. The systems H_A and H_B contain only two dimensional quantum registers. Higher dimensional systems can be constructed out of two dimensional systems. Alice and Bob can execute any unitary transformation on their respective system. In particular, they can introduce new quantum registers in a fixed state $|0\rangle$. States that correspond to different number of registers can be in linear superposition. Any mode of quantum communication can be adopted between Alice and Bob.

Without loss of generality, we can restrict ourselves to binary outcome measurements. The environment is of the form $H_E = H_S \otimes H_{E,A} \otimes H_{E,B}$ where $H_S = H_{S,A} \otimes H_{S,B}$ is a system that stores classical bits that have been transmitted from $H_{S,A}$ on Alice's side to $H_{S,B}$ on Bob's side or vice versa, and $H_{E,A}$ and $H_{E,B}$ store untransmitted classical bits that are kept on Alice's side and Bob's side respectively. To execute a binary outcome measurement, a participant $P \in \{A, B\}$, where A and B stand for Alice and Bob respectively, introduces a quantum register in a fixed state $|0\rangle$. The participant P entangles this register with the measured system initially in a state $|\phi\rangle$ and obtains a new state of the form $\alpha|0\rangle|\phi_0\rangle + \beta|1\rangle|\phi_1\rangle$. Then, he sends the new quantum register away to a measuring apparatus in $H_{E,P}$ which amplifies and stores each component $|x\rangle$ as a complex state $|x\rangle^{(E,P)}$. The resulting state is $\alpha|0\rangle^{(E,P)}|\phi_0\rangle + \beta|1\rangle^{(E,P)}|\phi_1\rangle$. Similarly, to generate a random bit one simply maps $|0\rangle$ into $\alpha|0\rangle + \beta|1\rangle$ and sends the register away in some part of $H_{E,P}$ that will amplify and store it as a state $\alpha|0\rangle^{(E,P)} + \beta|1\rangle^{(E,P)}$. The transmission of a classical bit x from Alice to Bob is represented by a transformation that maps $|x\rangle^{(E,A)}|0\rangle^{(E,B)}$ into $|x\rangle^{(S,A)}|x\rangle^{(S,B)}$. A similar transformation exists for the transmission of a classical bit from Bob to Alice.

Now, let us assume that the total system is in a super-

42

The Quantum Coin Flipping

Andris Ambainis (UC Berkeley)