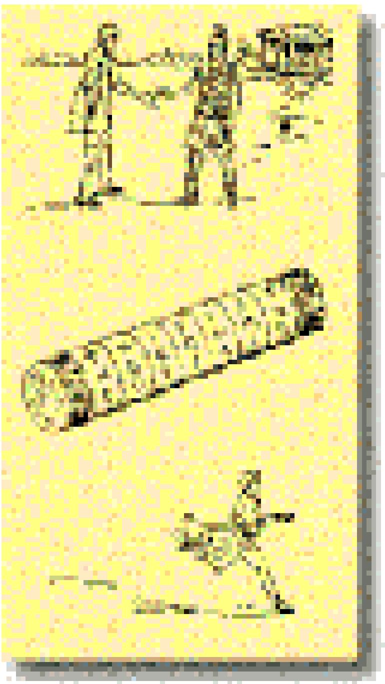
Cryptology

Enigma

Marian Rejewski,
Jerzy Róz’ycki,
Henryk Zygalski

From Scytale to Enigma

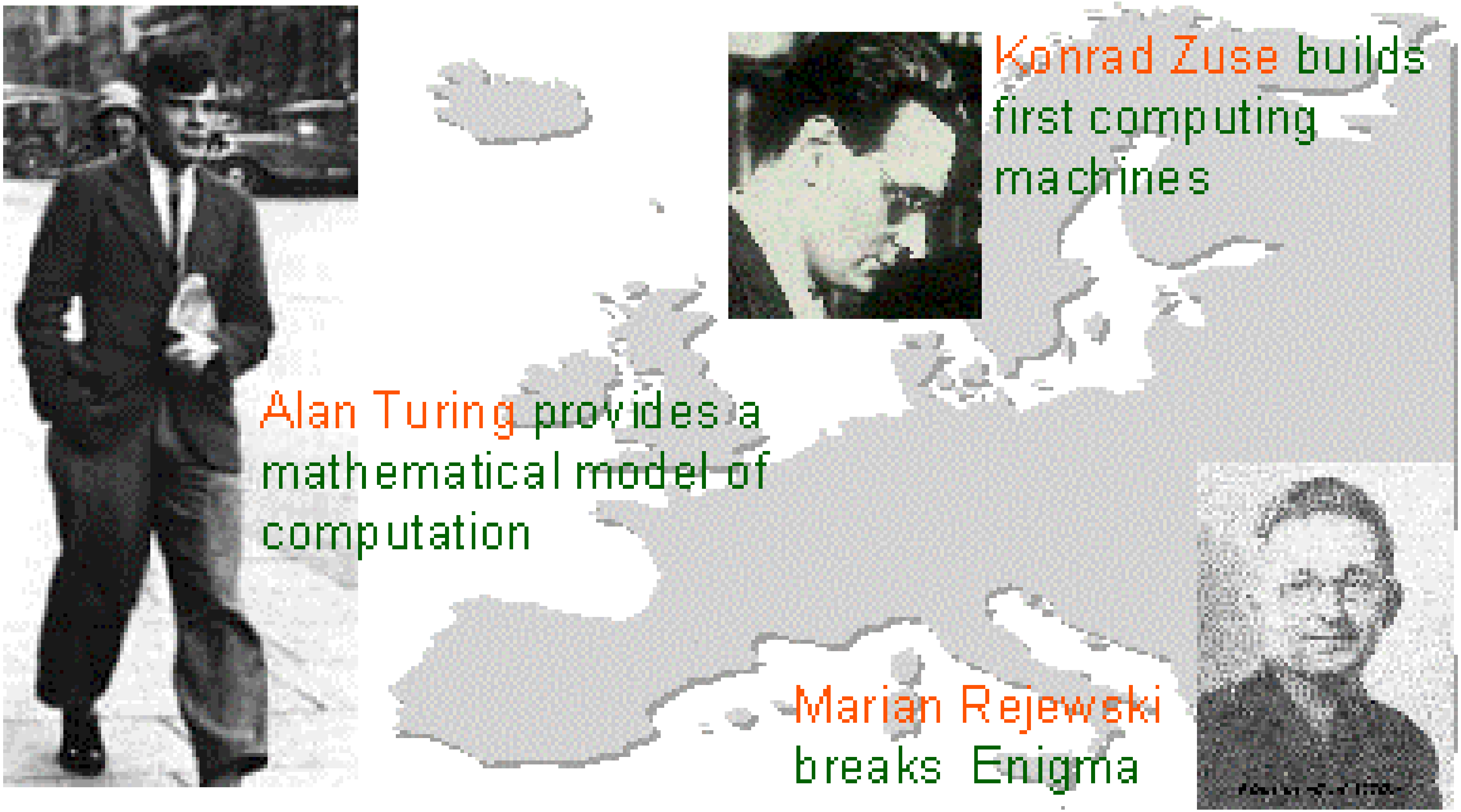


SCYTALE 400BC

POLYGRAPHIAE
1518

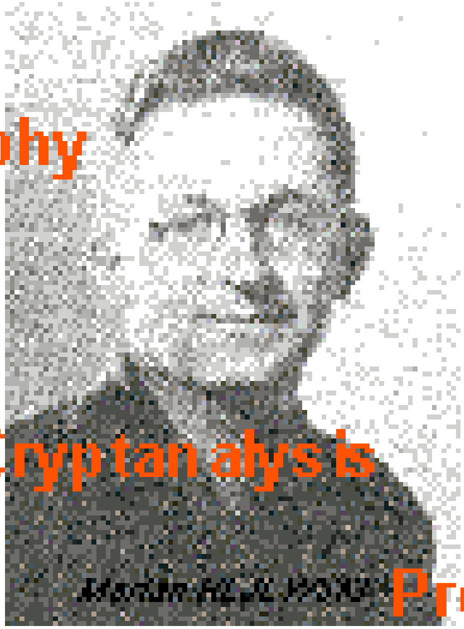
ENIGMA

Computers & Ciphers



From Enigma to Colossus

Cryptography

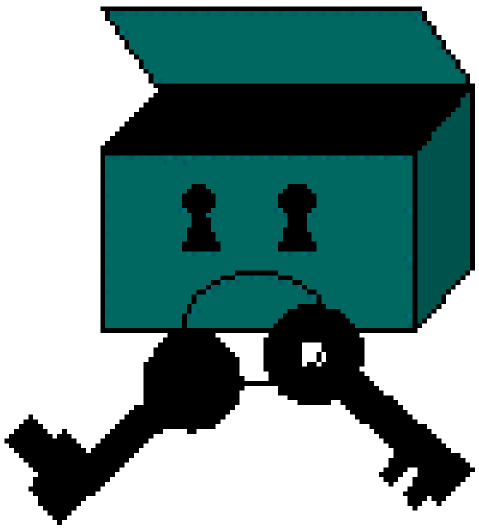


Cryptanalysis

Bletchley Park

Progress in computer technology

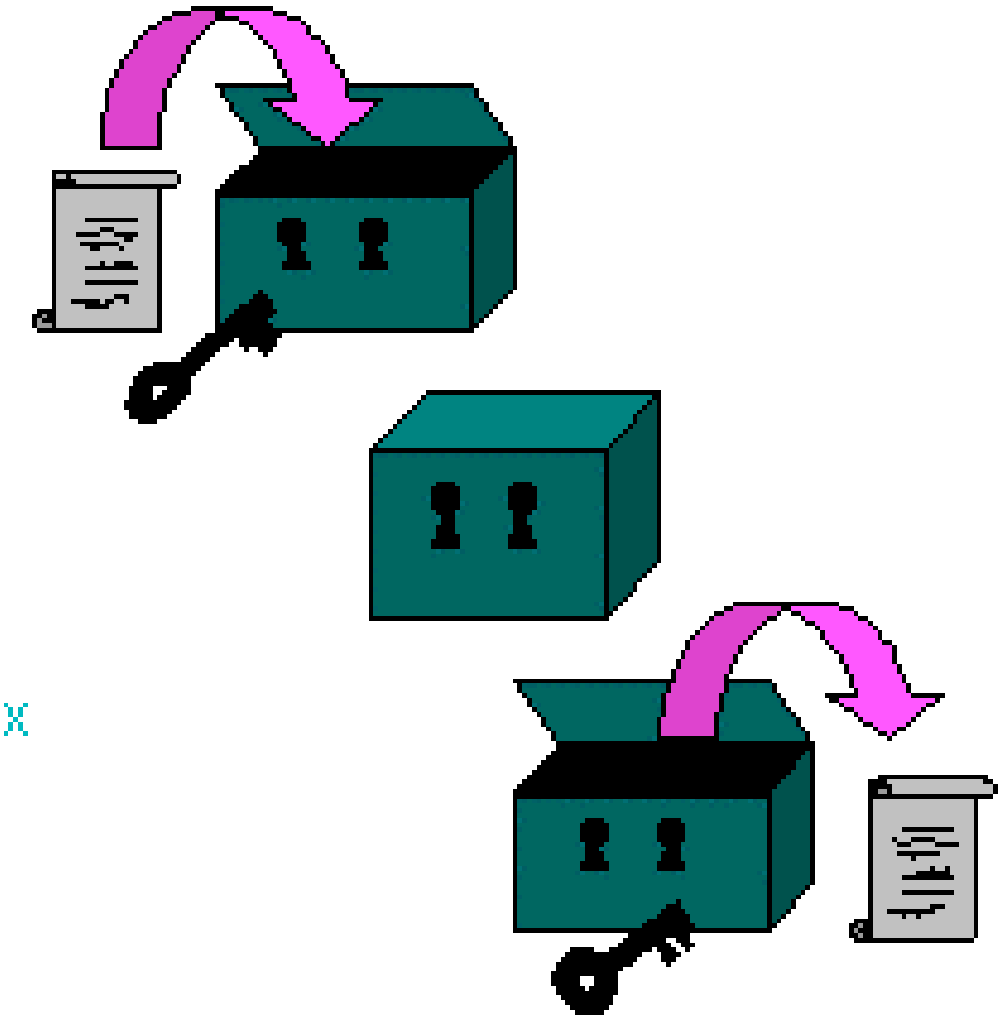
Public Key Cryptosystems



Public key
locks the box

Private key
unlocks the box

FACTORING



The Killer App': Factorization

The security of the RSA encryption method uses the difficulty of factorizing large numbers.

February 2, 1999:
140 digits required
+/- 2000 MIPS years.

(MIPS = Millions of Instructions Per Second)

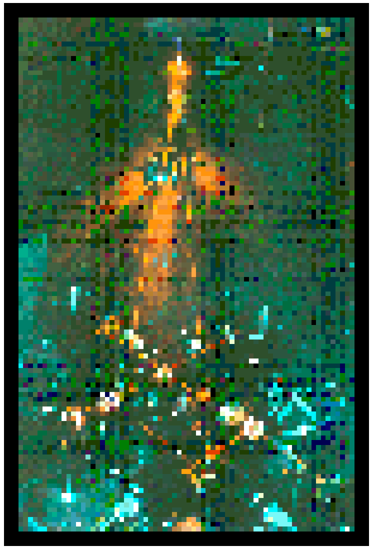
```
RSA-140 =
2129024631825875754749788201627151749780670396327721627\
8233383215381949984056495911366573853021918316783\
107387995317230889569230873441936471

can be written as the product of two 70-digit primes:

3398717423028438554530123627613875835633986495969597\
423490929302771479 * 6264200187401285096151654948264\
442219302037178623509019111660653946049
```

Quantum Cryptology

Quantum factoring means...

Alternatives...

QUANTUM CRYPTOGRAPHY

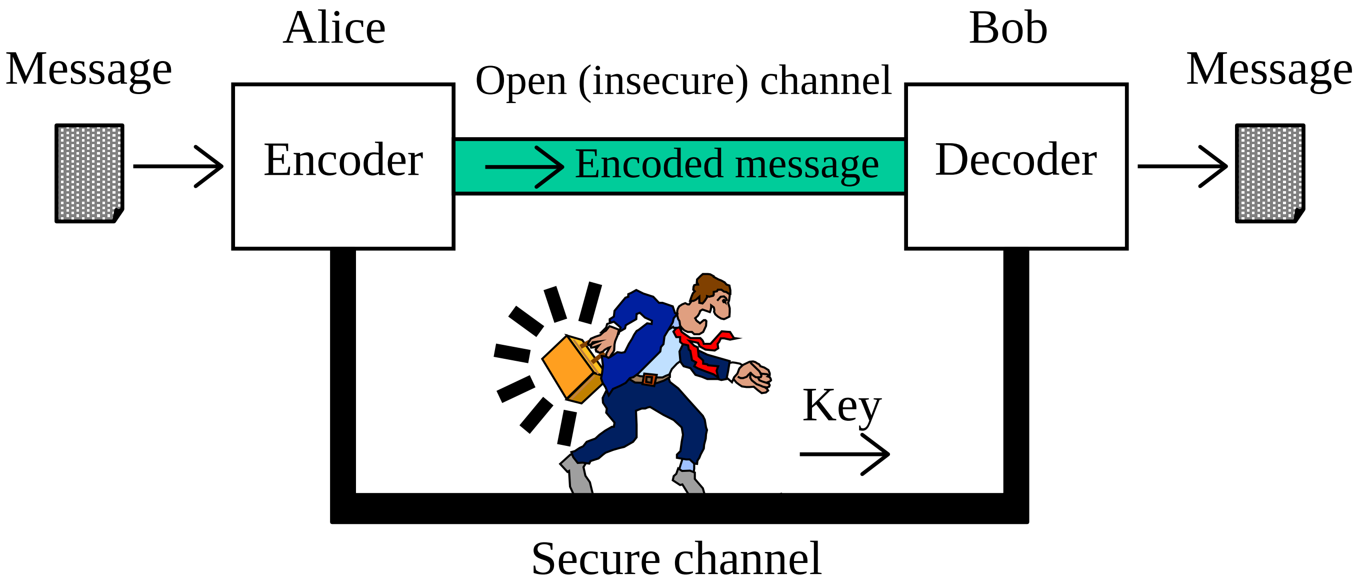


What is the problem with classical cryptography?

- Secret key cryptography
  - Requires secure channel for key distribution
  - *In principle* every classical channel can be monitored passively
  - Security is mostly based on complicated non-proven algorithms

- Public key cryptography
  - Security is based on non-proven mathematical assumptions (e.g. difficulty of factoring large numbers)
  - We DO know how to factorize in polynomial time! Shor's algorithm for quantum computers. Just wait until one is built.
  - Breakthrough renders messages insecure *retroactively*

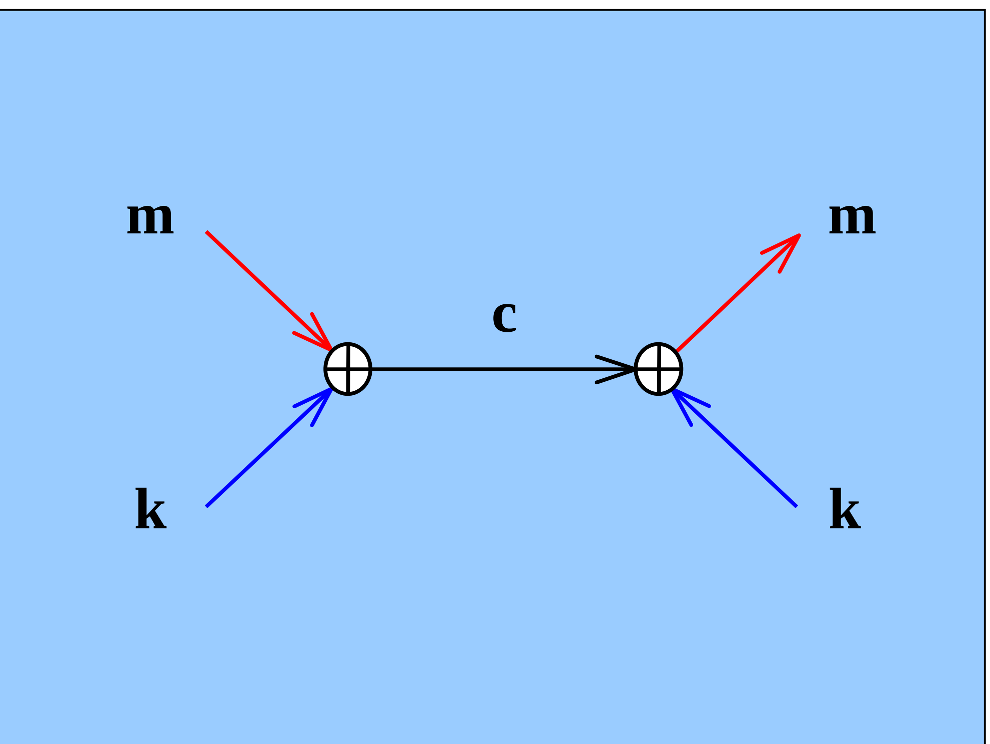
Key distribution

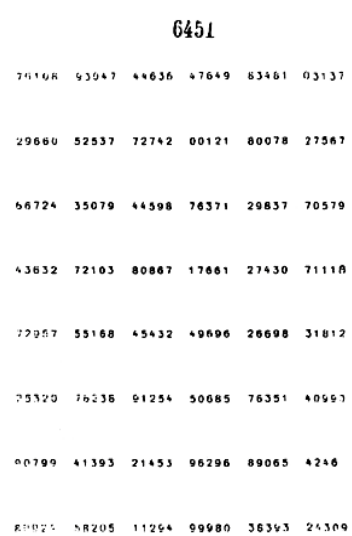


- **Secret key cryptography requires secure channel for key distribution.**
- **<u>Quantum cryptography</u> distributes the key by transmitting quantum states in *open channel.***

The holy grail: *One-time pad*

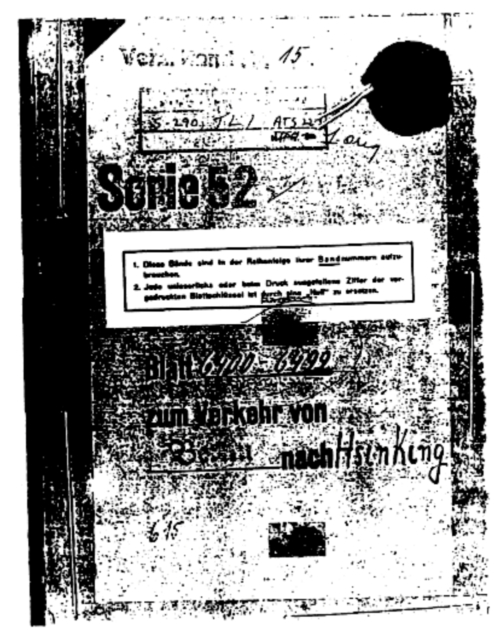
- The only cipher mathematically proven
- Requires massive amounts of key material





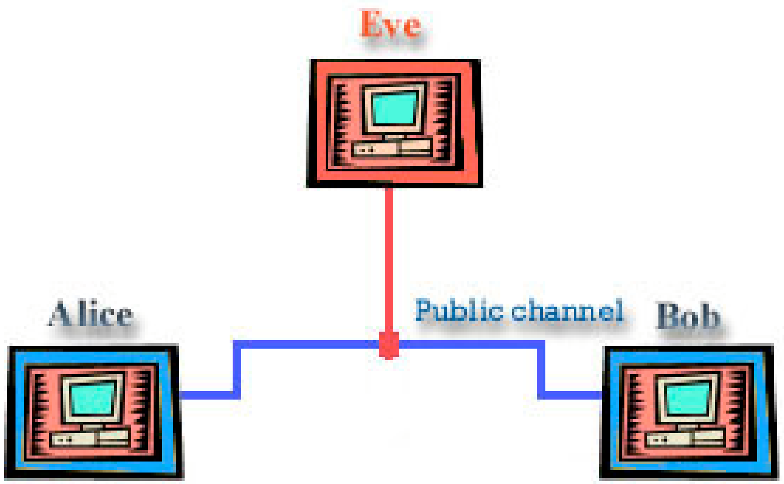
6451

76108	93947	44636	47649	83461	03137
29660	52537	72742	00121	80078	27567
66724	35079	44598	76371	29837	70579
43632	72103	80867	17661	27430	71118
72957	55168	45432	49696	26698	31812
75320	76236	91254	50685	76351	40993
00799	41393	21453	96296	89065	4246
[illegible]	58205	11294	99980	36393	24309



Crypto Definitions: Alice, Bob and Eve

- It is a standard in cryptography to define the sender, receiver, and interceptor as:
  - Alice is the one who sends the ciphertext
  - Bob is the one who receives the ciphertext
  - Eve is the (evil) one who tries to steal the plaintext or key



Quantum Cryptography

Quantum Cryptography

- Application of Quantum Information rather than Quantum Computing
- Not really Cryptography – <u>Quantum Key Distribution</u> would be better name
- Here we describe <u>one possible realization</u> using photon polarizations as qubits
  - Nicholas Gisin and his group in Geneva are one of the leading players in this field

Quantum Cryptography - key

One-Time Pads

- Most secure cryptosystem – encode each bit of message using different secret random number

  Encode: M = N + K modulo 2

  Decode: M + K modulo 2 = N

- Problem: both sender (Alice) and receiver (Bob) need to have copy of same set of keys that eavesdropper (Eve) does not have

Secure Cipher

- A <u>secure cryptosystem</u> can be produced from a random key which is as long as a message.

- **Process**: The ciphertext is the XOR of the random bits with the plaintext bits

Plaintext:	0 1 1 0 1 0 1 0 1 1 0 1 0 0 0
KEY:	1 1 0 0 1 1 1 0 0 1 0 0 1 0 1
Ciphertext:	1 0 1 0 0 1 0 0 1 0 0 1 1 0 1
KEY:	1 1 0 0 1 1 1 0 0 1 0 0 1 0 1
Plaintext:	0 1 1 0 1 0 1 0 1 1 0 1 0 0 0

Key Distribution

- The problem with a stream cipher of this form is the distribution of a key

- If the key is short so everyone can easily remember it, then it is also easy to break

- If the key is long, so it has to be sent between the users, it could be intercepted and compromised

Quantum Key Distribution

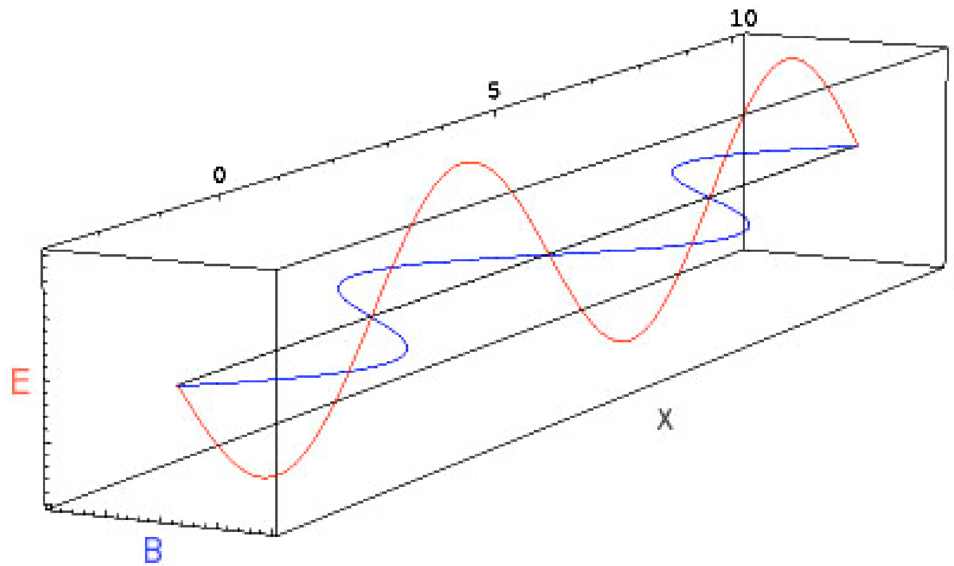
- Quantum effects can be used to distribute a long key with assurances that the key has not be intercepted

- To understand this process:
  - 1. Consider another form of a qubit
  - 2. The standard key distribution format
  - 3. Quantum effects

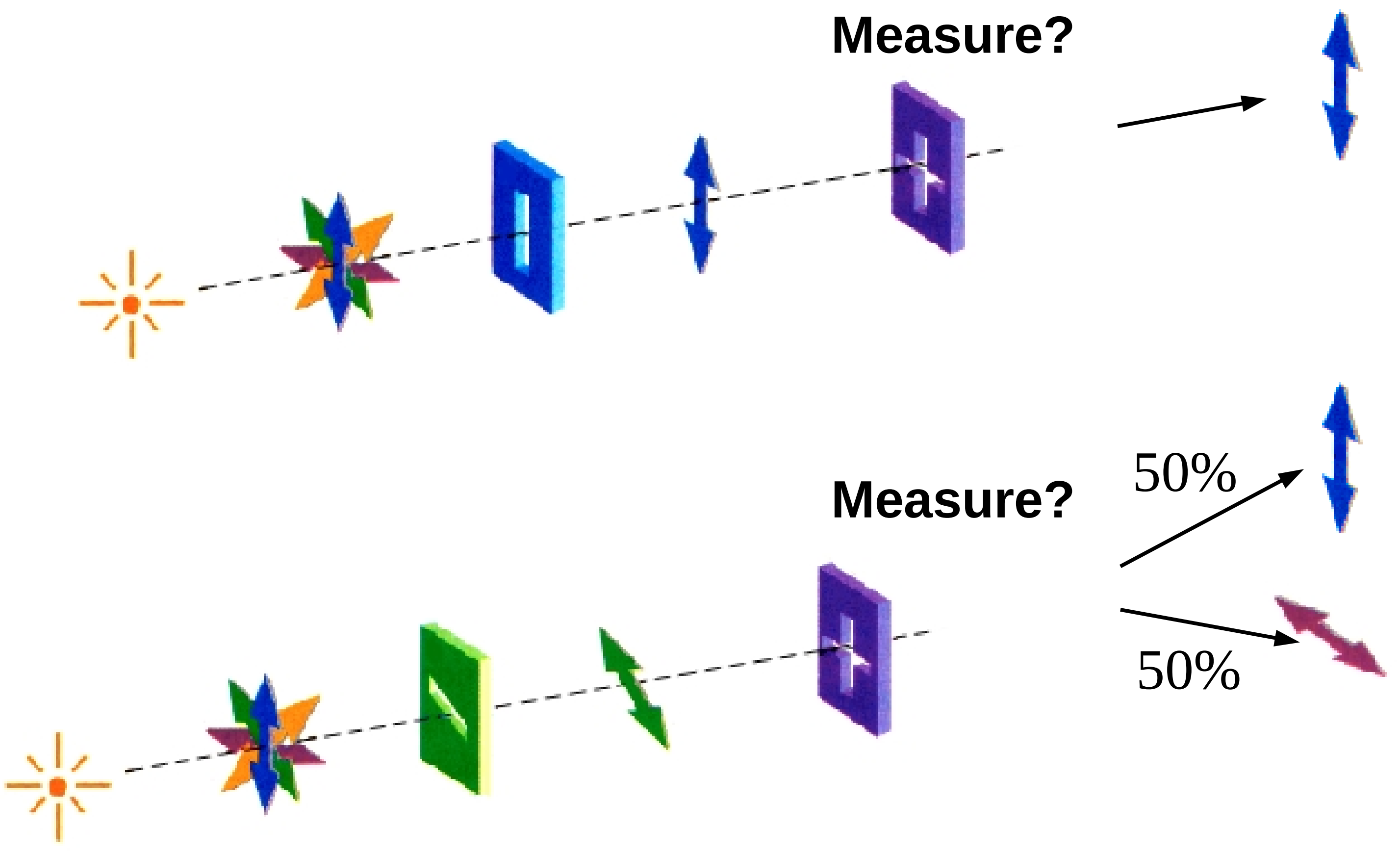
Photons

- Another form of a qubit could be a photon

- A photon is an electromagnetic wave (we know it as light)
  - A photon consists of an oscillating electric field and an oscillating magnetic field which lie in perpendicular planes



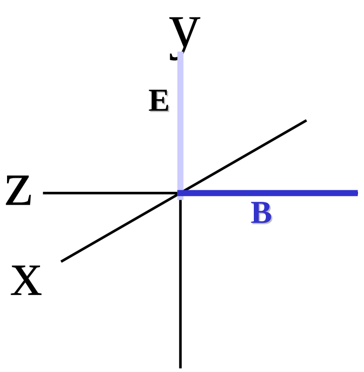
Qubit: polarization state of a single photon

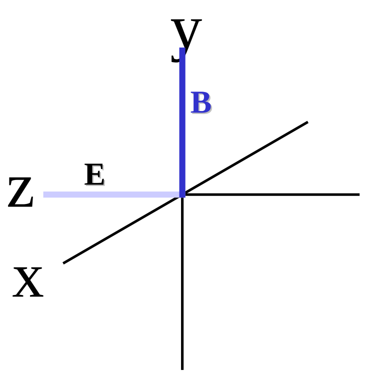


Polarization

- One <u>property of a photon</u> *that is of interest* is its polarization

- Polarization is a relative term that describes the plane of the electrical field
  - If the photon is traveling along the x-axis then the electric field can be in any plane





Photon Qubits

- Define a reference line

- A photon which is polarized at either 0 or 45 degrees of the line is a 0

- A photon which is polarized at either 90 or 135 degrees of the line is a 1

0 and 90 degrees are called *rectilinear polarization*
45 and 135 degrees are called *diagonal polarization*

Quantum Key Distribution I

- Alice and Bob want to exchange a key on a quantum channel and <u>ciphertext on a normal channel</u>

If photons are exchanged, then the quantum channel could be a fiber optics link

Quantum Cryptography - polarization bases

- Giles Brassard and Charles Bennett proposed using qubits to exchange secret keys in 1984
- BB84 Scheme uses polarization states of photon as qubit
- Alice can send photons :

Either - in Horizontal-Vertical Basis with polarizers set at 0 and 90 degrees

Or - in Diagonal Basis with polarizers set at 45 and 135 degrees

Quantum Cryptography - bases

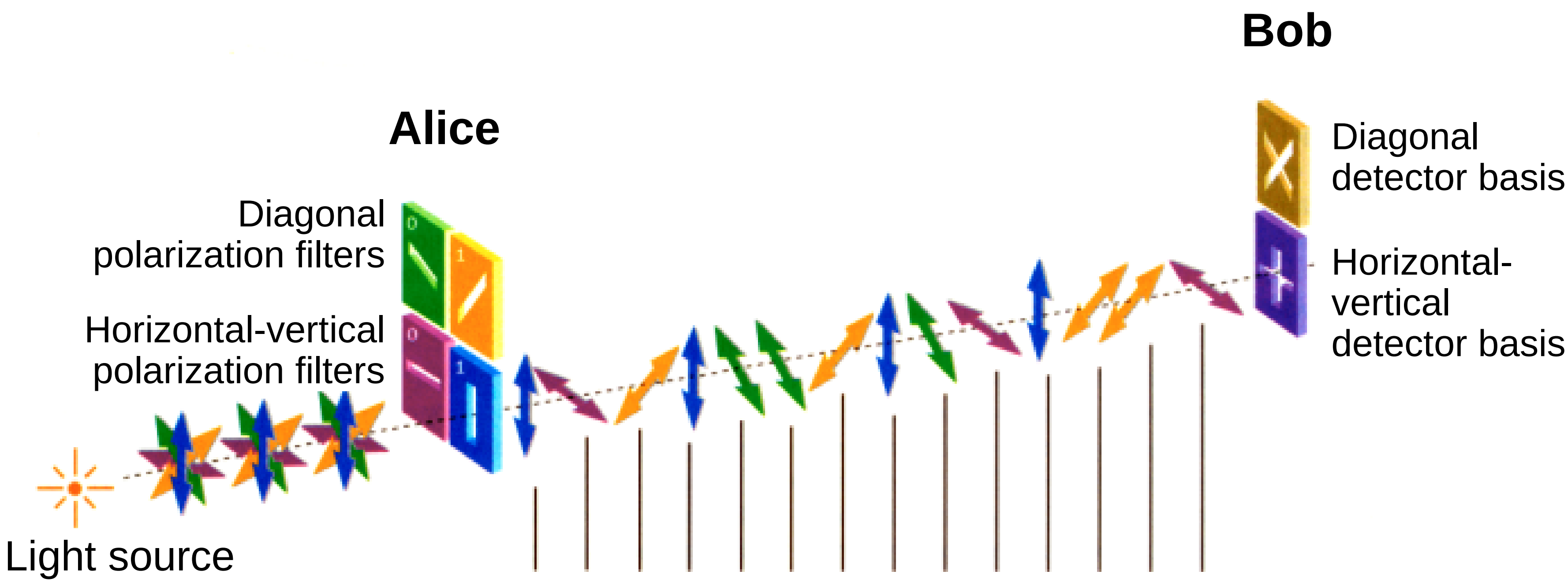
- Bob can also choose to receive photons <u>either</u> in H-V basis <u>or</u> in Diagonal basis
  - he does <u>not</u> know Alice's settings in advance
- If Alice sends a '1' using H-V setting but Bob measures photon in Diagonal setting, Bob will measure a '1' 50% of the time and a '0' for the remaining 50%

How does this help?

Quantum Cryptography
State of the Art

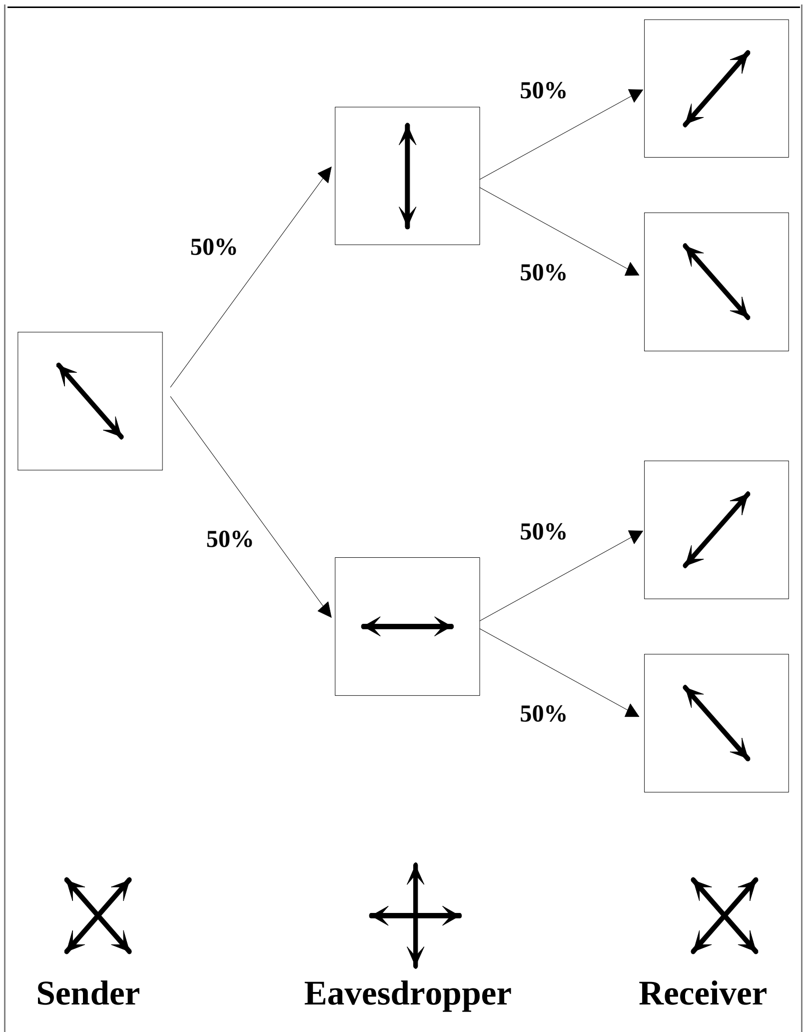
- First demonstration system built by Charles Bennett at IBM in 1989
- Many groups now demonstrated real systems transmitting keys down commercial optical fibres over many kilometres   e.g. Richard Hughes at LANL, Nicholas Gisin under Lake Geneva, Paul Townsend at BT
- Hughes group also demonstrated free space transmission possible

Quantum key distribution



Alice's bit sequence	**1**	**0**	**1**	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**1**	**1**	**1**	**0**
Bob's detection basis	+	×	+	+	×	×	+	+	×	+	×	×	+	+
Bob's measurement	**1**	**0**	**0**	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**1**	**0**	**0**
Retained bit sequence	**1**	**–**	**–**	**1**	**0**	**0**	**–**	**1**	**0**	**0**	**–**	**1**	**–**	**0**

Eavesdropping with wrong reference system



Sender	Tyvlytter			Mottaker
	Referanse	Resultat av måling		
"0"	Rett	"0"	Rett	Rett
	Galt	"0"	Rett	Rett Galt
		"1"	Galt	Rett Galt
"1"	Rett	"1"	Rett	Rett
	Galt	"0"	Galt	Rett Galt
		"1"	Rett	Rett Galt
"0"	Rett	"0"	Rett	Rett
	Galt	"1"	Galt	Rett Galt
		"0"	Rett	Rett Galt
"1"	Rett	"1"	Rett	Rett
	Galt	"1"	Rett	Rett Galt
		"0"	Galt	Rett Galt

Complete Example - Set Up

- Alice selects a random sequence of bits
  - Out of this sequence, Alice and Bob will ultimately construct a common key

- Example:

1 1 1 1 1 0 0 1 0 1 0 0 0 0 1 0 0 0 0 1 0 0 0 0 0 0 1 0 1 1

Alice must encode these into polarized photons and send them to Bob along the quantum channel

Encoding Process

- Alice chooses to encode each bit in either the rectilinear polarization (+) form or the diagonal polarization (x) form

- Summary of polarization forms: **1**: x /
  + -

  0: x \
  + |

1 in rectilinear

Alice's Choice

- Say Alice sends the random bits with the following choice of polarization:

```
1 1 1 1 1 0 0 1 0 1 0 0 0 0 1 0 0 0 0 1 0 0 0 0 0 0 1 0 1 1
x + x x x x x + x x + + + + x x + + x + + x x + + x x + x x
\ - \ \ \ / / - / \ | | | | \ / | | / - | / / | | / \ | \ \
```

polarization

received

Alice sends this sequence of polarized photons to Bob

Bob's Task

- Bob must measure the direction of the polarization of Alice's photons to reconstruct the set of bits
  - However, Bob does not know when Alice used rectilinear or diagonal polarization so he has to guess
  - If his guess is correct then he will recover the correct bit
  - If his guess is wrong, he has **only a 50-50 chance** of recovering the correct bit

Decoding

- Bob receives Alice’s polarized photons:

\ - \ \ \ / / - / \ | | | | \ / | | / - | / / | | / \ | \ \

+ + x + x x + x + x + + x x + x x + x + x + + + x + x + x +

0 1 1 1 1 0 0 0 1 1 0 0 0 1 0 0 0 0 0 1 1 1 1 0 1 1 1 0 1 0

Alice’s Polarization Choice

x + x x x x x + x x + + + + x x + + x + + x x + + x x + x x

Eavesdropping Test

- Now Alice tells Bob the polarizer orientation for a subset of the bits and Bob tells Alice the orientations he used on that same subset
  - For those cases where Alice and Bob agreed, Alice tells him what bit values he should have received

x	+	x	x	+	x	+	x	+	x	+	x	+	x
+	+	+	+	x	+	x	x	x	+	+	+	+	+
	1						0			0		0	
	1						0			0		0	

They agree so there was no eavesdropping

Common Key

- Since the channel is secure, Alice sends Bob the polarization orientation for another subset of the bits
  - Bob compares the actual polarization with his guess
  - He only uses the bits for which the two polarizations match (and so does Alice)

```
x     x x   x + x   +   + + x   +   x   + x x + + x     x x
+     + x   + x +   +   x x +   x   x   x + + + x +     x +
        1           0                   0         0         1
```

KEY

Quantum Cryptography - bad Eve

- After sending stream of bits in randomly chosen settings, Alice then telephones Bob and they agree which are the 'good' bits

What use is this?

- Suppose Eve is intercepting the bits from Alice and re-sending them on to Bob
- Since Eve has to guess which setting Alice used (H-V or Diagonal) there is now a probability of ¼ for Alice and Bob to disagree on the bit sent even when they use the same settings

The Effect of Eve

- If Eve intercepts and measures the photons, she has to send her measured values on to Bob

Alice's Message

\ - \ \ \ / / - / \ | | | | \ / | | / - | / / | | / \ | \ \

Eve's Guess

+ + x + x + + x x + + + x + + x + x + x x x + x x + x + x +

0 1 1 1 1 0 0 1 0 0 0 0 1 0 0 0 0 0 1 1 1 0 1 1 0 0 1 0 1 0

Eve's Message

| - \ - \ | | \ / | | | \ | | / | / - \ \ / - \ / | \ | \ |

Bob's Test

- Bob, unaware of Eve's presence, decodes the photons:

Eve's Message

```
| - \ - \ | | \ / | | | \ | | / | / - \ \ / - \ / | \ | \ |
```

Bob's Guess

```
+ + x + x x + x + x + + x x + x x + x + x + + + x + x + x +
0 1 1 1 1 1 0 1 1 1 0 0 1 0 0 0 0 0 1 1 1 1 1 0 0 0 1 0 1 0
```

Alice selects check bits – sends polarization and bit information

```
    1   1 0       1 0 0       0       1       0       0
```

ERROR

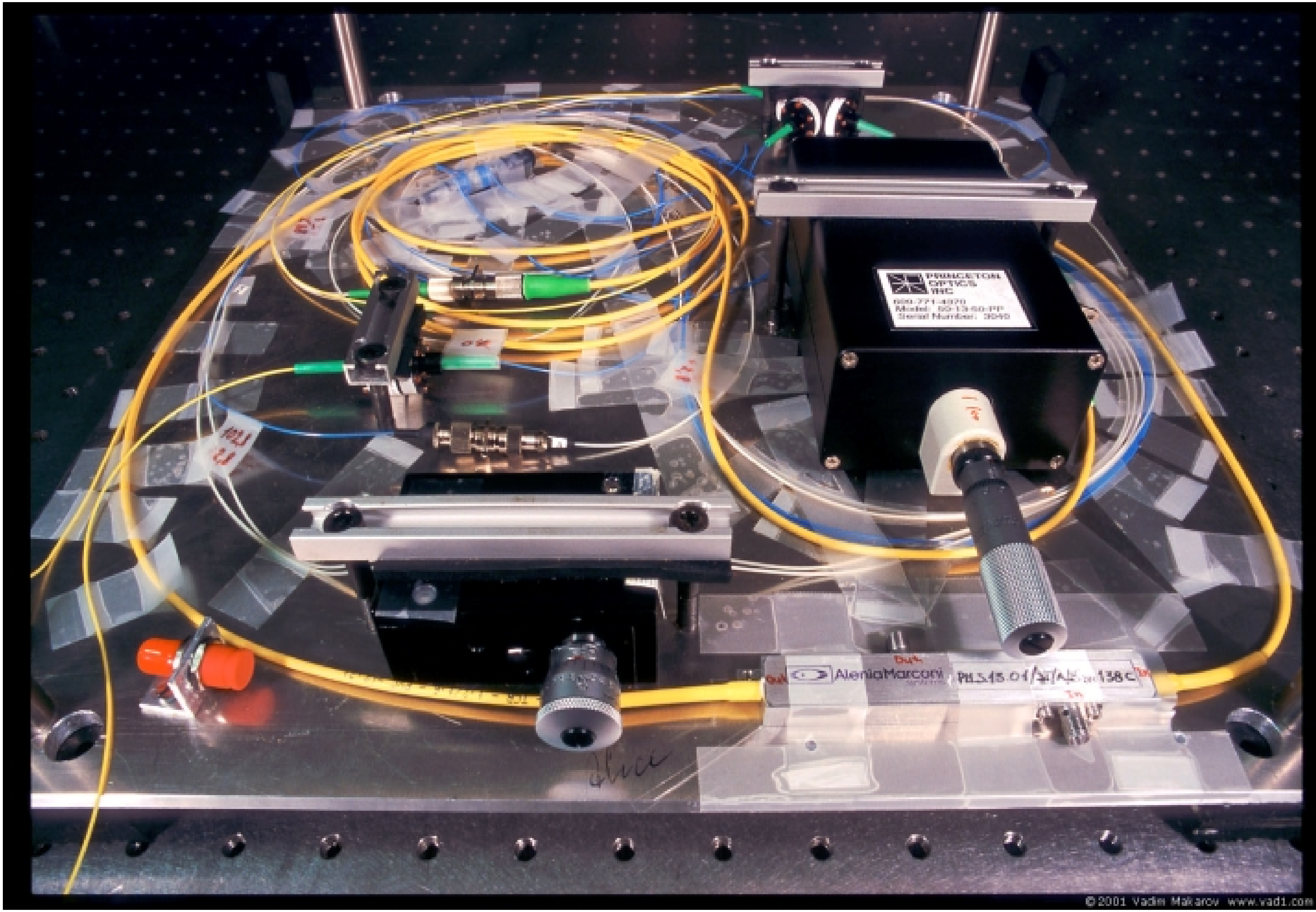


Photo 1. **Alice** (uncovered, no thermoisolation installed)

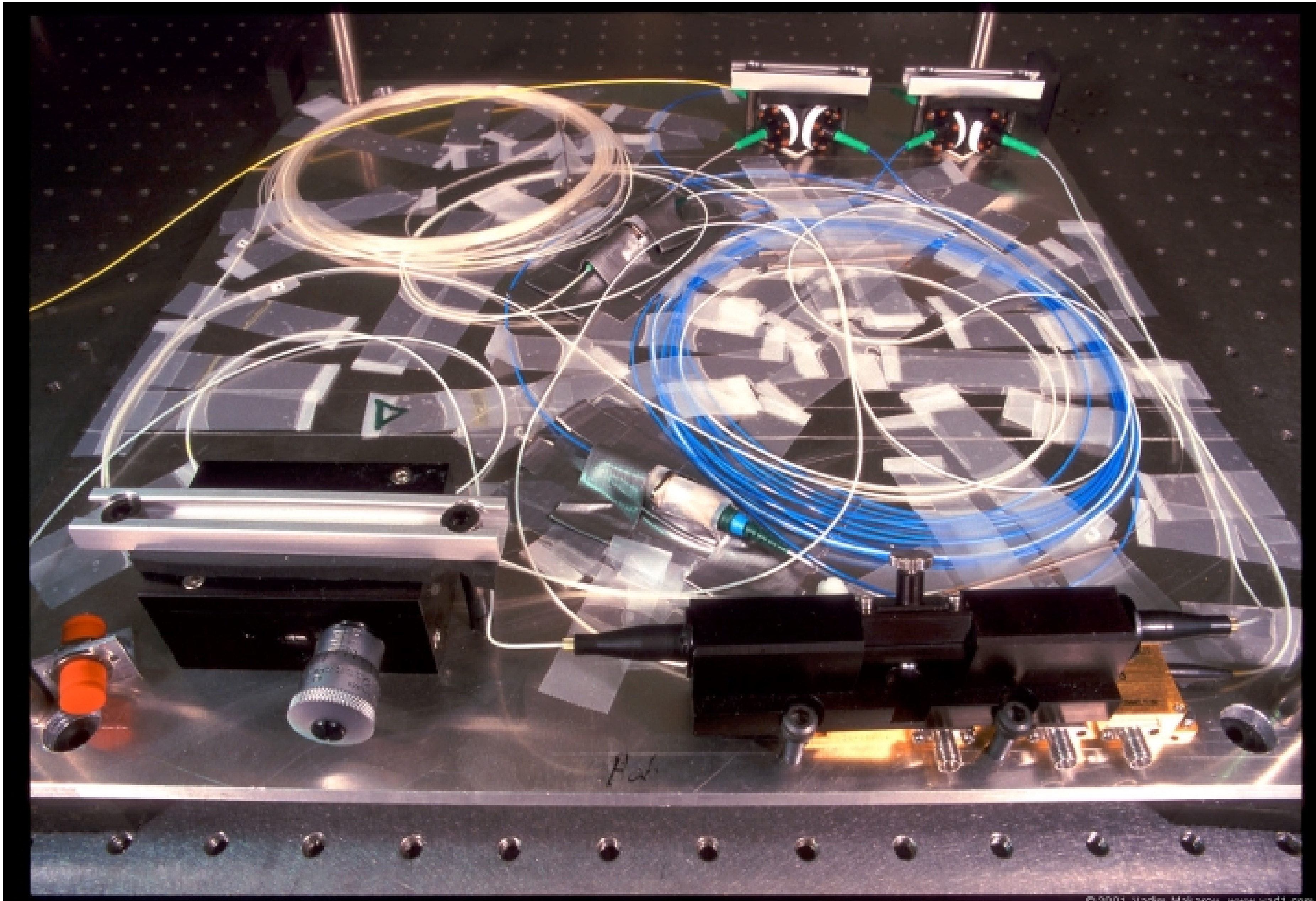
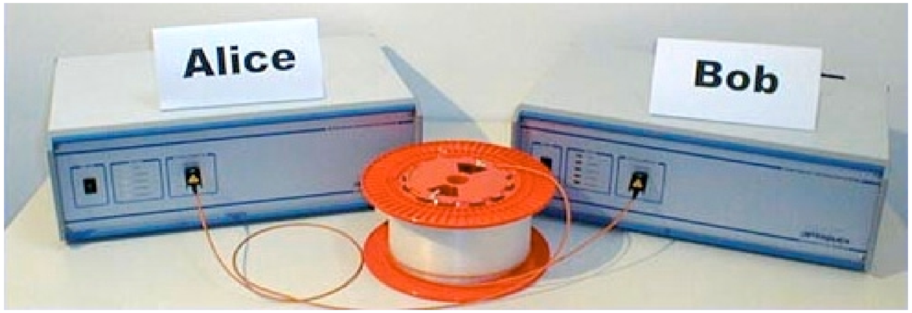


Photo 2. **Bob** (uncovered, no thermoisolation installed)

Commercial status

- id Quantique (Geneva)

  first commercially available quantum key distribution system:



- MagiQ Technologies (Boston)

- EQUIS project (Heriot-Watt University and Corning; UK)

  compact integration into standard PCs

- + several research groups, telecom/ electronics companies

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

10, rue Cingria 1205 Genève Switzerland
Tel: (+41) 022 702 69 29 Fax: (+41) 022 781 09 80
email: info@idquantique.com
web: http://www.idquantique.com

id Quantique
A Quantum Leap for Cryptography

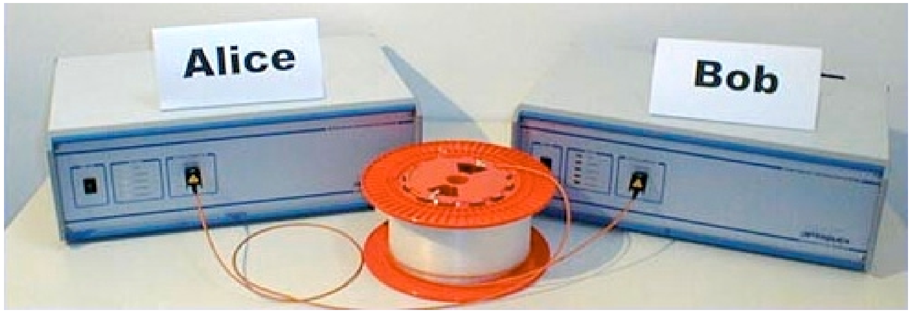
Geneva University spin-off makes quantum leap in secure communications

- Swiss company id Quantique has announced what it claims are the first commercially available quantum cryptography products - a key distribution system a random number generator.
- **id Quantique** is a spin-off of the University of Geneva. It was created in October 2001 by four researchers of the Group of Applied Physics.
- **id Quantique** is in the news for receiving the coveted Vigier Foundation Prize.
- The company has set its sights on becoming a leader in novel secure communication systems based on quantum photonics.
- In this domain, **id Quantique** has launched **two products**:
  - The first one, the "Quantum Random Number Generator" (QRNG), is a physical random number generator based on a quantum physical law.
  - It exploits a **truly random process** - the reflection or the transmission of a single photon upon incidence on a semi-transparent mirror -
  - to generate high quality random numbers for cryptographic purposes, numerical simulations, statistical studies or gambling.

- The company's main product is a QKD system, which enables remote parties to exchange a private cryptographic key in absolute secrecy, even if other parties are trying to eavesdrop.
- The key is exchanged in the form of a sequence of single photons in an optical fiber.
- Because of the quantum properties of the photons, eavesdropping inevitably perturbs the communication and so is immediately detected.

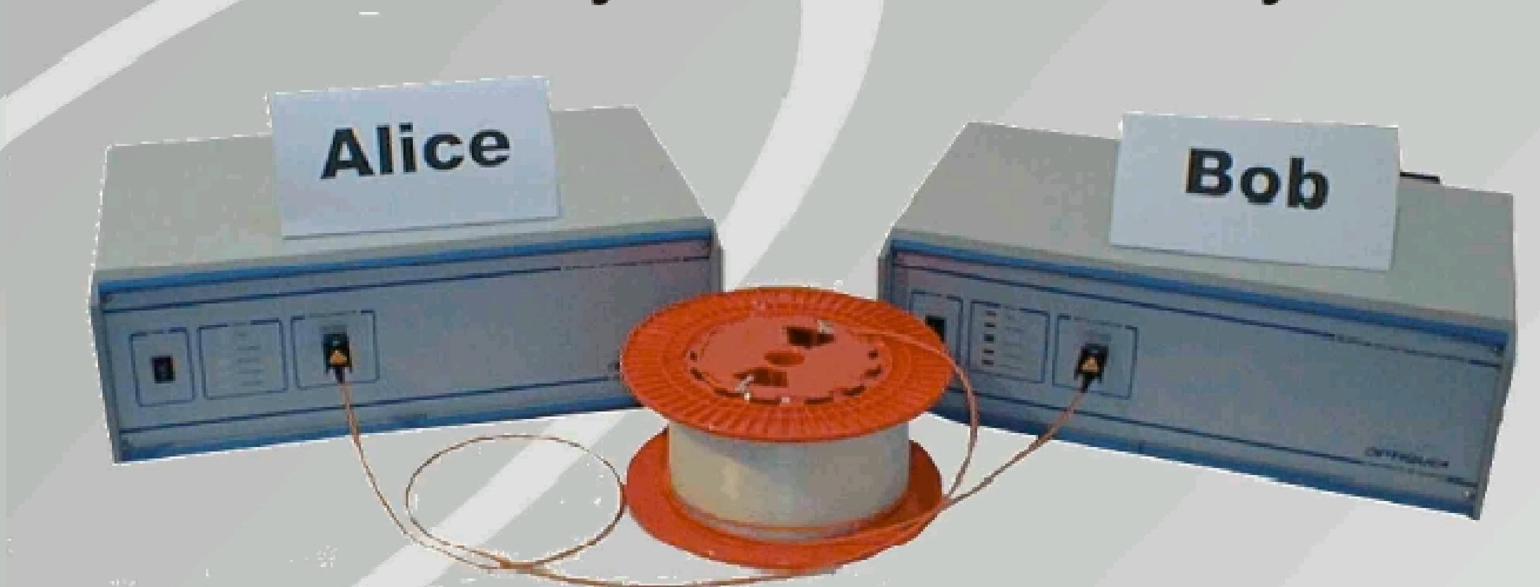
- The prototype commercial system consists of two PC-sized boxes at either end of a fiber-optic cable, containing lasers for generating the photons, detectors and cooling devices.
- It has been successfully tested over a 67-kilometer fiber-optic link between Geneva and Lausanne, Switzerland, with a net key distribution rate over that distance of 60 bps (bits per second).
- The system can be deployed over existing fiber-optic cables and the distribution rate rises to over 1000 bps over shorter distances, id Quantique said.

- Eavesdropping inevitably perturbs the communication, and is immediately revealed.
- Hence, unlike all other technologies, this quantum key distribution (QKD) system allows to exchange a cryptographic key with absolute security, guaranteed by the laws of physics.



Quantum Security...
at last

Quantum Key Distribution System



Key distribution over optical fiber
with absolute security

Performance

Key exchange rate[1] over			Units
	10 km :	4000	Bits/s
	20 km :	1500	Bits/s
	50 km :	100	Bits/s

Notes

[1]: The key exchange rate depends on the actual fiber attenuation.

Interface

Platform	Windows 98 2nd ed, 2000, ME, XP
Interface	USB version 1.0, 12 Mbit/s Plug & Play connection

General information

	Emitter		Receiver	
Optical connector [2]		FC/PC		
Operating temperature		+10 to +30		°C
Dimension (L×W×H)		32 x 46 x 16		cm
Weight	13		7	kg
Power supply		110 - 230		VAC

Notes

[2]: Other connector type available upon request

True randomness upon request

Quantum Random Number Generator QRNG

Although random numbers are required in countless applications, their generation is often overlooked. Being deterministic devices, computers are not capable of producing random numbers. A physical source of randomness is necessary. Quantum physics is intrinsically random. Therefore, it is natural to exploit a quantum process for such a source. It offers the advantage over conventional randomness sources like electronic noise of being robust and invulnerable to environmental perturbations.

The QRNG is a physical random number generator exploiting an elementary quantum optics process. Photons - light particles - are sent one by one onto a semi-transparent mirror and detected. The exclusive events (reflection - transmission) are associated to "0" - "1" bit values.

The operation of the QRNG is continuously monitored to ensure immediate detection of a failure.

A program supplied with the QRNG produces files of random numbers and implements standard randomness tests to analyze the data. A software development kit (option) allows simple and fast integration of the QRNG in an existing application.

Never worry again about the quality of your random numbers!

Main features

- First low-cost device based on quantum randomness
- Output data pass all randomness tests
- High generation rate
- Compact and reliable
- Immediate interruption in case of failure
- Easy integration in existing applications
- Acquisition and Randomness Tests program
- USB plug & play connection
- Self-powered through USB

Applications

- Cryptography
- Numerical Simulations
- Statistical research

id Quantique

10, rue Cingria   1205 Genève   Switzerland
Tel: (+41) 022 702 69 29 Fax: (+41) 022 781 09 80
email: info@idquantique.com
web: http://www.idquantique.com

id Quantique
A Quantum Leap for Cryptography

Performance

	Standard Version	Improved Version	Units
Random bits rate	10	100	kBits/s
Thermal noise contribution	< 2	< 0.5	%
Biasing factor*	< 0.1	< 0.1	-

Notes

*: $|p_1 - p_0|$ where p_1 and p_0 are the probabilities to register a "0", respectively a "1".

Interface

Platform	Windows 98 2nd ed, 2000, ME, XP
Interface	USB version 1.0, 12 Mbit/s Plug & Play connection QRNG power supply

Notes

Alternate platform (Unix) and interface (ethernet) in development

Software

- *QRNG Tester*	Distributed with the QRNG Intuitive graphical user interface Acquisition of random number files (binary or text) Unbiasing procedure (Von Neuman, and Peres) Standard randomness tests

Software

- *QRNG Tester*	Distributed with the QRNG Intuitive graphical user interface Acquisition of random number files (binary or text) Unbiasing procedure (Von Neuman, and Peres) Standard randomness tests
- *Software development kit*	Option Simple and fast integration in existing applications

General information

Operating temperature	+10 to +30	°C
Dimension (L×W×H)	68×150×188	mm
Weight	850	g

Sales Contact

For further information on this or other products, please contact *id Quantique* by phone:
(+41) 022 702 69 29 or email: info@idquantique.com

Disclaimer

Conclusions?

Feynman “not sure if there was a real problem with quantum mechanics”

- “Squeeze the difficulty of quantum mechanics into a smaller and smaller place”

Perhaps the foundation of a new multi-billion dollar industry!

Possible Homework Projects

- For a possible homework project, work out examples of quantum error correction schemes and compare them to digital error correction

Possible Exam Questions

- Remember that even though each question is worth only 5 to 10 points, the points do add up to a significant contribution to your overall grade

- If there is a quiz it *might* cover these issues:
  - What is a quantum dot?
  - Why are errors a problem with quantum systems?
  - What does a controlled NOT gate do?