Quantum Information Technologies
ECOC 2009

Workshop

Thomas Jennewein
University Waterloo, IQC

Paul Toliver
Telcordia Technologies, Inc.

Momtchil Peev
AIT Austrian Institute of Technology

Rupert Ursin
Austrian Academy of Sciences, IQOQI

Quantum Technologies

Planck, Einstein, Bohr

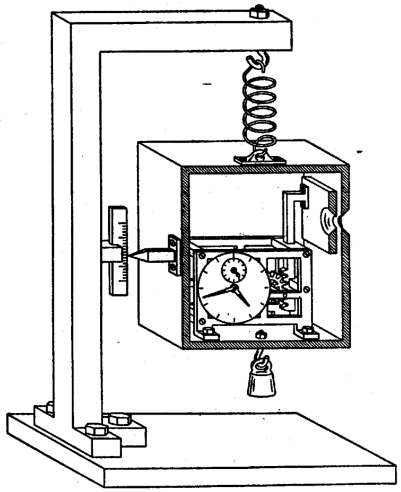


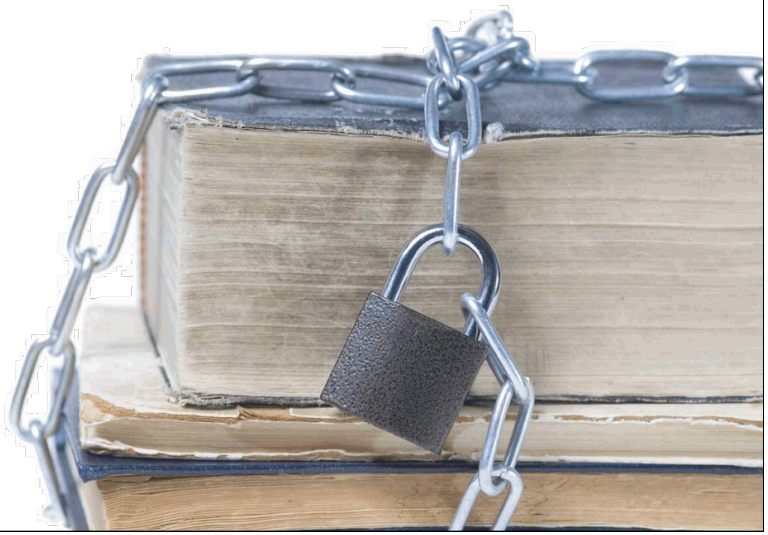
FIG. 8

- emerged from philosophical questions
  - such as uncertainty relations, interpretations, wave-particle duality...
- quantum technologies:
  - quantum communication
  - quantum random numbers
  - quantum computing

Communication

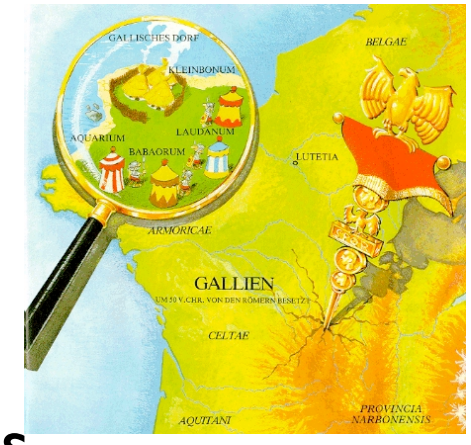
- is important to human interaction and societies.

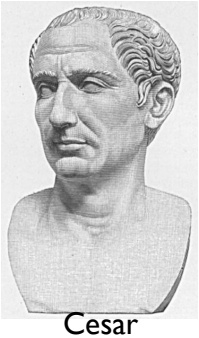
- secure communication: lock up the information in order to have an advantage over others.



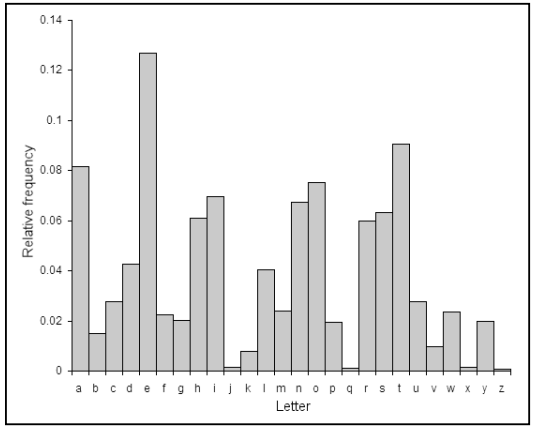
Early days of Cryptography

- simple example: Cesar cypher
- constant shift of the alphabet by n-letters
- easily cracked with statistical methods or brute-force





Cesar



More recent systems

- Algorithm & key:
  - Example Enigma: algorithm: Cylinders contain sequence of letters, and changed with every encoded letter; key: initial setting of the cylinders
  - Statistical attacks
- Public key cryptography
  - RSA: keys generated with classical communications and „hard to undo“ calculations.
  - Brute-force attack possible, just a matter of time
  - Quantum computers could crack these RSA keys

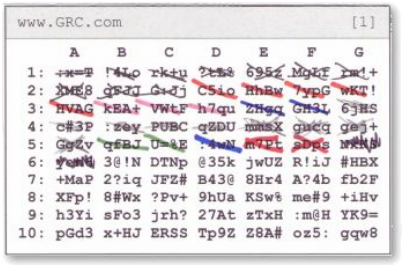
Worldwide many activities towards quantum computers. (Some studies expect them as soon as 2015) Gartner Group;
Also: Accenture http://www.accenture.com/xdoc/en/services/technology/vision/quantum_cryptography.pdf

One-time pad

- The only unconditional secure communication protocol
  - secure keys, completely random and only used once
  - key and message are encoded bit-by-bit, hence using the same amount of bits for keys and message

```
K = RUECKZUGVONDENHUEGELN
S = WZSLXWMFQUDMPJLYQOXXB

G = K + S
G = OUXOIWHMMJRQUXTTVVCJP
```



Quantum physics offers unique solution

- Nature has a solution for the exchange of keys, by using individual quanta (=photons).
- Important fact: individual photons cannot be copied!
- Any Eavesdropper will be discovered.

C. Bennett, G. Brassard, (1984). A. Ekert (1991)

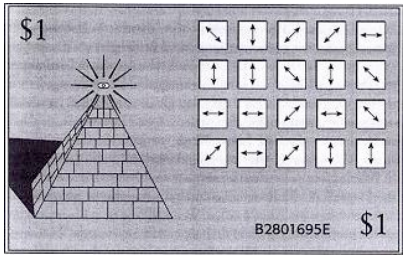
Reviews:

N. Gisin, et al., Rev. Mod. Phys (2002),

V. Scarani et al, to appear in Rev. Mod. Phys (2009)

Quantum Key Distribution

- 1970‘s Wiesner: quantum physics can make money safe against counterfeits
- 1984 Bennett & Brassard: BB84, scheme for using photons for secure key transfer
- 1989 Bennett & Brassard: experiment over 30 cm.



Stephen Wiesner‘s Quantum Money


C. Bennett

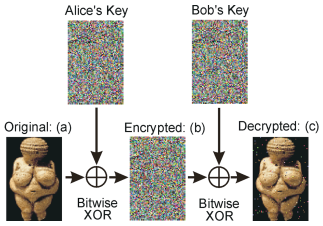

G. Brassard

„Nobody seemed interested to do the experiment, so we did it ourselves“, statement by BB

„ .. Initially, quantum cryptography was thought of by everyone (including ourselves) mostly as a work of science-fiction because the technology required to implement it was out of reach (for instance, one of the protocols in [BBBW] required the ability to keep a single photon bouncing back and forth between two mirrors for a significant amount of time without losing its polarization)....“
from Bennett + Brassard, CM SIGACT News, Volume 20 , Issue 4 (1996).

QKD has come a long way...

- Single photons
- Entangled photons
- optical fibers & free-space
- short range - long range
- Demos:
  bank transfer, elections, multi-user networks ....
- Commercial systems: IdQuantique, MagiQ, SmartQuantum...



PRL, 84, 4729 (2000)


N. Gisin et al,
Rev. Mod. Physics 2002

Quantum technologies are fun!
N.G., (1996)

Clavis2 (IdQuantique)


SECOQC, FP6
5 nodes in Vienna+
(see talk by M. Peev Monday, 21.9)

How QT moves on

QKD and quantum technologies will eventually be accepted as important tools for special applications.

Future activities focused in these areas:

- **Technology**: Larger distances & higher key rates (fiber links, satellite, quantum repeaters,..)
- **Markets**: which customers need this applications, where is the market pressure
- **Maturity**: size, cost, standards, user interface,...

Thank you...

- We hope you enjoy the workshop

Why, sir, there is every possibility that you will soon be able to tax it!
(to PM William Gladstone, on the usefulness of electricity)"
Michael Faraday quote