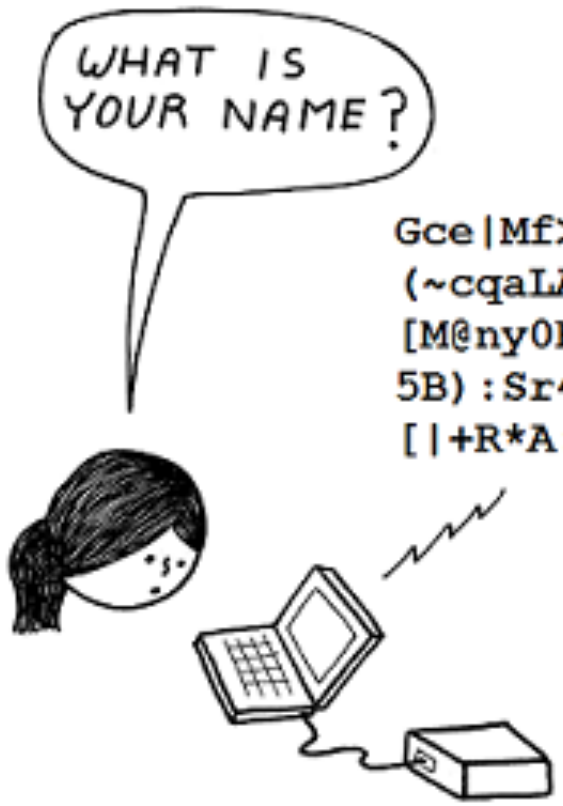
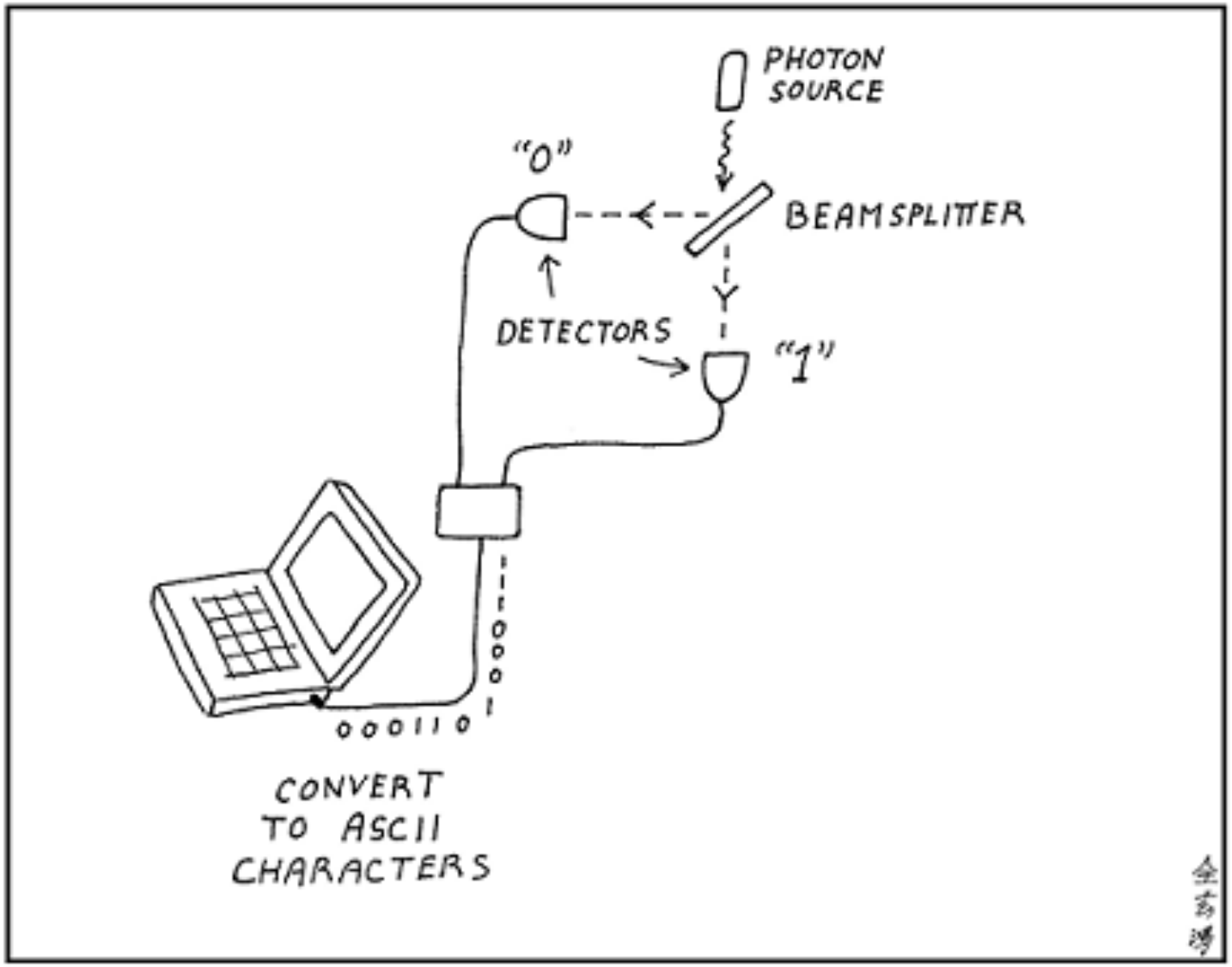
Quantenkryptographie

Renato Renner
Institut für Theoretische Physik
ETH Zurich

- Quanten-Computer
- Quanten-Kryptographie
- Quanten-Information
- Quanten-Zufallsgeneratoren
- Quanten-Teleportation
- Quanten-Detektion
- …
- …
- Quanten-Heilung
- Quantum of Solace

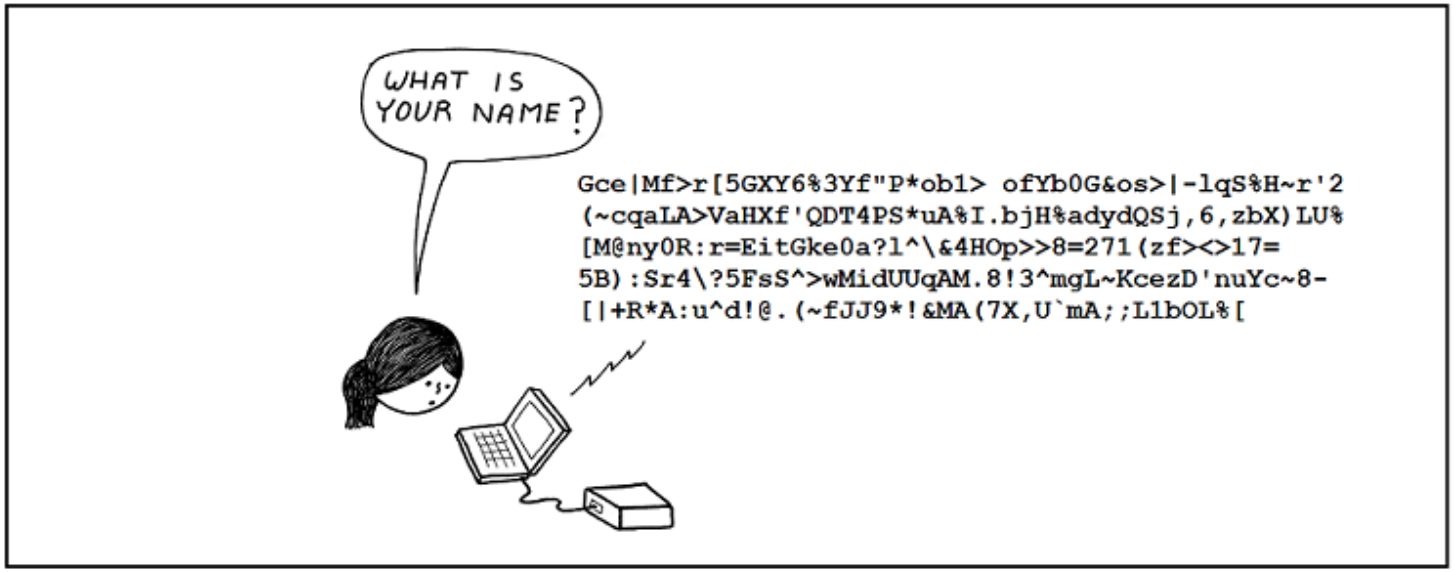


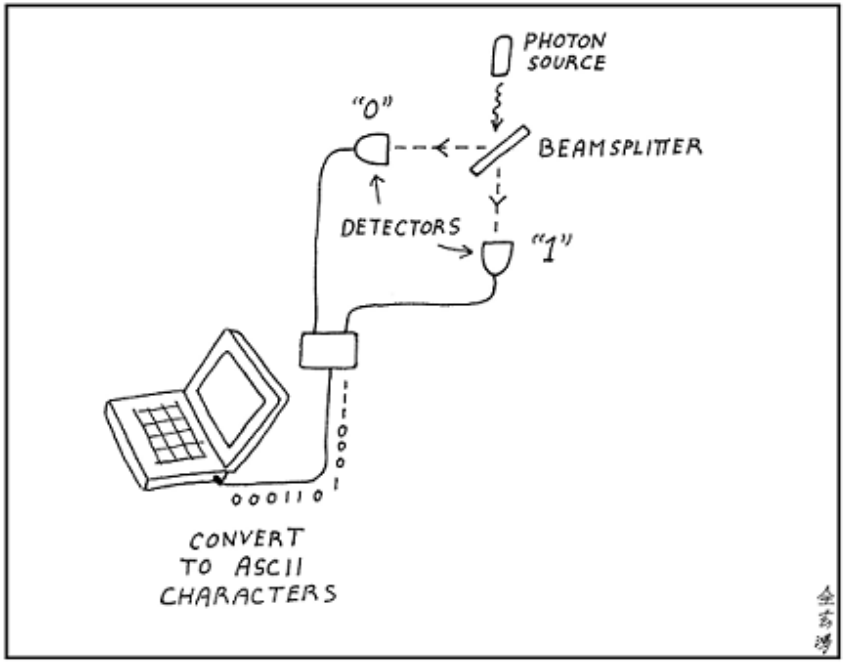

```
Gce|Mf>r[5GXY6%3Yf"P*ob1> ofYb0G&os>|-lqS%H~r'2
(~cqaLA>VaHXf'QDT4PS*uA%I.bjH%adydQSj,6,zbX)LU%
[M@ny0R:r=EitGke0a?l^\&4HOp>>8=271(zf><>17=
5B):Sr4\?5FsS^>wMidUUqAM.8!3^mgL~KcezD'nuYc~8-
[|+R*A:u^d!@.(~fJJ9*!&MA(7X,U`mA;;L1bOL%[
```



QUANTUM OUIJA BOARD

the best application of quantum physics so far (?)



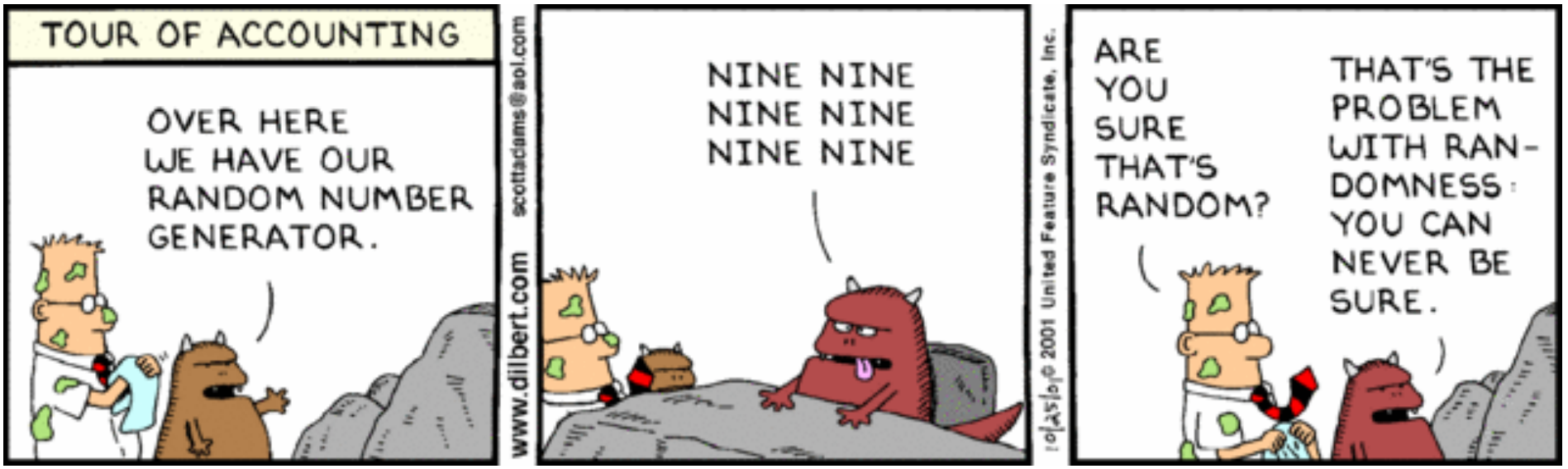


QUANTUM OUIJA BOARD

the best application of quantum physics so far (?)

aus abstrusegoose.com

Quanten-Zufallsgeneratoren



aus dilbert.com

Wann ist eine Zahl zufällig?

- 12345678901234567890123456789012345678901234567890123456789012345678901234567890123456789…
- 14159265358979323846264338327950288419716939937510582097494459230781640628620899862803482534211706 8…
- 14928918211763301459401981279646016526726623193154459652879981335270643243018606512286495129677858 2…

Wozu sind Zufallszahlen nützlich?

“One-Time-Pad”-Verschlüsselung

Gilbert Vernam
1890 - 1960

Joseph Mauborgne
1881 - 1971

Kryptographie

Hicks-Cipher

Enigma

AES

~~TOP SECRET DINAR~~ DRUG

[redacted]

Reissue (T1388)

From: NEW YORK

To: MOSCOW

No: 842

3 June 1943

To VIKTOR[i].

According to "MIRAGE's [MIRAZh]"[ii] information the Embassy of the COUNTRY [STRANA][iii] in Brazil advises the "BANK"[iv]:

The Brazilian Ambassador in Switzerland learned from two highly placed persons in the Swiss army that German troops [2 groups unrecovered] area of Schwarzwald supposedly with a view toward the invasion of Switzerland for

[5 groups unrecovered]

No.461 MAKSIM[v]

Comments:

[i] VIKTOR: Lt. Gen. P.M. FITIN

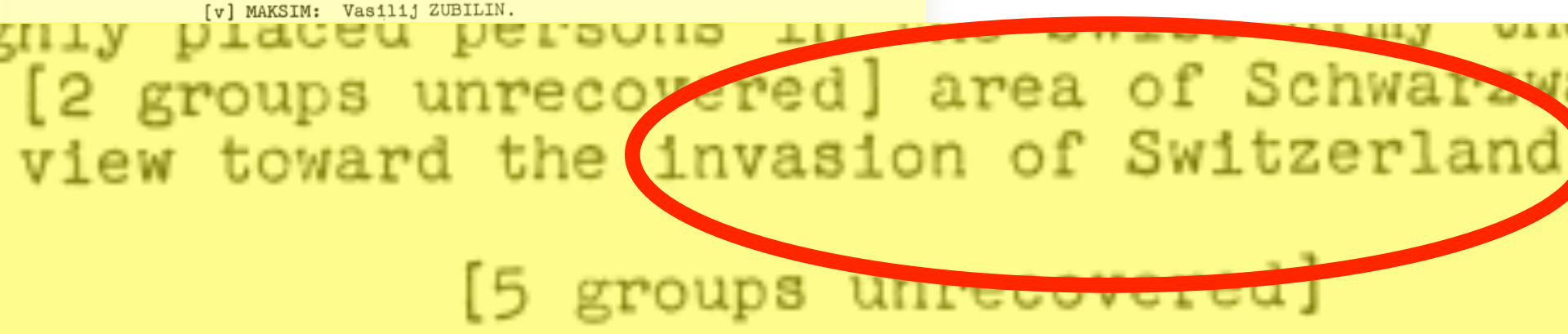
[ii] MIRAGE: Unidentified

[iii] COUNTRY: U.S.A.

[iv] BANK: U.S. State Department.

[v] MAKSIM: Vasilij ZUBILIN.

www.nsa.gov/venona

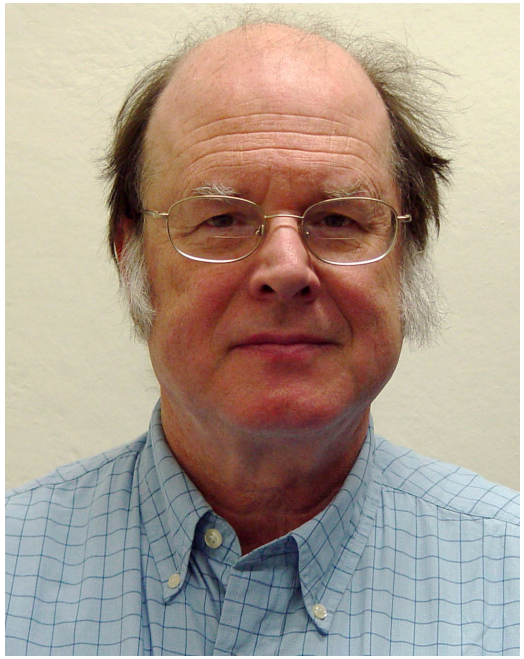


Shannons Theorem

Jedes (annähernd) perfekt sichere Verfahren um eine n-Bit-Meldung zu verschlüsseln verbraucht einen Schlüssel-String der Länge mindestens n.

Shannons Theorem ist nur in einer rein klassichen Welt gültig

Quanten-Schlüsselaustausch



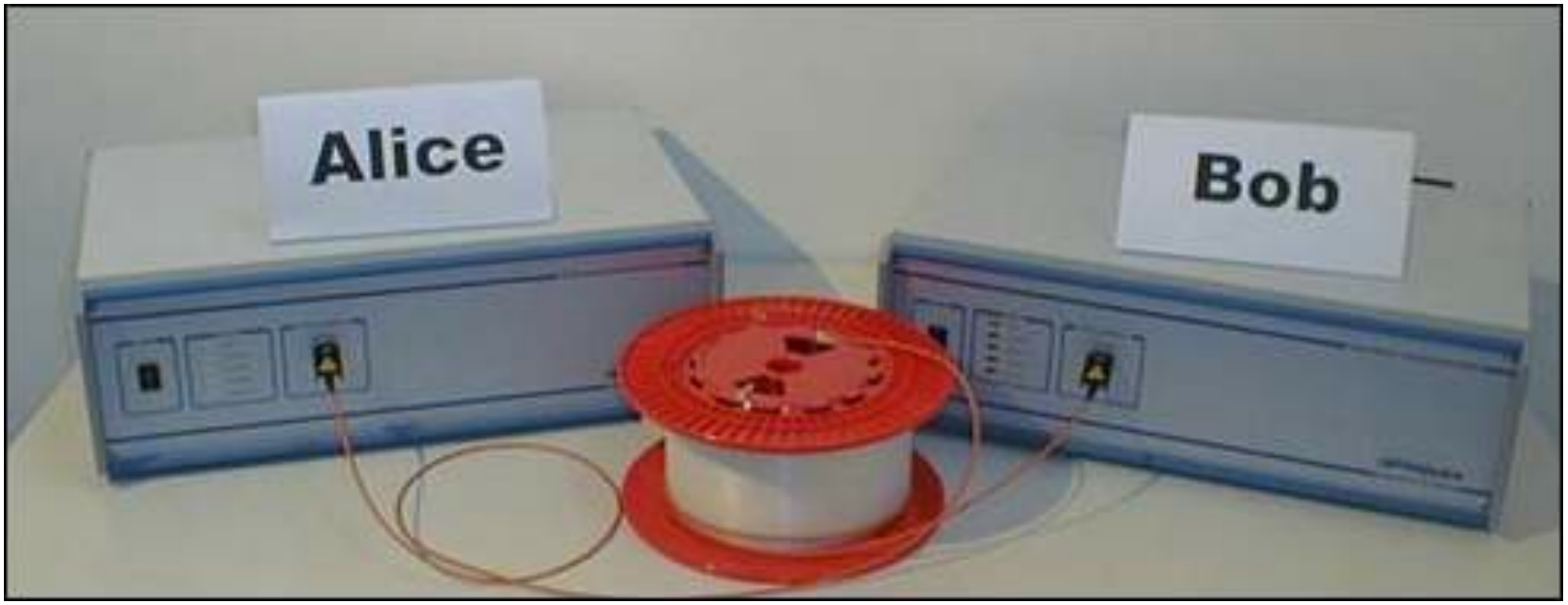
Charles H. Bennett

[Photo: ETH Zurich]

Gilles Brassard

[Photo: ETH Zurich]

Quanten-Schlüsselaustausch



Vielen Dank für Ihr Interesse an der Welt der Quanten