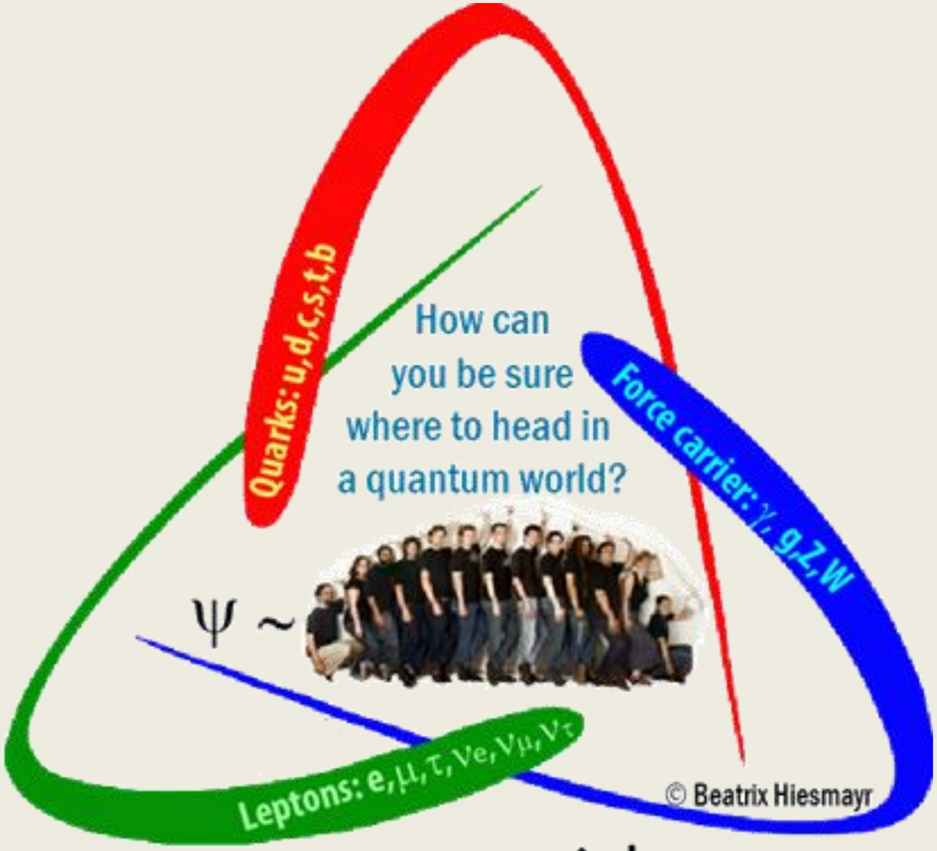
Quantum Theory & Beyond !?

by
Beatrix C. Hiesmayr
(University of Vienna)



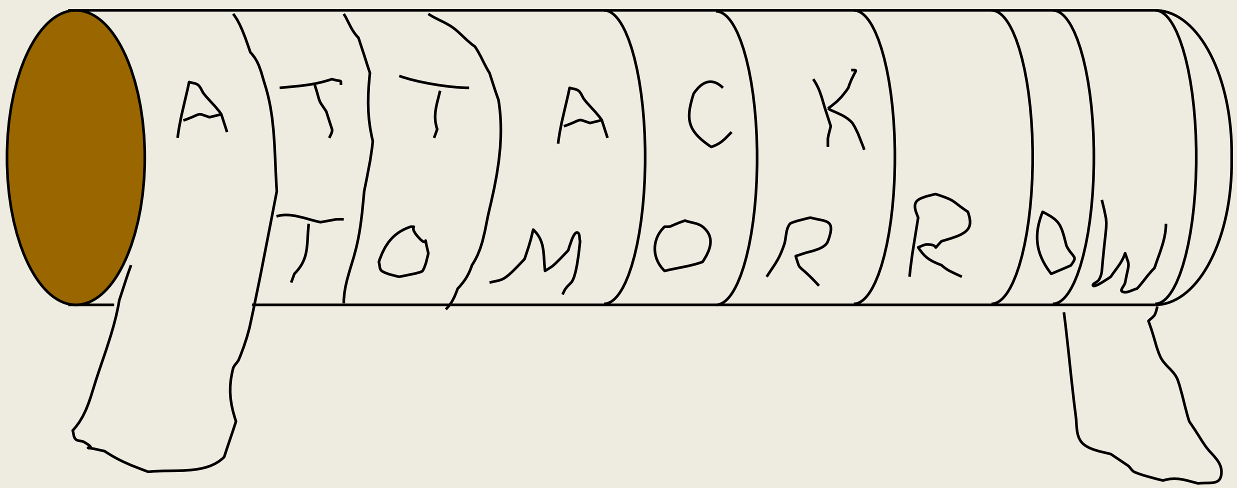
www.quantumparticlegroup.at

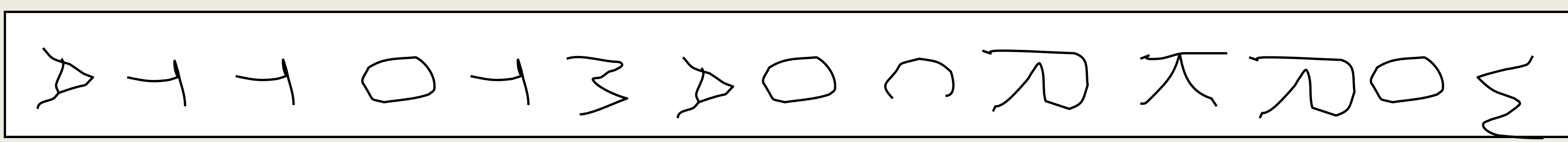
Communication security you enjoy daily:

- Paying by credit card in a supermarket
- Cell phone conversations, SMS
- Email, chat, online calls
- Secure browsing, shopping online
- Cloud storage and communication between your devices
- Software updates on your computer, phone, tablet
- Online banking
- Off-line banking: the bank needs to communicate internally
- Electricity, water: the utility needs to communicate internally
- Car keys, electronic door keys, access control
- Government services (online or off-line)
- Medical records at your doctor, hospital
- Bypassing government surveillance and censorship
- Security cameras, industrial automation, military, spies...

A little history….

400 BC, Sparta





A little history...

Cäsar Code

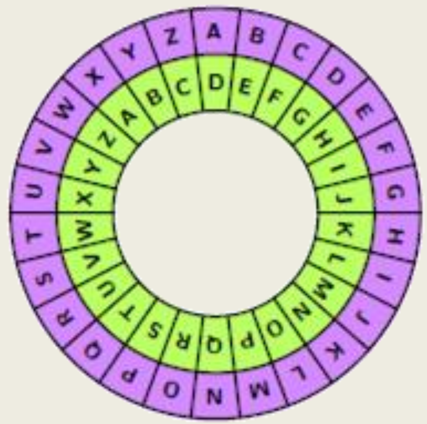
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ

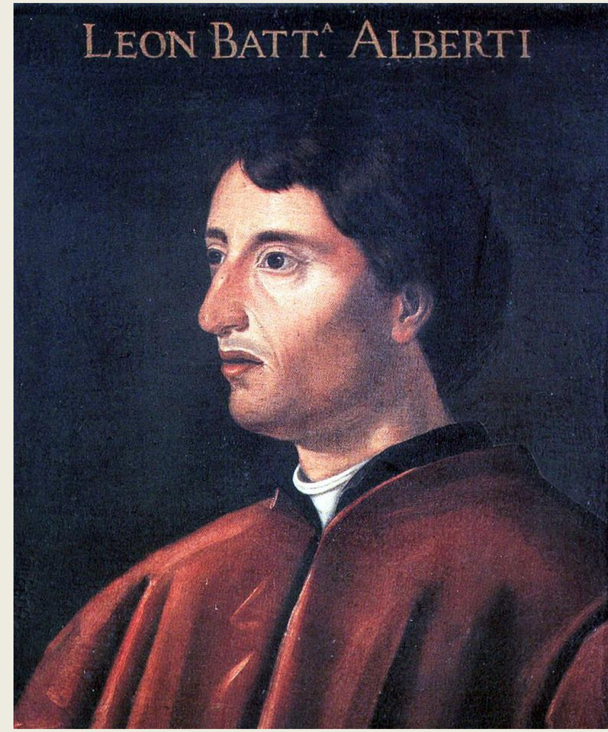
ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC

A T T A C K T O M O R R O W
DWWD F N WR P R U U R Z

A little history…

Leon Battista Alberti (1404–1472, Italy)





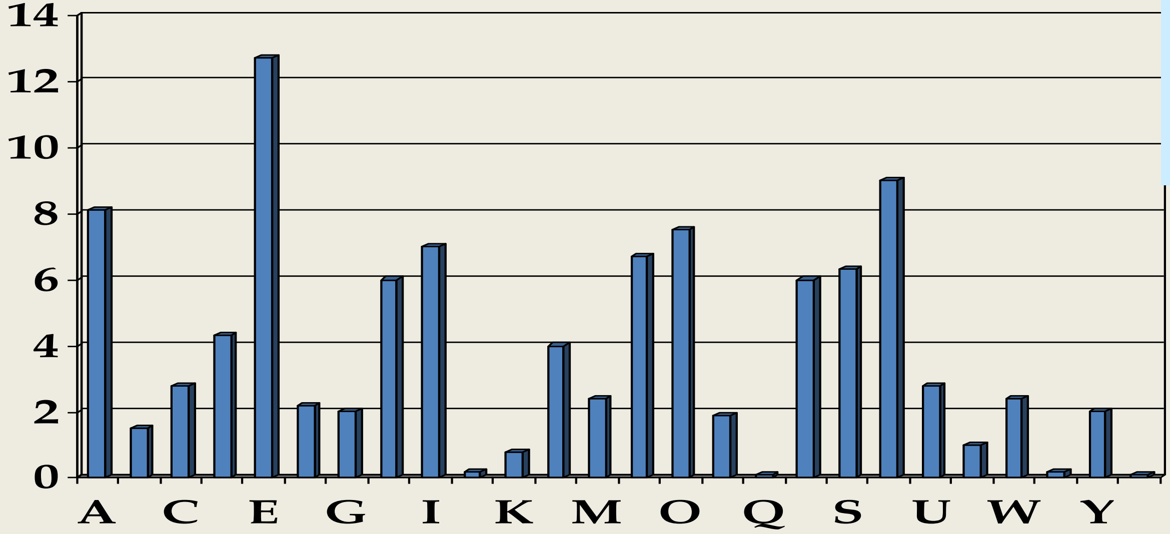
A T T A C K T O M O R R O W

DWWD F N WR P R U U R Z

How can this be broken?

A little history

English: ETAOINSHR
German: ENIRSATUD
French: EAISTNRUL
Spanish: EAOSNRILD
Italian: EAIONLRTS
Finnish: AITNESLOK



Frequency in the English languages

How to make Cäsar's code more secure?

Text m	MONOALPHABETISCHERSUBSTITUTIONSALGORITHMUS
	+
Key k	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
	=
Code c	SUTUGRVNGHKZOYINKXYAHYZOZAZOUTYGRMUXOZNSAY

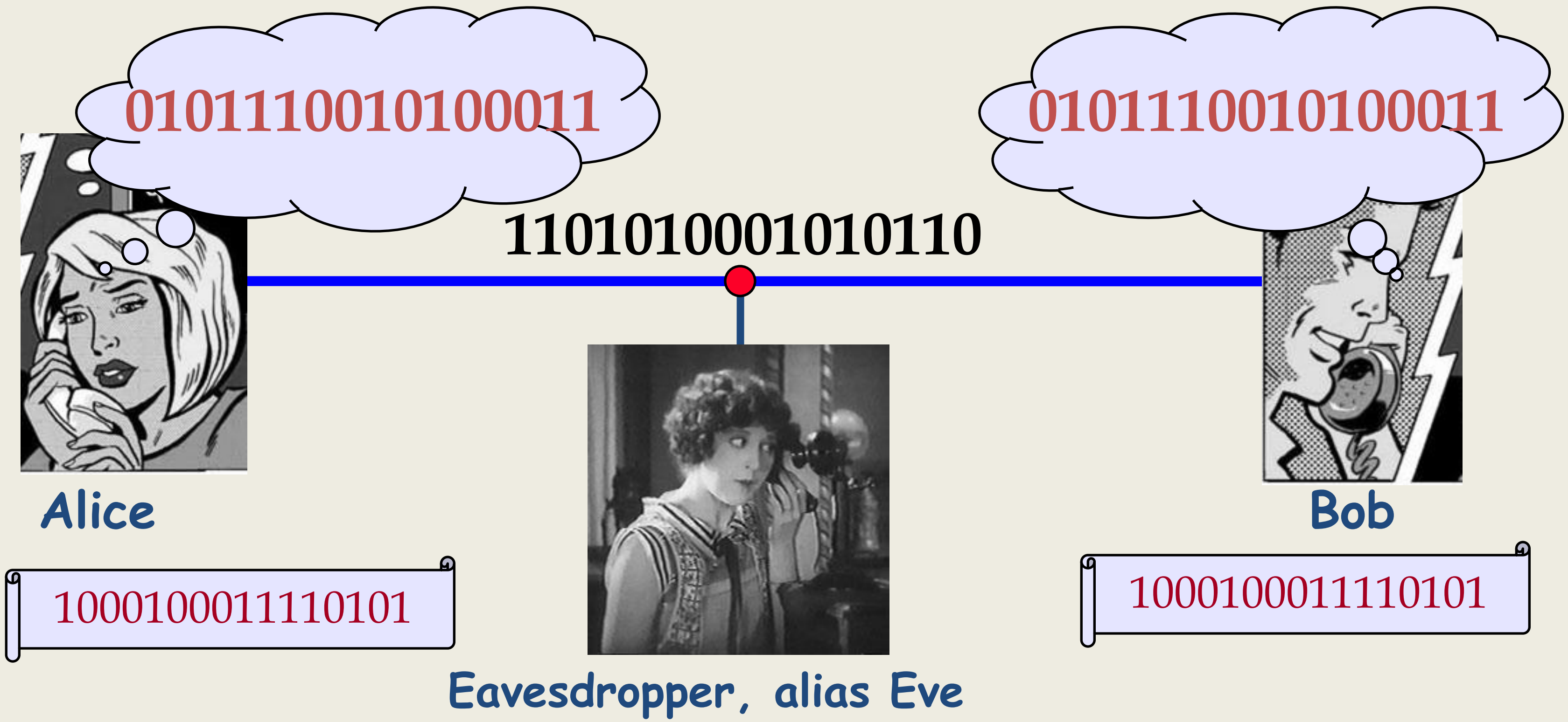
$$c_i = (m_i + k) \bmod N$$

Text m	POLYALPHABETISCHERSUBSTITUTIONSALGORITHMUS
	+
Key k	GEHEIMESWORTGEHEIMESWORTGEHEIMESWORTGEHEIM
	=
Code c	WTTDJYUAXQWNPXKMNEXNYHLCAZBNXAXTIVGLPYPRDF

$$c_i = (m_i + k_i) \bmod N$$

If key is generated randomly AND as long as message AND used only one time → 100% security (Vernan code/One-Time-Pad)

The Scenario: Vernan-Code, 1927



Message:	0 1 0 1 1 1 0 0 1 0 1 0 0 0 1 1
Key:	1 0 0 0 1 0 0 0 1 1 1 1 0 1 0 1
Tansmitted:	1 1 0 1 0 1 0 0 0 1 0 1 0 1 1 0

Rules:
- 0 + 0 = 0
- 0 + 1 = 1
- 1 + 0 = 1
- 1 + 1 = 0

Hiesmayr

Can quantum mechanics break the cryptography's curse?

		Broken?
Monoalphabetic cipher	invented ~50 BC (J. Caesar)	YES ~850 (Al-Kindi)
Nomenclators (code books)	~1400 – ~1800	YES
Polyalphabetic (Vigenère)	1553 – ~1900 1863	YES (F. W. Kasiski)
...		
Polyalphabetic electromechanical (Enigma, Purple, etc.)	1920s – 1970s	YES
Vernan Code	1918	**IMPOSSIBLE** (Shannon 1949)
DES	1977 – 2005	YES
Public-key crypto (RSA, elliptic-curve)	1977 –	will be once we have quantum computer (P. Shor 1994)
AES	2001 – **?**	**?**

Public-key crypto ('quantum-safe') in development **?**

Vernan-Code, 1927

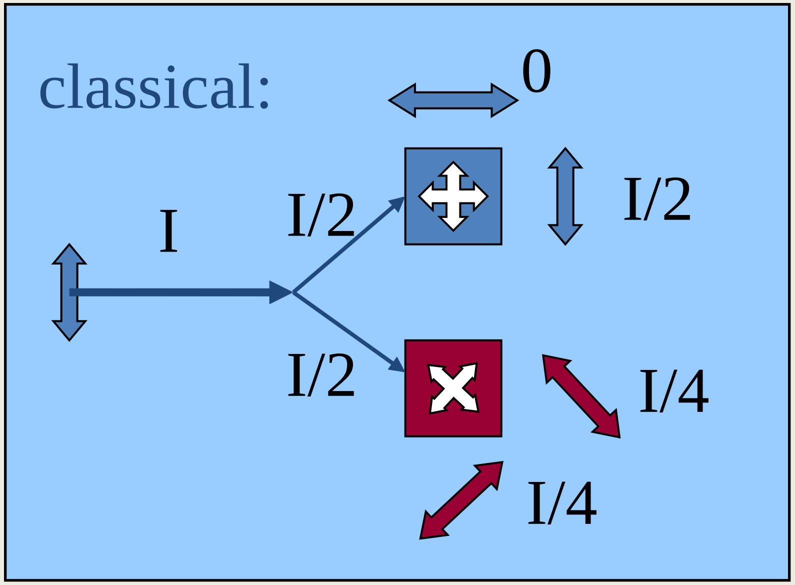
Alice	message:	0 1 0 1 1 1 0 0 1 0 1 0 0 0 1 1
	key:	1 0 0 0 1 0 0 0 1 1 1 1 0 1 0 1
Eve	transmitted:	1 1 0 1 0 1 0 0 0 1 0 1 0 1 1 0
Bob	key:	1 0 0 0 1 0 0 0 1 1 1 1 0 1 0 1
	message:	0 1 0 1 1 1 0 0 1 0 1 0 0 0 1 1

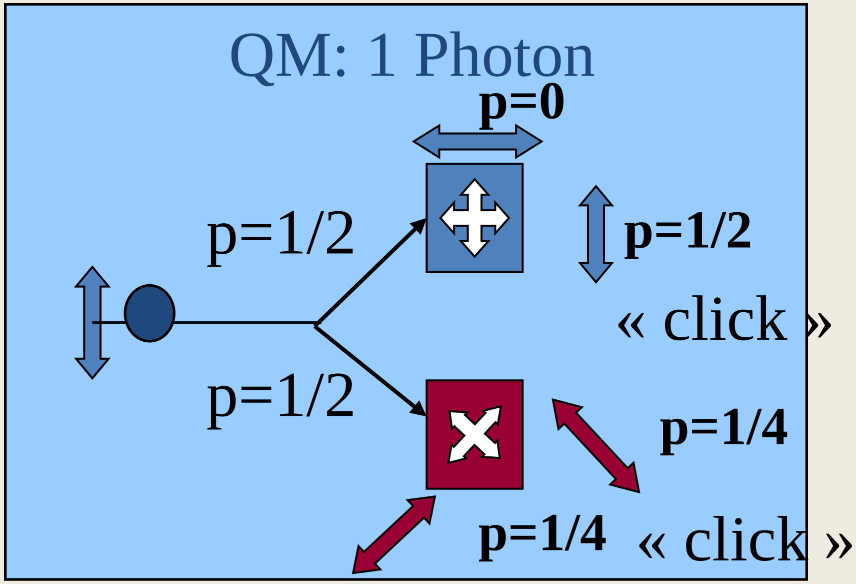
Rules:
- 0 + 0 = 0
- 0 + 1 = 1
- 1 + 0 = 1
- 1 + 1 = 0

→ Secure if Eve has not the key

Laws of quantum mechanics allow the generation of the key!

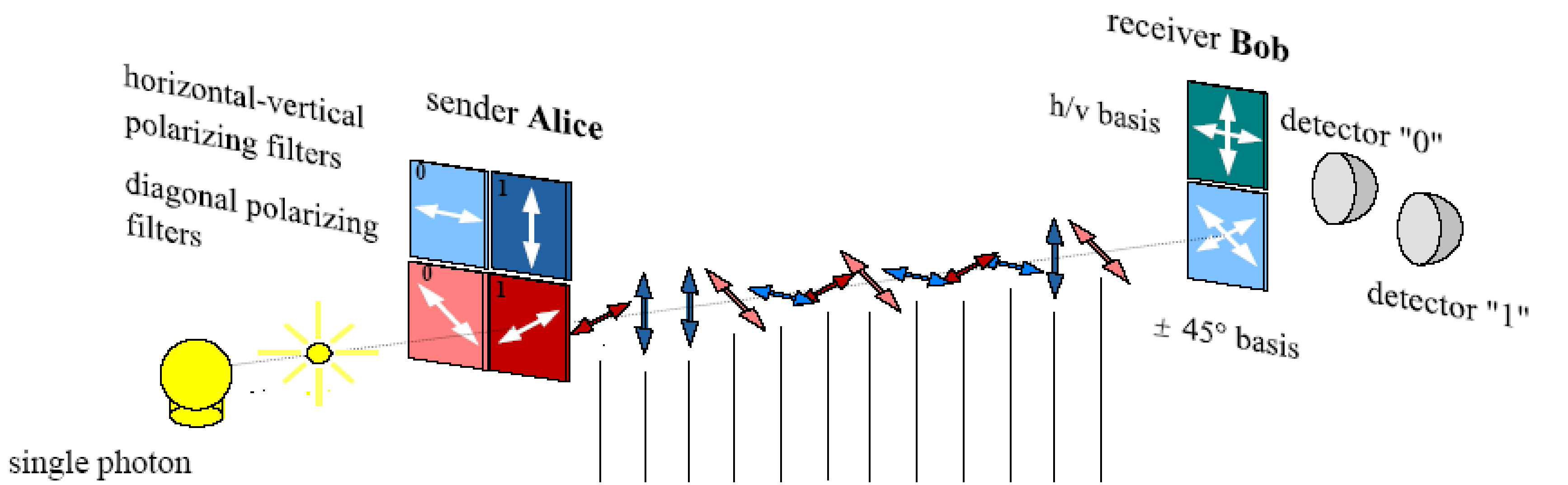
Measurement of polarisation





For as single photon you can not determine the polarisation with 100% security!

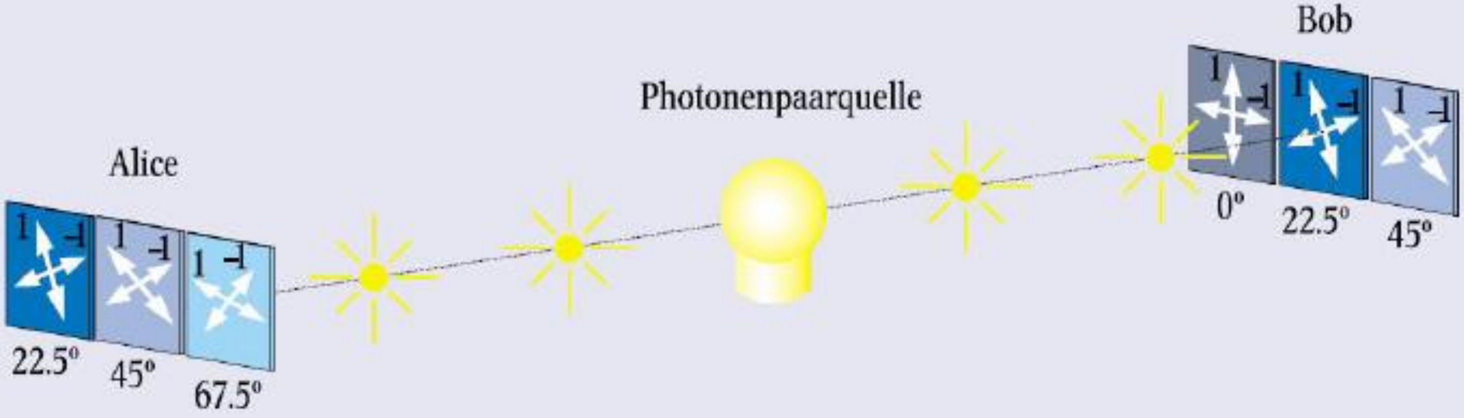
Das BB-84 Protokoll:



Alice's bits	1	1	1	0	0	1	0	0	1	0	1	0
Bob's basis	+	+	×	×	+	×	+	×	×	+	+	×
Bob's result	0	1	0	-	0	1	0	1	1	-	1	0

S. Wiesner, rejected around 1970. C.H. Bennett and G. Brassard, Int. Conf. Computers, Systems & Signal Processing, Bangalore, India, Dec. 10-12, 175 (1984)

Ekert protokol: 1991



Alice Basis	22.5°	67.5°	45°	22.5°	67.5	45°	45°	45°	67.5°	67.5°	22.5°	45°
Alice Ergebnis	–1	1	–1	1	1	–1	1	–1	–1	1	–1	1
Bobs Basis	45°	0°	45°	0°	22.5	45°	22.5°	22.5°	0°	45°	22.5°	22.5°
Bobs Ergebnis	1	–1	–1	1	–1	–1	1	–	1	1	–1	1
Differenz	22.5°	67.5°	0°	22.5°	45°	0°	22.5°	22.5°	67.5°	22.5°	0°	22.5°
Klasse	Bell	Bell	Code	Bell	–	Code	Bell	–	Bell	Bell	Code	Bell
Schlüssel	–	–	0	–	–	0	–	–	–	–	0	–

What are Bell inequalities?

realism
locality
freedom of choice*

No spooky action at distance!

*exerting the independence of both experimenters; sharing randomness; free will

Local realistic theories:

Bell's locality hypothesis

$$P(a,b)=\int d\lambda\,\rho(\lambda)\,p_A(a,\lambda)\cdot p_B(b,\lambda)$$

with $\int d\lambda\,\rho(\lambda)=1$

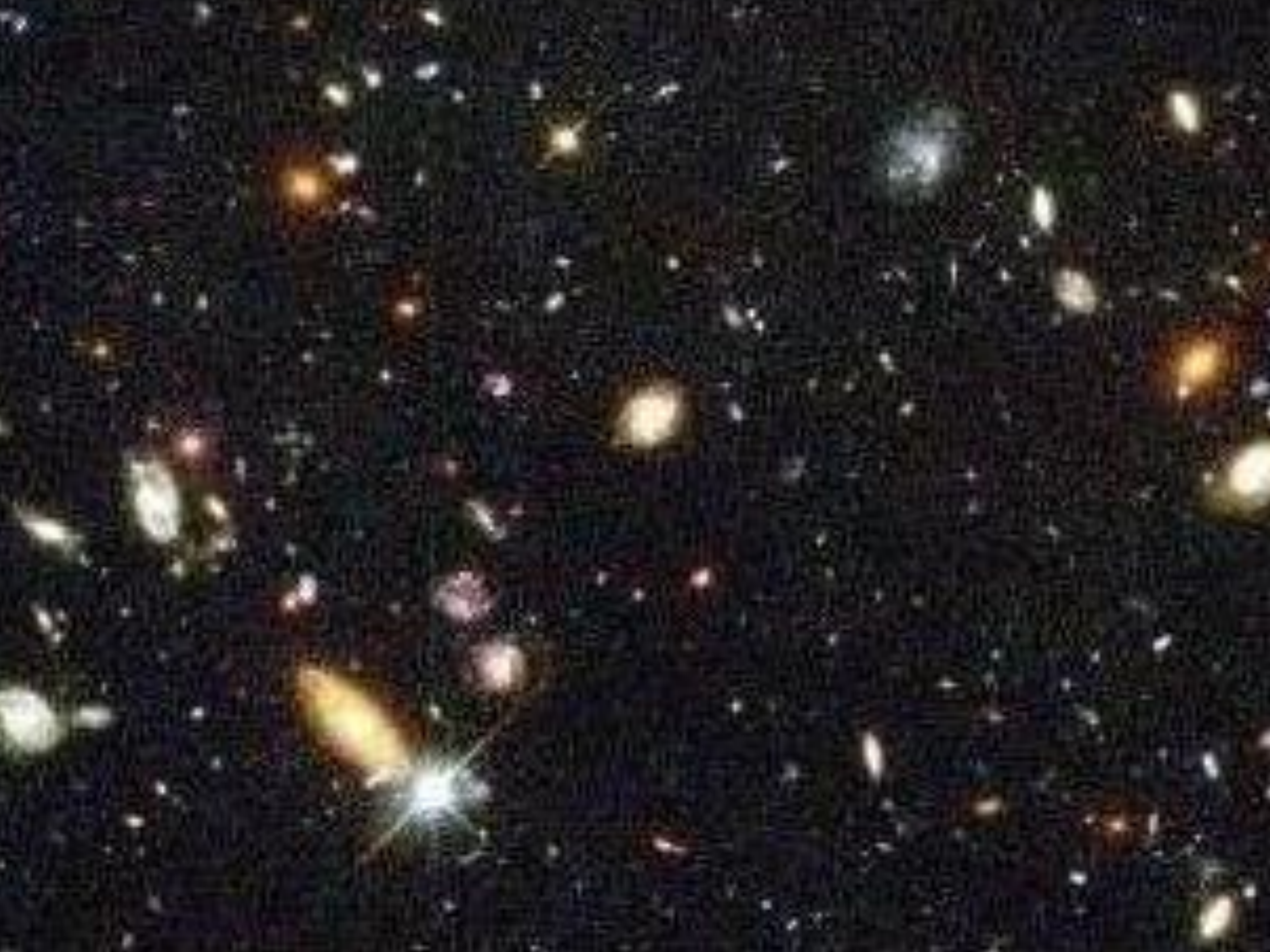
inequalities for probabilities → *always* satisfied!

$$P(a,b)\leq P(a,c)+P(c,b)$$

Quantum Mechanics:

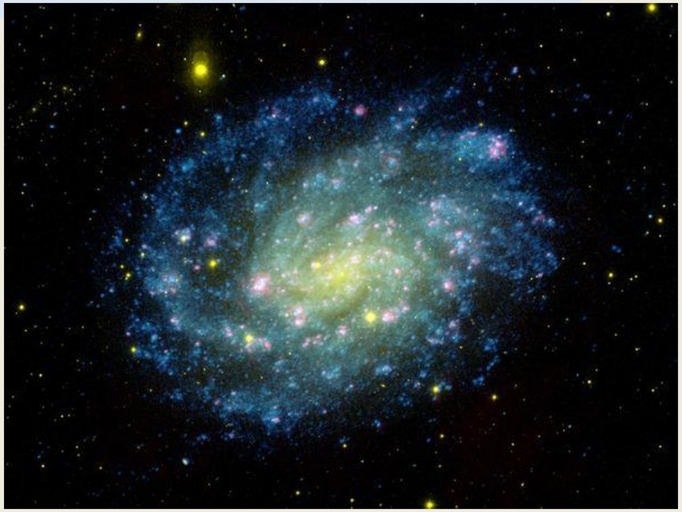
→ QM probabilities may violate the inequalities!

Experiment has to decide!




Where did the antimatter disappear?

How did antimatter slip off the map?



Average cubic-meter today:

10^9 photons, 0 antiprotons, 1 proton

Average cubic-meter short after Big Bang:

10^9 photons, 10^9 antiproton, 10^9 + 1 (?!) protons

Sacharow criteria

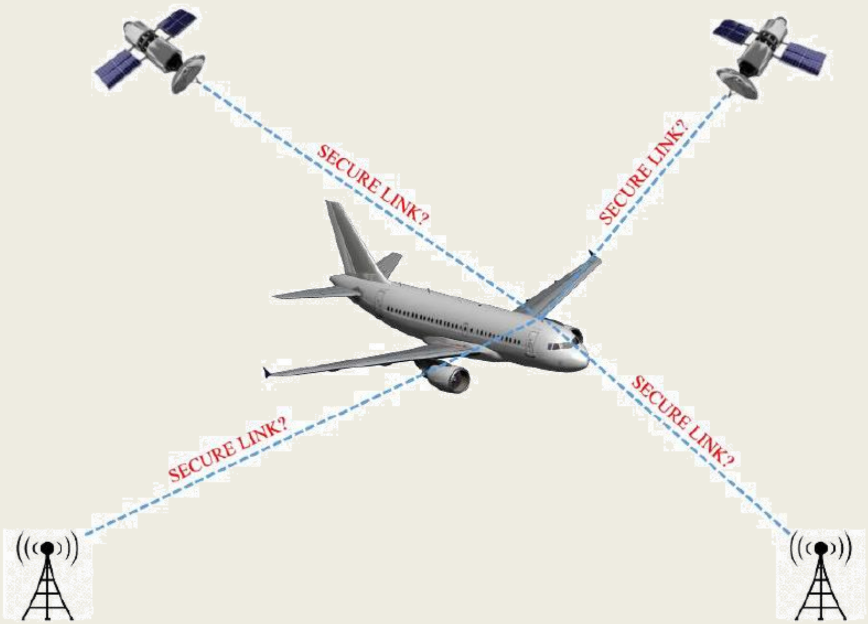
1.) Baryon number violation
2.) CP violation
3.) Non-equilibrium

ARE WE DONE?

Do we understand how the antimatter disappeared?

NO!

Relation between…



difference between matter and antimatter…

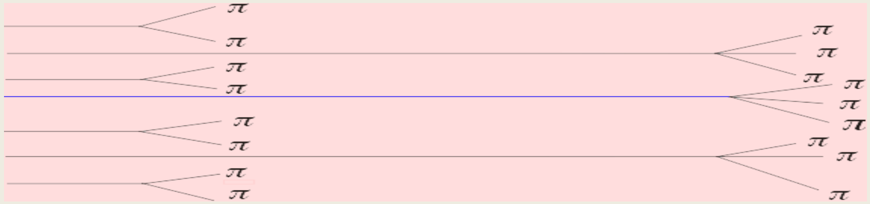
…and security in quantum cryptographic protocols

Crash course on neutral kaons:

Strangeness: $S\left|K^0\right\rangle = +\left|K^0\right\rangle$

$S\left|\overline{K}^0\right\rangle = -\left|\overline{K}^0\right\rangle$

$K^0(s\bar{d}), \overline{K}^0(\bar{s}d) \rightarrow 2\pi, 3\pi$



Mass-eigenstates: $\left|K_S\right\rangle, \left|K_L\right\rangle$

$$\left|K^0\right\rangle \cong \tfrac{1}{\sqrt{2}}\left\{\left|K_S\right\rangle + \left|K_L\right\rangle\right\}$$

„A kaon is a kind of double slit"

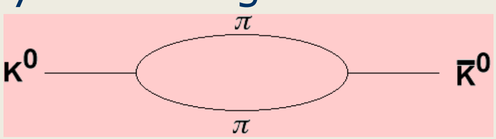
Bramon, Garbarino, H., PRA (2004)

Kaon in time:

short-lived state ↓ long-lived state ↓

$$\left|K^0(t)\right\rangle \cong \tfrac{1}{\sqrt{2}}\left\{e^{-\frac{\Gamma_S}{2}t - i m_S t}\left|K_S\right\rangle + e^{-\frac{\Gamma_L}{2}t - i m_L t}\left|K_L\right\rangle\right\}$$

Feynman diagram



$\Gamma_S \approx 10^{10}\,\frac{1}{s}$ ...decay width of K_S

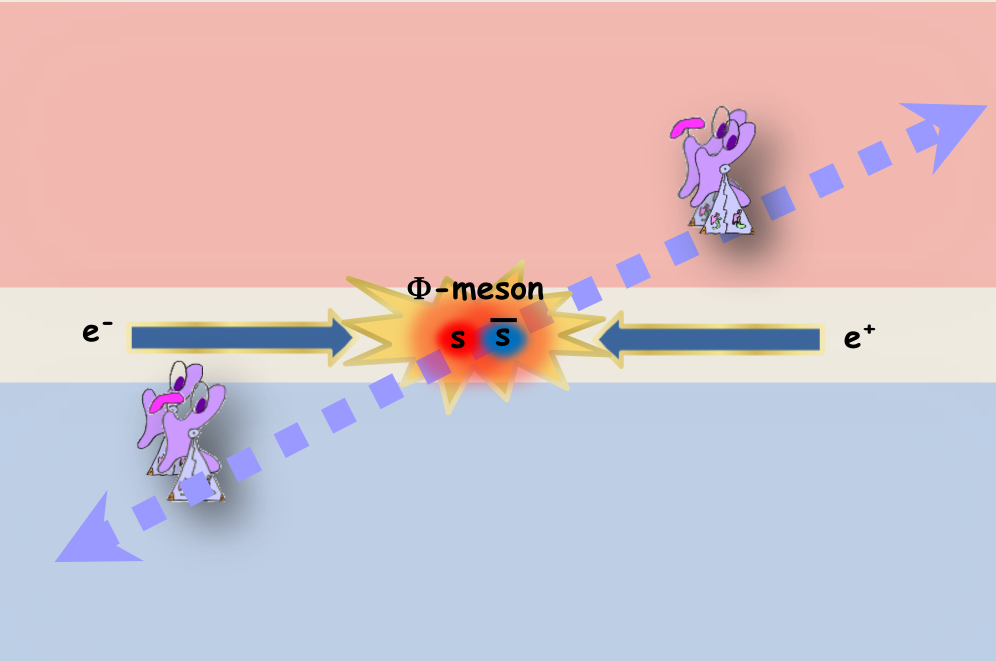
$\Gamma_L \approx 1/600\,\Gamma_S$ ...decay width of K_L

$\Delta m = m_L - m_S \approx 0.5\,\Gamma_S$ ...mass difference

CP violation (C…charge conjugations,P…parity)

$|K^0\rangle, |\overline{K}^0\rangle \rightarrow \quad 2\pi \;, \quad 3\pi$

Entanglement-Quantum Correlations



Anti-symmetric maximally entangled Bell state:

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}\left\{|\Uparrow\rangle_A \otimes |\Downarrow\rangle_B - |\Downarrow\rangle_A \otimes |\Uparrow\rangle_B\right\} \text{ ... spin 1/2}$$

$$= \frac{1}{\sqrt{2}}\left\{|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B\right\} \text{... qubit}$$

$$= \frac{1}{\sqrt{2}}\left\{|H\rangle_A \otimes |V\rangle_B - |V\rangle_A \otimes |H\rangle_B\right\} \text{... photon}$$

$$= \frac{1}{\sqrt{2}}\left\{|late\rangle_A \otimes |early\rangle_B - |early\rangle_A \otimes |late\rangle_B\right\} \text{ ... molecules}$$

$$= \frac{1}{\sqrt{2}}\left\{|\Uparrow\rangle_A \otimes |\alpha(t)\rangle_B - |\Downarrow\rangle_A \otimes |-\alpha(t)\rangle_B\right\} \text{ ... (single) trapped ion}$$

$$= \frac{1}{\sqrt{2}}\left\{|I\rangle_A \otimes |\Uparrow\rangle_B - |II\rangle_A \otimes |\Downarrow\rangle_B\right\}$$

$$= \frac{1}{\sqrt{2}}\left\{|K^0\rangle_A \otimes |\bar{K}^0\rangle_B - |\bar{K}^0\rangle_A \otimes |K^0\rangle_B\right\} \text{ ... K-mesons}$$

$$= \frac{1}{\sqrt{2}}\left\{|B^0\rangle_A \otimes |\bar{B}^0\rangle_B - |\bar{B}^0\rangle_A \otimes |B^0\rangle_B\right\} \text{ ... B-meson}$$

$$= \ldots$$

High Energy Physics

1935: Einstein-Podolsky-Rosen

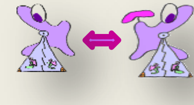
Quantum Correlations

Photons

$$\left|\psi^-\right\rangle = \tfrac{1}{\sqrt{2}}\left\{\left|H\right\rangle_A \otimes \left|V\right\rangle_B - \left|V\right\rangle_A \otimes \left|H\right\rangle_B\right\}$$

$$P(H\,\vec{n}; H\,\vec{m}) = P(V\,\vec{n}; V\,\vec{m}) = \tfrac{1}{4}\left(1 - \cos 2\phi_{nm}\right)$$

Kaons



$$\left|\psi^-\right\rangle = \tfrac{1}{\sqrt{2}}\left\{\left|K^0\right\rangle_A \otimes \left|\bar{K}^0\right\rangle_B - \left|\bar{K}^0\right\rangle_A \otimes \left|K^0\right\rangle_B\right\}$$

$$P(K^0\,t_l; K^0\,t_r) = P(\bar{K}^0\,t_l; \bar{K}^0\,t_r)$$

$$= \tfrac{1}{8}\left(e^{-\Gamma_S t_l - \Gamma_L t_r} + e^{-\Gamma_L t_l - \Gamma_S t_r} - \cos \Delta m \underbrace{(t_l - t_r)}_{\Delta t} \cdot e^{-\frac{\Gamma_S + \Gamma_L}{2}(t_l + t_r)}\right)$$

No decay $\Gamma_S = \Gamma_L = 0$

$$P(K^0\,t_l; K^0\,t_r) = P(\bar{K}^0\,t_l; \bar{K}^0\,t_r)$$

$$= \tfrac{1}{4}\left(1 - \cos \Delta m \underbrace{(t_l - t_r)}_{\Delta t}\right)$$

Einstein-Podolsky-Rosen-Correlations

Requirements for tests LRT versus QM

Requirements for a *conclusive* proof of the existence of correlation stronger than those explainable by *locality* and *realism/explainable by local resources & shared randomness*:

(1) "*Active* " measurements (opening the possibility for Alice and Bob to choose among alternative setups→ free choice)

Only for kaons & strangeness measurements!!

(2) "*Use all information*" (test the *whole* ensemble; decay product states are included→ this "additional" information cannot be ignored)

was/is overlooked by many researchers !!

→ are not "*only*" loopholes!

Generalized Bell inequality for kaons

local realistic theories ↓

$$S_{CHSH}(k_n,k_m,k_{n'},k_{m'};t_a,t_b,t_c,t_d)$$
$$=\left|E(k_n,t_a;k_m,t_b)-E(k_n,t_a;k_{m'},t_c)\right|+\left|E(k_{n'},t_d;k_m,t_b)+E(k_{n'},t_d;k_{m'},t_c)\right|\leq 2$$

I. Vary in time:

$$k_n = k_m =$$
$$k_{n'} = k_{m'} = \overline{K}^0$$

$$E(\overline{K}^0,t_a;\overline{K}^0,t_b)\cong -\cos\Delta m(t_a-t_b)\cdot e^{-\Gamma(t_a+t_b)}$$

$$S^{Photon}=2\sqrt{2}\cong 2.8$$ Violation!

•Bertlmann, Bramon, Garbarino, H., Phys. Lett. A (2004)
•Bertlmann, H.,Phys. Rev. A (2001)

Kaons?

$$S^{Kaon}(t_a,t_b,t_c,t_d)\leq 2$$ NO violation!

Strangeness oscillation/decay:

$$x=\frac{\Delta m}{\Gamma}\approx\frac{2\Delta m}{\Gamma_S}\approx 1$$

PROPOSITION:

The CHSH-inequality is violated iff x>2 for kaons or for other mesons x>2.6.

B-mesons: x=0.77
D-meson: x=0.01
B_s-mesons: x=26.2

Is there really no possibility to test for correlations stronger than those for classical systems in the neutra kaon system?

What has a symmetry violation to do with nonlocality?

$$S_{CHSH}(k_n,k_m,k_{n'},k_{m'};t_a,t_b,t_c,t_d)$$
$$=\left|E(k_n,t_a;k_m,t_b)-E(k_n,t_a;k_{m'},t_c)\right|+\left|E(k_{n'},t_d;k_m,t_b)+E(k_{n'},t_d;k_{m'},t_c)\right|\leq 2$$

II. Vary in quasi-spin:

$k_n = K_S, k_m = \overline{K}^0$

$k_{n'} = k_{m'} = K_1$

$$\delta \leq 0$$

?! CP violation related to nonlocality !?

- Bertlmann, Grimus, Hiesmayr, PRA (2001)
- Hiesmayr, Found. of Phys. Lett (2001)

$$k_m = K^0 \rightarrow \left.\begin{matrix}\delta\leq 0\\ \delta\geq 0\end{matrix}\right\}\Rightarrow \delta = 0$$

single kaon experiment

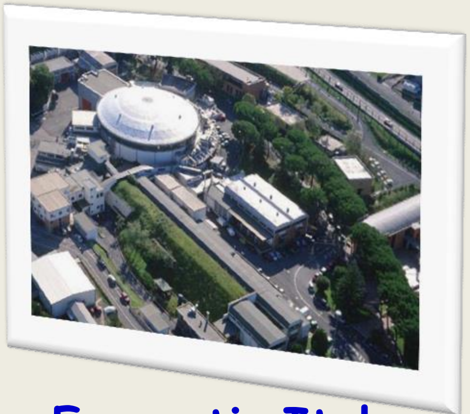
Leptonic charge asymmetry:

$$\delta = \frac{\Gamma(K_L\rightarrow \pi^- l^+ \nu_l)-\Gamma(K_L\rightarrow \pi^+ l^- \overline{\nu_l})}{\Gamma(K_L\rightarrow \pi^- l^+ \nu_l)+\Gamma(K_L\rightarrow \pi^+ l^- \overline{\nu_l})} = (3.27\pm 0.12)\cdot 10^{-3}$$

Summarizing…

If we believe in QM, then there is "*spooky action at distance*" also for this system at different energy scale, but there exists NO CONCLUSIVE EXPERIMENT so far.

Hiesmayr, Eur. Phys. J. C (2007)



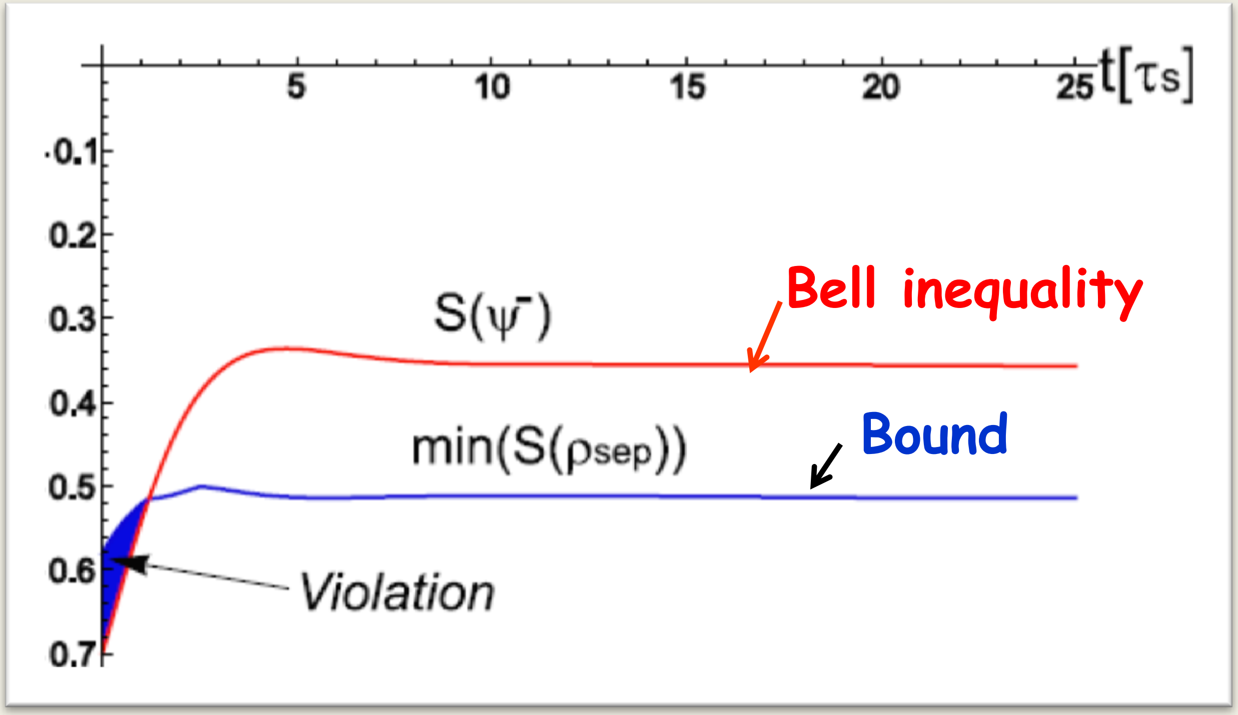
Frascati, Italy

A violation for observables that can be *actively* measured can be found, but for an initial non-maximally entangled state.

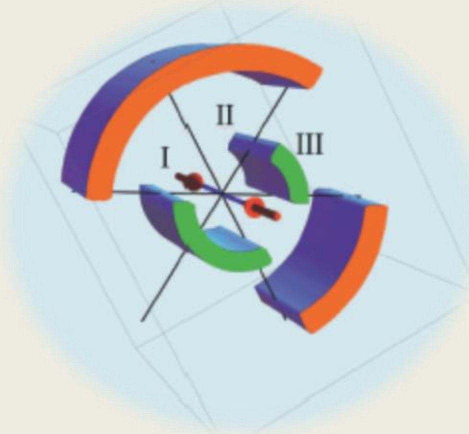
Hiesmayr, Domenico, Curceanu, Gabriel, Huber, Larsson, Moskal,
Eur. Phys. J. C (2012)

New Bell inequality for unstable systems that is experimentally feasible & can be performed with current technology!

Conclusive test for kaons

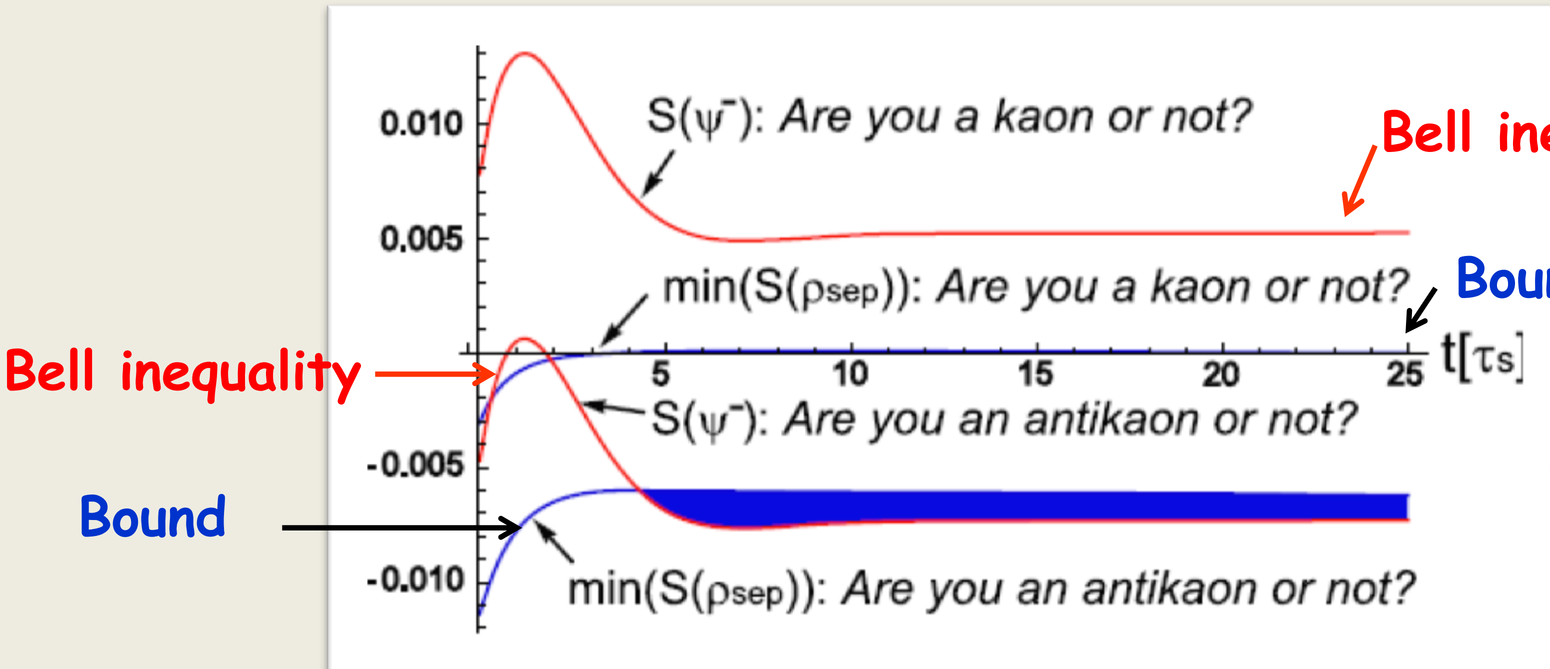


$t_m = t_{n'} = 1.34\tau_S,\ t_{m'} = 2.80\tau_S$ varied over $t_n = t$



Conclusive test for kaons

→ **sensitive to CP violation !!!**

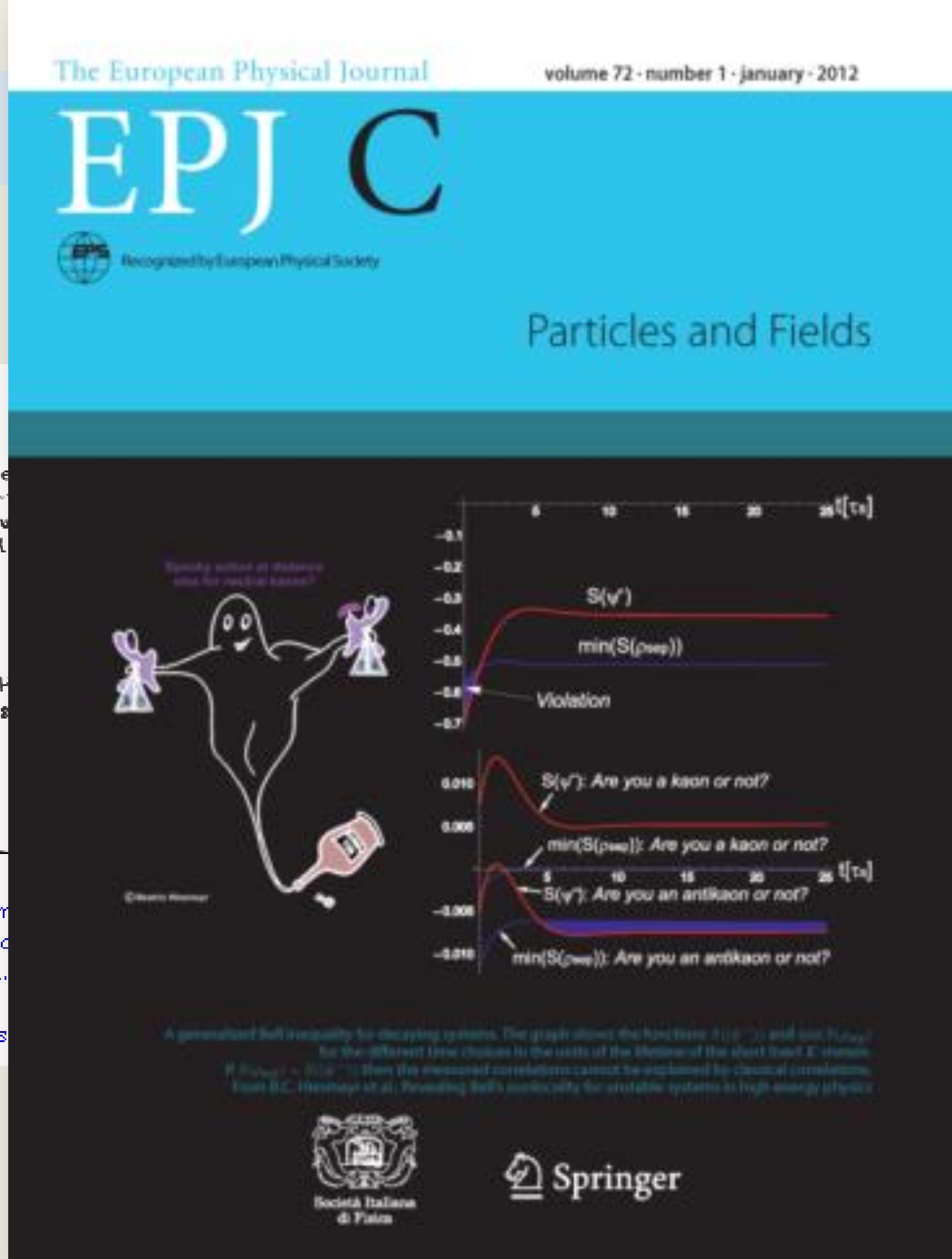


$t_n = 4.48\tau_S, t_m = t_{n'} = 4.81\tau_S$

Les chausse
de M. Ber
et la natu
de la réal

Fondation H
juin 17 198

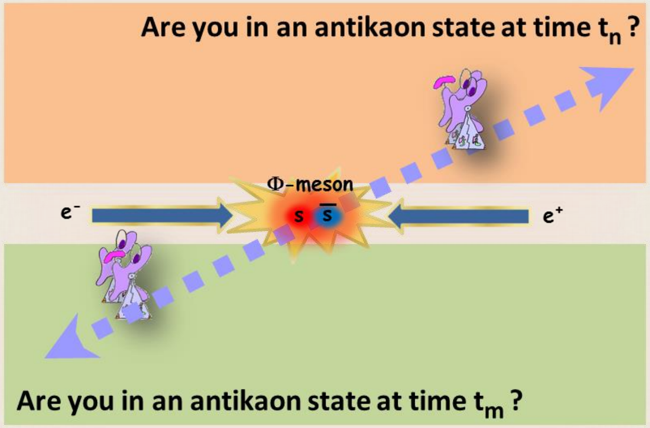
from: J.S. Bell, "Bertlm
Journal de Physiq
No. 3, mars 1981.
reprinted in: J.S. Bell,
mechanics



...or davon überzeugt,
...echanik nur eine un-
...reibung der Wirklich-

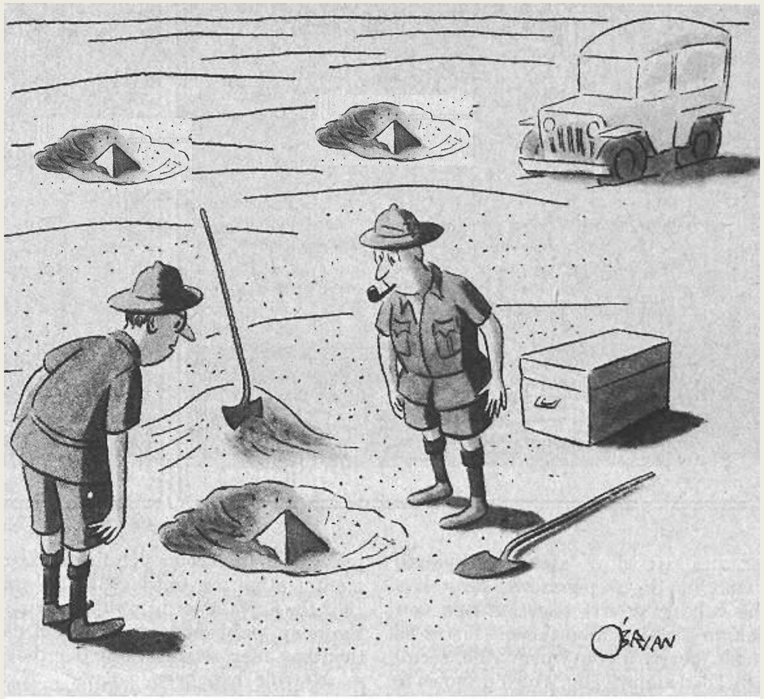
...ertlmann to the
...60th birthday of John Bell

Ekert-Cryptographic Protocol



Alice's choice	t_n	$t_{n'}$	t_m	t_n	$t_{n'}$	t_m	t_m	t_m	$t_{n'}$	$t_{n'}$	t_n	t_m	...
Alice's outcome	Y	N	Y	N	N	Y	N	Y	Y	N	N	N	...
Bob's choice	t_m	$t_{m'}$	t_m	$t_{m'}$	t_n	t_m	t_n	t_n	$t_{m'}$	t_m	t_n	t_n	...
Bob's outcome	N	Y	N	N	Y	N	N	-	N	N	Y	N	...
class	BELL	BELL	CODE	BELL	-	CODE	BELL	-	BELL	BELL	CODE	BELL	...
KEY	-	-	0	-	-	0	-	-	-	-	1	-	...

Summary



"This could be the discovery of the century. Depending, of course, on how far down it goes."

… stay tuned!

Thank You for Your attention!

The Quantum-Particle Group

www.quantumparticlegroup.at

(2008)

FWF
Der Wissenschaftsfonds.

Projects:
- **FWF-P21947**
- **FWF-P23627**
- **FWF-P26783**

Quantum Mechanics

cost
EUROPEAN COOPERATION
IN SCIENCE AND TECHNOLOGY