CONTEXTUALITY OFFERS DEVICE INDEPENDENT SECURITY

Karol Horodecki(1,2), Michał Horodecki(3,2), Paweł Horodecki(4,2)
Ryszard Horodecki(3,2), Marcin Pawłowski(3,2), Mohamed Bourennane(5)

1Institute of Informatics, University of Gdańsk, 80-952 Gdańsk, Poland
2 National Quantum Information Centre of Gdańsk, 81-824 Sopot, Poland
3 Institute of Theoretical Physics and Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland
4 Faculty of Applied Physics and Mathematics,Gdańsk University of Technology, 80-952 Gdańsk, Poland and
5 Department of Physics, Stockholm University, SE-10691 Stockholm, Sweden

Integrated Project FET/QIPC „Q-ESSENCE“

QIPA HRI Institute Allahabad 2011

Outline of the talk

•Contextuality

•Device independent security

•Peres-Mermin boxes

•Local randomnes of PM box

•Local randomnes – quantitative approach

•The scenario

•The protocol based on PM box

•Security from ideal PM box

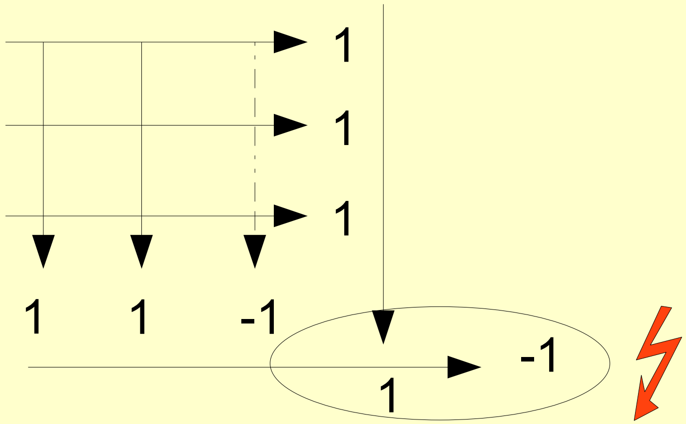
•Security from noisy PM box

Contextuality of Quantum Mechanics

Consider 9 two-qubits dychotomic observables:

$$RS = T\,,\; rs = t\,,\; \alpha\beta = \gamma$$
$$Rr = \alpha\,,\; Ss = \beta\,,\; Tt = -\gamma$$

$$\begin{array}{lll} R = \sigma_z^{(1)} & S = \sigma_z^{(2)} & T = \sigma_z^{(1)}\sigma_z^{(2)} \\ r = \sigma_x^{(2)} & s = \sigma_x^{(1)} & t = \sigma_x^{(1)}\sigma_x^{(2)} \\ \alpha = \sigma_z^{(1)}\sigma_x^{(2)} & \beta = \sigma_x^{(1)}\sigma_z^{(2)} & \gamma = \sigma_y^{(1)}\sigma_y^{(2)} \end{array}$$

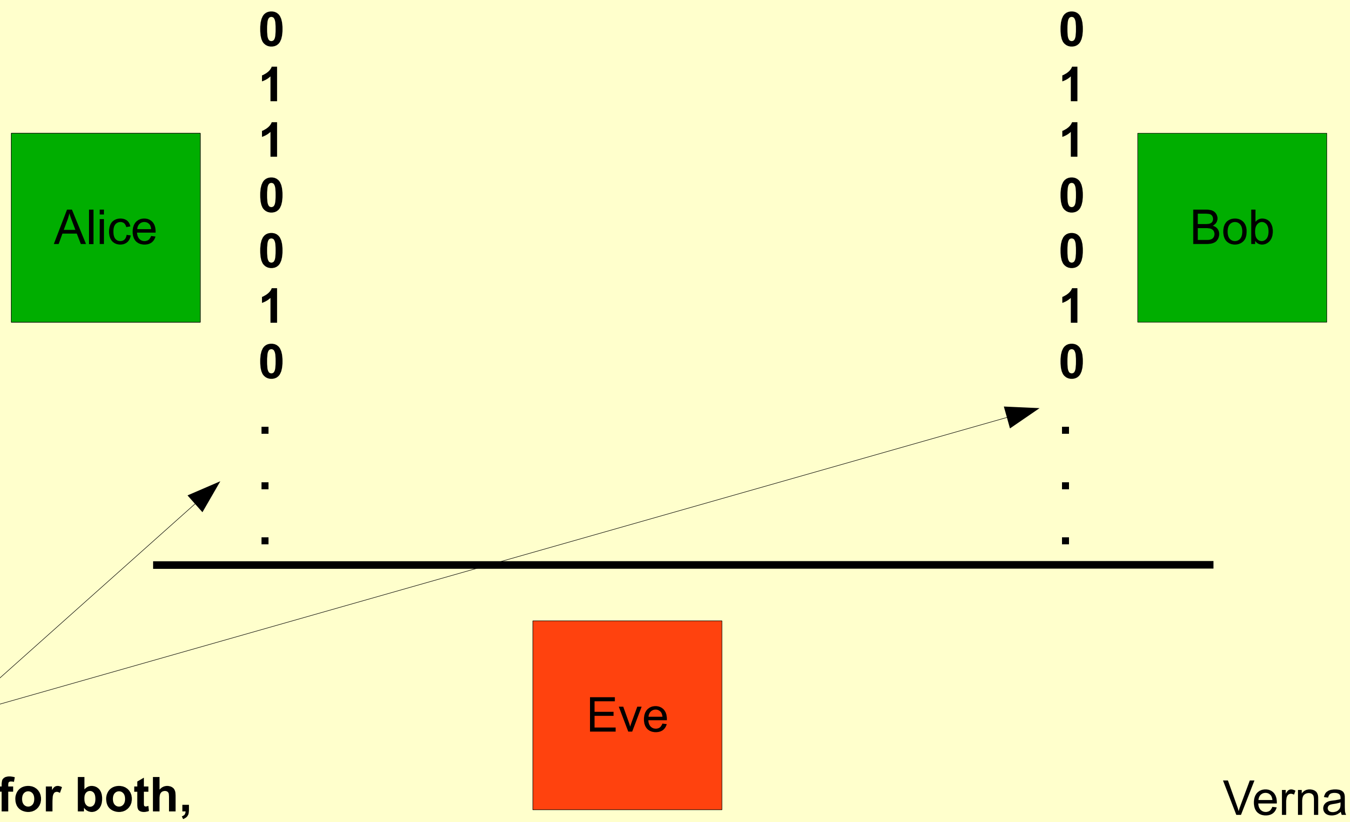


[Peres, Mermin 1990]

Conclusion: Values of the measurements of these 9 observables could not all preexist!

At least one observable must **depend on the context**: if it is measured in row or in column

Quantum based key distribution



Secret key

1) the same for both,
2) random
3) unknown to Eve

Vernam 1927

Quantum mechanics allows to distribute such a key

[Bennet, Brassard 1984]

Bennet Brassard Mermin (BBM) protocol

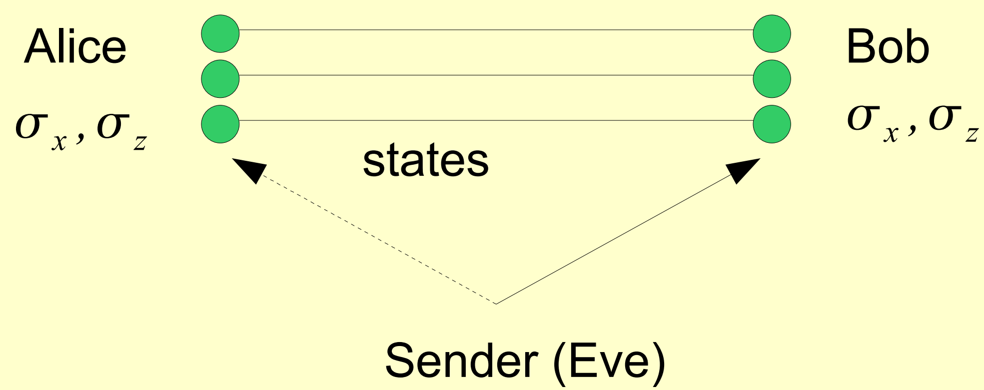
Alice and Bob are provided N states

On a random sample 1, they measure both σ_z

On a random sample 2, they measure both σ_x

If they are correlated in both basis, measure the rest with σ_z

Perform error correction and privacy amplification => the key



Alice | **Device A** | **Device B** | **Bob**

WORNING ! **Alice and Bob trust their devices**

Device independent security

security against melicious producer of secure devices

[Mayers, Yao 1998]

Device is quantum-mechanical

Device can not signal from Alice to Bob and vice versa

[Acin et al. 2006]

[Barret Hardy Kent 2005]

Ex: no assumptions about dimension of an underlying Hilbert space

[Acin et al., Magniez et al. 2006]

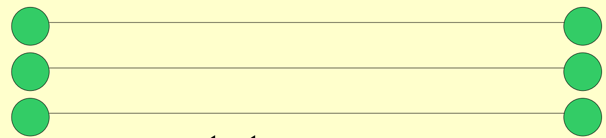
Importance: BBM is not secure if Alice and Bob do not control dimension and operations

Ex: they can measure some observables on a separable, maximally correlated state

Device independent security – idea of the proof of security

Ekerts' 1991 protocol Alice

$\sigma_z, \sigma_x, (\sigma_z+\sigma_x)/\sqrt{2}$



Bob

$\sigma_z, (\sigma_z+\sigma_x)/\sqrt{2}, (\sigma_z-\sigma_x)/\sqrt{2}$

states

Basis disagree => check violation of CHSH inequality: $\langle AB\rangle+\langle AB'\rangle+\langle A'B\rangle-\langle A'B'\rangle\leq 2$
Basis agree => raw key

E91 protocol has device independent security version:

Idea: Bell inequality is violated

=> no hidden variable model

=> no Eavesdropper

(otherwise Eve's symbol would be a hidden variable)

[Ekert 1991]

[Barret Hardy Kent 2005]

[Acin et al. 2006]

The more violation of Bell inequality, the more secure is the protocol

Motivation

E91 has received device independent extension

What about BB84 ?

Problem: melicious device can imprint all operations
That Alice made on system

=> no security

Wayout: Consider BBM protocol.

What is in hends of Alice will never be in hends of Eve later !

Goal: find device independent extension of BBM:

Idea: Alice and Bob will measure PM-observables on singlets

Peres-Mermin (PM) boxes

Definition A PM box is a family of 9 distributions P(a,b|AB)

where A = 1,2,3 B = 1,2,3 are inputs
and a=(a1,a2,a3) and b=(b1,b2,b3) are triples of outcomes

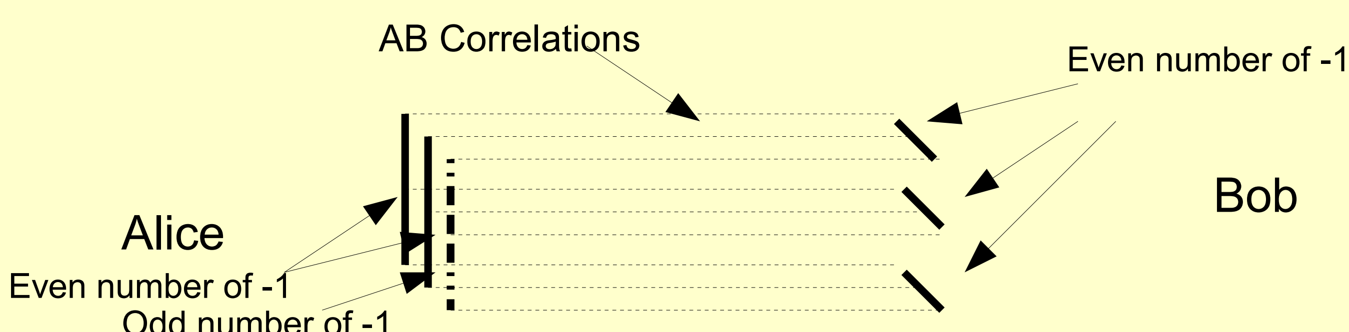
Which satisfies conditions:

PM: For A=1,2 B = 1,2,3
$a, b \in \{+1+1+1; -1+1-1; -1-1+1; +1-1-1\}$ (Even nr of -1)

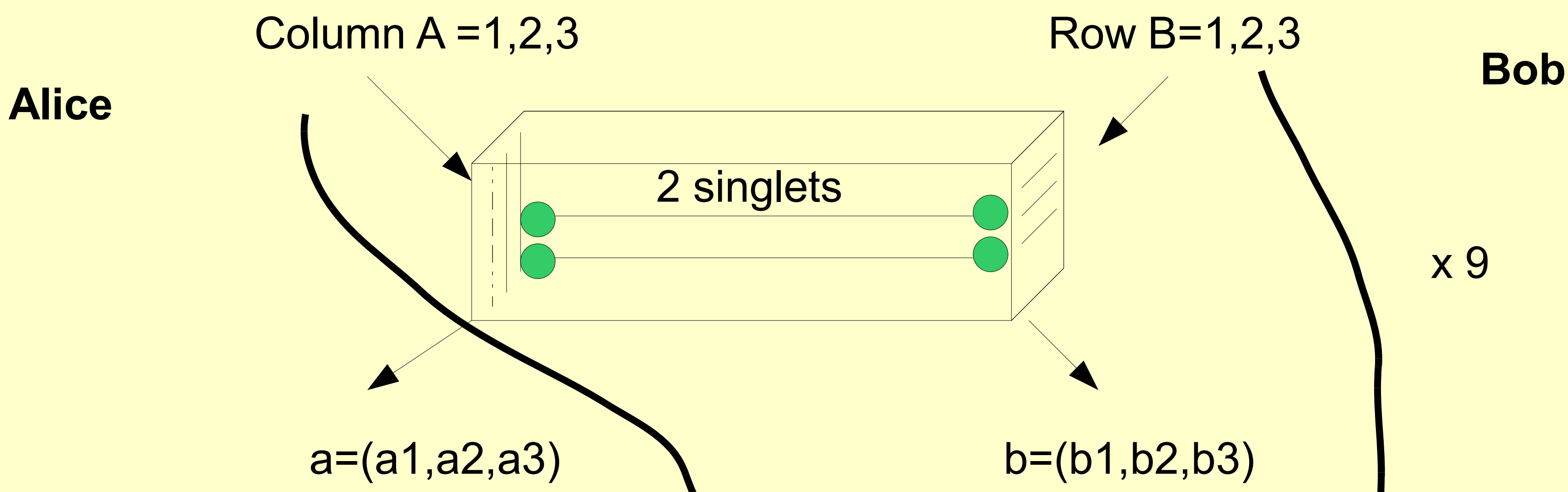
For A=3 $a \in \{-1-1-1; -1+1+1; +1-1+1; +1+1-1\}$ (Odd nr of -1)

AB correlations: For $A=i, B=j \quad a_i = b_j$

AB No-signalling: P(a|AB) does not depend on B
P(b|AB) does not depend on A



Peres Mermin box - example:



1	2	3	
$R=\sigma_z^{(1)}$	$S=\sigma_z^{(2)}$	$T=\sigma_z^{(1)}\sigma_z^{(2)}$	1
$r=\sigma_x^{(2)}$	$s=\sigma_x^{(1)}$	$t=\sigma_x^{(1)}\sigma_x^{(2)}$	2
$\alpha=\sigma_z^{(1)}\sigma_x^{(2)}$	$\beta=\sigma_x^{(1)}\sigma_z^{(2)}$	$\gamma=\sigma_y^{(1)}\sigma_y^{(2)}$	3

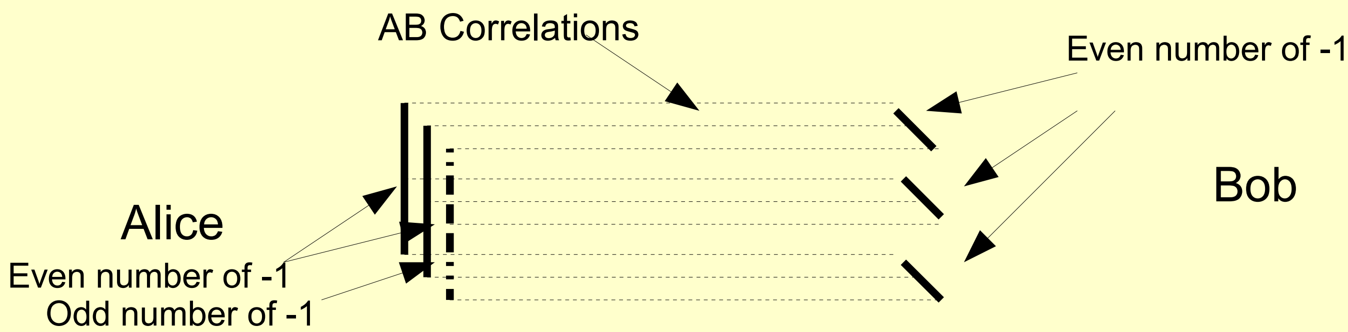
Checking conditions for PM box:

1) non-signalling becuse quantum

2) AB correltions because of singlets

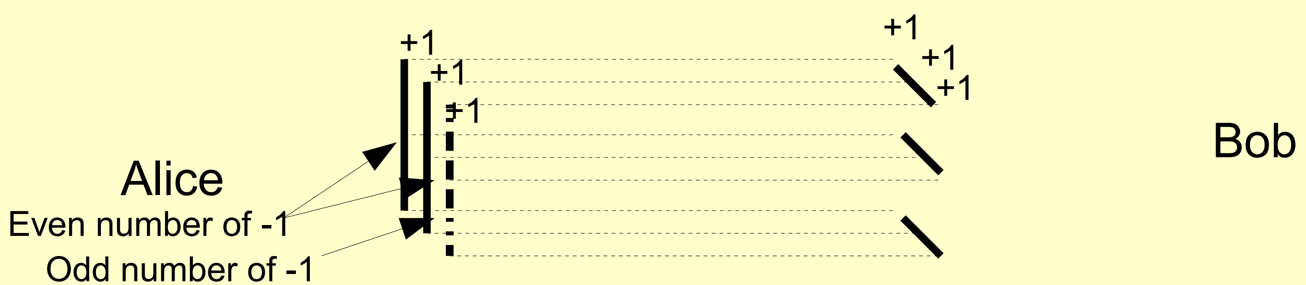
3) PM condition because
$$RS=T\,,\, rs=t\,,\, \alpha\beta=\gamma$$
$$Rr=\alpha\,,\, Ss=\beta\,,\, Tt=-\gamma$$

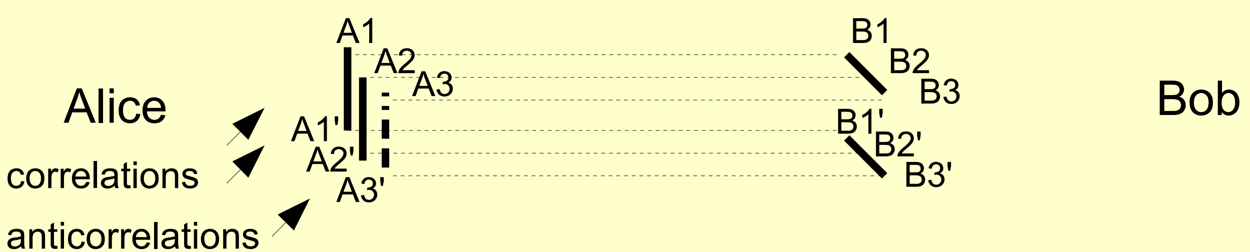
Local randomness of the PM box (I)

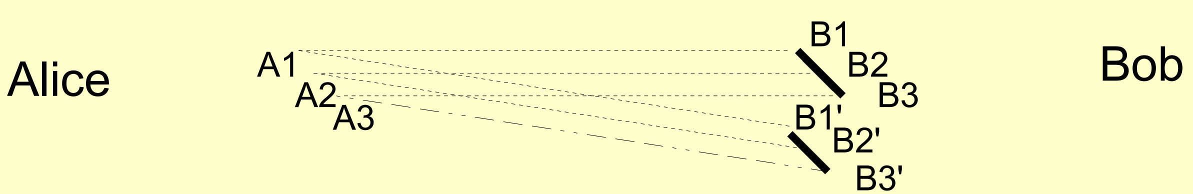


Theorem: Bob's first row can not have all deterministic values

Proof: suppose by contradiction, that measuring first row gives (1,1,1) with prob. 1

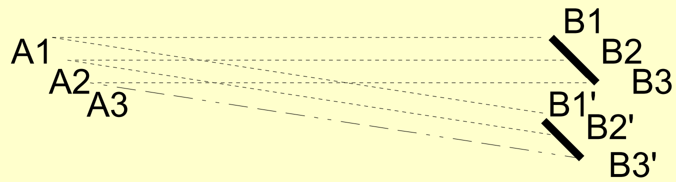
1)


2)


3)


Local randomness of the PM box (II)

3) Alice



Bob

A new Bell inequality

$$\gamma(A:B)=\langle A_1 B_1\rangle+\langle A_2 B_2\rangle+\langle A_3 B_3\rangle+\langle A_1 B'_1\rangle+\langle A_2 B'_2\rangle-\langle A_3 B'_3\rangle\leq 4$$

Picture 3) means:

Determinism of the first row leads to **maximal** violation of this Bell inequality (up to 6)

This Bell inequality is of type 3 x 2

Algebraic violation possible only if classical theory reaches the same bound 6

[Gisin Methot Scarani 2007]

Contradiction !

Conclusion: Bob's row is non-deterministic Q.E.D.

Local randomness of the PM box III

QM can not violate $\gamma(A:B)$ **up to 6**

By the „method of hierarchies“ violation by QM satisfies

[Wehner 2006]
[Navascues, Pironio 2008]

$$\gamma(A:B)\leq 5.6364$$

Idea: Bell inequality can be cast as $Tr\,X\,W$ X is positive semidefinite

Mathematica + SDPT3 for Matlab

Consequences:

Let

$$\left.\begin{aligned} q_0&=Pr(B_1=+1,B_2=+1,B_3=+1)\\ q_1&=Pr(B_1=+1,B_2=-1,B_3=-1)\\ q_2&=Pr(B_1=-1,B_2=+1,B_3=-1)\\ q_3&=Pr(B_1=-1,B_2=-1,B_3=+1)\end{aligned}\right\}$$

possible Bob's results due to PM condition

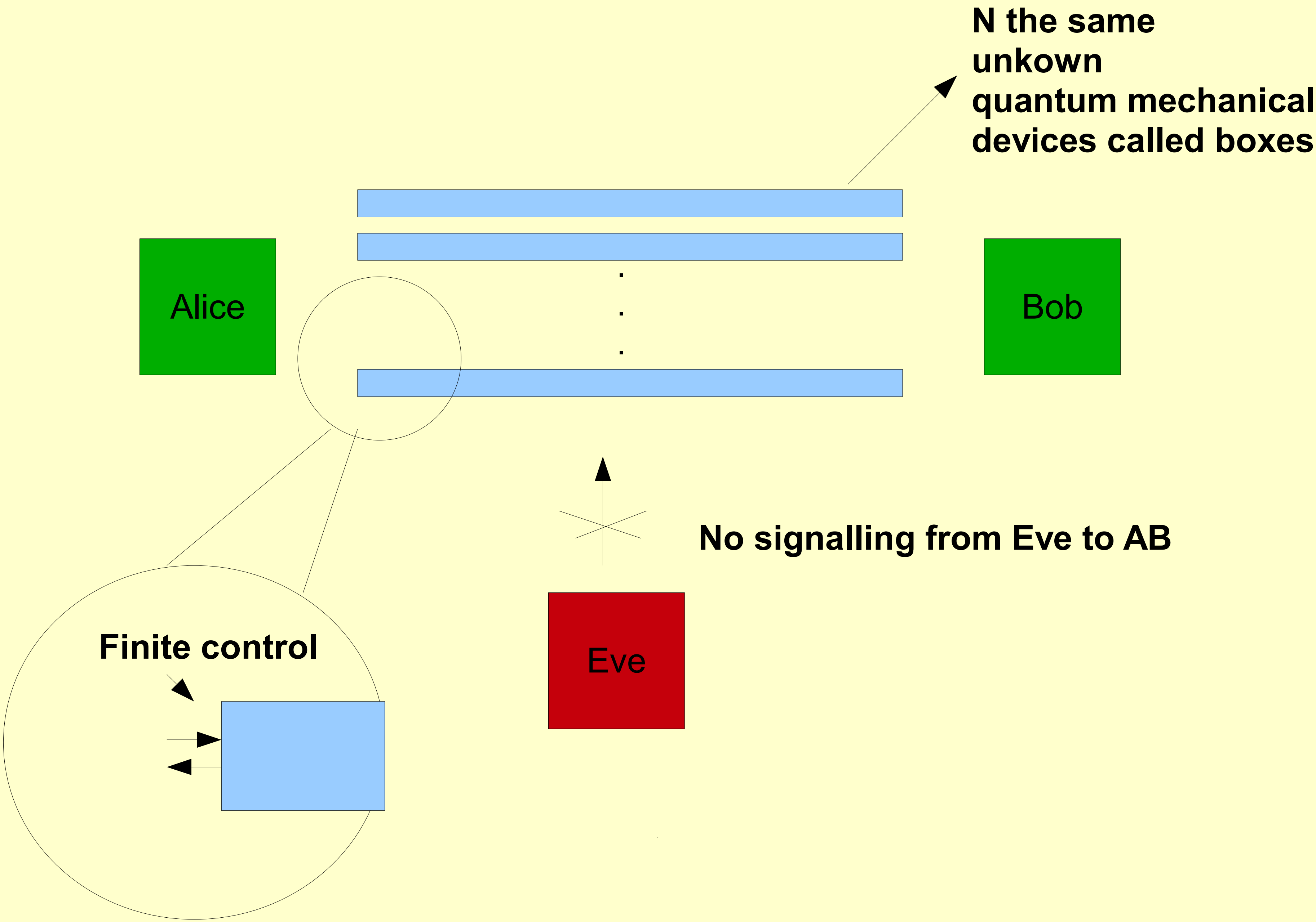
$$q_i\leq\frac{1}{4}(\gamma(A:B)-2)=0.9091$$

Bob's row is not deterministic

Observation: the proof of security will be different than that of Bell based ones:

Instead of high enough violation of Bell inequality we base on not too high violation by QM

The scenario



The protocol

Alice and Bob obtain n the same unknown QM boxes

1) **Select 2 samples:**

1.1) *On the first* sample measure randomly „columns“ and „rows“ respectively

Colum -row test

Check PM condition and AB correlations

1.2) *On the second sample* measure the „first row“ Row test

Check AB correlations

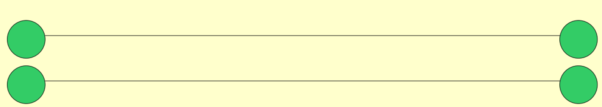
2) **On remaining boxes:**

Measure the „first row“ => raw key (if passed the above test)

3) Standard error correction and privacy amplification methods

QM implementation:

Measure Peres-Mermin observables on two singlet states:

Alice  Bob

	1	2	3	
	$R=\sigma_z^{(1)}$	$S=\sigma_z^{(2)}$	$T=\sigma_z^{(1)}\sigma_z^{(2)}$	1
	$r=\sigma_x^{(2)}$	$s=\sigma_x^{(1)}$	$t=\sigma_x^{(1)}\sigma_x^{(2)}$	2
	$\alpha=\sigma_z^{(1)}\sigma_x^{(2)}$	$\beta=\sigma_x^{(1)}\sigma_z^{(2)}$	$\gamma=\sigma_y^{(1)}\sigma_y^{(2)}$	3

Security from ideal PM box I

Alice and Bob are given by Eve ideal PM boxes

Individual attacks: Eve creates boxes ABE, and (after having listened to Alice and Bob) measures her shares E in the same way each => splitting a PM box Into different boxes

$$R^{AB} \rightarrow \Sigma_i r_i R_i^{AB}$$

QN: What are possible ensambles that Eve can produce measuring her system ?

Theorem: Eve can split a PM box only into PM boxes again.

Obs1: $\Sigma_i r_i R_i^{AB}$ Is again a PM box (no-singalling from Eve)

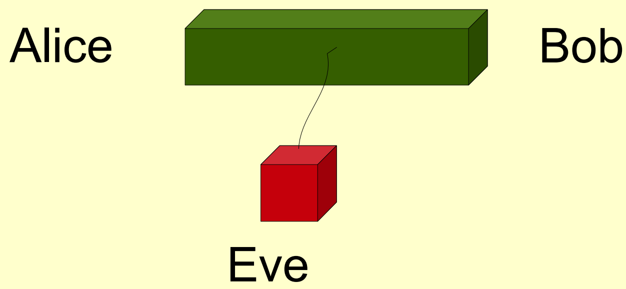
Obs2 : any ensamble of PM box is a mixture of PM boxes

Proof: PM box is described by conditions that certin probabilities are zero

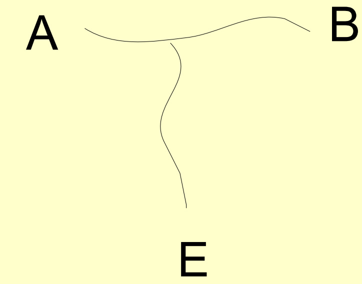
=> members of ensamble has also to have these probabilities zero.

Q.E.D.

Security from ideal PM box II



=>
measurements



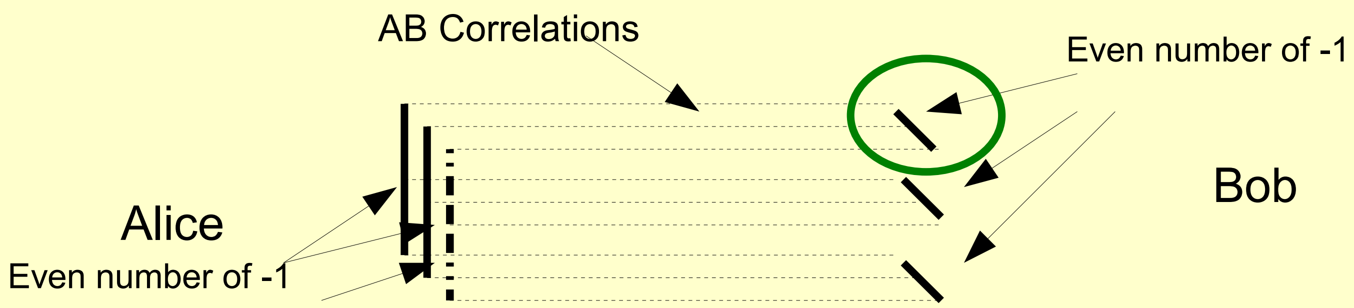
Now we can compute *Csiszar Koerner formula*:

$$K \geq I(A:B) - I(B:E) = H(B|E) - H(B|A)$$

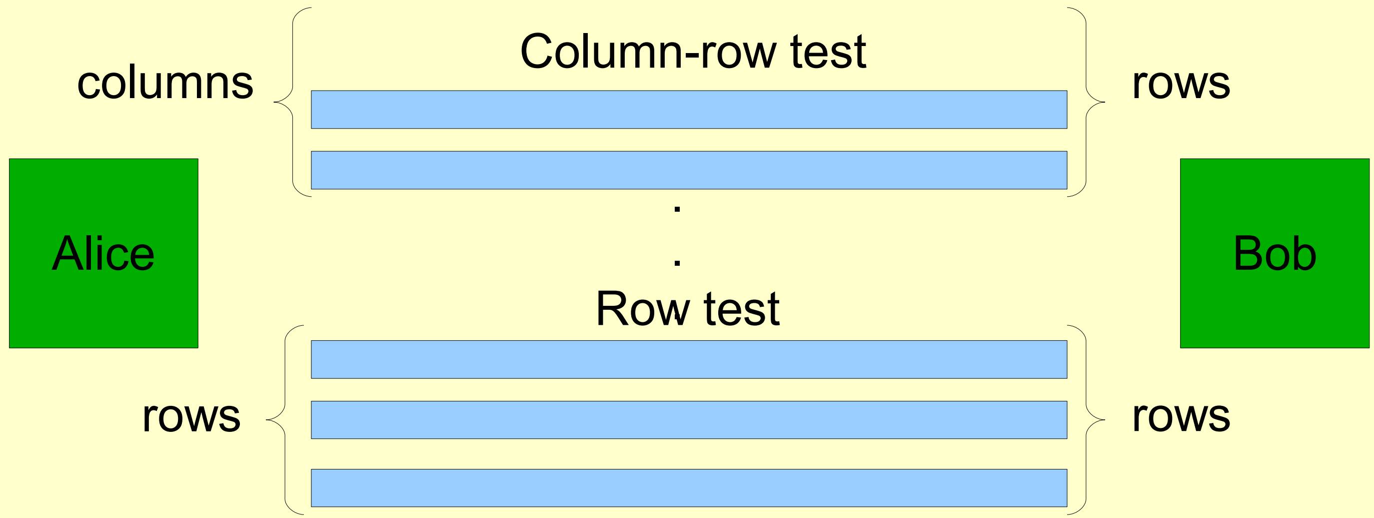
$H(B|A) = 0$ Because PM box is ideal

$H(B|E) \geq 0.439$ Because every box in ensamble is PM, hence satisfies $q_i \leq 0.9091$

In other words: Bob's results of the first row are partially secure



Some observations



Observation 1: In row test Alice may be cheated by the provider of device to measure something totally different.

However: Bob has security in his row.

=> if Alice is correlated with Bob, she is secure

Observation 2: Alice and Bob do not need to check PM condition. Instead: enforce it: produce each third outcome from the first and second:

ex.instead of measuring B1 B2 B3, measure B1 B2 and put $B_3 = B_1 B_2$

Observation 3: Unlike in E91, they measure usual correlations i.e. If A = B, and thanks to Obs. 2, only this.

Key from noisy PM box (I)

Noise in PM Alice and Bob do not need to measure PM, they can fabricate each third result

Noise in correlations Two types: column - row test ϵ

row test $\tilde{\epsilon}$

$$K \geq H(B|E) - H(B|A)$$

$$q_i \leq 0.9091 + 4.5\epsilon$$

$$H(B) \geq h(x) \equiv f(\epsilon),\ x = min(0.9091 + 4.5\epsilon, 1)$$

$H(B|E) = \Sigma_i r_i H(B)_i$ where box is splited into $\Sigma_i r_i R_i^{AB}$

The new boxes satisfy $\Sigma_i r_i \epsilon_i = \epsilon$

By Markov inequality $\Sigma_{i:\epsilon_i<\delta} r_i \geq 1 - \frac{\epsilon}{\delta}$

$$H(B|E) \geq inf\ \Sigma_i r_i f(\epsilon_i) \geq \Sigma_{i:\epsilon_i<\delta} r_i f(\epsilon_i) \geq (1 - \frac{\epsilon}{\delta}) f(\delta)$$

$$\boxed{H(B|E) \geq (1 - \frac{\epsilon}{\delta}) h(0.9091 + 4.5\delta)}$$

Key from noisy PM box (II)

$$K \geq H(B|E) - H(B|A)$$

By Fano's inequality we obtain

$$H(B|A) \leq h(\tilde{\epsilon}) + \tilde{\epsilon} \log(|B|-1)$$

There is $\epsilon = \frac{2}{3}\tilde{\epsilon}$ hence

$$H(B|A) \leq h(\frac{3}{2}\epsilon) + \frac{3}{2}\epsilon \log(3)$$

Overall rate reads:

$$\boxed{K \geq H(B|E) - H(B|A) \geq (1 - \frac{\epsilon}{\delta}) h(0.9091 + 4.5\delta) - \{h(\frac{3}{2}\epsilon) + \frac{3}{2}\epsilon \log(3)\}}$$

δ Is arbitrary => $\delta = 1.8\epsilon$

Noise treshold is $\boxed{\epsilon_0 \leq 0.68\,\%}$

(much smaller than 2% in usual Bell based protocols)

Conclusions and further work

- Prove the same for collective (coherent) attacks (there were some attempts)

  [Acin Masanes Pironio 2011, Hanggi Renner 2011]

- Can the noise threshold be higher ?

- Is it generic for state-independent KS paradoxes (other than PM) ?

Thank you for your attention !