MAX PLANCK RESEARCH GROUP

Institute of Optics,
Information and Photonics
University Erlangen-Nuremberg

Quantum Correlations as Necessary Precondition for Secure Communication

Phys. Rev. Lett. **92,** 217903 (2004)
quant-ph/0307151

Marcos Curty[1], Maciej Lewenstein [2], Norbert Lütkenhaus[1]

[1] Institut für Theoretische Physik
and
Max Planck Research Group
Universität Erlangen-Nürnberg

[2] Institut für Theoretische Physik
Universität Hannover

Overview

- **Interface Physics – Computer Science in Quantum Communication**
  - Physics provides correlations with a promise
  - Computer Science uses correlations within complex communication task

- **Classical and Quantum Correlations**
  - If Physics is to add something, then we need correlations with quantum features

- **'Entanglement' as necessary conditions for quantum communication**

- **Exploitation of conditions**
  - entanglement witnesses
  - application to 6-state, 4-state and 2-state protocol (QKD)

- **Conclusions**

Bennett Brassard Protocol

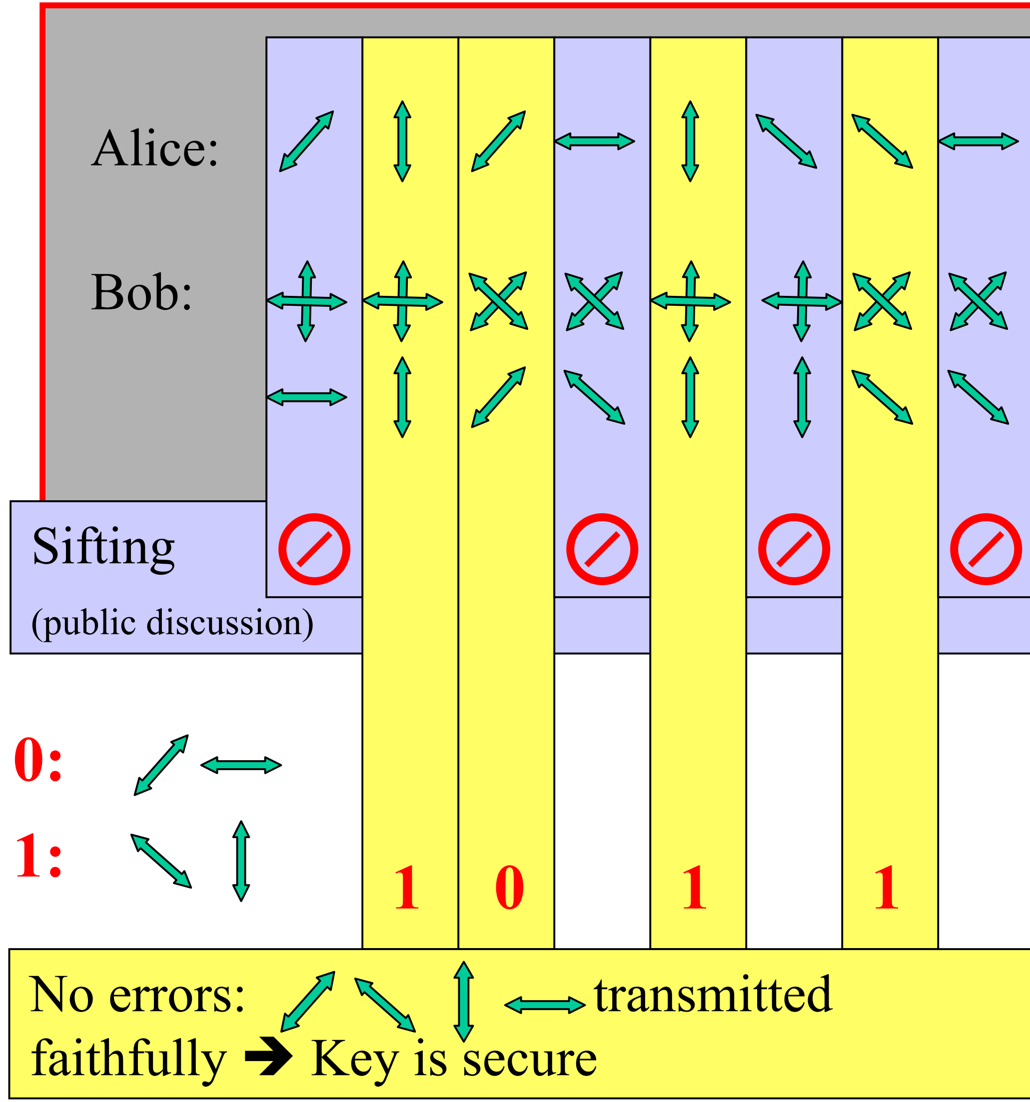
Quantum Part:

Create random key:

→ random signals

→ random measurements

Public discussion over faithful classical channel: distinguish **deterministic** from **random processes**



Quantum Communication and Correlations

Phase I: Physical Set-Up

Generation of correlations between Alice and Bob
➔ possibly containing hidden correlations with Eve

Physics:
correlated data with a promise.

Which type of correlations are useful for Quantum Communication?

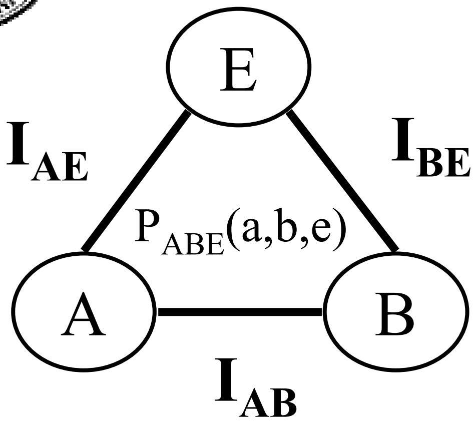
(Classical) Computer Science:
Solve Communication Problem with classically correlated data …

Phase II: Classical Communication Protocol

Advantage distillation (e.g. announcement of bases in BB84 protocol)
Error Correction (➔ Alice and Bob share the same key)
Privacy Amplification (➔ generates secret key shared by Alice and Bob)

Note: classical communication for QKD can be improved:
e.g. in QKD with weak light pulses [Acín, Gisin, and Scarani, Phys. Rev. A 69, 012309 (2004)]
or two-way communication [Lo, Gottesman, quant-ph/0105121]

Key extraction from correlated classical data



Lower bound on secrecy capacity C_S:
(rate of secret communication between Alice and Bob)
- Csiszar, Körner, IEEE, IT 24, 339 (1978).

$$\boxed{C_S > \max \{I_{AB} - I_{AE}, I_{AB} - I_{BE}\}}$$

! Derived for classical three-party correlations
Eve: quantum system!
- I. Devetak, A. Winter, quant-ph/0307053.

Upper Bounds on secrecy capacity C_S:

- U. M. Maurer, IEEE Trans. Inf.Theo. 39, 1733 (1993);
-U. Maurer and S. Wolf, IEEE T. I. T. **45**, 499 (1999).

$$\boxed{Cs \leq I(A;B\downarrow E)}$$

- Intrinsic Information: $I(A;B\downarrow E)$

$I(A,B\downarrow E) = \min_{E\to\underline{E}} I(A;B|\underline{E})$ with $I(A;B|E) = H(A,E) + H(B,E) - H(A,B,E) - H(E)$

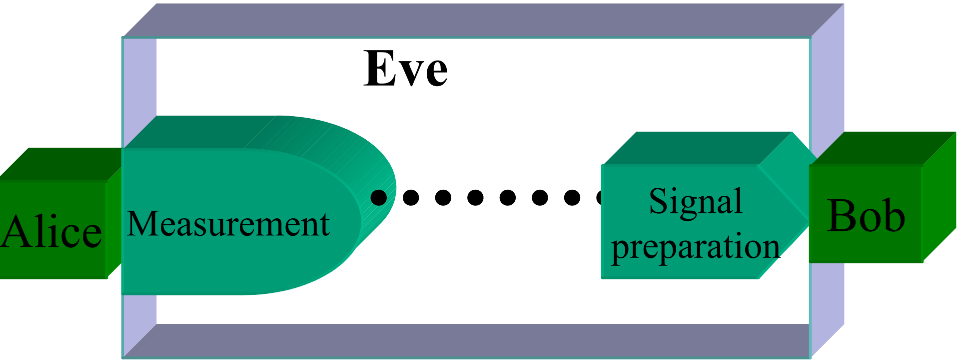
Quantum

$P_F(A,B,E) = P(a,b)\ \mathrm{Tr}\,(\rho_E(a,b)\, F_E)$

$$\boxed{I(A;B\downarrow E) = \inf_F I_F(A,B|E)}$$

'Information' Bob can gain about Alice's data by looking at his own data, whatever Eve told him about Alice's data.

Intercept/Resend attack



➔P(a,b,e)=p(a,e) p(b|e) (Markov Chain)

➔ Intrinsic information vanishes, no secret communication possible!

Example:

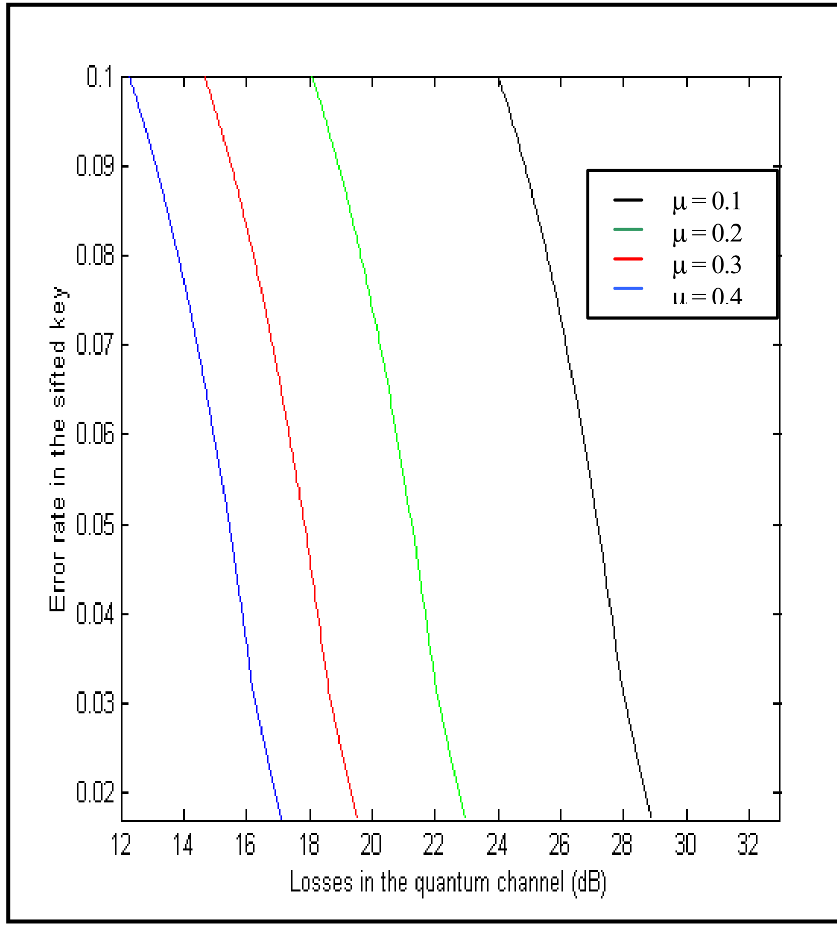
BB84 with

•Poissonian photon number distribution

•losses in the quantum channel

•symmetric error rate in signals

➔implementing **specific** intercept/resend

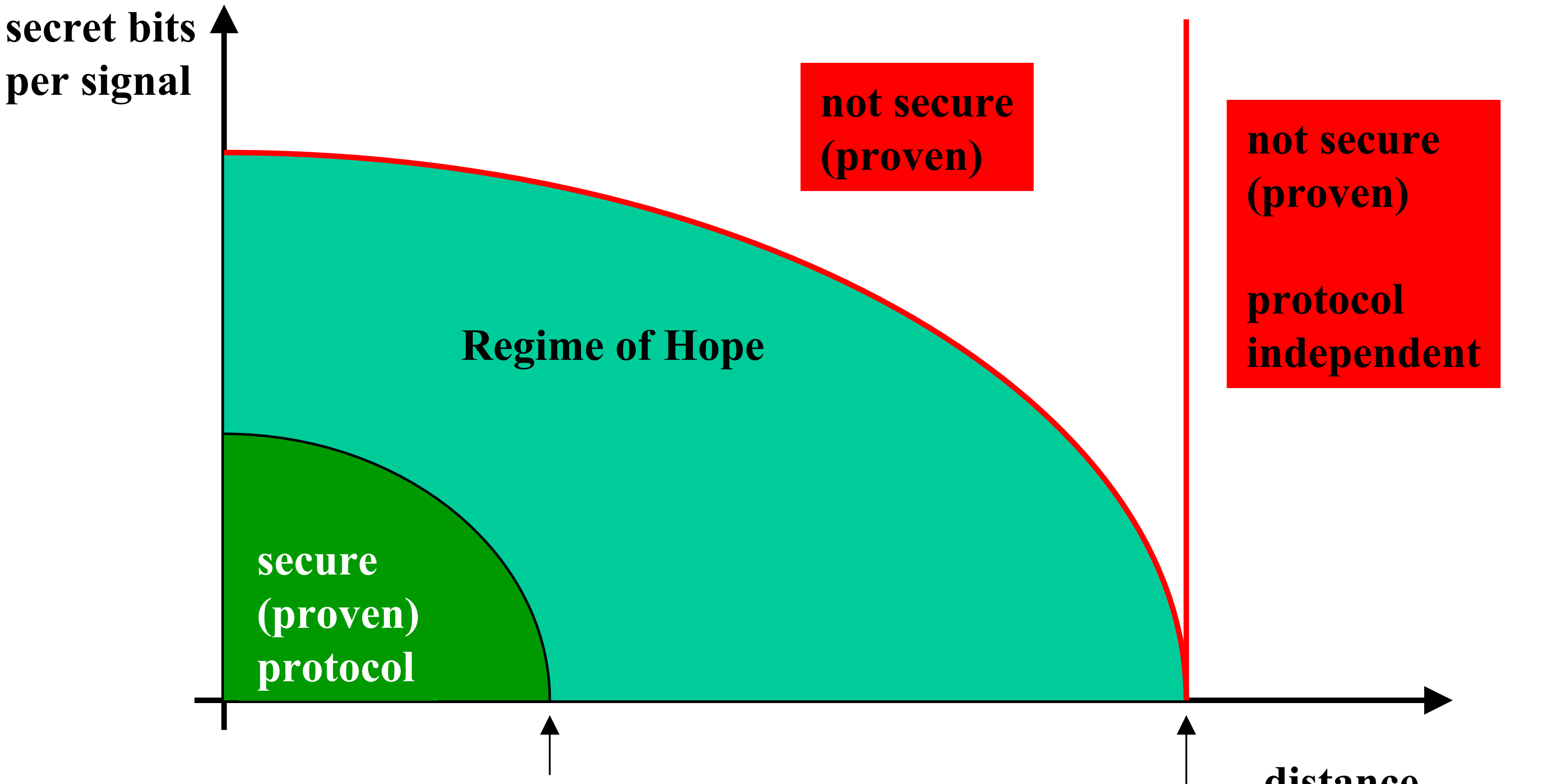


[M.Curty, N.L, in preparation]

(for vanishing error rate:

[Jahma, Dusek, NL, Phys. Rev. A 62, 022306 (2000)]

Potential for correlations



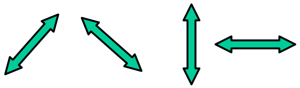
e.g. weak coherent pulse BB84
Inamori, NL, Mayers quant-ph/0107017
➔ typically 20 km

e.g about 100 km

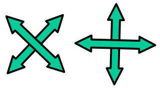
Are these correlations useful?

Assumptions:

trusted ideal source of ideal BB84 protocol



trusted ideal detector of ideal BB84 protocol



Probability Distribution P(A,B)

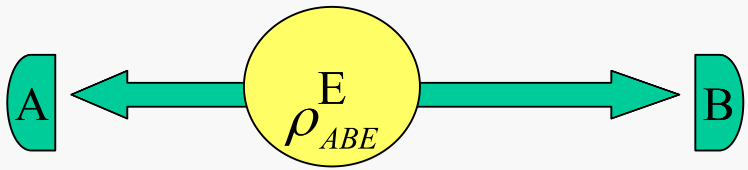
	0	1	+	-
0	0.07987	0.04516	0.00913	0.11591
1	0.04508	0.07986	0.11593	0.00901
+	0.11599	0.00909	0.08001	0.04507
-	0.00897	0.11593	0.04505	0.07985

Error Rate: 36%

Entanglement behind the scene

How to generate correlated classical data:

Entanglement based QKD:

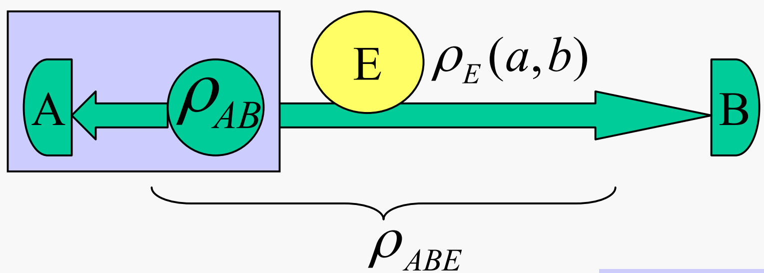


Prepare & Measure Schemes:

orthonormal states

$$|\psi\rangle_{AB} = \sum_i \sqrt{p_i}\,|a_i\rangle_A |\varphi_i\rangle_B$$

effective signal states



Bennett, Brassard, Mermin Phys. Rev. Lett. **68** 557, 1992.

This scheme fixes ρ_A !

➔Entanglement based schemes and P&M schemes can be based on three-party entangled states!

Necessary condition for secure communication

Knowledge available to Alice and Bob:

•measurement POVM $\{A_i\}_i$, $\{B_j\}_j$
(may contain imperfections!)

•observed joint probability distribution P(A,B)

•[red. density matrix ρ_A (P&M schemes)]

Theorem (Entanglement Based and P&M):

• If P(A,B) together with $\{A_i\}_i$, $\{B_j\}_j$ [and ρ_A for P&M schemes] allows interpretation as separable state then $I(A;B\downarrow E) = 0$, and therefore $C_S = 0$.

M. Curty., M. Lewenstein and N. L, quant-ph/0307151.

Theorem: (converse)

• $I(A;B\downarrow E) > 0$
iff P(A,B) together with $\{A_i\}_i$, $\{B_j\}_j$ cannot be interpreted as coming from a separable state.

-A. Acín and N. Gisin, quant-ph/0310054.

NOTE: does *not* guarantee a secret key …

Observation of quantum correlation excludes intercept/resend attack!

Approach allows for realistic implementations!
-detection inefficiency goes into $\{B_j\}_j$
-full mode description of sender and receiver

Entanglement verification

Problem structure:

- Unknown density matrix ρ_{AB}
- constraints via observed correlations (data) P(A,B)
  [for P&M schemes: fixed ρ_A]
- **Question:** any separable ρ_{AB} compatible with constraints?

Specific experiment and data:

search for entanglement proof (sufficient, not necessary)

- rule out separability e.g. via Bell inequality
- violation of local uncertainty relations [Hofmann, Takeuchi, PRA 68 032103 (2003)]
- numerical optimisation via entanglement witnesses [Eisert, Hyllus, Gühne, Curty, quant-ph/040713

Specific experiment:

- general efficient numerical method for any possible data?
- find analytic complete necessary and sufficient condition for any possible data
  - ➔ approach in following part for simple qubit protocols

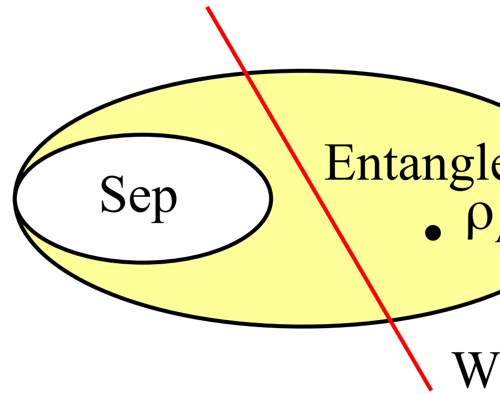
Entanglement Witnesses

Entangled States: ρ_{AB} is entangled iff $\rho_{AB} \neq \sum_i p_i \, |a_i\rangle\langle a_i|_A \otimes |b_i\rangle\langle b_i|_B$

Entanglement Witnesses (EW):

- ρ_{AB} is entangled iff $\exists$ W hermitian such that:

$$\boxed{\begin{array}{l} \mathrm{Tr}\{W\cdot\rho_{AB}\} < 0 \\ \mathrm{Tr}\{W\cdot\sigma_{AB}\} \geq 0 \;\; \forall \; \sigma_{AB} \text{ separable} \end{array}}$$

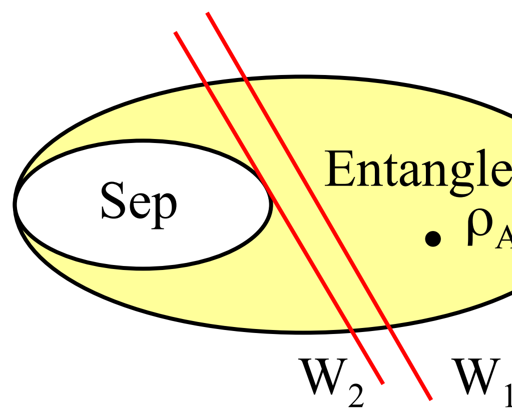


-M. Horodecki, P. Horodecki and R. Horodecki, Phys. Lett. A **223**, 1 (1996).

-M.B. Terhal, Phys. Lett. A **271**, 319 (2000).

Optimal EW (OEW):

-M. Lewenstein, B. Kraus, J.I. Cirac and P. Horodecki, PRA **62**, 052310 (2000).



Local Measurement of Entanglement Witnesses

Decomposition of Witnesses in Local Measurements:

Any bipartite hermitian operator W can be decomposed as a *pseudo-mixture*:

$$W = \Sigma_{ij}\, c_{ij}\, A_i \otimes B_j \qquad \text{with} \qquad c_{ij} \in \Re,\ \ \Sigma_{ij}\, c_{ij} = 1$$

where $A_i \otimes B_j$ forms a POVM operator basis.

$\Rightarrow$ $\{A_i\}_i$, $\{B_j\}_j$ describe measurements (positive, add up to identiy)

Evaluation:

Then: $$\boxed{Tr\{W \cdot \rho_{AB}\} = \Sigma_{ij}\, c_{ij}\, Tr\{A_i \otimes B_j\, \rho_{AB}\} = \Sigma_{ij}\, c_{ij}\, P(a_i, b_j)}$$

-A. Sanpera, R. Tarrach and G. Vidal, PRA **58**, 826 (1997).
-O. Gühne, P. Hyllus, D. Bruss, A. Ekert, M. Lewenstein, C. Macchiavello and A. Sanpera, PRA **66**, 062305 (2002).
-O. Gühne, P. Hyllus, D. Bruss, A. Ekert, M. Lewenstein, C. Macchiavello and A. Sanpera, J. Mod. Opt. **50** (6-7), 1079 (2003).

Necessary condition based on entanglement witnesses

Theorem:

• Given a set of local operations with POVM elements $A_i \otimes B_j$ together with the probability distribution of their ocurrence, P(A,B), then the correlations P(A,B) cannot lead to a secret key via public communication unless one can prove the presence of entenglement in the (effectively) distributed state via an entanglement witnesses $W = \sum_{ij} c_{ij} A_i \otimes B_j$ with c_{ij} real such that $\mathrm{Tr}\{W\sigma_{AB}\} \geq 0$ for all separable states σ_{AB} and $\sum_{ij} c_{ij} P(i,j) < 0$.

-M. Curty, M. Lewenstein and N. L., Phys. Rev. Lett. **92**, 217903 (2004).

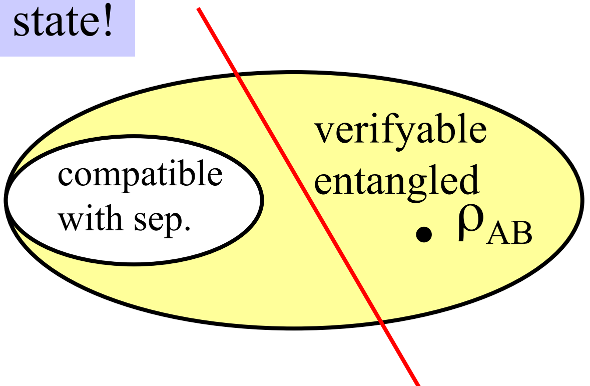
Important point:

entanglement witness criterion is necessary and sufficient even for restricted knowledge about the shared quantum state!

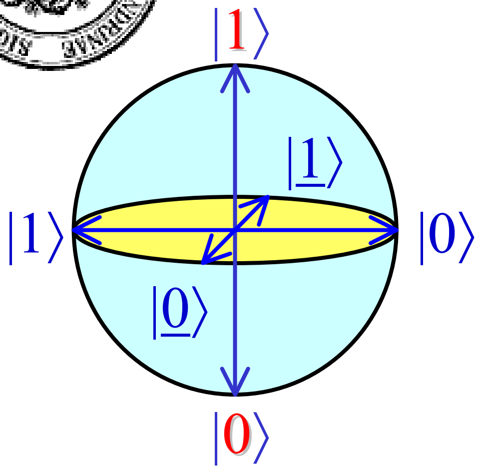
Idea:

states with verifiable entanglement form a convex set

➔restricted class of witnesses can testify the verifiable entanglement



6-State QKD protocol



Use three mutually unbiased bases:
e.g. X,Y,Z direction in Bloch sphere

- Bruß, Phys. Rev. **81**, 3018 (1998);
- Bechmann-Pasquinucci et al, PRA **59**, 4238 (1999) .

6-State (EBS and P&M) EW:

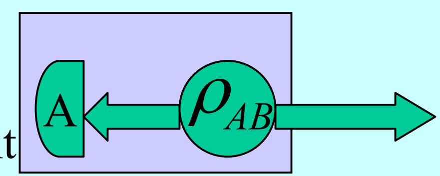
$$W_6 = \sum_{ij} c_{ij}\, \sigma_i \otimes \sigma_j$$

with $\mathbf{i,j} = \{\mathbf{0,x,z,y}\}$, and $\boldsymbol{\sigma_0} = \mathbf{1}$.

- Include all Optimal DEW: $W = |\psi_e\rangle\langle\psi_e|^{T_B}$
- All entangled states can be detected.

Simplified thought experiment:
use two-qubit state:

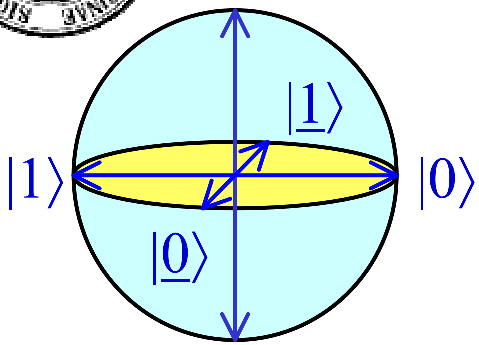
X, Y or Z
measurement



max. ent. 2x2 state

Searching for quantum correlations:
- parametrize $|\psi_e\rangle$
- evaluate locally $\mathrm{Tr}[\rho\, |\psi_e\rangle\langle\psi_e|^{T_B}]$
- search for negative expectation values

4-State QKD protocol



Use two mutually unbiased bases:
e.g. X,Z direction in Bloch sphere

-C.H. Bennett and G. Brassard, Proc. IEEE Int. Conf. On Computers, System and Signal Processing, 175 (1984).

4-State (EBS) EW:

$$W_4^{EBS} = \sum_{ij} c_{ij}\, \sigma_i \otimes \sigma_j$$

with $\mathbf{i,j = \{0,x,z\}}$, and $\boldsymbol{\sigma_0 = 1}$.

➔ restricted class of witnesses

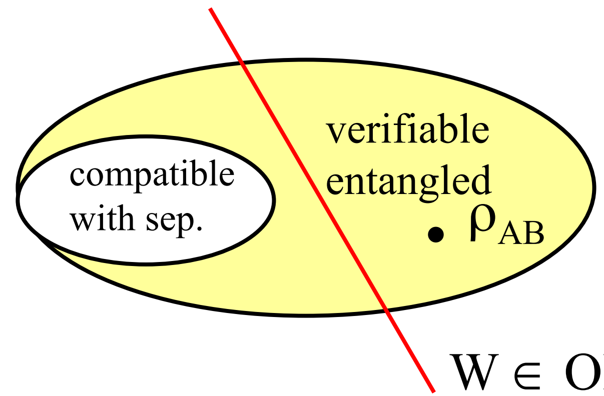
Observation:

$$W \in W_4^{EBS} \;\text{ iff }\; W = W^T = W^{T_B}$$

- Alice and Bob cannot evaluate Optimal DEW.
- Not all entangled states can be detected.

4-State QKD protocol

Optimal W_4^{EBS} (OEW_4)



$W \in OEW_4^{EBS}$

Observation:

Given $W \in W_4^{EBS}$
necessary to detect entanglement in state ρ_{AB} is that the operator

$$\Omega = \rho_{AB} + \rho_{AB}^{T} + \rho_{AB}^{T_B} + \rho_{AB}^{T_A}$$

is a non-positive operator.

Theorem: The EW that are optimal within the four-state protocol are given by

$$\boxed{OEW_4^{EBS} = \tfrac{1}{2}(Q + Q^{T_B})}$$

with $Q = |\psi_e\rangle\langle\psi_e|$ such that $Q = Q^T$

-M. Curty., M. Lewenstein and N. L., quant-ph/0307151.

- OEW_4^{EBS} provides necessary and sufficient conditions for detection of quantum correlations in P(A,B).
- For P&M schemes we find $OEW_4^{P\&M} = OEW_4^{EBS}$

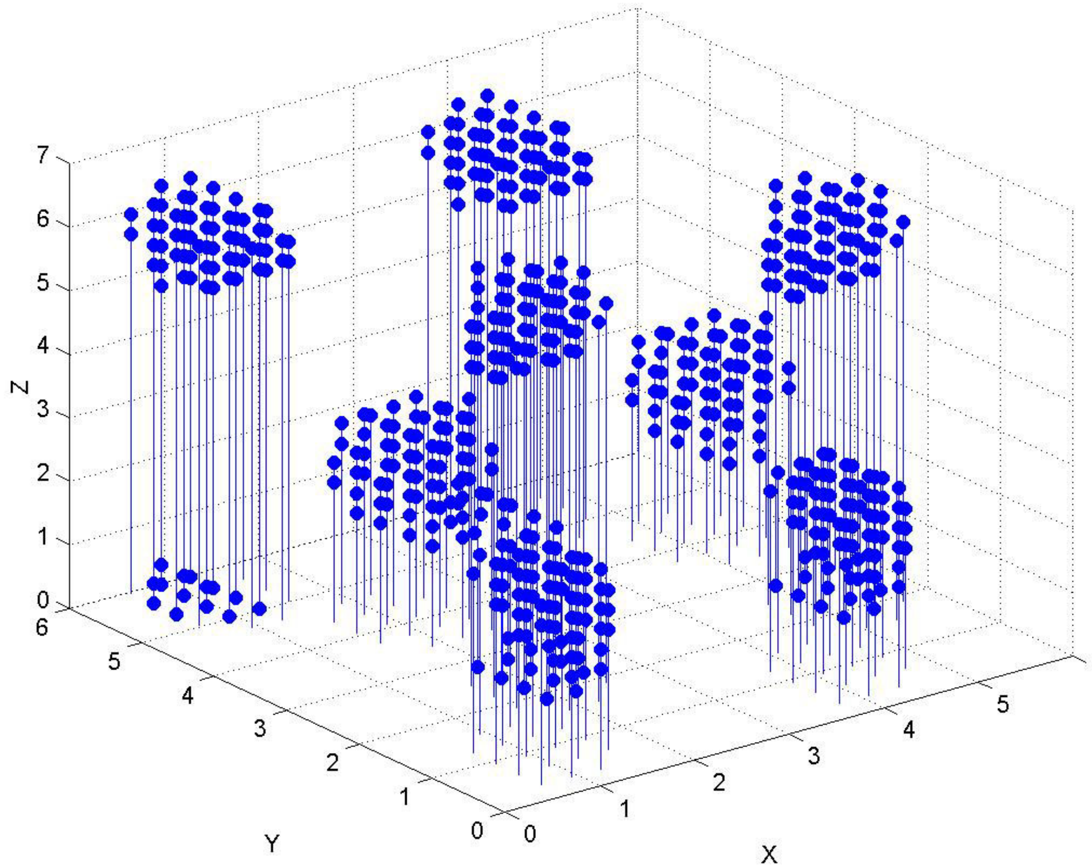
Quantum Correlations? (II)

Assumptions: (BB84 setup)
trusted ideal source
trusted ideal detector

Probability Distribution P(A,B)

A\B	0	1	+	-
0	0.07987	0.04516	0.00913	0.11591
1	0.04508	0.07986	0.11593	0.00901
+	0.11599	0.00909	0.08001	0.04507
-	0.00897	0.11593	0.04505	0.07985

Error Rate: 36 %



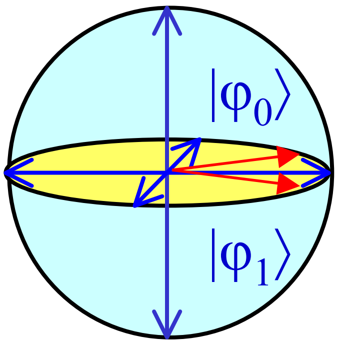
(only parameter combinations leading to negative expection values are marked)

Witness Class:

$$OEW_4^{EBS} = \tfrac{1}{2}\left(|\psi_e\rangle\langle\psi_e| + |\psi_e\rangle\langle\psi_e|^{T_B}\right)$$

$$|\psi_e\rangle = \cos(X)|00\rangle + \sin(X)(\cos(Y)|01\rangle + \sin(Y)(\cos(Z)|10\rangle + \sin(Z)|11\rangle))$$

2-State QKD protocol



Use two non-orthogonal states, e.g., $|\varphi_0\rangle$ and $|\varphi_1\rangle$

-C.H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

2-State EW:

$$W_2 = \sum_i c_i\, \sigma_0 \otimes \sigma_i + \sum_j c_j\, \sigma_z \otimes \sigma_j + \sum_k c_k\, \sigma_k \otimes \sigma_0$$

with **i,j = {x,z}**, **k = {0,x,z,y}**, and $\boldsymbol{\sigma_0 = 1}$.

➔ restricted class of witnesses

Theorem: The family

$$\boxed{W_2 = |0\rangle\langle 0| \otimes A + |1\rangle\langle 1| \otimes B + x\, C(\theta)}$$

with $A = A^T$, $B = B^T$, $A \geq 0$, $B \geq 0$, rank(A) = rank(B) =2, $\theta \in [\,0, 2\pi\,)$, and

$$\boxed{x = \min_{|\phi\rangle} \left(\langle\phi|A|\phi\rangle\langle\phi|B|\phi\rangle\right)^{1/2}}$$

is sufficient to detect all entangled states that are detectable in the 2-state protocol.

-M. Curty., O. Gühne, M. Lewenstein and N. L, (*in preparation*).

Conclusion

nterface Physics – Computer Science:

Classical Correlated Data with a Promise

ecessary condition for secure QKD is the proof of presence of quantum correlations

uantum correlations: for entanglement based <u>and</u> prepare&measure schemes.

For experiments: show the presence of such entanglement

- no need to enter details of classical communication protocols
- prevents oversights in preliminary analyses
- one properly constructed entanglement proof (e.g entanglement witness) suffices

For theory:

- show in which situation quantum correlations are **sufficient** to generate secret key
- develop **figure of merit** (secrecy capacity) to measure secrecy potential of correlations.
- develop proper **entanglement proofs** for realistic experiments (for given measurements)
- develop **compact description for restricted class of entanglement witnesses** (allows effective search of quantum correlations)
- include **detection inefficiencies** into the witness construction