Quantum Key Distribution with Continuous Variables – beating the 3 dB loss limit

Christine Silberhorn, Gerd Leuchs

Quantum Information Processing Group

Norbert Lütkenhaus

Quantum Information Theory Group

Center of Modern Optics

University of Erlangen-Nürnberg

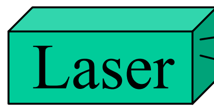
Timothy C. Ralph

University of Queensland, Brisbane

Overview

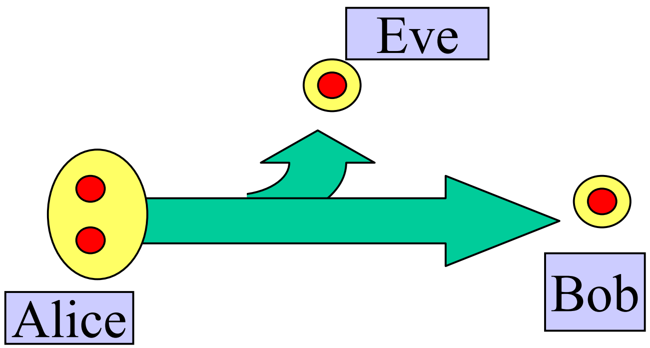
- losses & QKD: BB84 with weak coherent pulses
- ideas for better performance
- classical information theory background
- postselection in continuous variable schemes:
  beating the 3 dB loss limit

Realistic Signals and Loss (BB84)



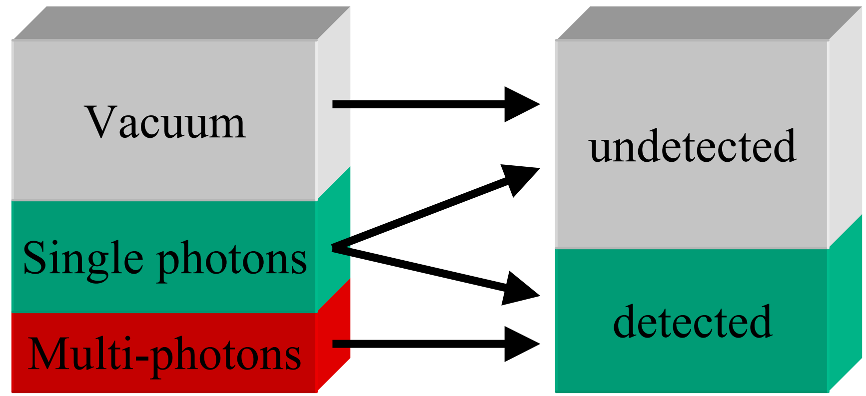
$$\rho = e^{-|\alpha|^2} \sum_{n=0}^{\infty} \frac{|\alpha|^{2n}}{n!} |n\rangle\langle n|$$

Multi-photon signals



- ➔Several copies of signal state
- ➔Eve can single out a copy
- ➔No errors are caused
- ➔Delayed measurement gives full information to Eve

Blocking Signals



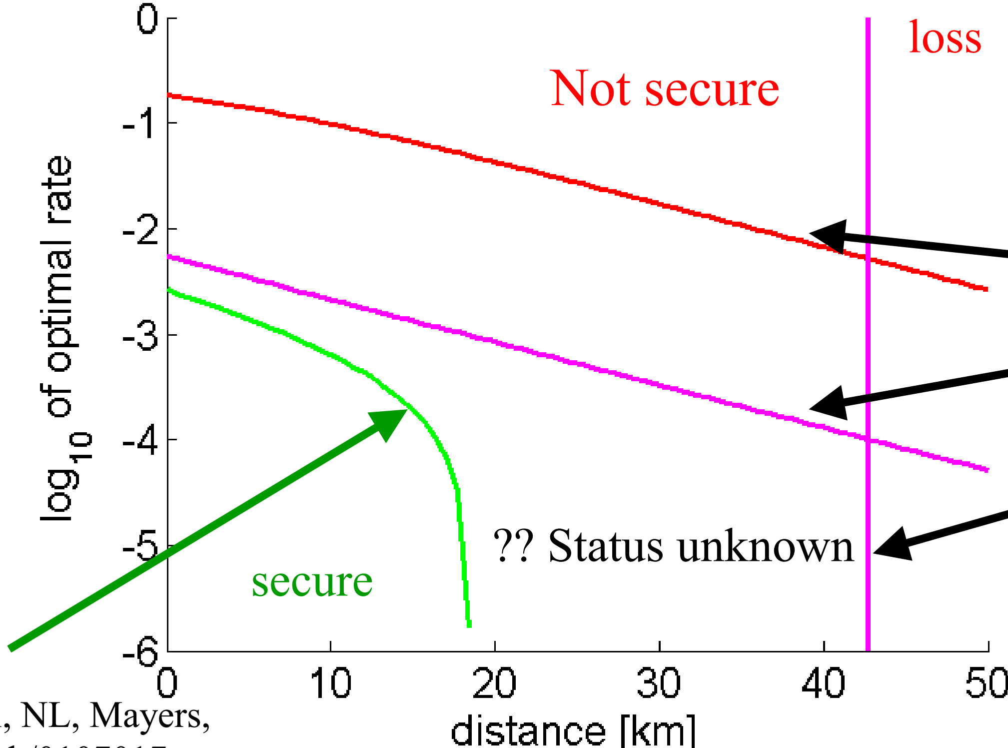
$$\boxed{G \leq \tfrac{1}{2}\left(p_{\exp} - p_{\text{multi}}\right)}$$

$p_{\exp}$ Detection probability of apparatus

p_{multi} Multi-photon probability of source

WCP security for BB84 protocol

Secure bits per time slot:



Bound on rate due to multi-photon signals and loss

$$G \leq \tfrac{1}{2}\left(p_{\exp} - p_{\text{multi}}\right)$$

NL, PRA **61**, 052304 (2000)

Loss in
- channel
- channel and receiver

$$G \approx \tfrac{1}{4}\eta^2$$

Bound on distance due to loss and darkcounts

$$e \frac{p_{\exp}}{p_{\exp} - p_{\text{multi}}} \leq \frac{1}{4}$$

Brassard, NL, Mor, Sanders, PRL **85,** 1330 (2000)

Inamori, NL, Mayers, quant-ph/0107017

Example: Bourennane et al, Opt. Express **4**, 383 (1999) [1.5 μm]

High photon number
➔ More multi-photon signals

Low photon number
➔ low rate

➔ optimal photon number

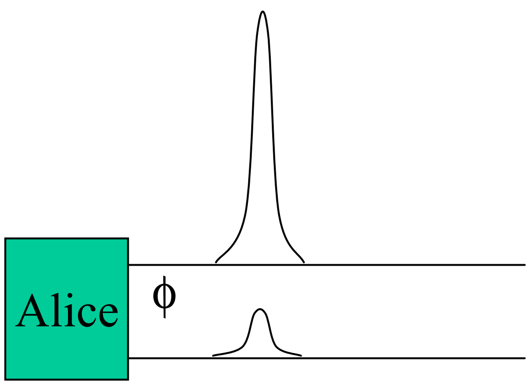
$$\mu \approx \eta_{\text{tot}}$$

Strong reference pulse schemes

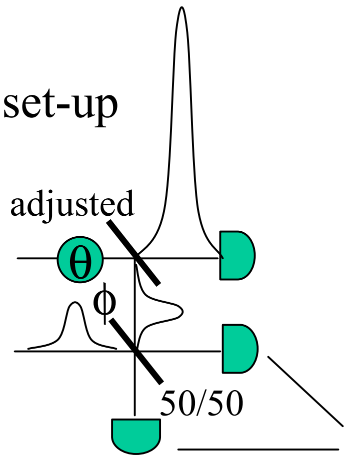
Basic idea:

Eve cannot block signals

Bennett (1992)



a) Monitor set-up



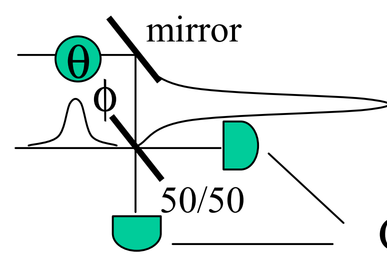
Classical photo-detector

Single-photon counter

Extension to BB84:

Huttner, Imoto, Gisin, Mor
PRA 51, 1863 (1995)

b) Homodyne measurement

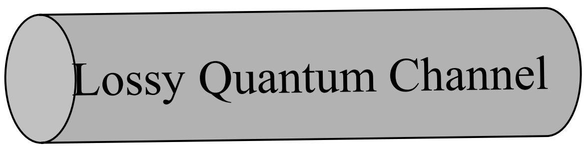


Hirano, Konishi, Namiki
quant-ph/0008037

Classical photo-detector

Eavesdropping attacks exploiting lossy channels

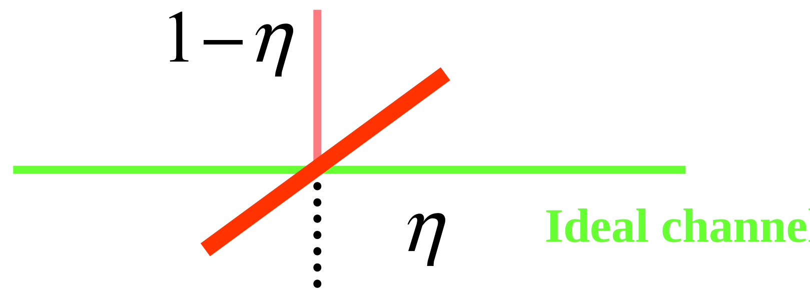
Lossy quantum channels ...



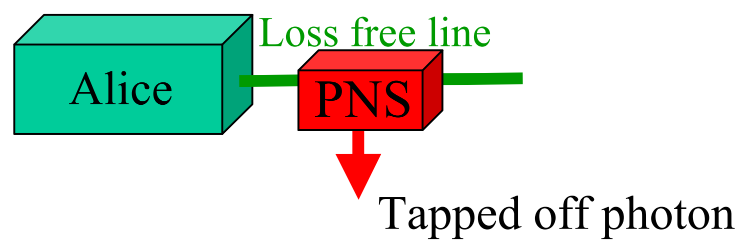
Transmission efficiency

... and their replacements

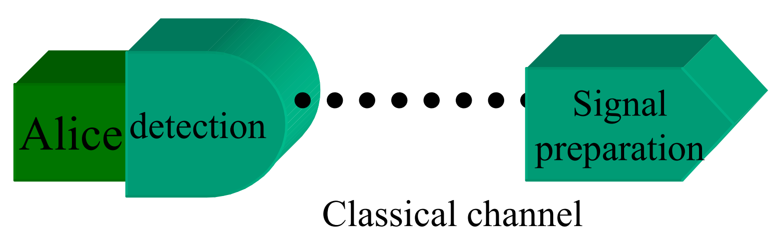
a) Beam-splitting



b) Photon number splitting

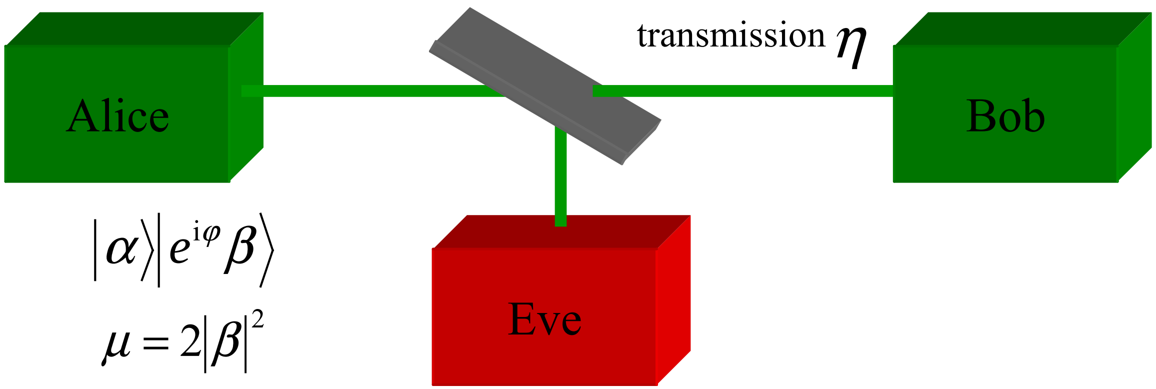


c) Classical channel



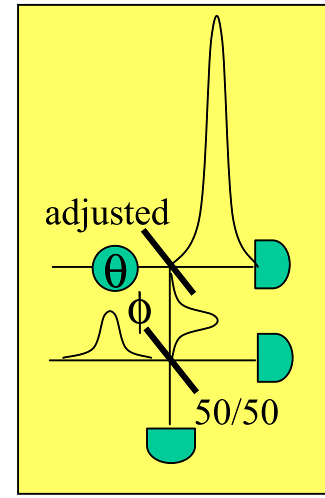
Choose quantum signals and measurements to narrow down possible channels to beam-splitting!

Beam splitting attack with strong reference pulse and monitor



$$|\alpha\rangle|e^{i\varphi}\beta\rangle$$

$$\mu = 2|\beta|^2$$



Example:
(weak laser pulses)

$$p_{\exp} = 1 - e^{-\eta\mu}$$

$$p_{split} = \left(1 - e^{-\eta\mu}\right)\left(1 - e^{-(1-\eta)\mu}\right)$$

$$G = \frac{1}{2}\left(p_{\exp} - p_{split}\right)$$

$$= \frac{1}{2}\left(1 - e^{-\eta\mu}\right)\ e^{-(1-\eta)\mu}$$

Gain rate positive for all values of μ and η !
➔optimal choice is
$\mu \approx 1$
➔ $G \approx \frac{1}{2}\eta$

Comparison:

standard WCP BB84	single photon BB84
$G \approx \frac{1}{2}\eta^2$	$G \approx \frac{1}{2}\eta$

Potential for Continuous Variable QKD

Properties of continuous variable QKD

•Source (strong laser pulses)

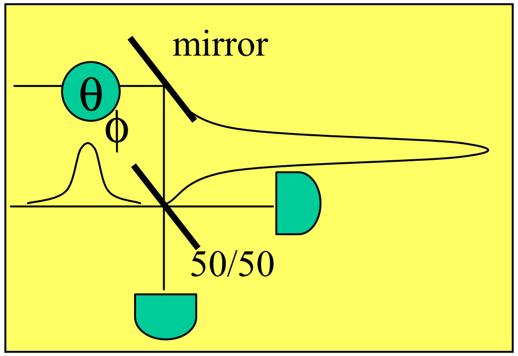
-unconditional

-fast (THz)

•Detection (intensity)

-Highest rates (> 10 Gb/s)

-high efficiency (>>90%)



Open problems:

• efficient protocols for high losses??
• full security protocols (but Gottesman/Preskill)

Basic Model of QKD protocols

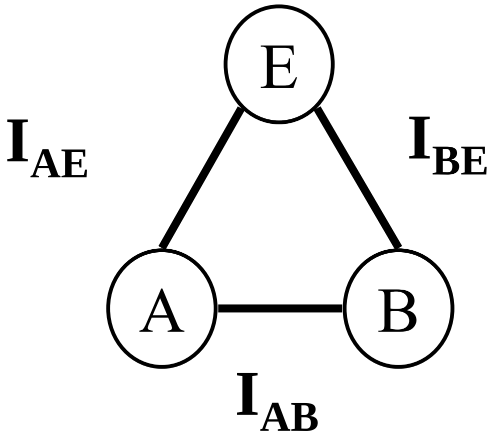
a) Quantum part makes available

1. knowledge of signal states $\{\rho_i\}_i$
2. knowledge of generalised measurement $\{F_k\}_k$
3. (via public communication) joint probability distributions $\Pr(i,k)$

b) Classical processing

1. Use quantum mechanics to infer possible distributions $\mathrm{P}(I_A, K_B, \rho_E)$ between the three parties:
   Alice (signals),
   Bob (measurements),
   Eve (auxiliary quantum system)
2. Use classical tools (e.g. error correction, privacy amplification) to generate secret key.

Key extraction from correlated classical data



Joint probability distribution

P(A, B, E)

Bounds on secrecy capacity C_S

U. M. Maurer, IEEE Trans. Inf.Theo. 39, 1733 (1993);

$$\boxed{C_S \le I_{AB\downarrow E}}$$

intrinsic information:
mutual information A-B given all
possible public announcements by E

Csiszar, Körner, IEEE, IT 24, 339 (1978).

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

biggest information gap

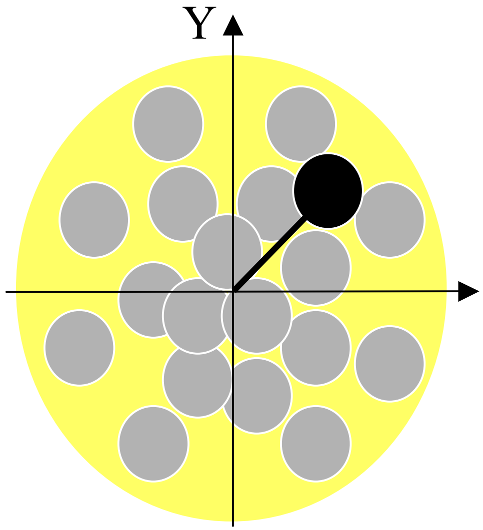
➔ secrecy capacity of entanglement breaking channel vanishes!

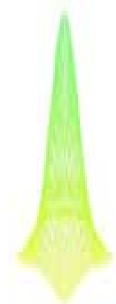
$$\left.\begin{aligned} p(a,b,e) &= p(a)\,p(e\,|\,a)\,p(b\,|\,e) \\ &= p(e)\,p(a\,|\,e)\,p(b\,|\,e) \end{aligned}\right\} \Rightarrow p(a,b\,|\,e) = p(a\,|\,e)\,p(b\,|\,e) \Rightarrow I_{AB|E} = 0$$

QKD with coherent states

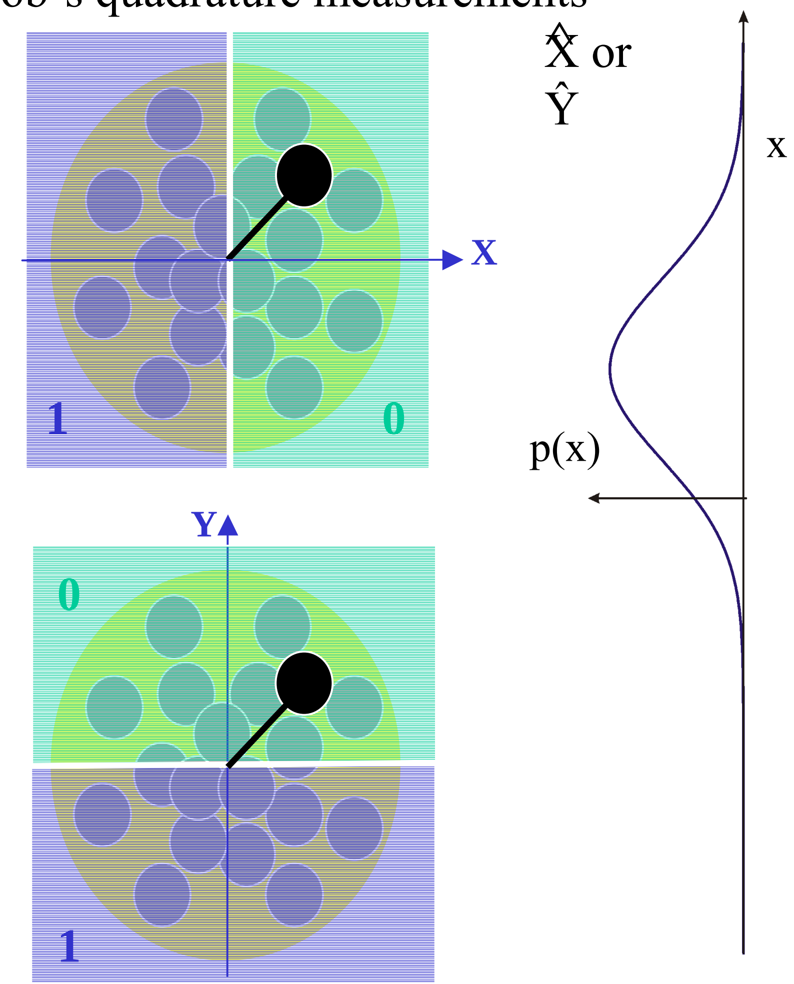
F. Grosshans, P. Grangier, Phys. Rev. Lett. 88, 057902 (2002).

Alice's state preparation

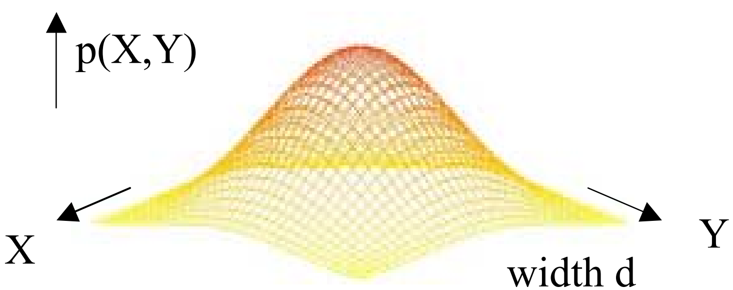




Bob's quadrature measurements



Gaussian distribution of complex amplitudes

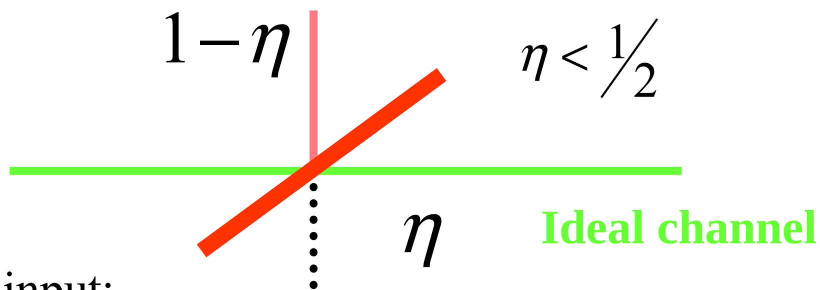


Implicit assumption: phase reference available to all parties!

Beam-splitting beyond 3 dB loss???

Eve receives better signals than Bob

$$\mathrm{I}_{\mathrm{AE}} > \mathrm{I}_{\mathrm{AB}}$$



beamsplitter does not entangle coherent state input:

$$|\alpha\rangle_S |0\rangle_E \to \left|\sqrt{\eta}\,\alpha\right\rangle_S \left|\sqrt{1-\eta}\,\alpha\right\rangle_E$$

$$I(B;E) \le I(A,B;E) = I(A;E) + \underbrace{I(B;E\,|\,A)}_{=0}$$

$$\Rightarrow I_{AE} \ge I_{BE}$$

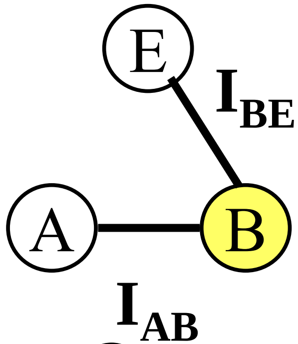
$$I(B;E) \le I(B;A,E) = I(A;B) + \underbrace{I(B;E\,|\,A)}_{=0}$$

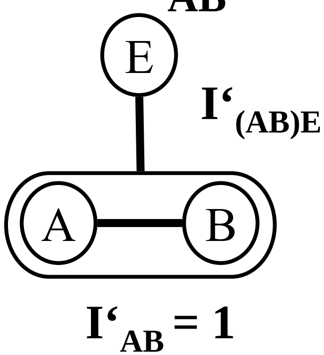
$$\Rightarrow I_{AB} \ge I_{BE}$$

$$\boxed{\mathrm{I}_{\mathrm{AE}} > \mathrm{I}_{\mathrm{AB}} \ge \mathrm{I}_{\mathrm{BE}}}$$

detection of information gap: $\mathrm{I}_{\mathrm{AB}} \ge \mathrm{I}_{\mathrm{BE}}$
Grosshans, Grangier, quant-ph/0204127)

Attaining Csiszar-Körner Bound





1) Bob's bit string defines key
2) Amount of required classical communication B➔A to allow Alice to correct her errors: (1-$\mathbf{I_{AB}}$) bits
3) Change of Eve's relevant information
   [C. Cachin, U.M. Maurer,IEEE Trans. Inf. Theo. 39, 1733 (1993).]
   $$I_{BE} \to I'_{(AB)E} < I_{BE} + (1 - I_{AB}) = 1 - (I_{AB} - I_{BE}) \qquad \boxed{I_{AB} > I_{BE}}$$
4) Privacy amplification:
   Shorten key by fraction τ $\qquad C_S = 1 - \tau = 1 - I'_{(AB)E}$

Requires one-way error correction➔not efficient??

Other error correction methods:

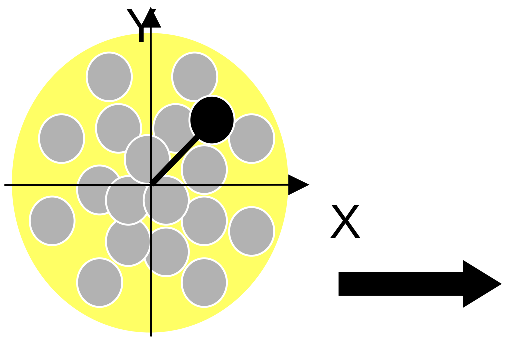
$$I_{AE} \to I'_{(AB)E} < \begin{cases} 1 - (I_{AB} - I_{AE}) & \text{A➔B} \\ 1 - (I_{AB} - I_{AE}) & \text{A🡐B} \\ 1 - (I_{AB} - I_{AE}) & \text{A⬄B} \end{cases}$$

(special case)

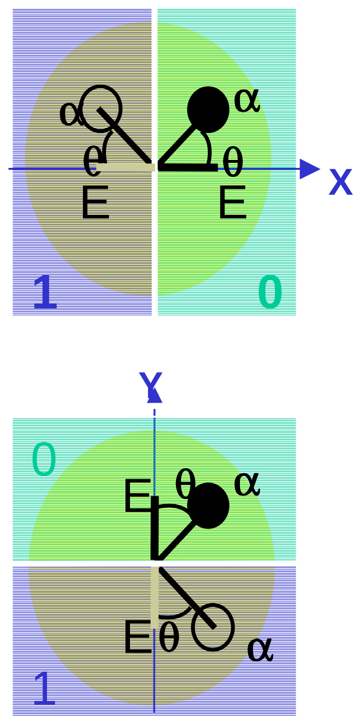
leaking of error positions in two-way:
here: conditional density matrix of Eve does not change in our cont. var. protocol!

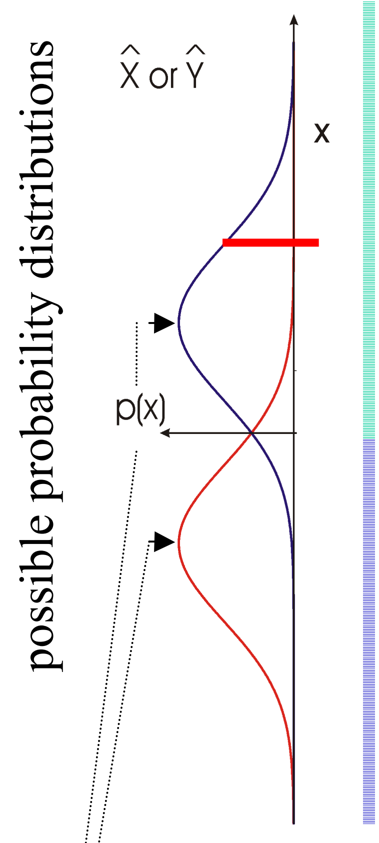
Quantum key distribution with coherent states: modified protocol

Alice‘s state preparation



Bob‘s measurements





measurement result x

publish |x|

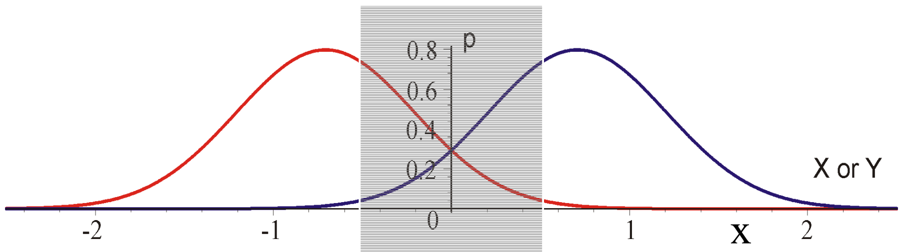
$\mathrm{Abs}(\,X_{max}\,) = E$ (public)

published parameter radius α, angle θ

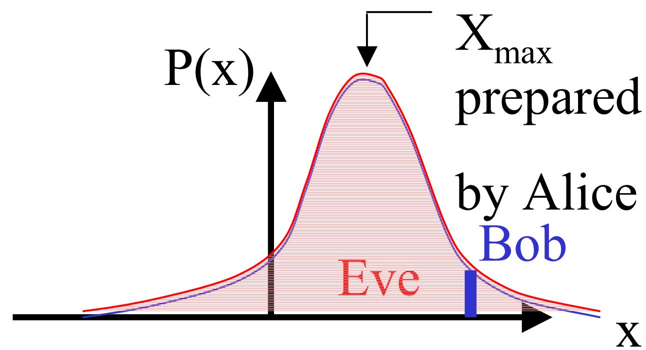
$\Rightarrow$ **$E = |\alpha \cos(\theta)|$**

Effective mix of channels, each described by (E,|x|)

Post-selection for continuous Variables



Product states for Bob and Eve:



basic idea for BB84
for weak signal and strong reference pulse

T. Hirano, T.Konishi, and R.Namiki,
quant-ph/0008037 (2000).

divide overall information into different *information channels*:

known parameters:
state preparation: $E = a \cos\theta$
measurement result: $|x|$

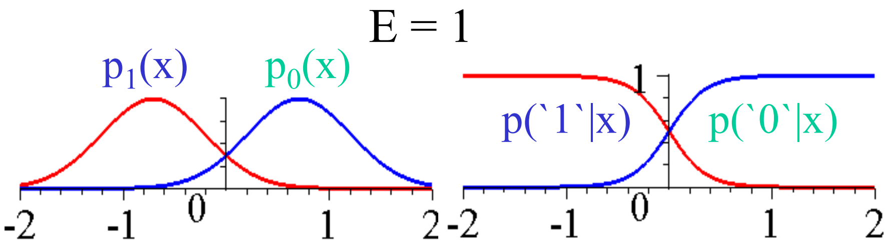
$$I^{tot} = \int_{|x|,E} p(|x|,E)\, I(|x|,E)\; d|x|\, dE$$

select information channels with

$$\mathbf{I_{AB}(|x|,E) \;>\; I_{AE}(|x|,E)}$$

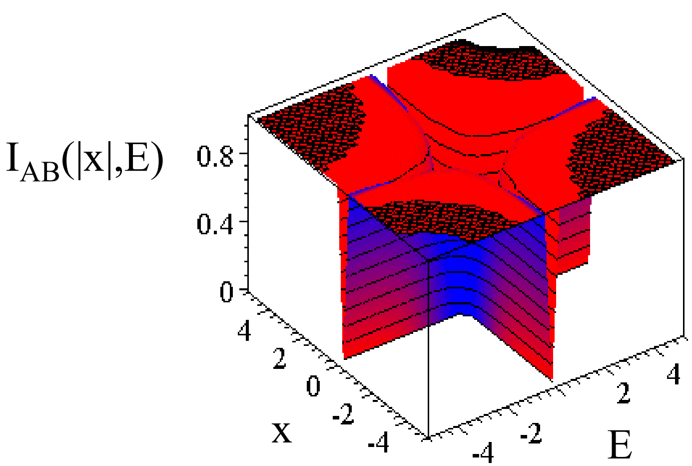
Mutual Information of Communicating Parties

Mutual information of Alice and Bob

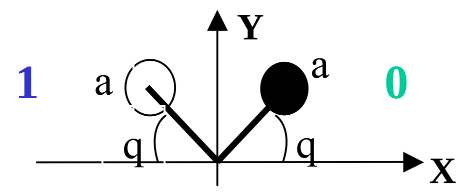


Shannon formula:

$$I_{AB}(|x|,E) = 1 + p_e \log_2 p_e + (1-p_e)\log_2(1-p_e)$$



Eve‘s accessible information

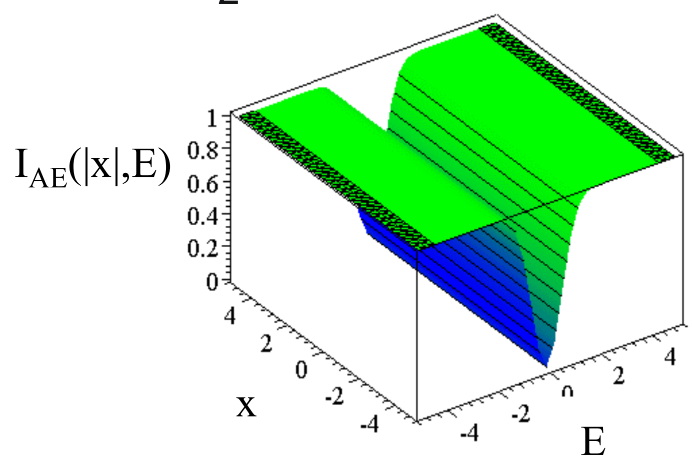


f: overlap of possible states

$I_{BE}(E) < I_{AE}(E)$

accessible information for pure states: *

$$I_{AE}(E) = \frac{1}{2}\left(1+\sqrt{1-f^2(E)}\right)\log_2\left(1+\sqrt{1-f^2(E)}\right) + \frac{1}{2}\left(1-\sqrt{1-f^2(E)}\right)\log_2\left(1-\sqrt{1-f^2(E)}\right)$$



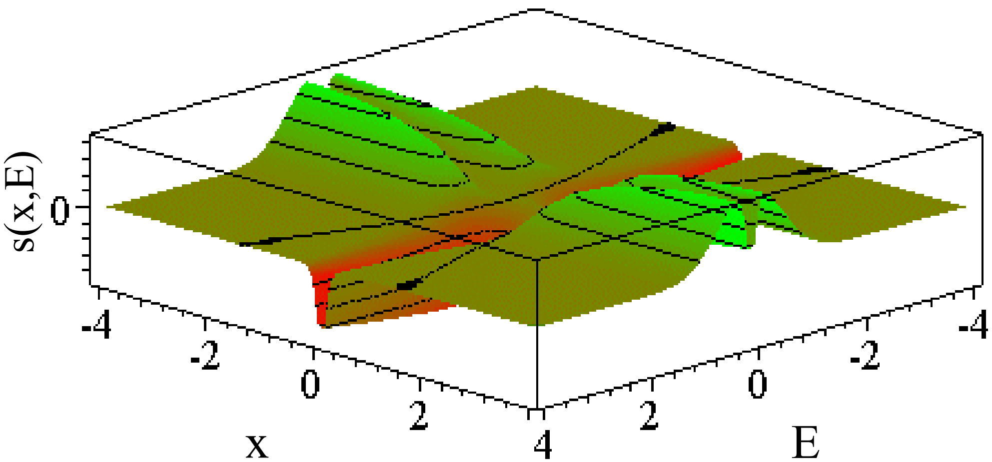
* L.B. Levitin (QCM 1995)

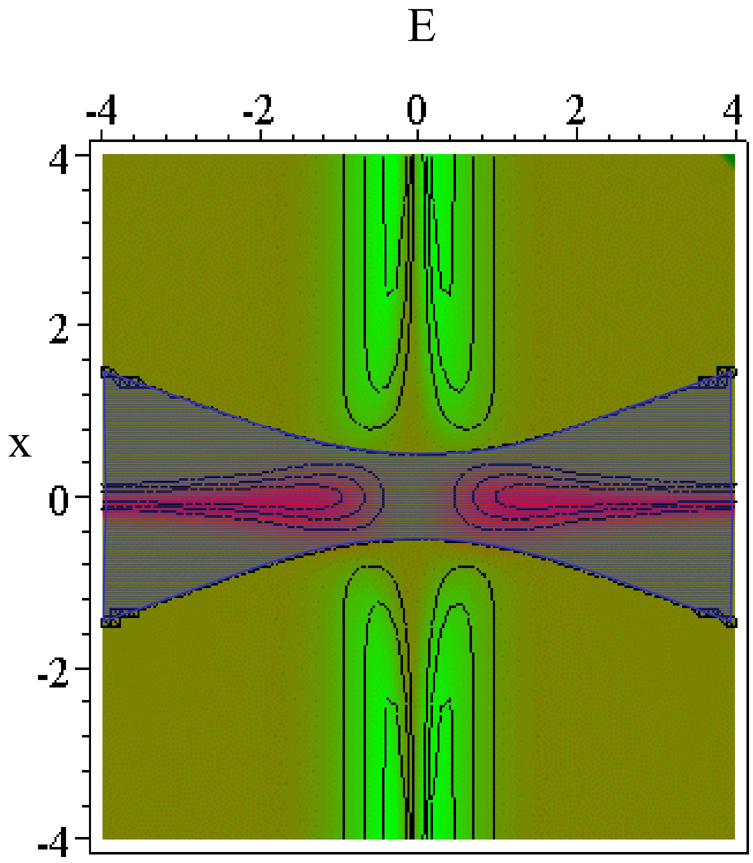
Selection of suitable channels

Comparison of the mutual information $I_{AB}(|x|,E)$ and $I_{AE}(|x|,E)$

$$\boxed{s(|x|,E) = I_{AB}(|x|,E) - I_{AE}(|x|,E)}$$

suitable channels for postselection: $s(|x|,E) > 0$



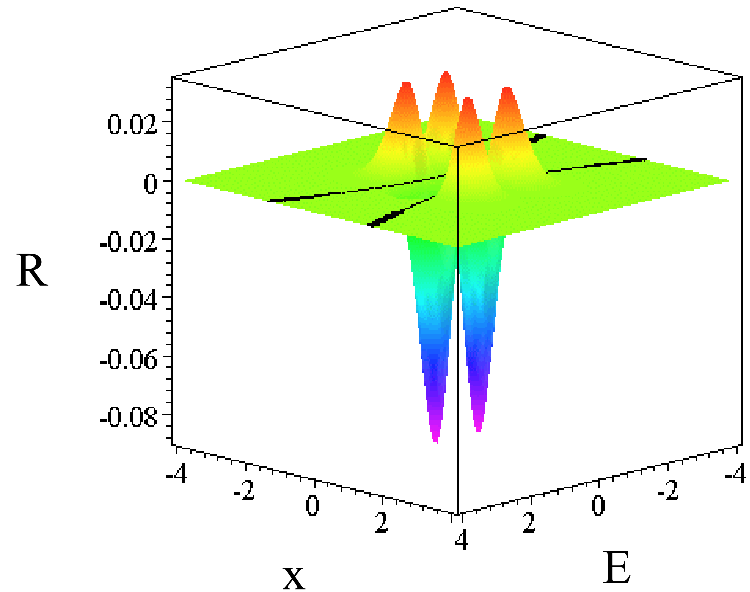


Estimate of bit rates

selected channels: $S=\{(x,E)\in \mathbf{R}^2 \mid s(x,E)>0\}$

$$R_k = R_r \times \int_S p(x,E)\cdot s(|x|,E)\, dx\, dE$$

with $p(x,E) = \sqrt{\frac{2}{\pi}}\, e^{-2E^2/d}\ \frac{1}{2}\cdot\left(p(x|'0') + p(x|'1')\right)$



for optimized parameter d = 2,1:

$R_k \approx 0{,}0667 \times R_r$

Key rate ~ 7% of raw rate at 3 dB loss

Not optimized over distribution of coherent states ...
Maybe- only four states???? (enough to restrict to beamsplitting?????)

Conclusions

- QKD with weak laser pulses unconditionally secure (BB84),

  rate scales as $G \approx \frac{1}{2}\eta^2$

- BB84 with strong reference pulse: expect $G \approx \frac{1}{2}\eta$

- single photon detection slow ➔ continuous variable QKD (fast detection)

- coherent state QKD with practical schemes (two-way error correction)

  without apparent loss limit

  (no rigerous security proof yet)

- rate needs optimization of protocol

- improvement for squeezed and entangled states?

  see D. Gottesman, J. Preskill, PRA 63, 022309 (2001)

Need clean analysis of optimal protocols based on basic correlations from prepare&measure scheme in QKD!