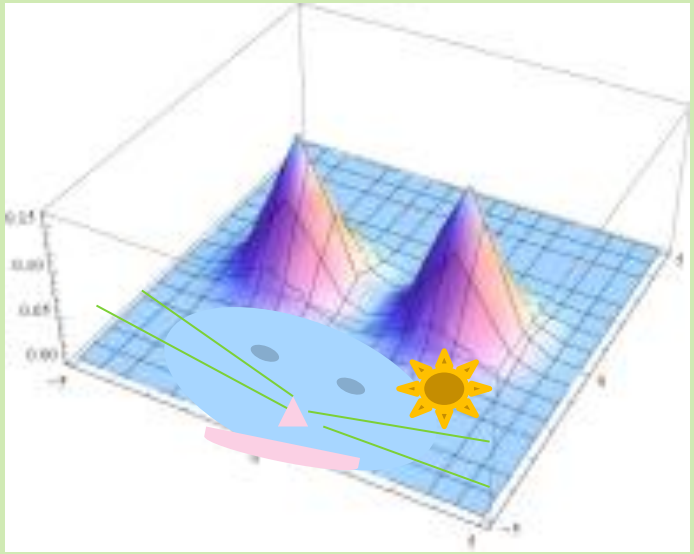
Bit Commitment with Quantum Continuous Variables

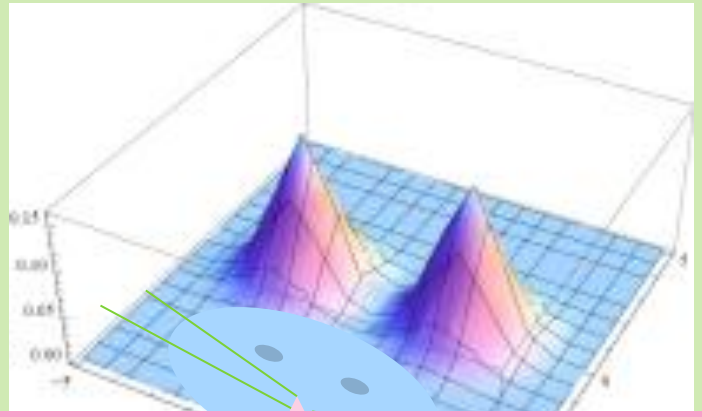
Aikaterini Mandilara



Paris 11 **Paris 7**

Bit Commitment with Quantum Continuous Variables

(a) with entanglement
(b) or without



(a) A. Mandilara and N.Cerf
PRA 85,062310 (2012)

ULB, Brussels QuIC

(b) A. Mandilara, E. Diamanti and D. Markham

TELECOM ParisTech

Game (Blum81)
2 untrustful parties
Commit Phase: One of the parties commit to either 0 or 1
…
Reveal Phase: Announcement and verification from the other party

Bit Commitment (the idea)

A

B

a={0 ,1}

a={0 ,1}

No Binding!

b=0,1

a=0 : I won!!

Did you?

Bit Commitment (the idea)

a={0 ,1}

No good Concealing!

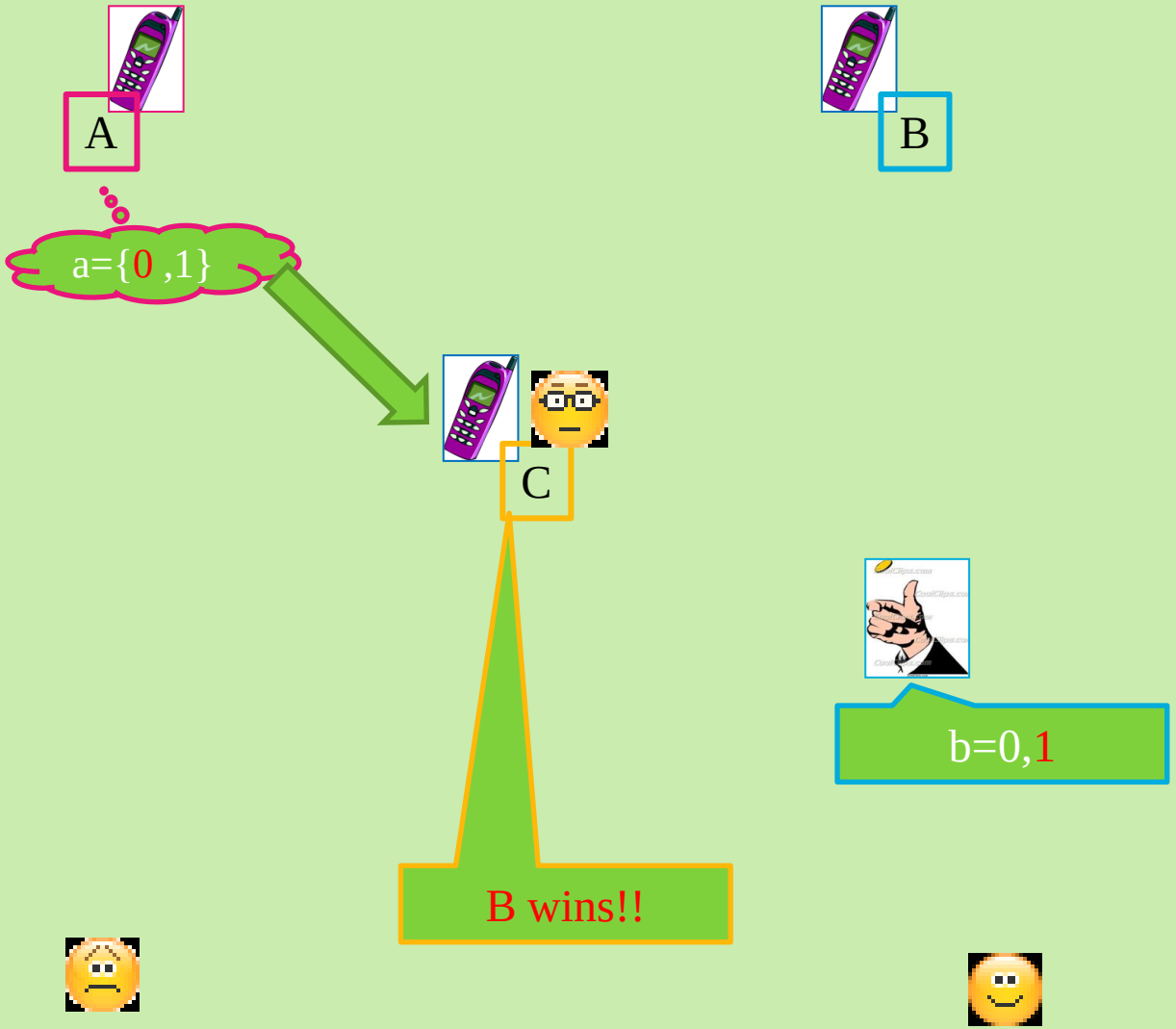
b=0,1

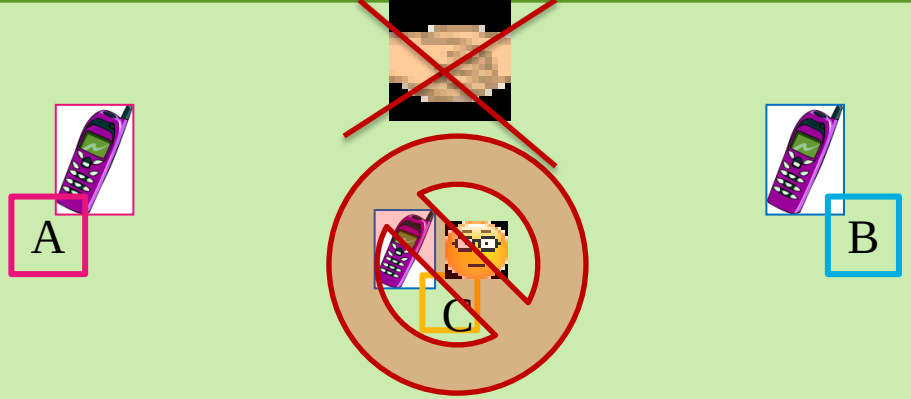
a=0

Did you?

I won!!

Bit Commitment (the idea)





In a Classical world:
Bit Commitment is impossible

In a Quantum world:
Bit Commitment is impossible

	Statist. Secure
Binding	X
Concealing	X

- Mayers (1996)
- Lo, Chau (1996)
- .....
- D'Ariano, Kretscmann, Sclingenmann, Werner (2007)

Naor (1991)
Ostrovsky (1992)

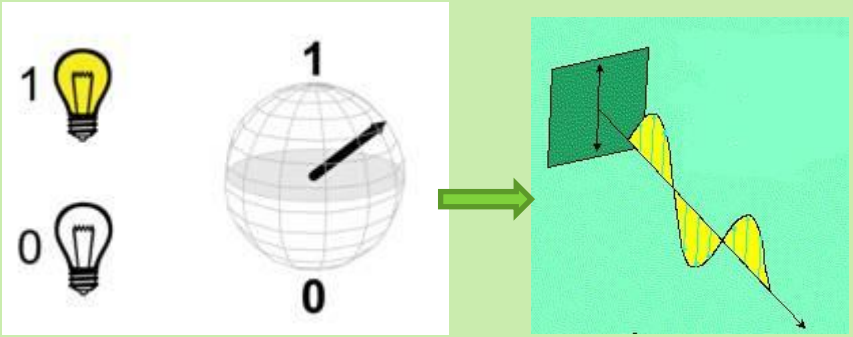
Brassard, Chaum, Crepeau (1988)
Halevi (1995)
Halevi, Micali (1996)

In a Classical world:
Bit Commitment is possible
Under assumptions

tive one-way functions,.. Pseudorandom number generator..

	Statist. Secure	Comput. Secure	Statist. Secure	Comput. Secure
Binding	X			X
Concealing		X	X	

In a Classical world:
Bit Commitment is possible
Under assumptions



In a Quantum Qubit world
Bit Commitment is possible
Under Superselection Rules
DiVincenzo, Smolin, Tehral (2004)

In a Quantum world
(infinite dim Hilbert space) can we build a
Secure Bit Commitment
under some assumptions?

- One way or many rounds
- Purification Protocols (use of entanglement)
- BB84 type (without entanglement)
- Fault-tolerant ones (no need of quantum memory)
- etc

One way +entanglement

A

B

$|\chi_{0,1}\rangle = \sum_{i,j} c_{i,j}^{0,1} |i\rangle_A \otimes |j\rangle_B$

$\langle \chi_0 | \chi_1 \rangle = 0$

$|\Psi_?\rangle$

$\rho_B^{0,1}$

Commit Phase

$(U_A^{\max} \otimes 1)$ $\rho_A^{0,1}$ $(U_A^{\max +} \otimes 1)$

$\rho_B^{0,1}$

$\rho_A^{0,1}$

Unveil Phase

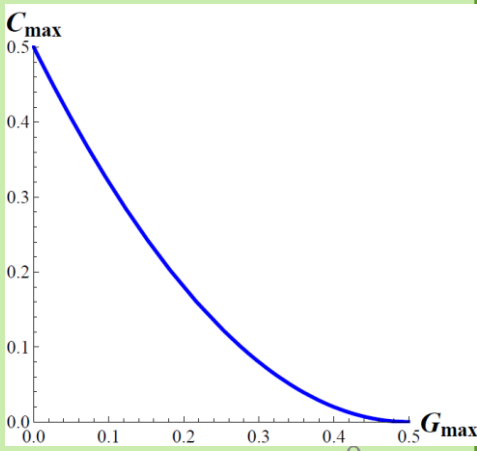
$X = \varepsilon_0 |\chi_0\rangle\langle\chi_0| + \varepsilon_1 |\chi_1\rangle\langle\chi_1| + \ldots$

Security of the protocol

Max(**Pa**)-0.5: Cmax : *Uhlmann's theorem*

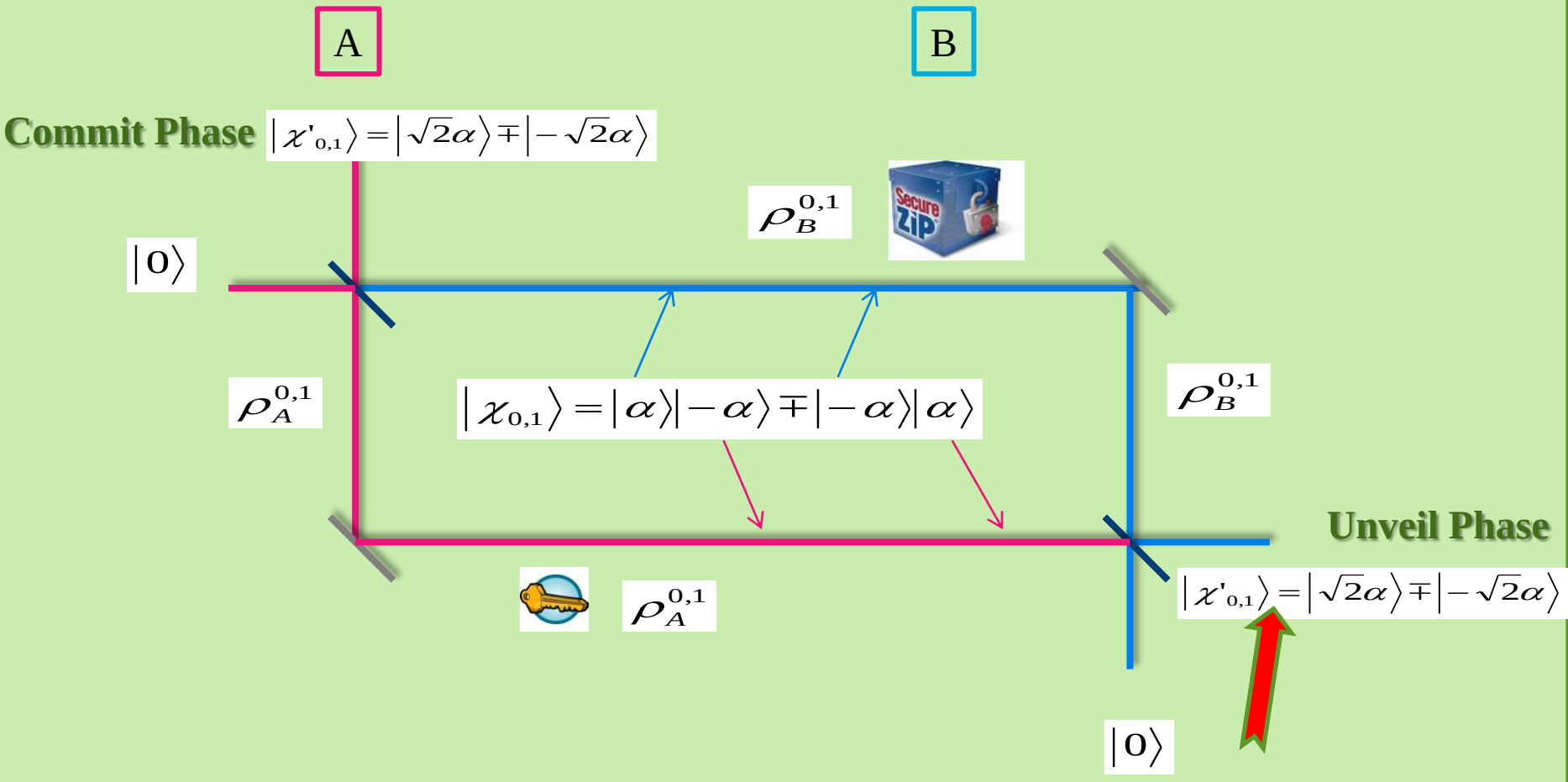
Max(**Pb**)-0.5: Gmax: $\frac{1}{2} Tr|\rho_B^0 - \rho_B^1|$

Perfect	Broken
0	0.5
0	0.5



Spekkens and Rudolph (2001)

Our protocol -Basic Unit

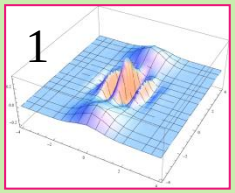


Photon Counting n: $\hat{\mathbf{P}} = (-1)^n$

Odd: 0

Even: 1

Our protocol-In phase-space



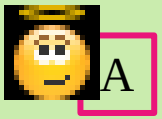
$\alpha = 3/2$

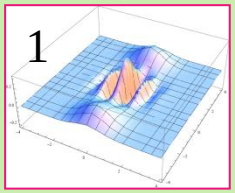
$\alpha_{cat} = 3/\sqrt{2}$

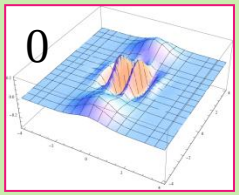
$|\alpha\rangle = \exp\left[\alpha \hat{a}^{+} - \alpha^{*}\hat{a}\right]0\rangle$

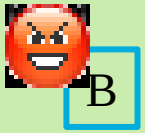
$W(x,y) = \frac{1}{\pi}\exp\left[-\left(x-\sqrt{2}\alpha\right)^2 - p^2\right]$

Best Bob's cheating

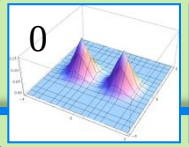


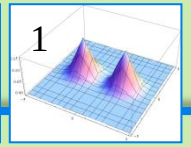


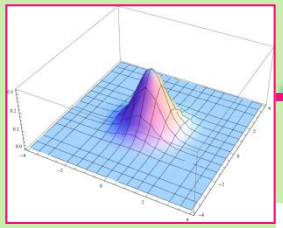




Commit Phase



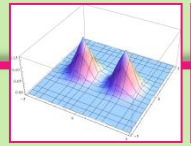


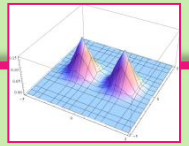


$\rho_A^{0,1}$

$|\chi_{0,1}\rangle = |\alpha\rangle|-\alpha\rangle \mp |-\alpha\rangle|\alpha\rangle$

$\rho_B^{0,1}$



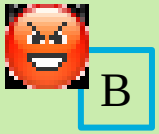


$|\chi'_{0,1}\rangle = |\sqrt{2}\alpha\rangle \mp |-\sqrt{2}\alpha\rangle$

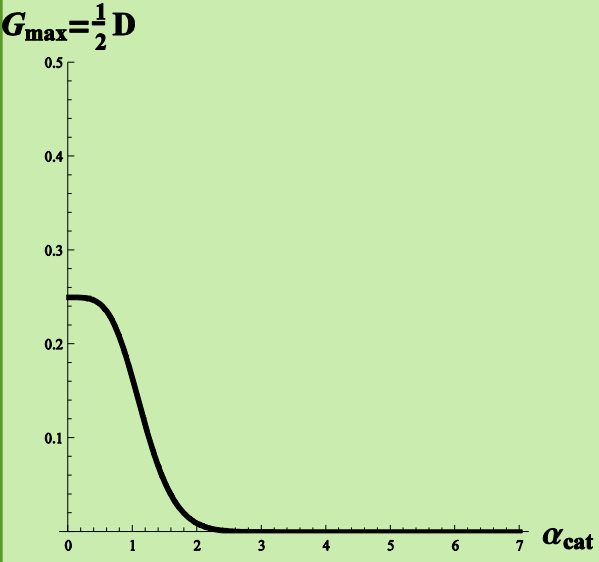
Unveil Phase

$|0\rangle$

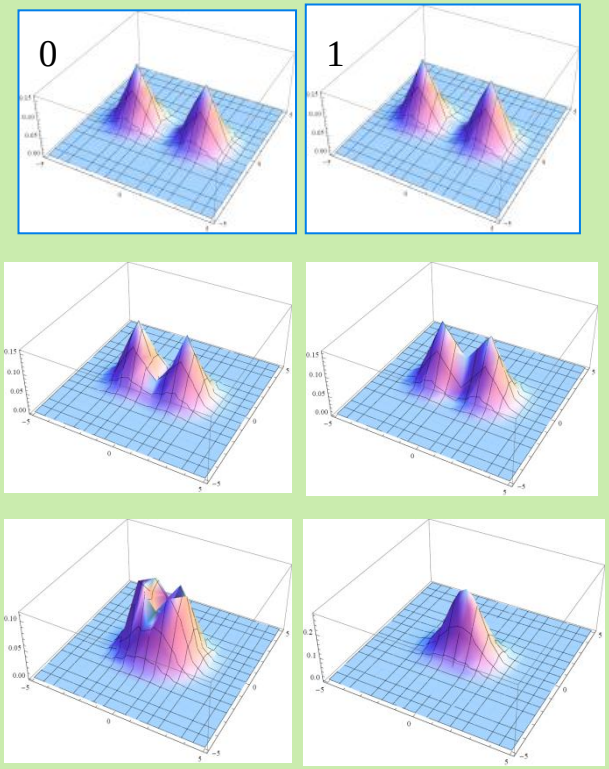
Best Bob's cheating



$$D(\rho_B^0, \rho_B^1) = \frac{1}{2} Tr|\rho_B^0 - \rho_B^1| \propto \exp(-2\alpha^2)$$



ρ_B^0 ρ_B^1



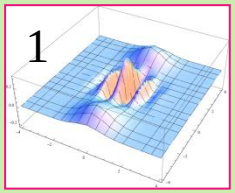
$$|\chi'_{0,1}\rangle = |\sqrt{2}\alpha\rangle \mp |-\sqrt{2}\alpha\rangle$$

$\alpha_{cat} = 2$

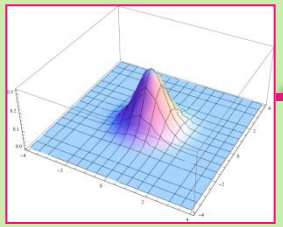
$\alpha_{cat} = 1.4$

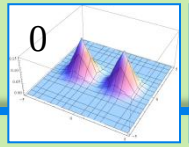
$\alpha_{cat} = 0.7$

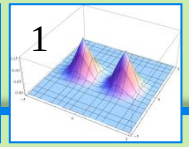
Best Alice's cheating in the hold phase



Commit Phase





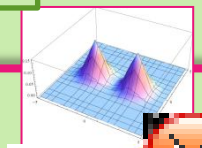


ρ_B^1

ρ_A^1

$|\chi_1\rangle = |\alpha\rangle|-\alpha\rangle + |-\alpha\rangle|\alpha\rangle$

Hold Phase



$|\chi'_{0,1}\rangle = |\sqrt{2}\alpha\rangle \mp |-\sqrt{2}\alpha\rangle$

Photon Counting n:

Odd: 0

Even: 1

$|0\rangle$

Assumption:

Non-Gaussian operations=

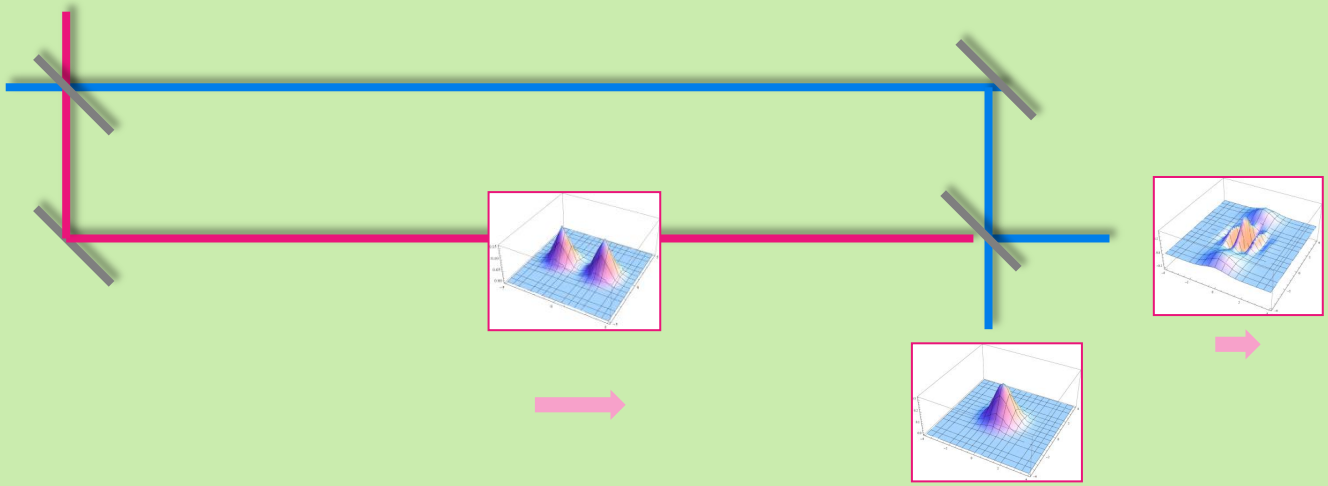
Probabilistic Operations

Best Deterministic cheating/Gaussian Cheating

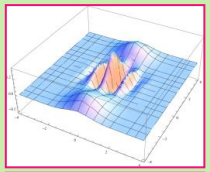
Best Gaussian Cheating strategy?

- Displacement
- Rotation
- Squeezing

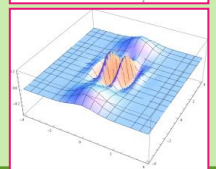
$$\left\langle \hat{P} \right\rangle = \pi W(0,0)$$



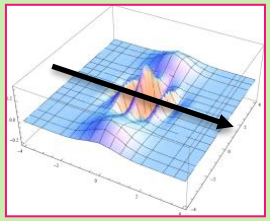
$\left\langle \hat{\mathbf{P}} \right\rangle = 1$ $\quad W(0,0) = \frac{1}{\pi}$



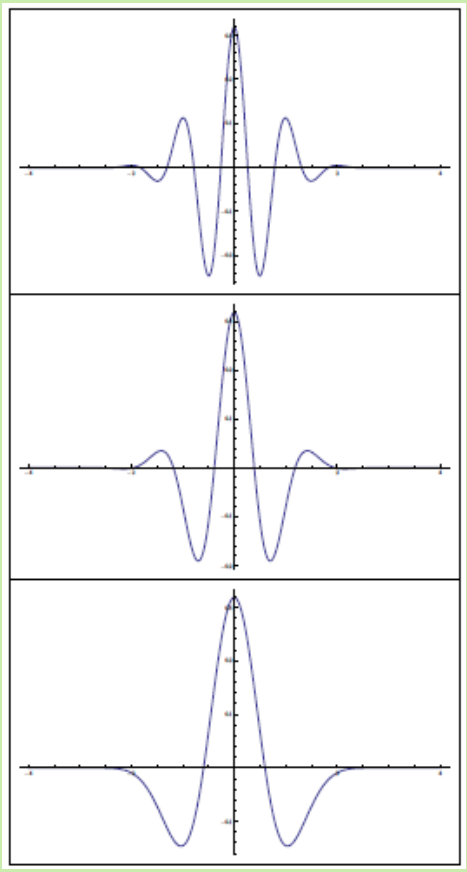
$\left\langle \hat{\mathbf{P}} \right\rangle = -1$ $\quad W(0,0) = -\frac{1}{\pi}$



Best Gaussian Cheating



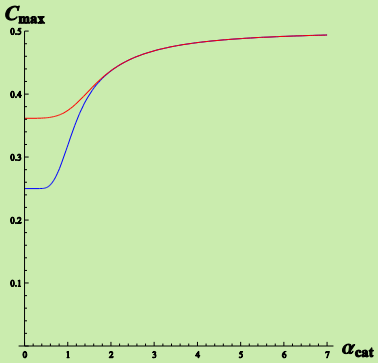
$$\left\langle \hat{P} \right\rangle = \pi W(0,0)$$

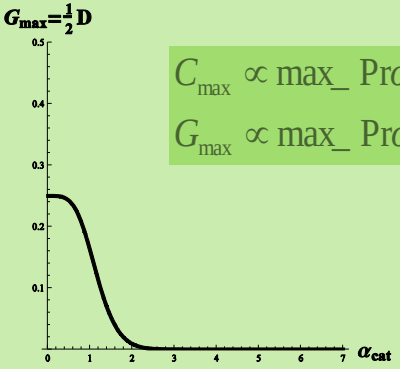


$\alpha_{cat} = 2$ $\left\langle \hat{P} \right\rangle = 1 \to -0.9$

$\alpha_{cat} = 1.4$

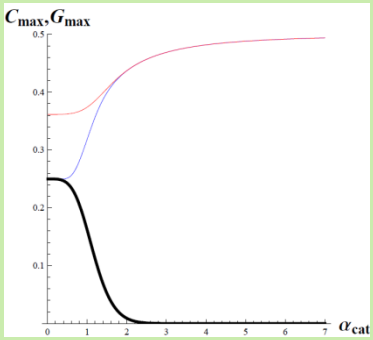
$\alpha_{cat} = 0.7$

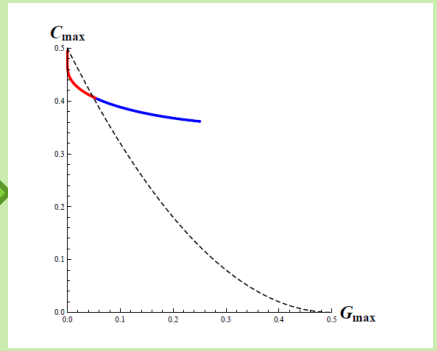


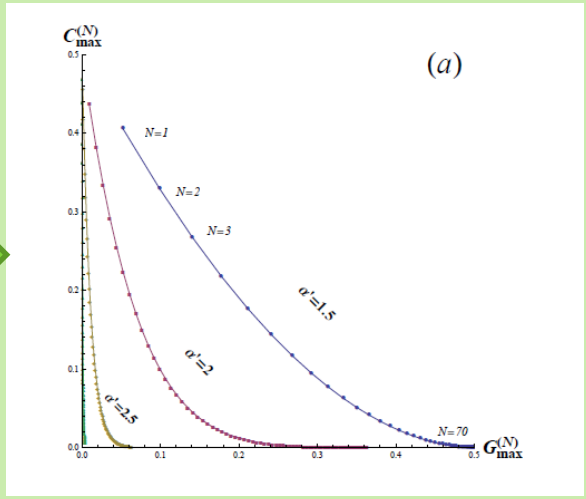


$C_{max} \propto \max\_Probability\_for\_Alice\_to\_cheat$

$G_{max} \propto \max\_Probability\_for\_Bob\_to\_cheat$



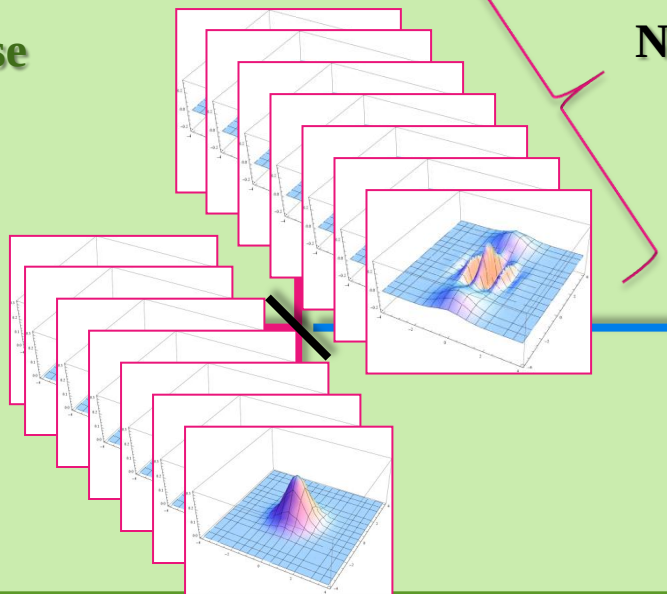




Finalizing the protocol

A

Commit Phase



$$\rho_B^0$$
$$\rho_B^1$$

$$\underbrace{\rho_B^0 \otimes \rho_B^0 \cdots \rho_B^0}_{N}$$
$$\underbrace{\rho_B^1 \otimes \rho_B^1 \cdots \rho_B^1}_{N}$$

Conclusions from this protocol

It is secure but not-practical

- Long-distance interferometer fragile
- Need memory
- Need big values of α
- The probability that N cat states are produced in sequence is very low.

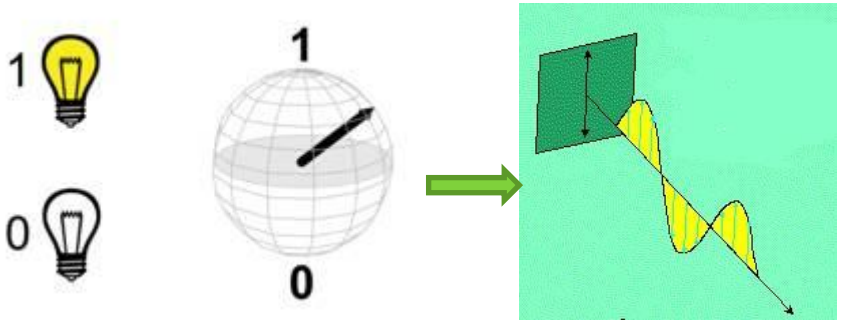
Constructive Conclusions:

- Non-Gaussian operations= probabilistic a reasonable constraint

- Multiple copies it is a good solution for a continuous variable protocols.

- Dependence on a parametre α, we have immediatly a class of protocols

Without constaints we would like
Max(Pa,Pb)=0.5



In a Classical world:
Bit Commitment is impossible
Max(Pa,Pb)=1

Can we construct a `practical' cv quantum protocol
1>Max(Pa,Pb)>0.739?

In a Quantum world:
Bit Commitment is impossible BUT
1>Max(Pa,Pb)>0.739

- **One way** or not
- Purification Protocols (use of entanglement)
- **BB84 type** (without entanglement)
- **Fault-tolerant** ones (no need of quantum memory)
- etc

A

B

$|x_{0,1}\rangle = \sum_{i,j} c_{i,j}^{0,1} |i\rangle_A \otimes |j\rangle_B$

$\langle x_0 | x_1 \rangle = 0$

Commit Phase

$\rho_A^{0,1}$

Entanglement
Quantum Memory

$\rho_B^{0,1}$

$\rho_A^{0,1}$

Unveil Phase

c'= 0 or c'= 1

or

c= 0
$|x1\rangle = |0\rangle$
$|x2\rangle = |1\rangle$

c= 1
$|x1\rangle = |+\rangle$
$|x2\rangle = |-\rangle$

c'
(x')

No Entanglement
No memory

Commit Phase

$\rho_0 = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$

$\equiv \rho_1 = \frac{1}{2}(|+\rangle\langle +| + |-\rangle\langle -|)$

$|\Psi_{EPR}\rangle = \frac{1}{2}(|01\rangle - |10\rangle)$

$\Rightarrow \mathbf{P}_A = 1$

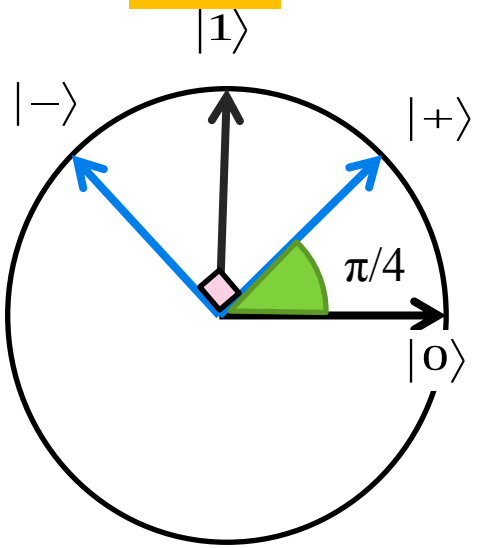
c
(x)

Unveil Phase

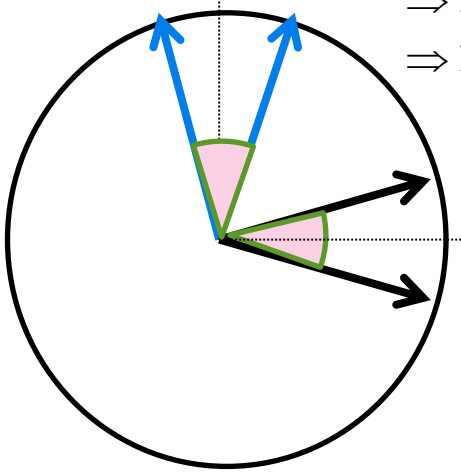
c=c', x'=x, worked
c=c', x'≠x, not worked
c≠ c', ? worked

Generalized BB84

BB84



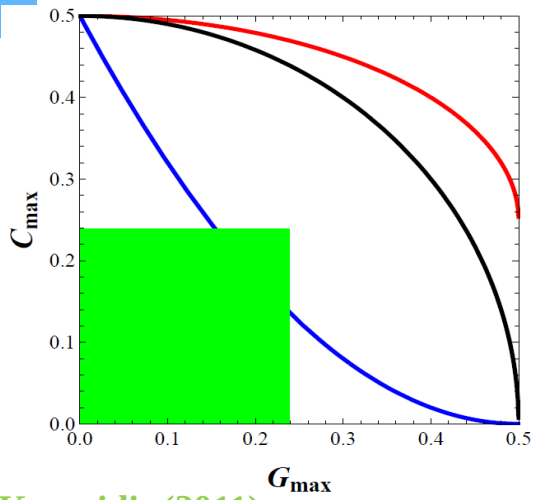
ATVY



$\rho_0 \neq \rho_1$

$\Rightarrow P_B > 0$

$\Rightarrow P_A < 1$



Chailloux, Kerenidis (2011)

(ATVY), Aharonov, Ta-Shma, Vazirani, Yao (2000)

Spekkens, Rudolph (2002)

Berlin, Brassard, Bussieres, Godbout (2009)

c= 0

$|x1\rangle = |0\rangle$

$|x2\rangle = |1\rangle$

c= 1

$|x1\rangle = |+\rangle$

$|x2\rangle = |-\rangle$

cvBB84

c= 0

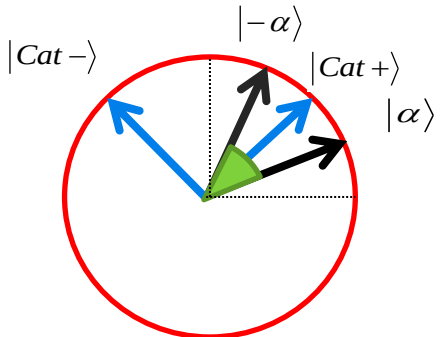
$|x1\rangle = |\alpha\rangle$

$|x2\rangle = |-\alpha\rangle$

c= 1

$|\mathbf{x1}\rangle = |Cat+\rangle = \dfrac{|\alpha\rangle + |-\alpha\rangle}{\sqrt{2\left(1+e^{-2\alpha^2}\right)}}$

$|\mathbf{x2}\rangle = |Cat-\rangle = \dfrac{|\alpha\rangle - |-\alpha\rangle}{\sqrt{2\left(1-e^{-2\alpha^2}\right)}}$



c= 0

$|x1\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$

$|x2\rangle = \cos\theta|0\rangle - \sin\theta|1\rangle$

c= 1

$|x1\rangle = \sin\theta|0\rangle + \cos\theta|1\rangle$

$|x2\rangle = -\sin\theta|0\rangle + \cos\theta|1\rangle$

Conclusions