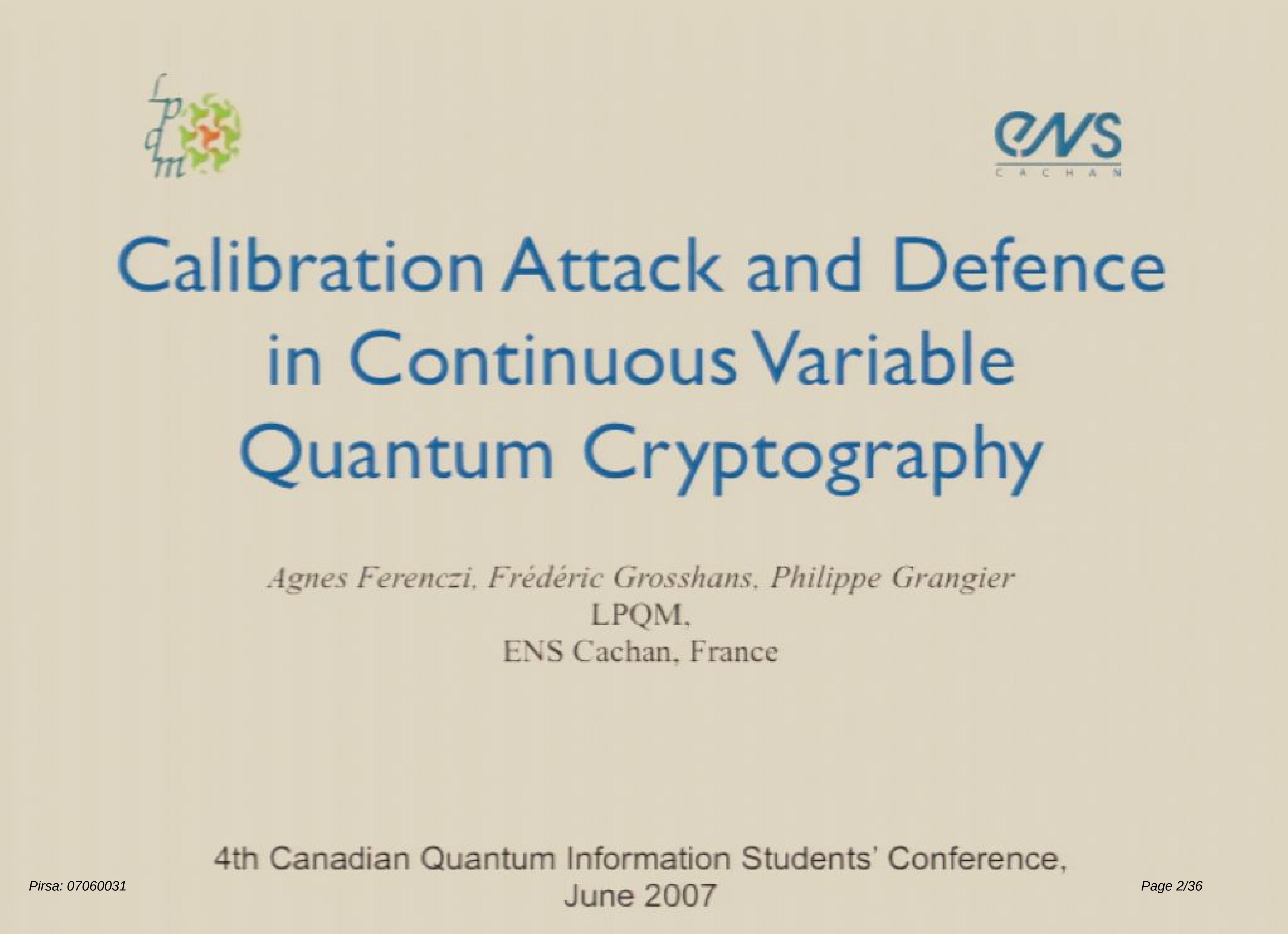
Title: Calibration Attack and Defense in Continuous Variable Quantum Key Distribution

Date: Jun 05, 2007 11:40 AM

URL: http://pirsa.org/07060031

Abstract:

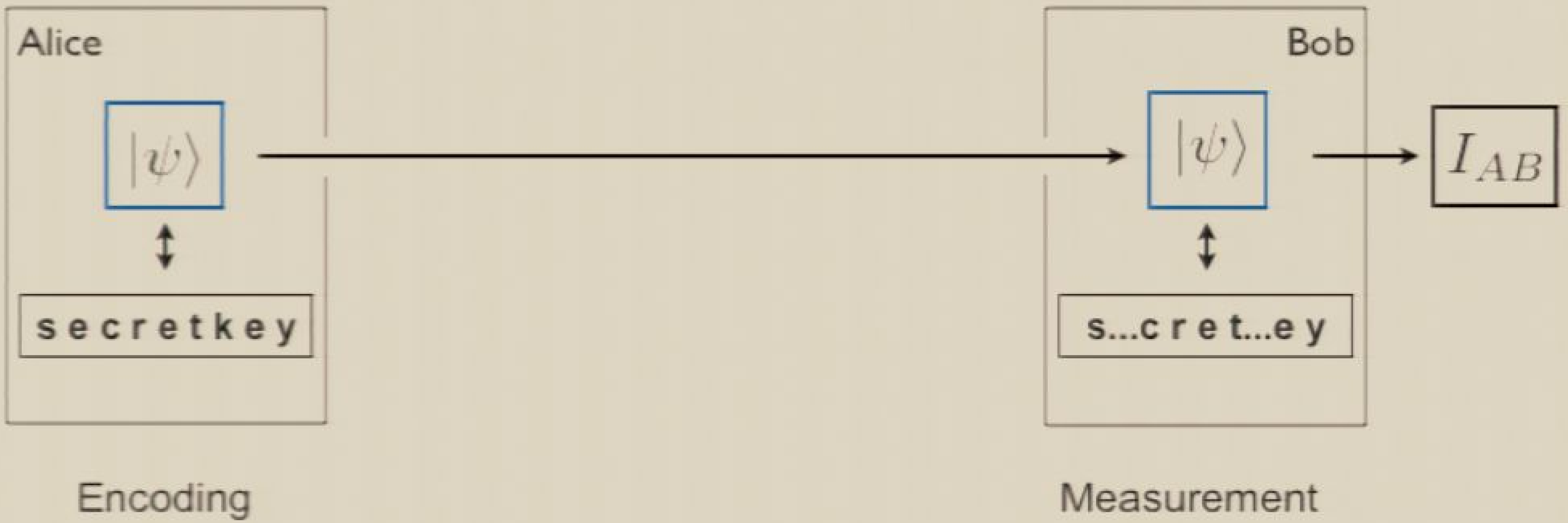


Calibration Attack and Defence in Continuous Variable Quantum Cryptography

Agnes Ferenczi, Frédéric Grosshans, Philippe Grangier
LPQM,
ENS Cachan, France

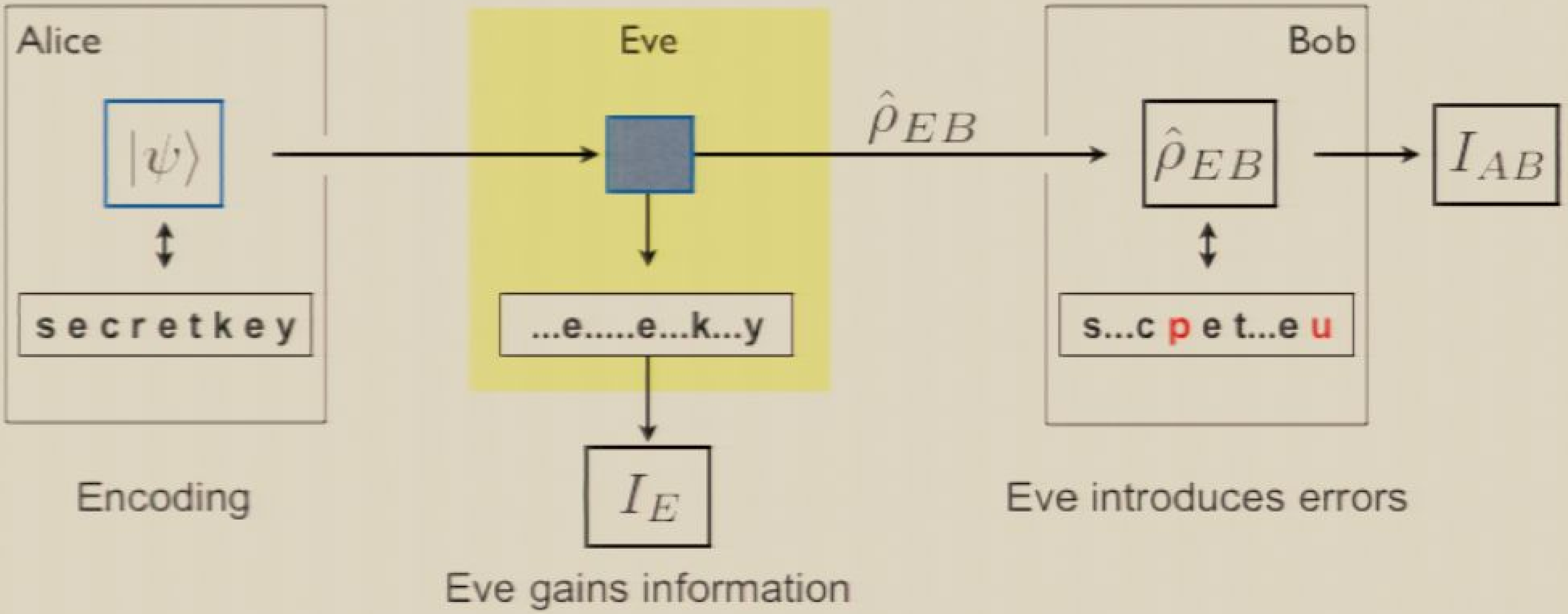
4th Canadian Quantum Information Students' Conference,
June 2007

Quantum Cryptography



Alice and Bob share information $\boxed{I_{AB}}$

Quantum Cryptography



Alice

$|\psi\rangle$

s e c r e t k e y

Encoding

Eve

...e.....e...k...y

I_E

Eve gains information

$\hat{\rho}_{EB}$

Bob

$\hat{\rho}_{EB}$

I_{AB}

s...c p e t...e u

Eve introduces errors

Secret key length: $\Delta I = I_{AB} - I_E$

Continuous Variables

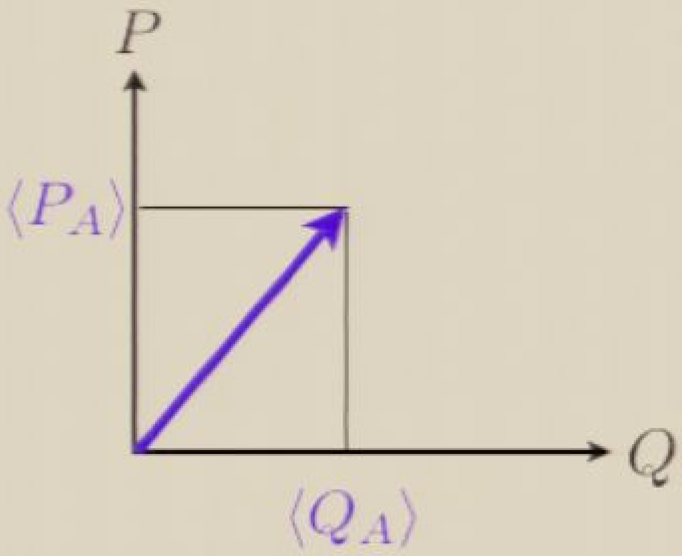
Qubits	Continuous variables
Single photons	Gaussian wave packets ~100 photons at the time
Information: Polarisation basis	Information: Quadratures of the electromagnetic field
Slow detection: MHz	Fast detection: GHz Photodiodes

Continuous Variables

Classical

Electromagnetic field described by Q_A and P_A

$$E(t) = Q_A \cos\omega t + P_A \sin\omega t$$



Continuous Variables

Classical

Electromagnetic field described by Q_A and P_A

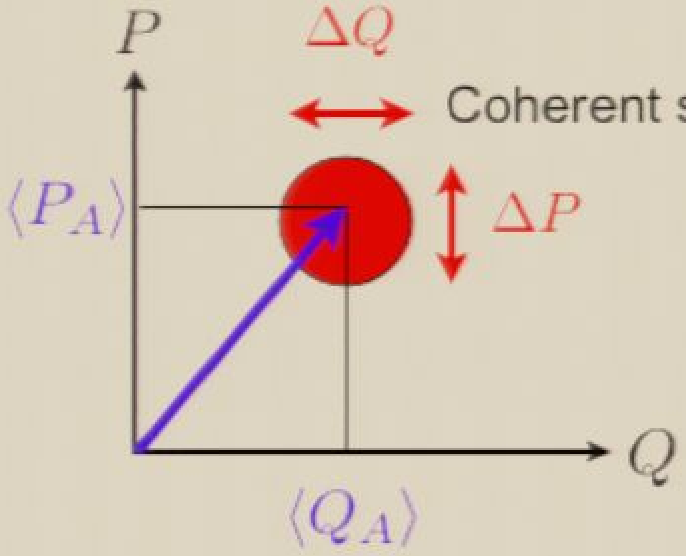
$$E(t) = Q_A \cos\omega t + P_A \sin\omega t$$

Quantum mechanical

Quadratures Q and P
Commutation relation: $[Q, P] = 2i$
Quantum noise $\Delta Q, \Delta P$

Heisenberg inequality:

$$\Delta Q \times \Delta P = 1$$



Continuous Variables

Classical

Electromagnetic field described by Q_A and P_A

$$E(t) = Q_A \cos \omega t + P_A \sin \omega t$$

Quantum mechanical

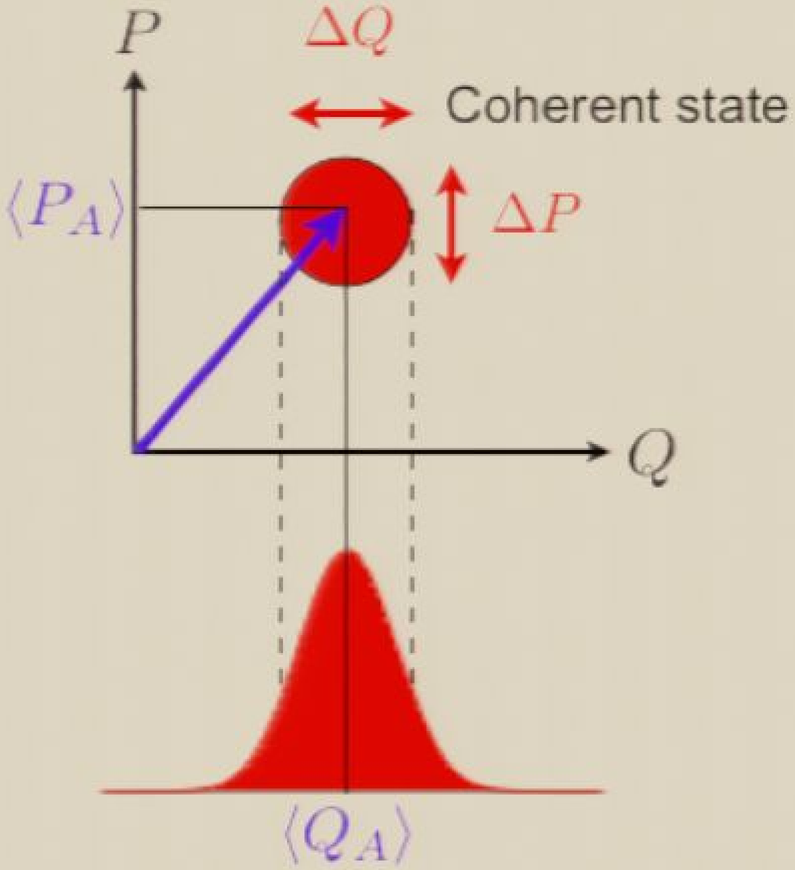
Quadratures Q and P

Commutation relation: $[Q, P] = 2i$

Quantum noise $\Delta Q, \Delta P$

Heisenberg inequality:

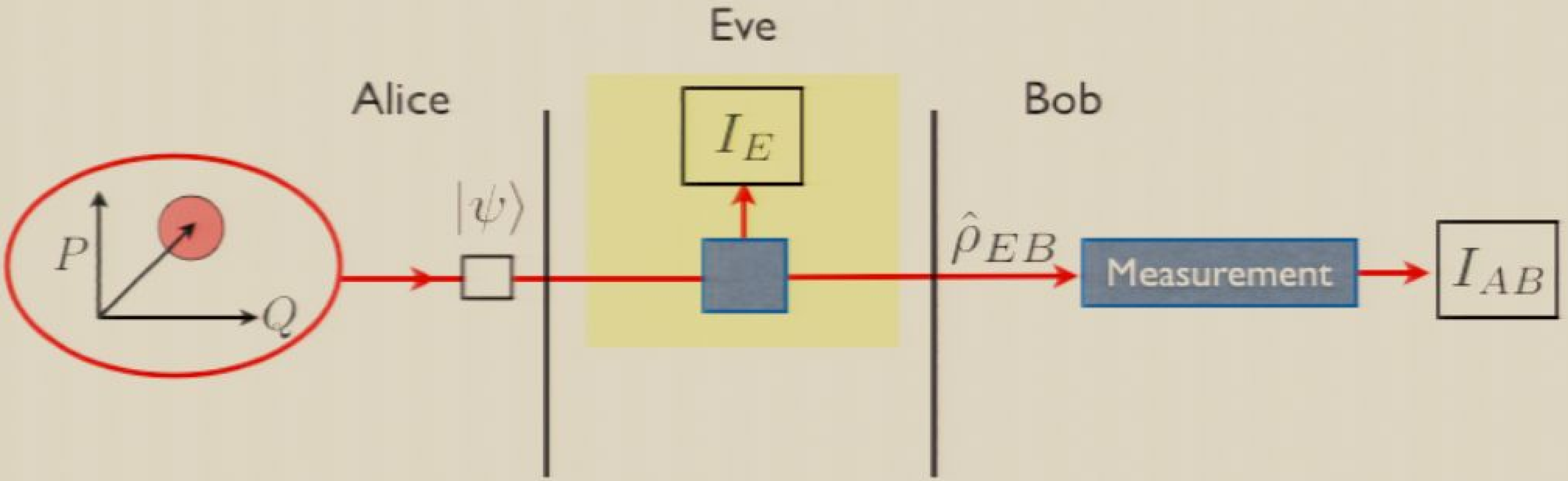
$\Delta Q \times \Delta P = 1$ →



Minimal uncertainty wave packet
Gaussian wave packet

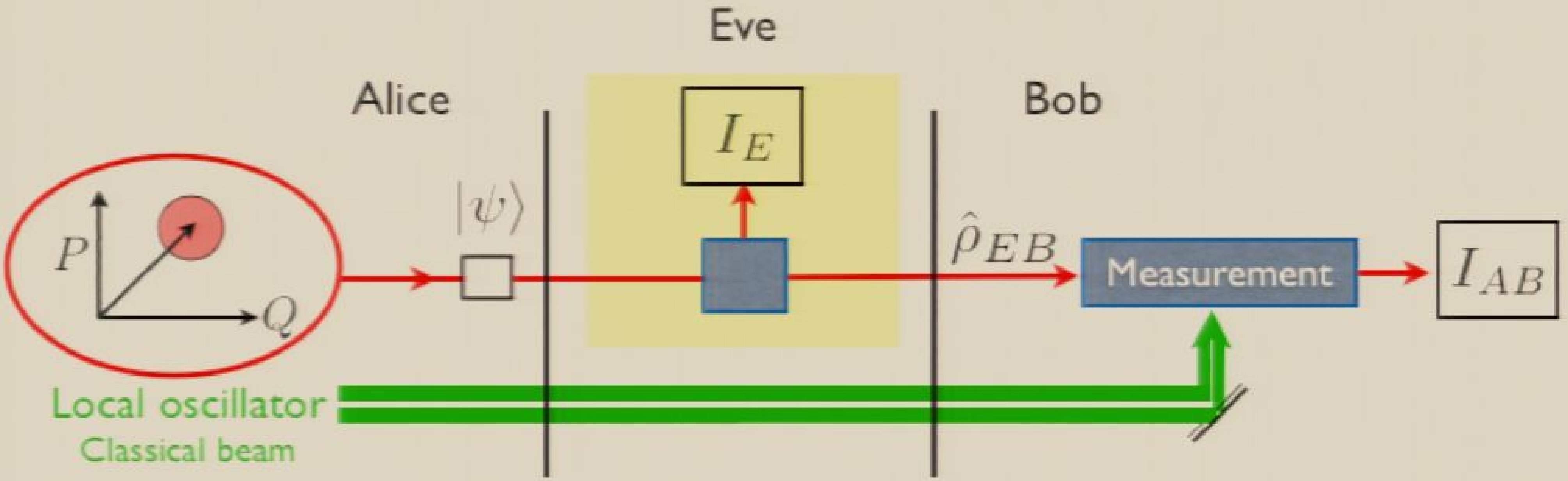
Cryptography with Continuous Variables

Until now: Attack on signal



Cryptography with Continuous Variables

Until now: Attack on signal

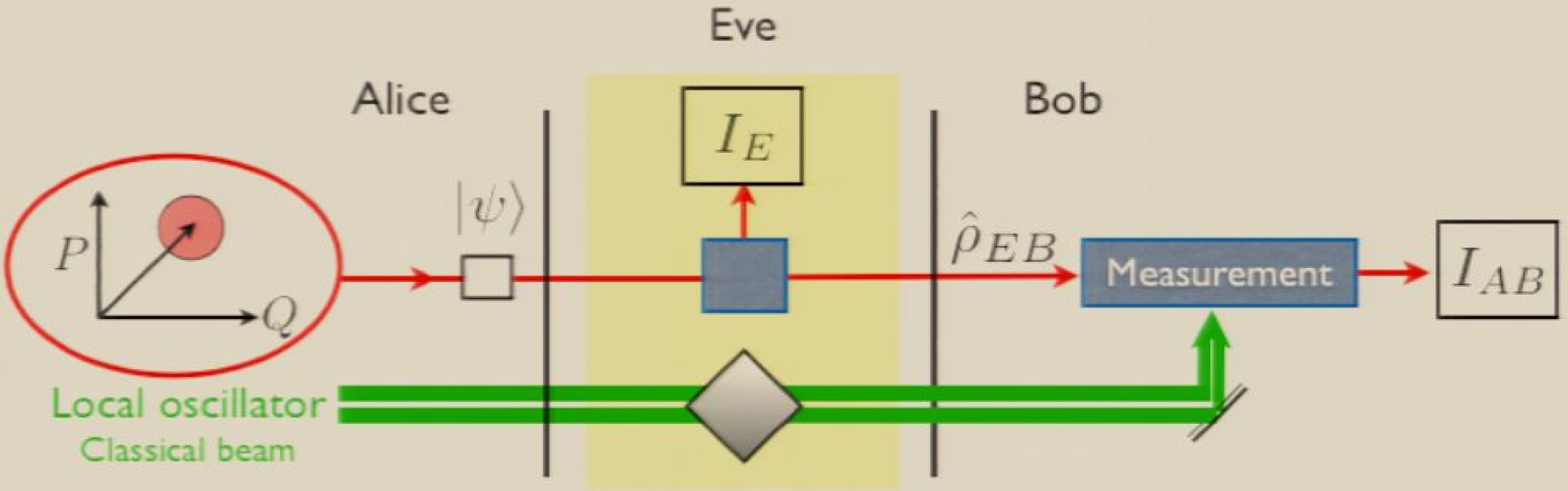


Local oscillator:

- Necessary for the measurement (phase and intensity reference) in the experimental setup.
- Travels along the signal and is unprotected.

Cryptography with Continuous Variables

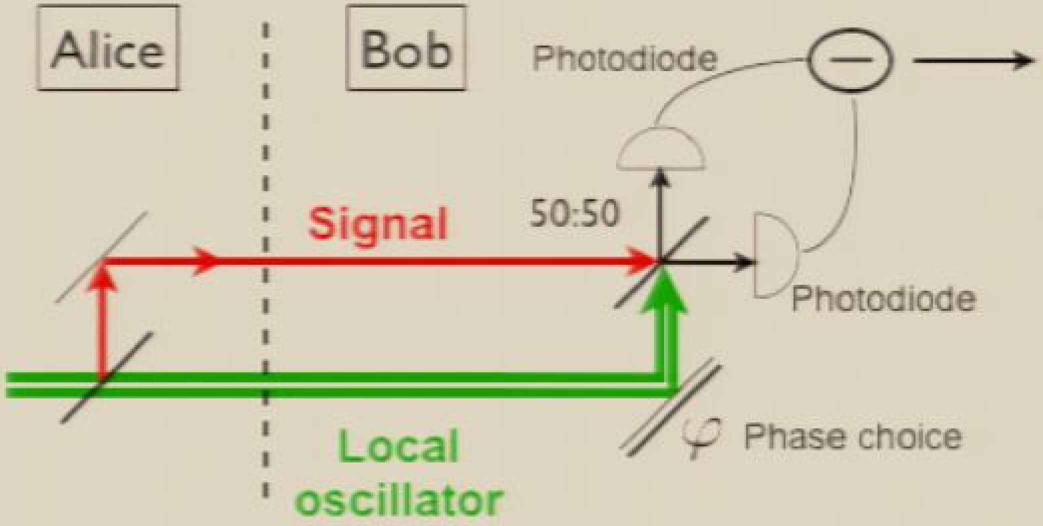
Until now: Attack on signal → New: Attack on signal and local oscillator



Local oscillator:

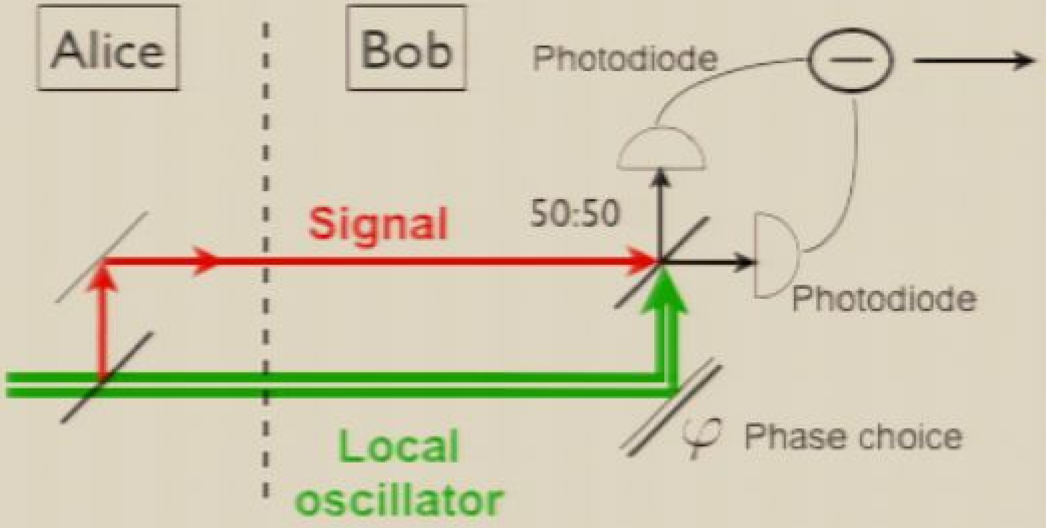
- Necessary for the measurement (phase and intensity reference) in the experimental setup.
- Travels along the signal and is unprotected.

Homodyne measurement

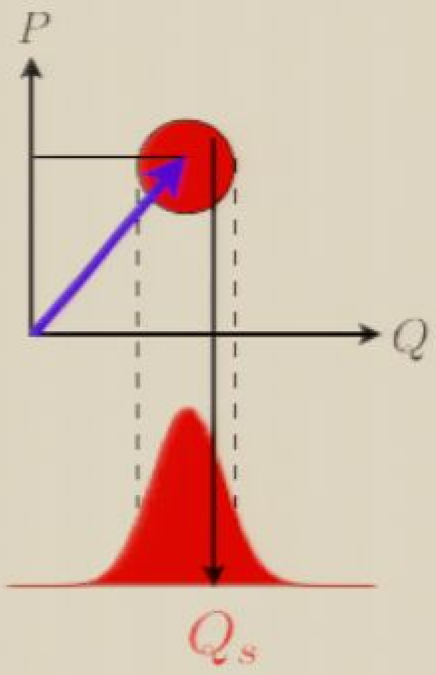


$$\boxed{\sqrt{I_{LO}}(Q_s \cos\varphi + P_s \sin\varphi)}$$

Homodyne measurement



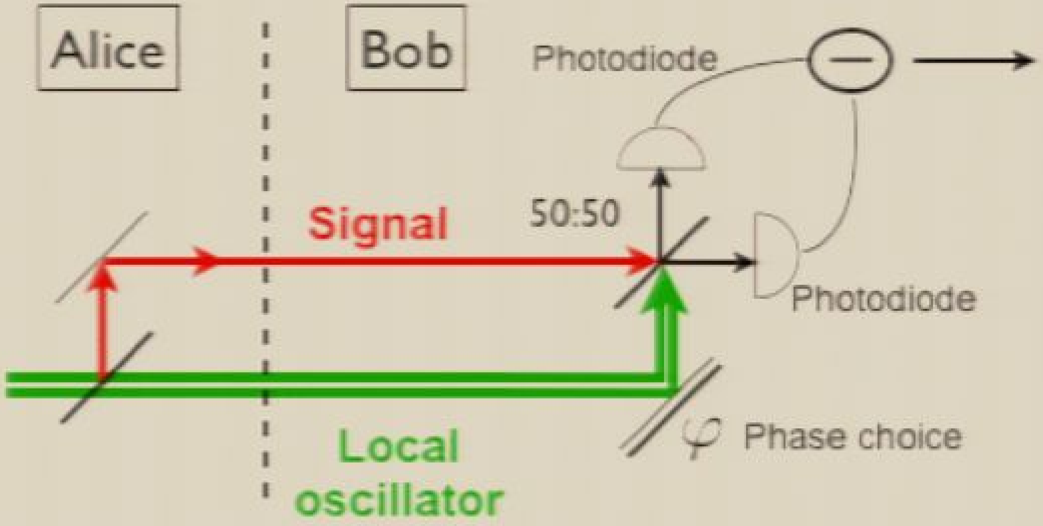
$$\boxed{\sqrt{I_{LO}}(Q_s \cos\varphi + P_s \sin\varphi)}$$



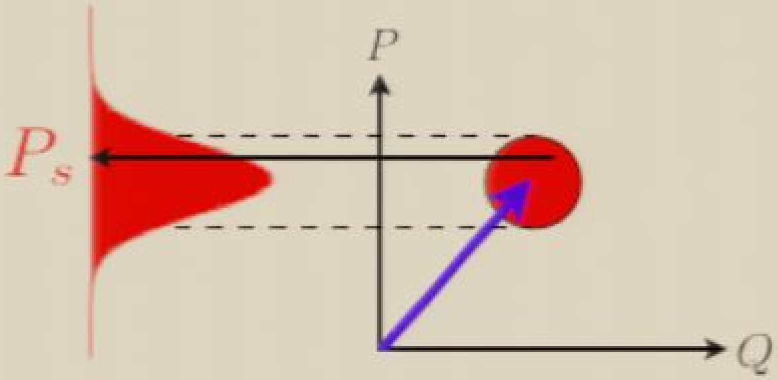
Choice between Q_s and P_s

$\varphi = 0 \longrightarrow Q_s$

Homodyne measurement



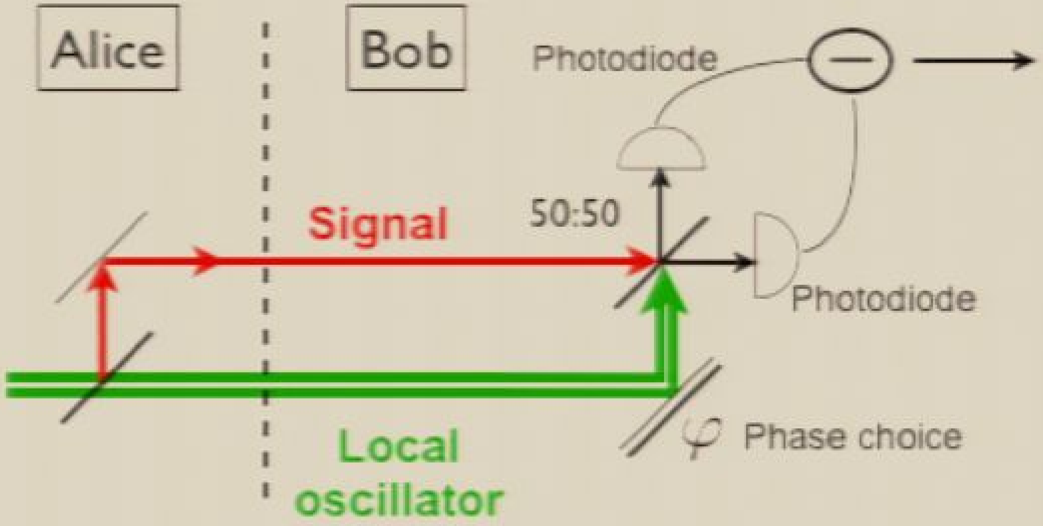
$$\sqrt{I_{LO}}(Q_s \cos\varphi + P_s \sin\varphi)$$



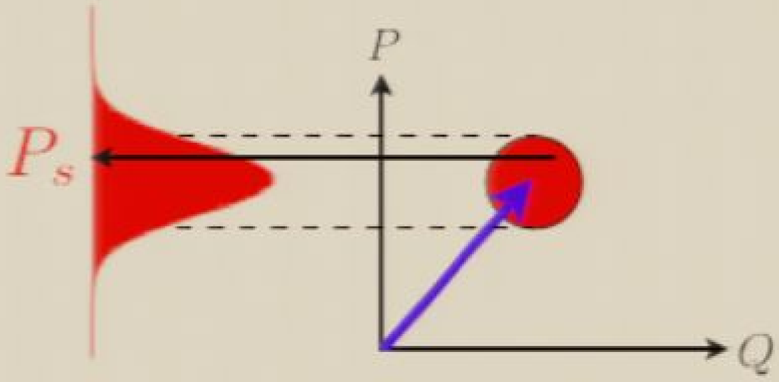
Choice between Q_s and P_s

$\varphi = \pi/2 \longrightarrow P_s$

Homodyne measurement



$$\sqrt{I_{LO}}(Q_s \cos\varphi + P_s \sin\varphi)$$



Choice between Q_s and P_s

$\varphi = 0 \longrightarrow Q_s$

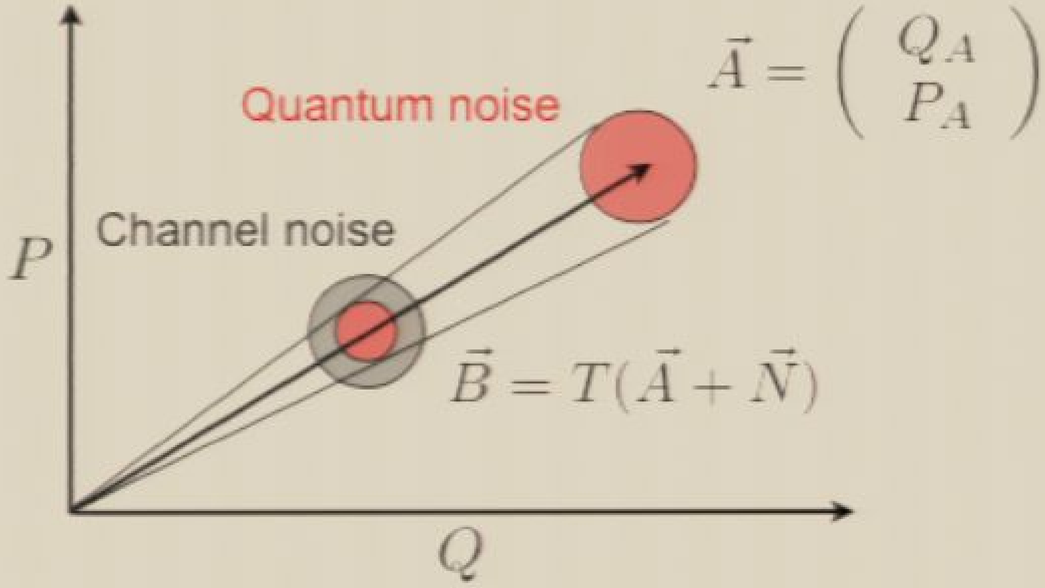
$\varphi = \pi/2 \longrightarrow P_s$

↔

Choice of basis in qubit based protocols

Transmission through Quantum Channel

Noisy channel with transmission T<1:



$$\vec{A} = \begin{pmatrix} Q_A \\ P_A \end{pmatrix}$$

$$\vec{B} = T(\vec{A} + \vec{N})$$

Alice and Bob

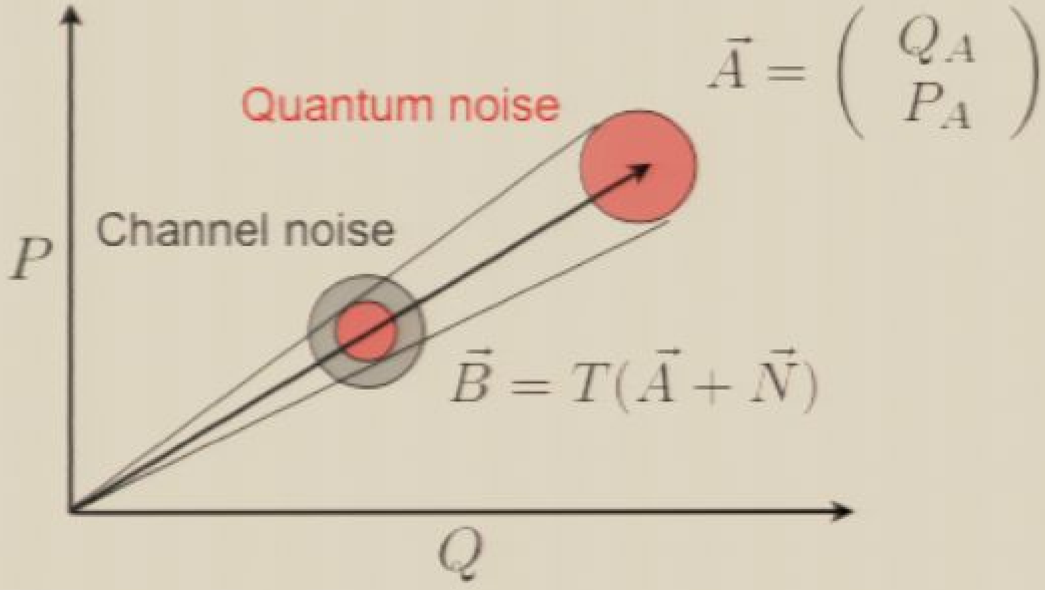
- Estimate Noise & transmission T

Bob

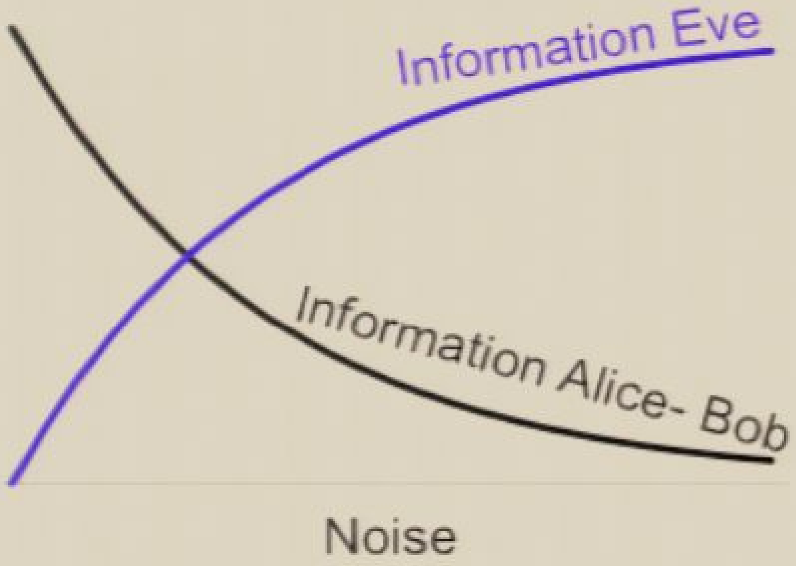
- Information is lost
- Noise is added

Transmission through Quantum Channel

Noisy channel with transmission T<1:



$\vec{A} = \begin{pmatrix} Q_A \\ P_A \end{pmatrix}$
Quantum noise
Channel noise
P
$\vec{B} = T(\vec{A} + \vec{N})$
Q



Alice and Bob

- Estimate Noise & transmission T

Bob

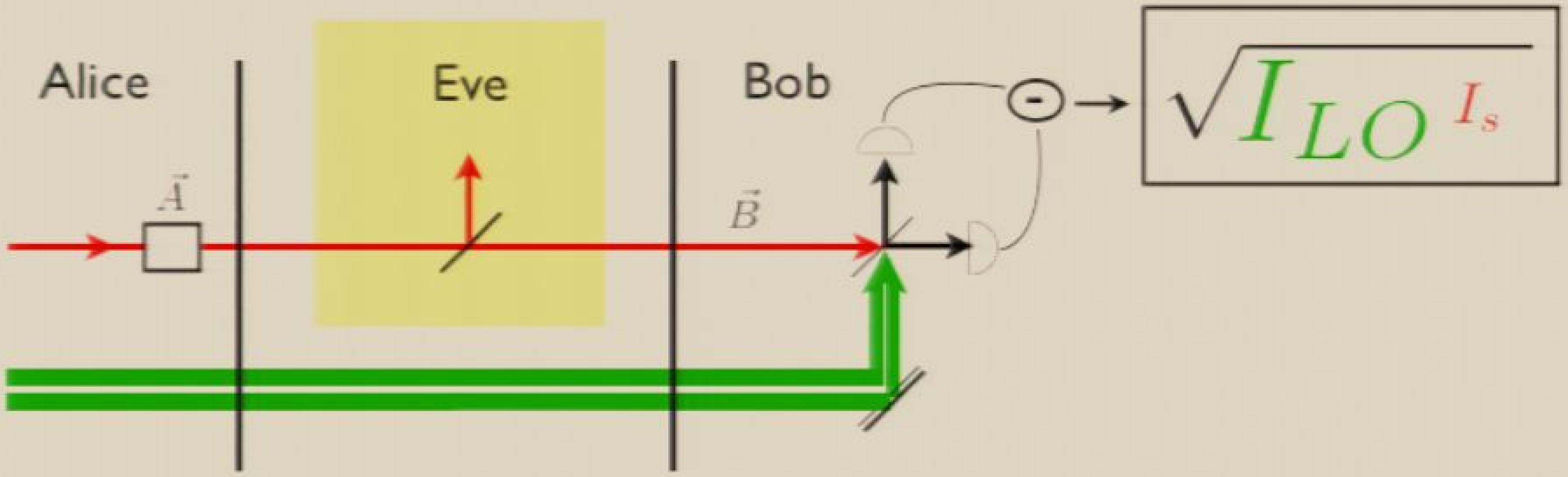
- Information is lost
- Noise is added

Heisenberg uncertainty relation

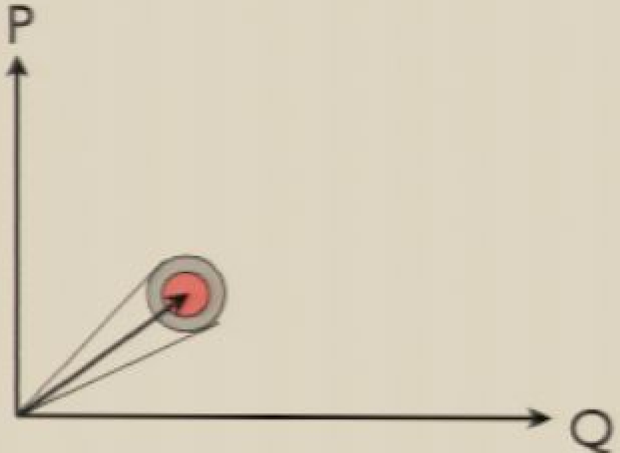
$$\Delta \mathrm{N_B} \times \Delta \mathrm{N_E} \geq 1$$

Calibration Attack

Attack only on Signal



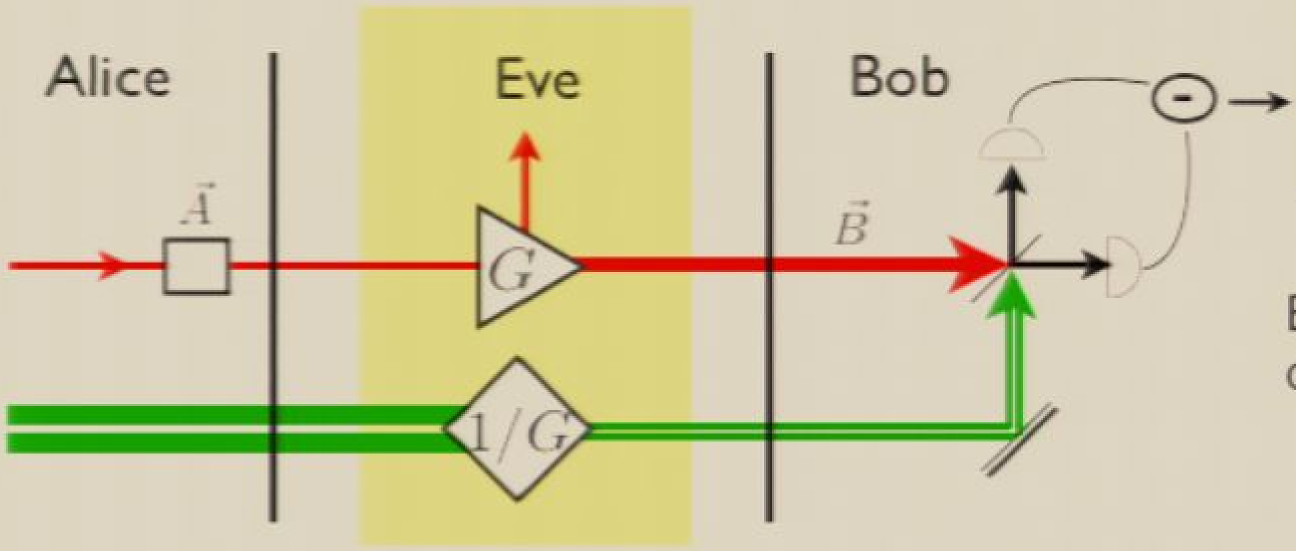
$$\sqrt{I_{LO}\, I_s}$$



Calibration Attack

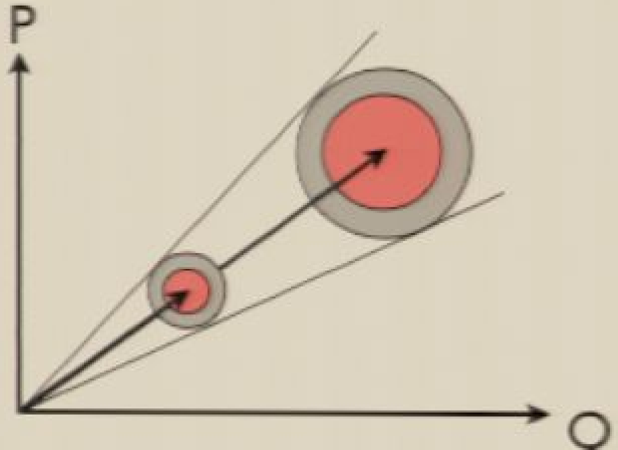
Attack on Signal and Local Oscillator: Calibration Attack

Eve amplifies the signal, and decreases the intensity of the local oscillator.



$$\sqrt{I_{LO}\ I_s}$$

Eve has more information on the amplified signal.



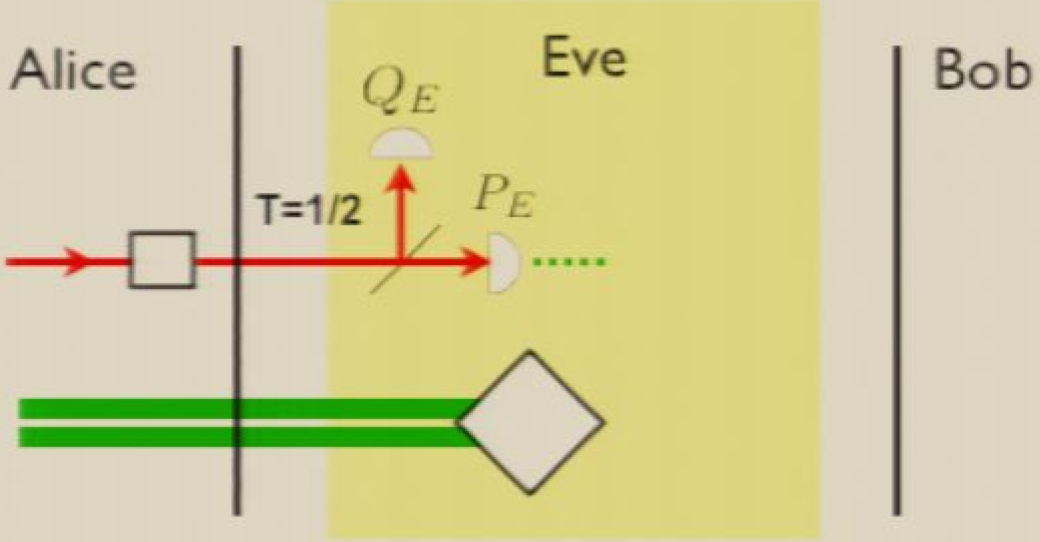
Bob can not distinguish between these states.

↓

Eve remains undiscovered.

Intercept - Resend Attack

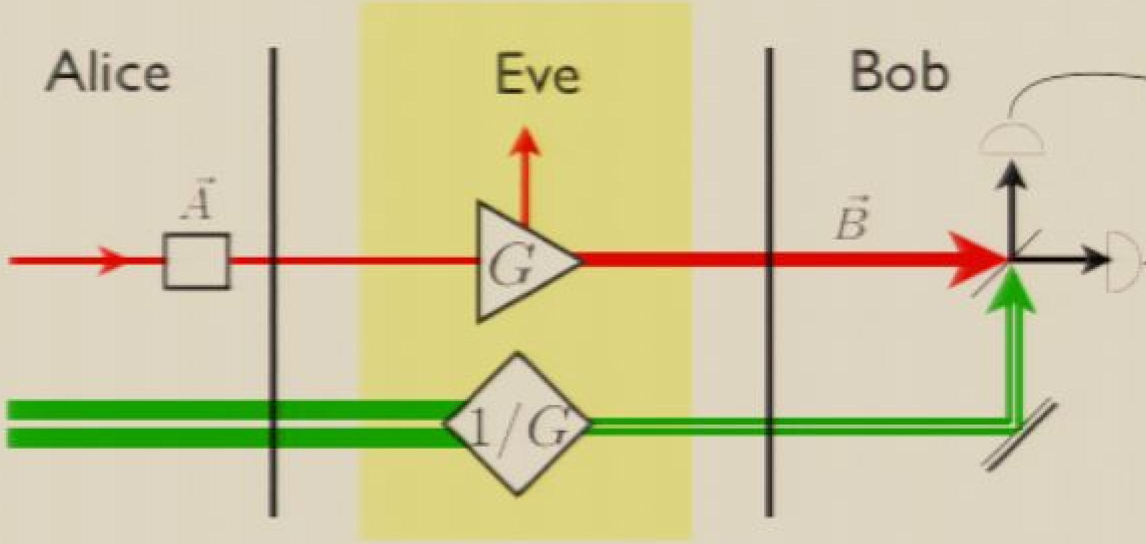
Extreme case of the calibration attack



Calibration Attack

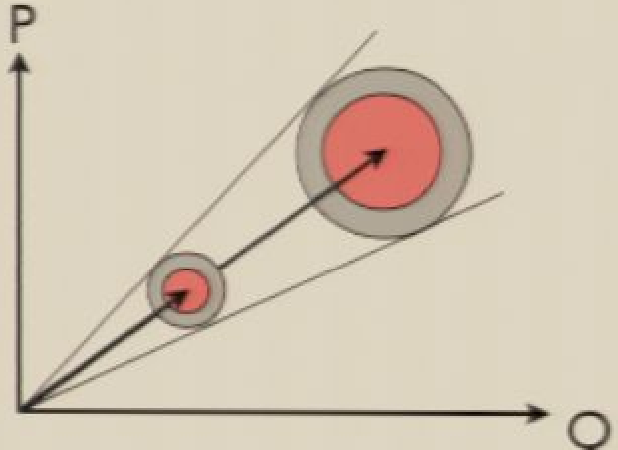
Attack on Signal and Local Oscillator: Calibration Attack

Eve amplifies the signal, and decreases the intensity of the local oscillator.



$$\sqrt{I_{LO}\ I_s}$$

Eve has more information on the amplified signal.



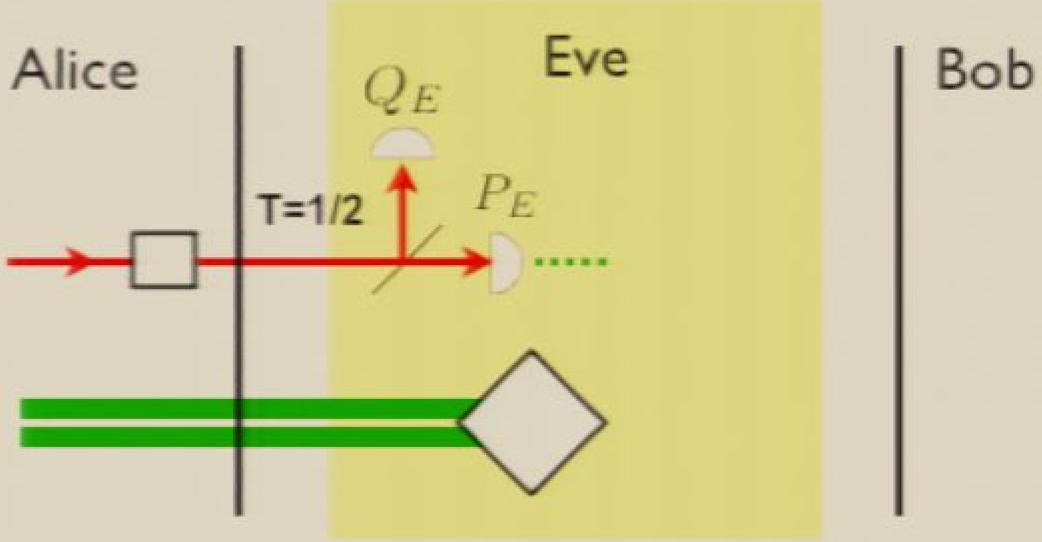
Bob can not distinguish between these states.

↓

Eve remains undiscovered.

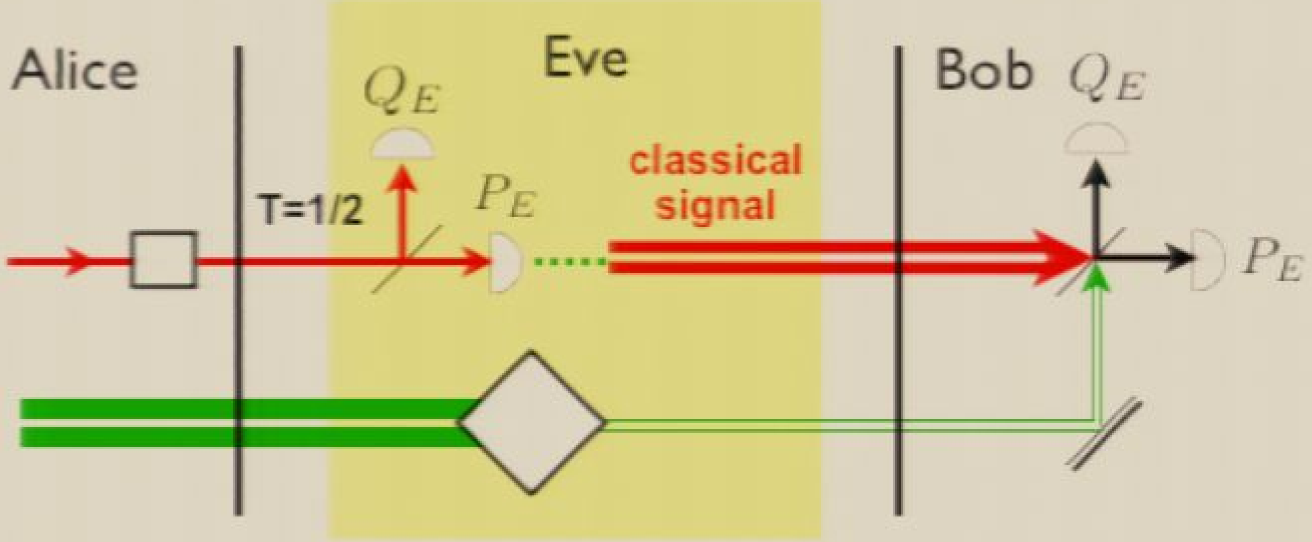
Intercept - Resend Attack

Extreme case of the calibration attack



Intercept - Resend Attack

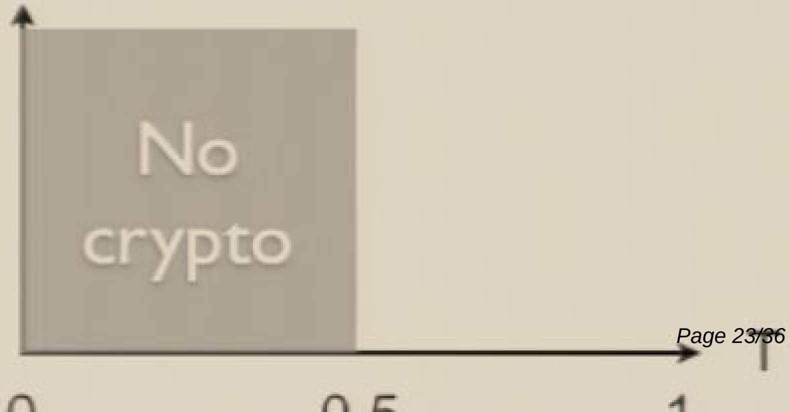
Extreme case of the calibration attack



Eve knows exactly what Bob knows!

For every channel with $\mathrm{T} \leqslant 1/2$, Eve can make an intercept-resend attack.

No cryptography for $T \leqslant 0.5$!

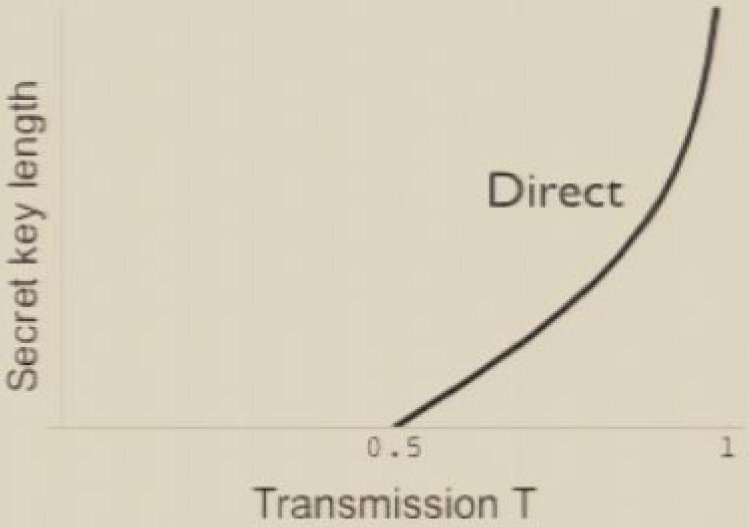


Direct and Reverse Reconciliation Protocols

Direct protocols:

Alice | Classical communication | Bob

Threshold: T=0.5

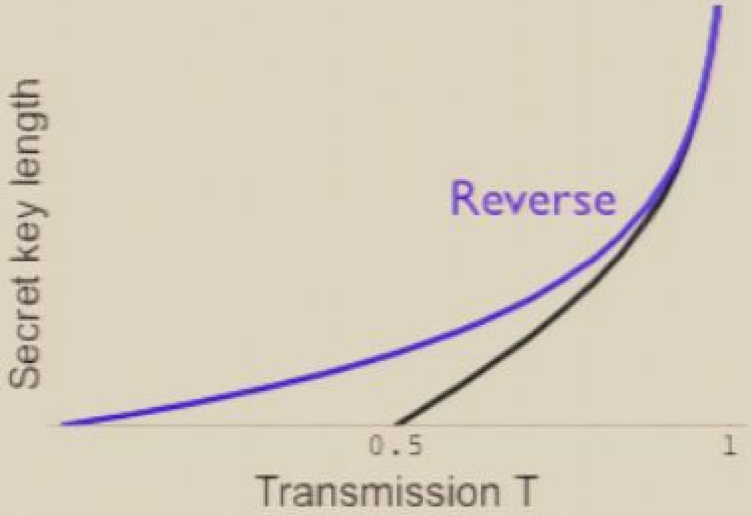


Reverse protocols:

Grosshans & Grangier: quant-ph/0204127

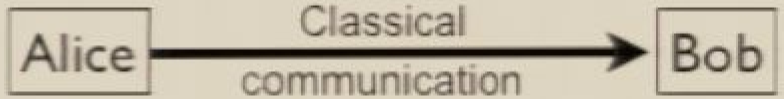
Alice | Classical communication | Bob

No threshold



Direct and Reverse Reconciliation Protocols

Direct protocols:

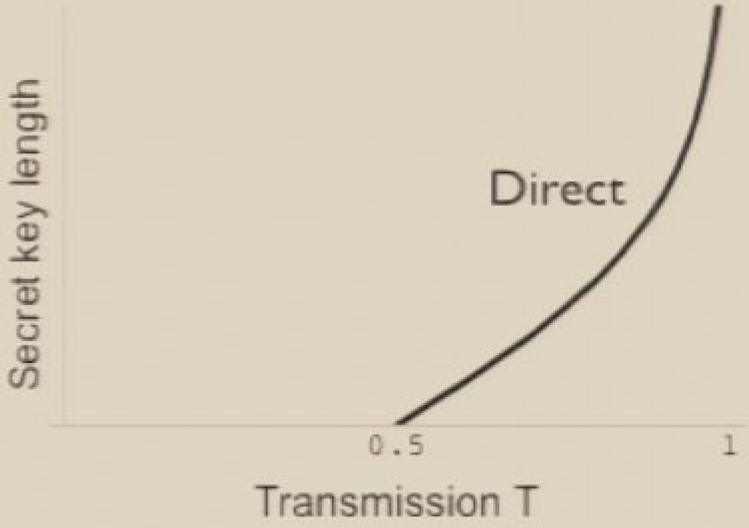


Alice

Classical communication

Bob

Threshold: T=0.5



Reverse protocols:

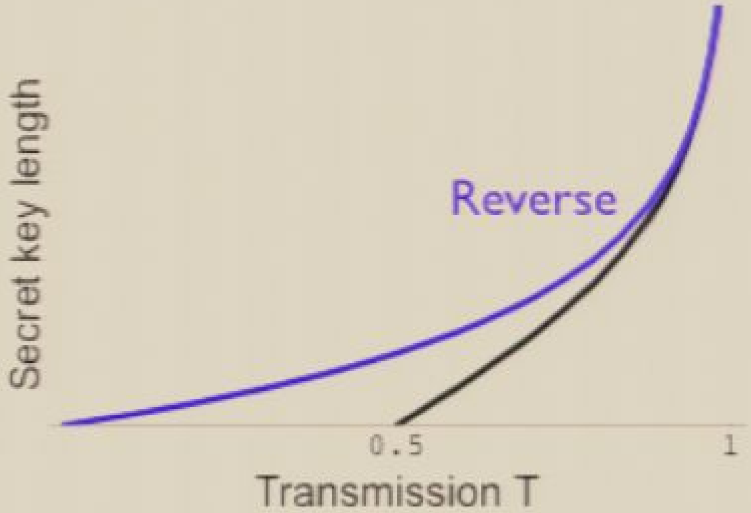
Grosshans & Grangier: quant-ph/0204127

Alice

Classical communication

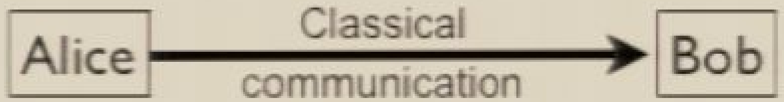
Bob

No threshold

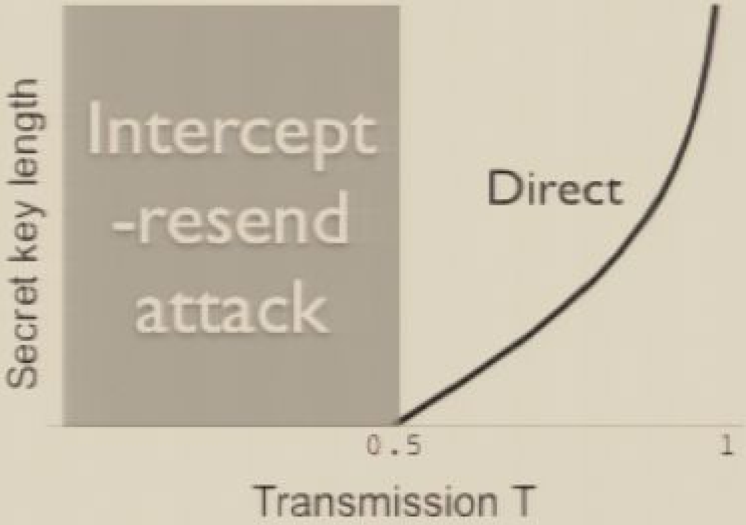


Direct and Reverse Reconciliation Protocols

Direct protocols:

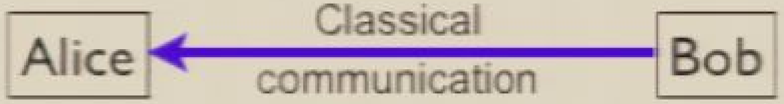


Threshold: T=0.5

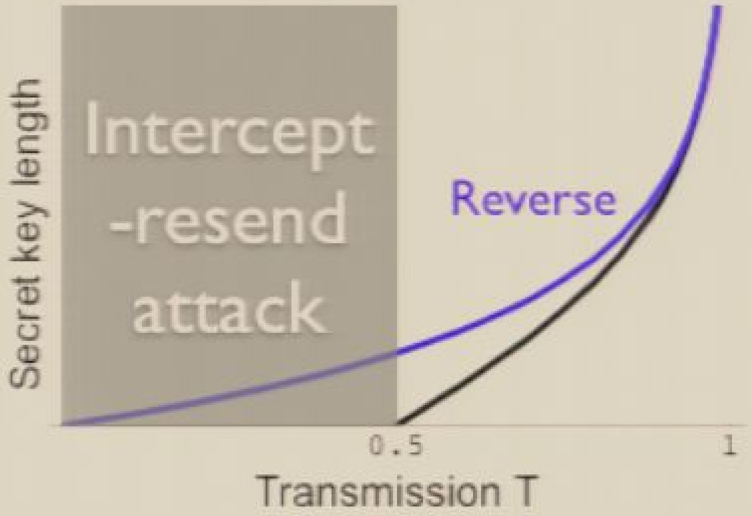


Reverse protocols:

Grosshans & Grangier: quant-ph/0204127

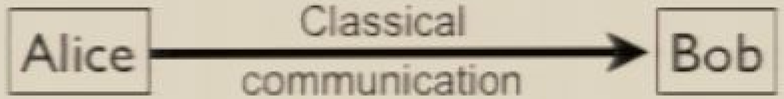


No threshold



Direct and Reverse Reconciliation Protocols

Direct protocols:

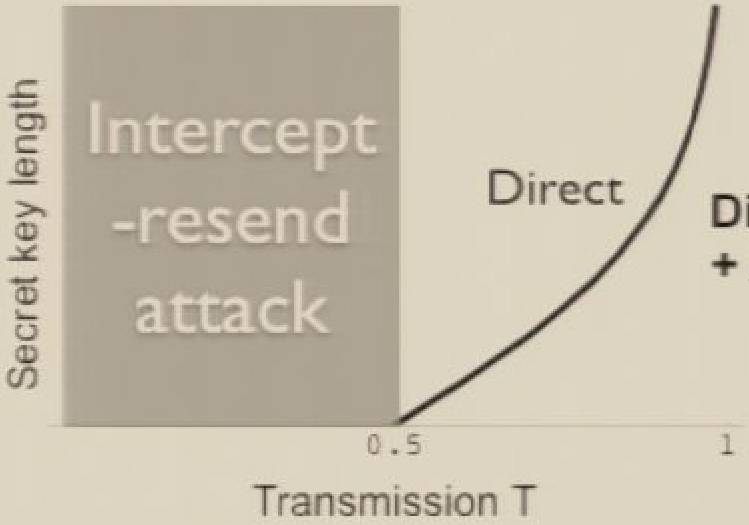


Alice

Classical communication

Bob

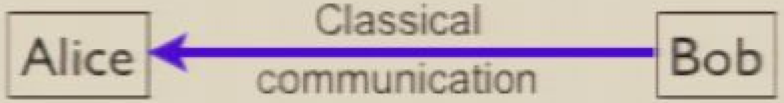
Threshold: T=0.5



Direct protocol + Attack on LO = SAME

Reverse protocols:

Grosshans & Grangier: quant-ph/0204127

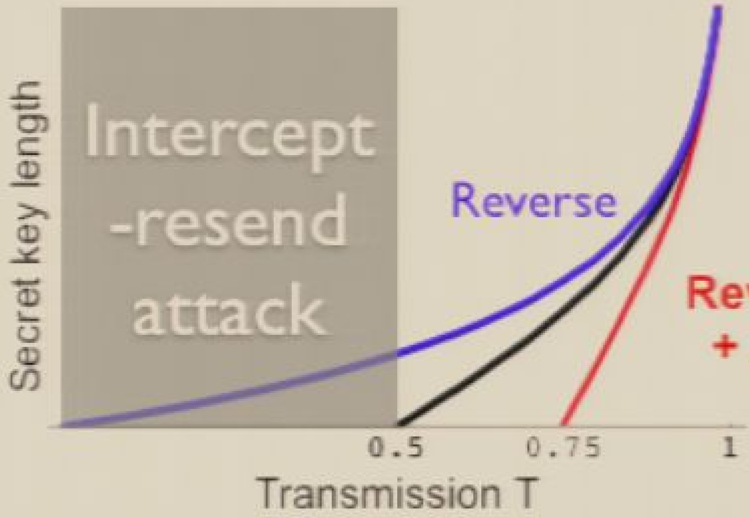


Alice

Classical communication

Bob

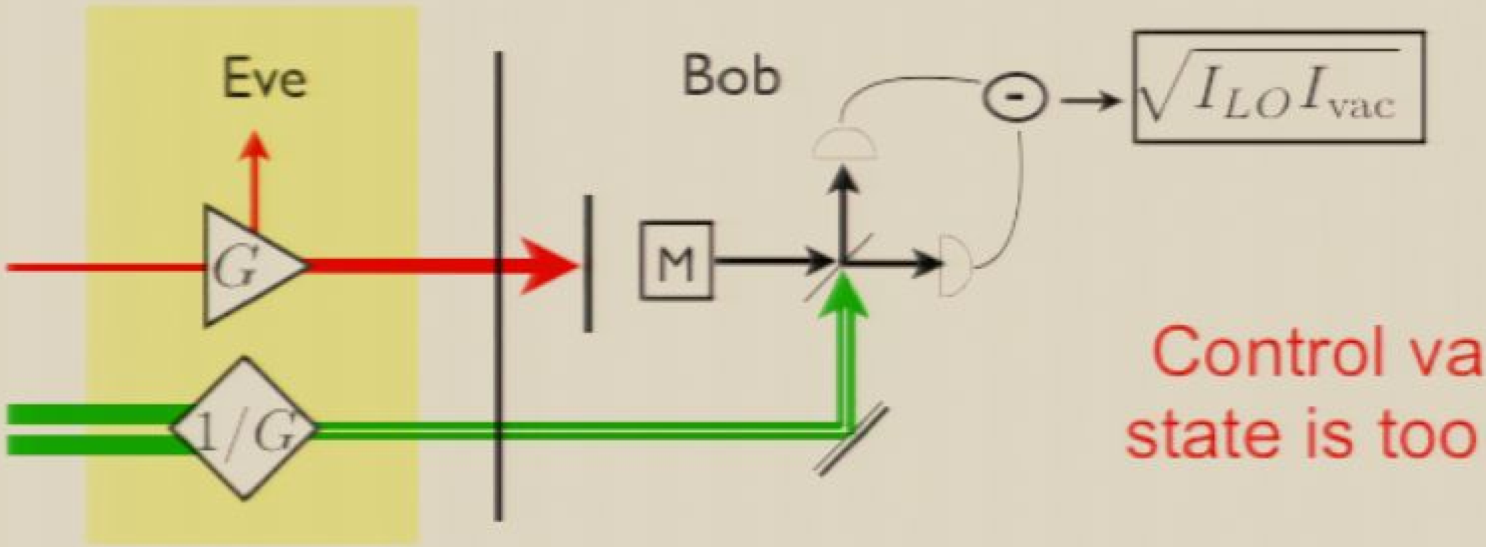
No threshold



Reverse protocol + Attack on LO

Countermeasure I

Bob measures the real vacuum noise

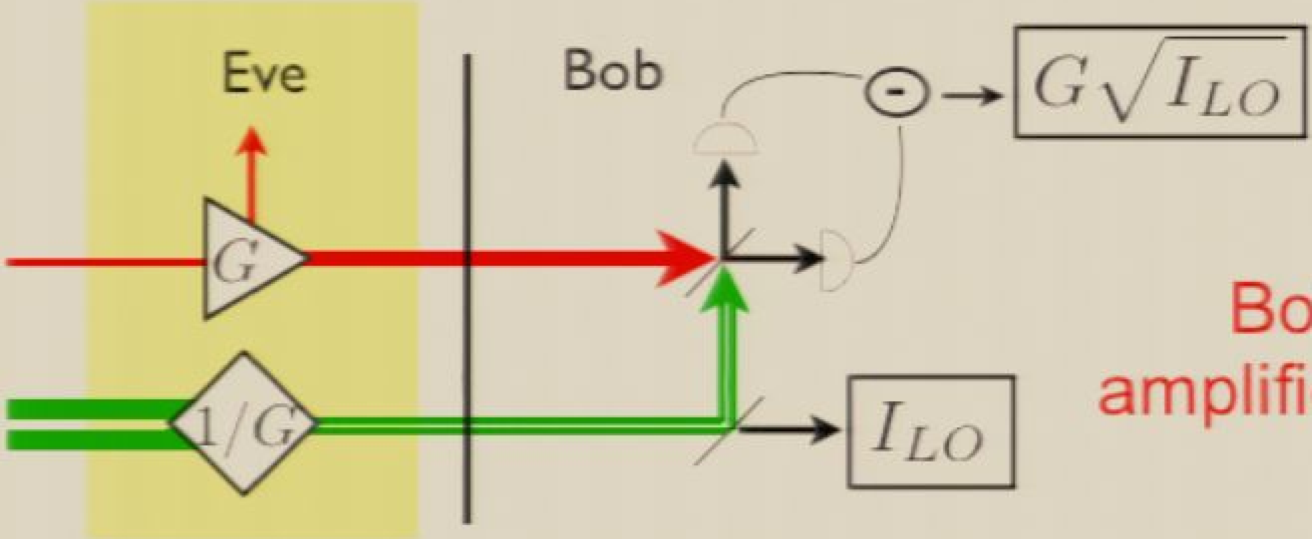


Control vacuum state is too small!

Bob randomly blocks the signal to make a control measurement of the vacuum state

Countermeasure 2

Bob measures the intensity of the LO

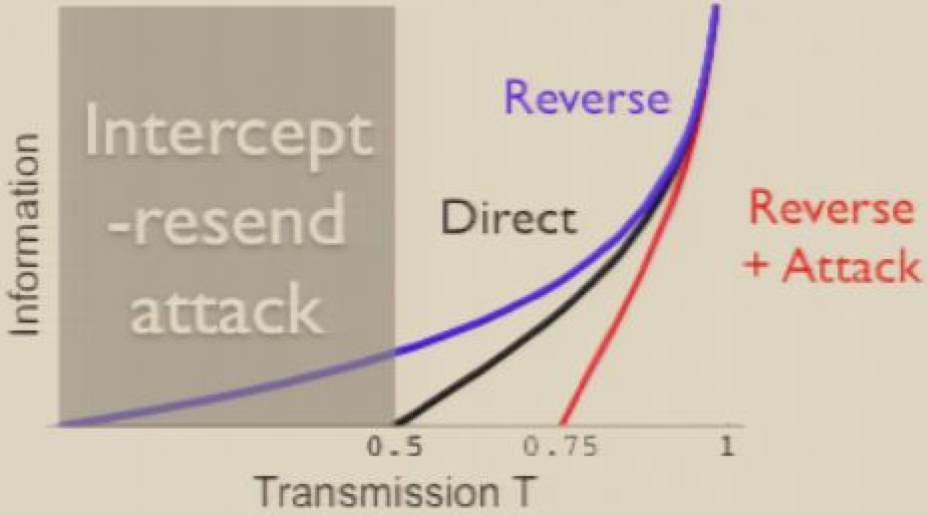


Bob finds the amplification factor G

Summary and Conclusion

New and powerful attack...

- •Calibration attack
- •Attack on signal and LO
- •Very bad for reverse protocols

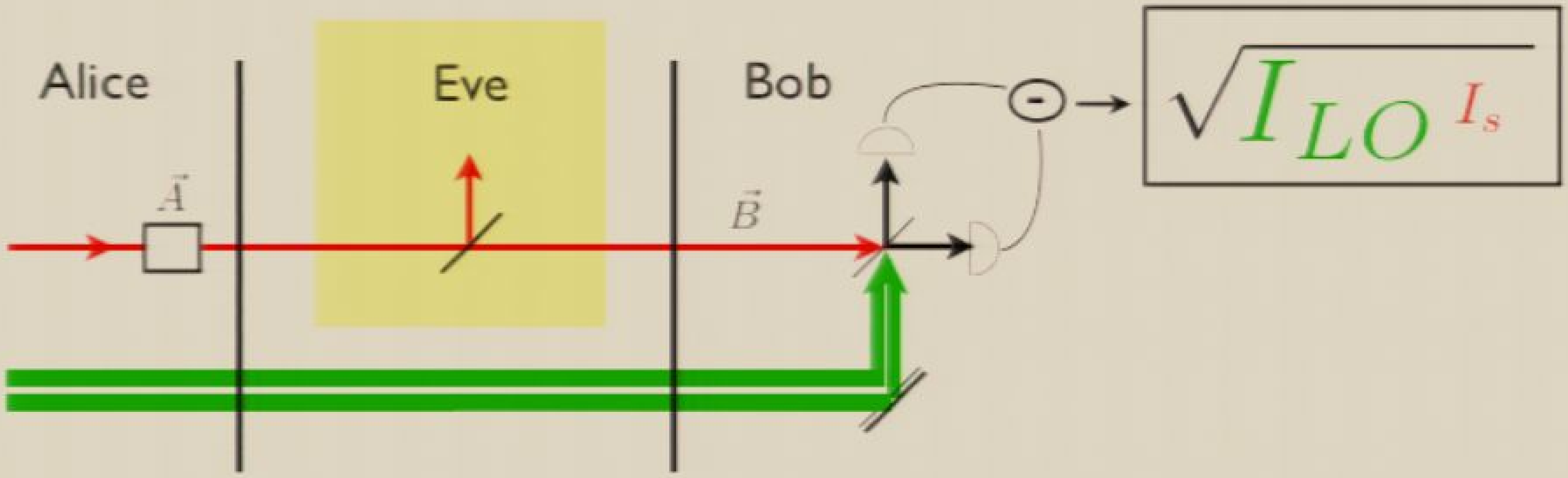


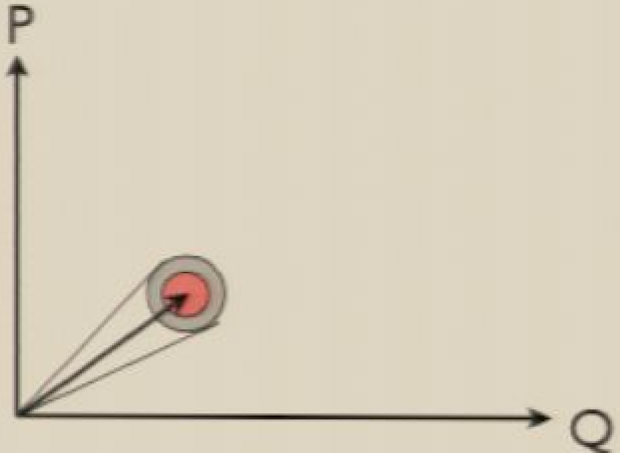
...easy countermeasures !

- •Bob measures true vacuum noise
- •Bob measures the intensity of the LO

Calibration Attack

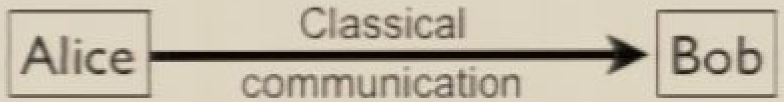
Attack only on Signal





Direct and Reverse Reconciliation Protocols

Direct protocols:

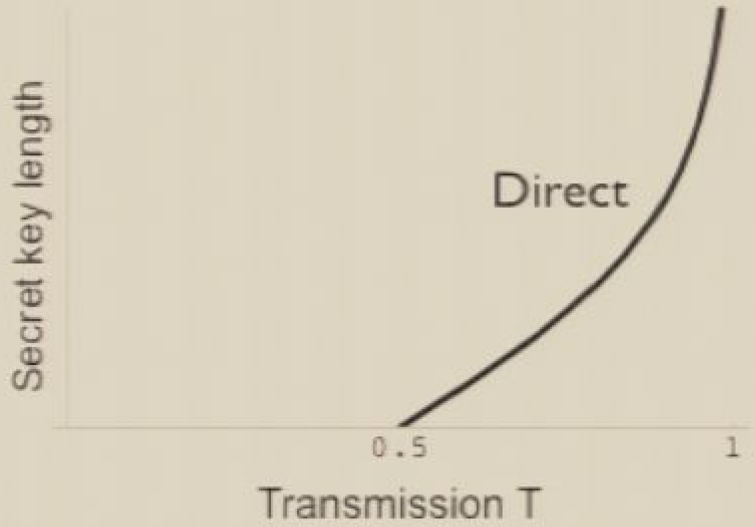


Alice

Classical communication

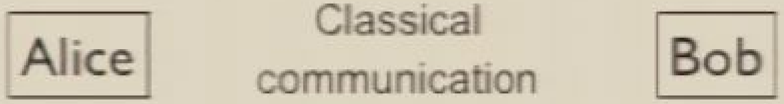
Bob

Threshold: T=0.5



Reverse protocols:

Grosshans & Grangier: quant-ph/0204127

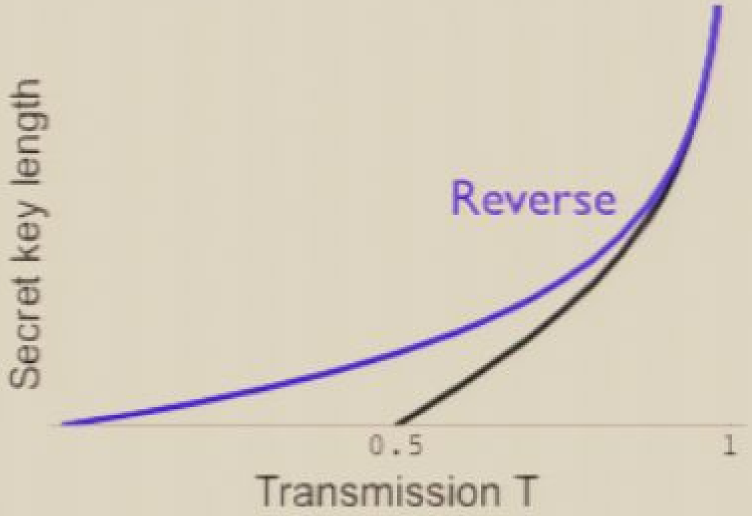


Alice

Classical communication

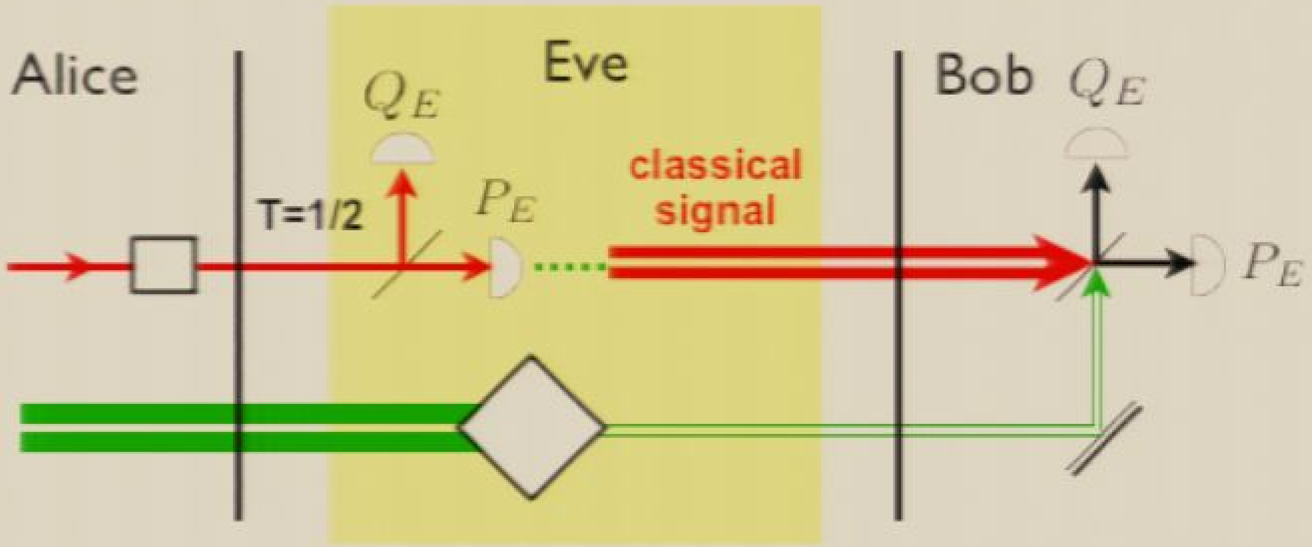
Bob

No threshold



Intercept - Resend Attack

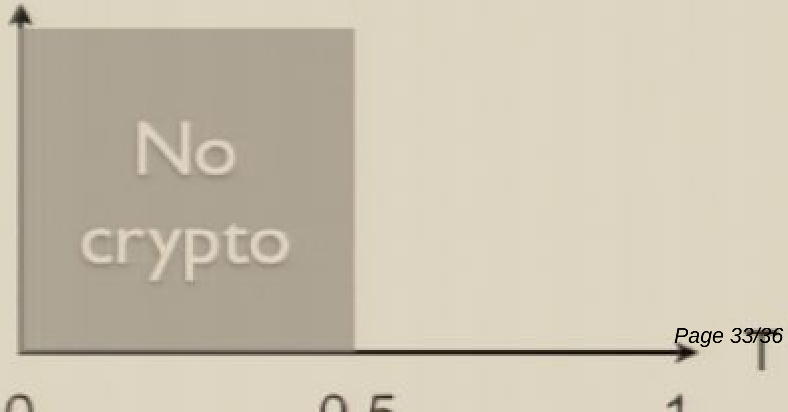
Extreme case of the calibration attack



Eve knows exactly what Bob knows!

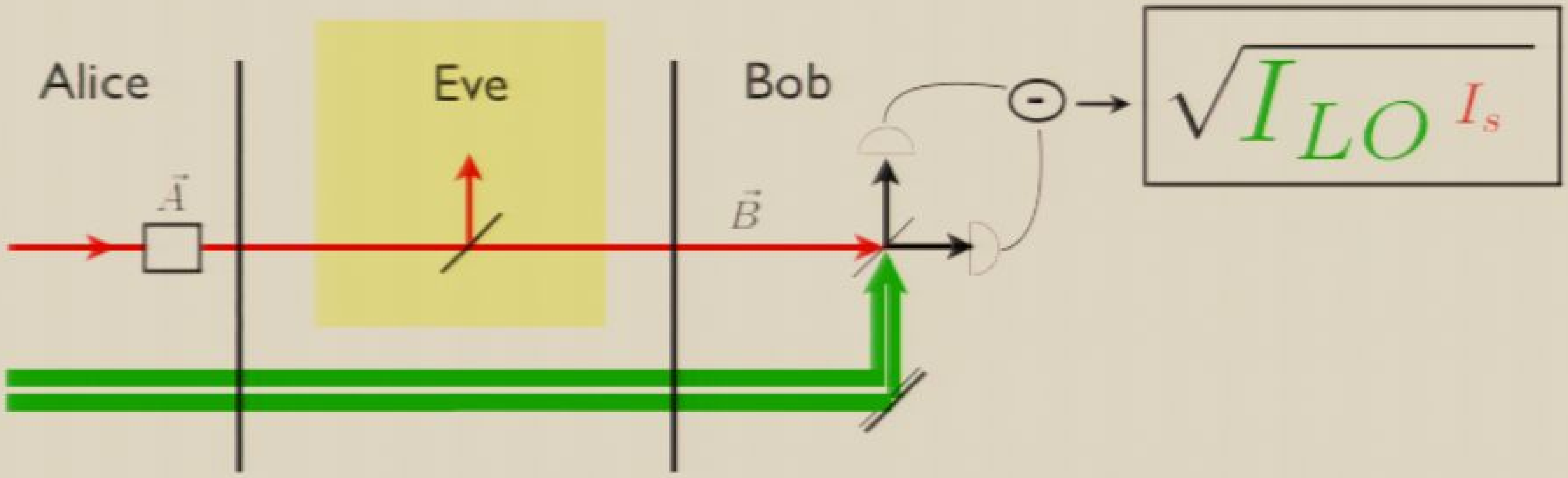
For every channel with $\mathrm{T} \leqslant 1/2$, Eve can make an intercept-resend attack.

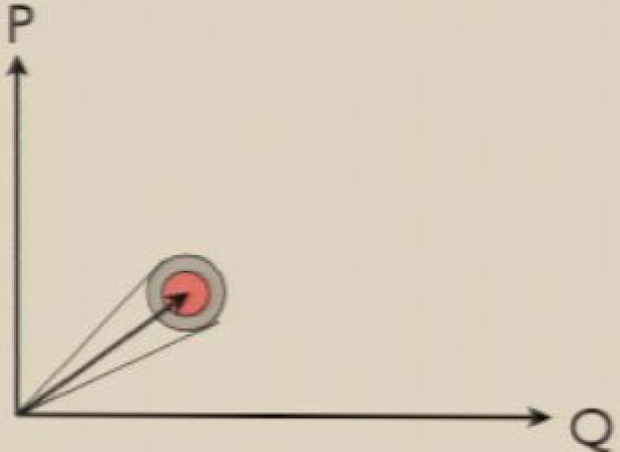
No cryptography for $T \leqslant 0.5$!



Calibration Attack

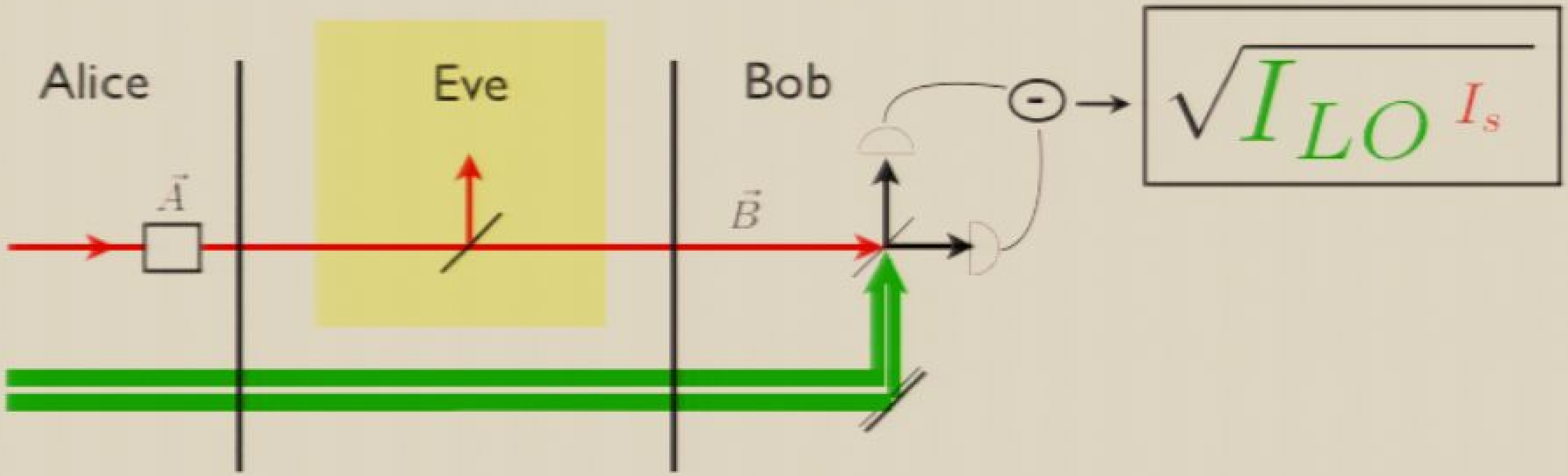
Attack only on Signal



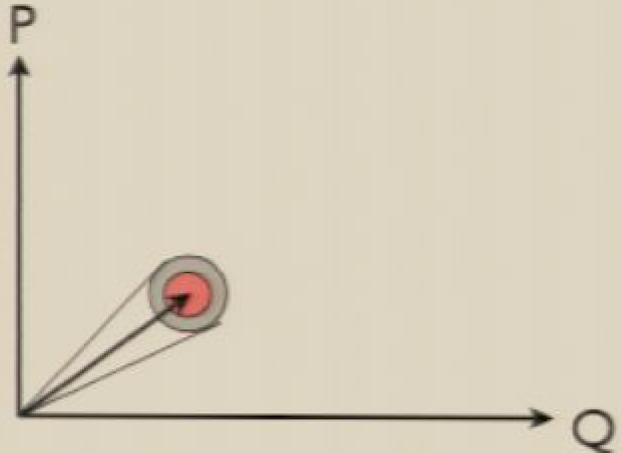


Calibration Attack

Attack only on Signal



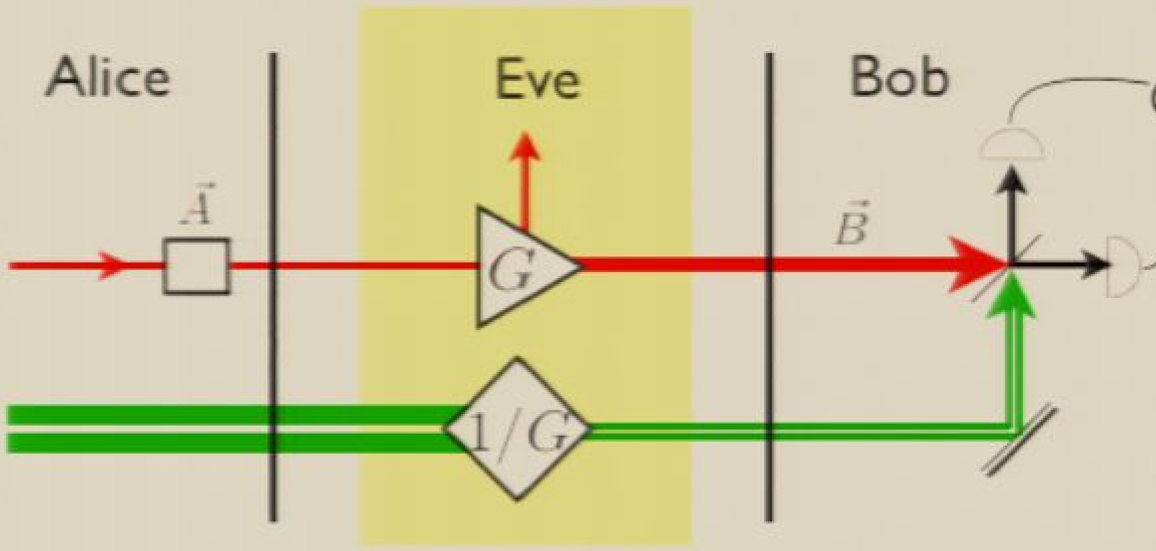
$$\sqrt{I_{LO}\, I_s}$$



Calibration Attack

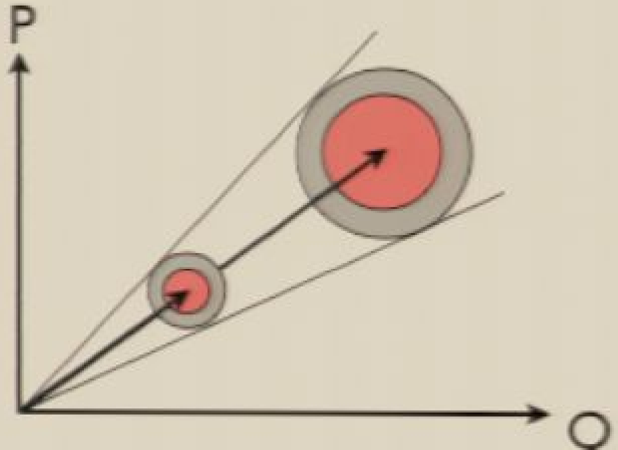
Attack on Signal and Local Oscillator: Calibration Attack

Eve amplifies the signal, and decreases the intensity of the local oscillator.



$$\boxed{\sqrt{I_{LO}\ I_s}}$$

Eve has more information on the amplified signal.



Bob can not distinguish between these states.

↓

Eve remains undiscovered.