Communication et Cryptographie Quantiques avec des Variables Continues

Frédéric Grosshans

sous la direction de Philippe Grangier

Groupe d'Optique Quantique

Laboratoire Charles Fabry de l'Institut d'Optique

Université Paris XI

12 décembre 2002

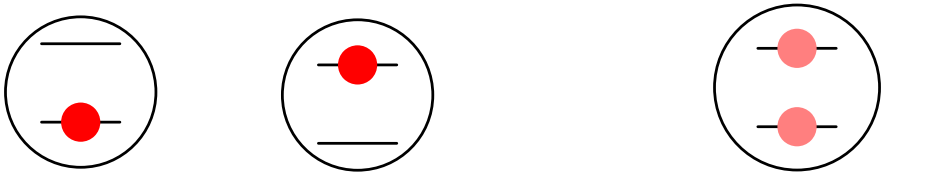
I. Introduction

I.a Information Quantique

Exploitation des propriétés quantiques pour accomplir des tâches inacessibles à la physique classique.

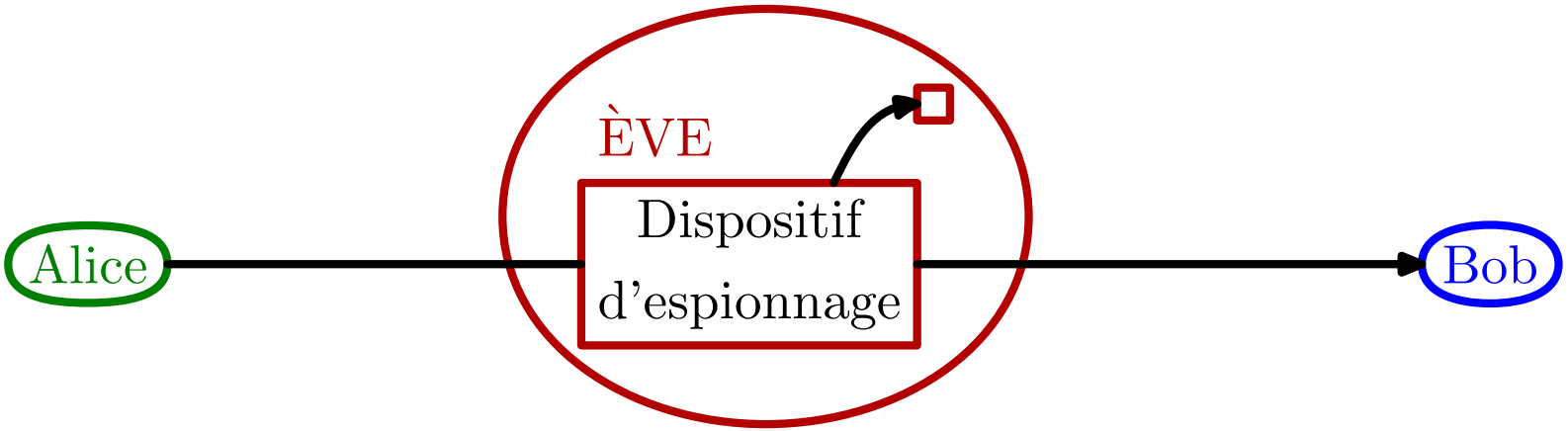
- Ordinateurs Quantiques
- Communications Quantiques { Téléportation Quantique / Cryptographie Quantique

En général, fondée sur des systèmes à 2 niveaux, ou *qubits*.



I.b Cryptographie Quantique

Permet un échange de clef secrète entre Alice et Bob



I.c Variables Utilisées

En général, polarisation d'un photon unique

Fondée sur observables incompatibles d'un objet quantique

Ici, amplitude d'impulsions cohérentes de $\sim$100 photons

I.d Plan

I Introduction

II Quadratures du Champ

III Détection Homodyne

IV Des Variables Continues aux Bits

V Cryptographie Quantique

VI Protocoles Inverses

VII Réalisation Expérimentale

VIII Conclusion

II. Quadratures du champ

I Introduction

II Quadratures du Champ

III Détection Homodyne

IV Des Variables Continues aux Bits

V Cryptographie Quantique

VI Protocoles Inverses

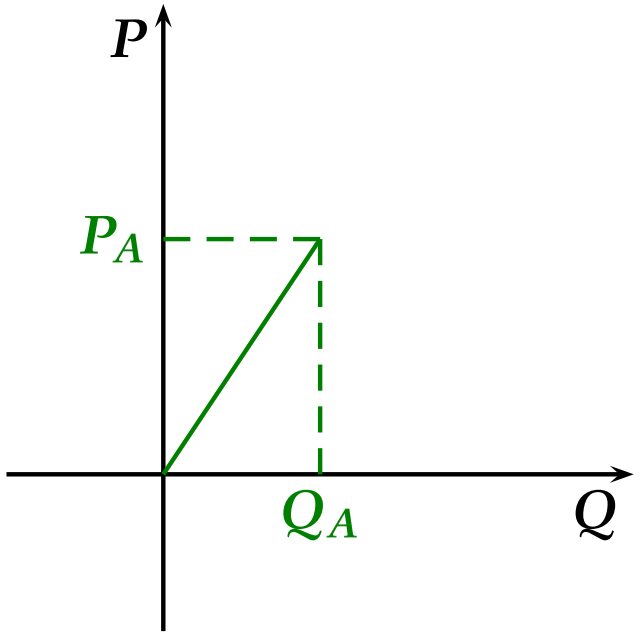
VII Réalisation Expérimentale

VIII Conclusion

II.a État Classique

L'état d'un mode du champ est défini par $\begin{matrix} Q_A \\ P_A \end{matrix}$

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

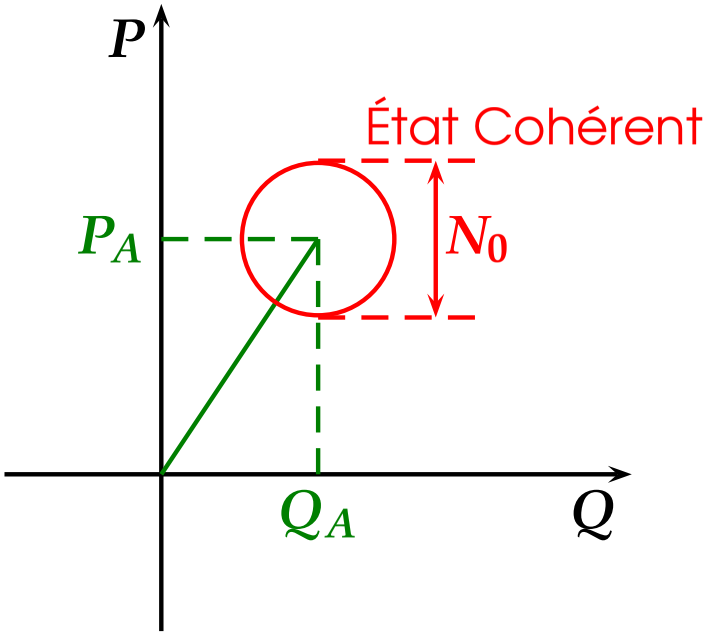


II. Quadratures du champ

II.a État Classique

L'état d'un mode du champ est défini par $\begin{matrix} Q_A \\ P_A \end{matrix}$

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



II.b État Quantique

Q et P ne commutent pas : $[Q, P] = 2iN_0$.

Un « Bruit Quantique » doit être ajouté :

$$Q = Q_A + A_Q \text{ and } P = P_A + A_P$$

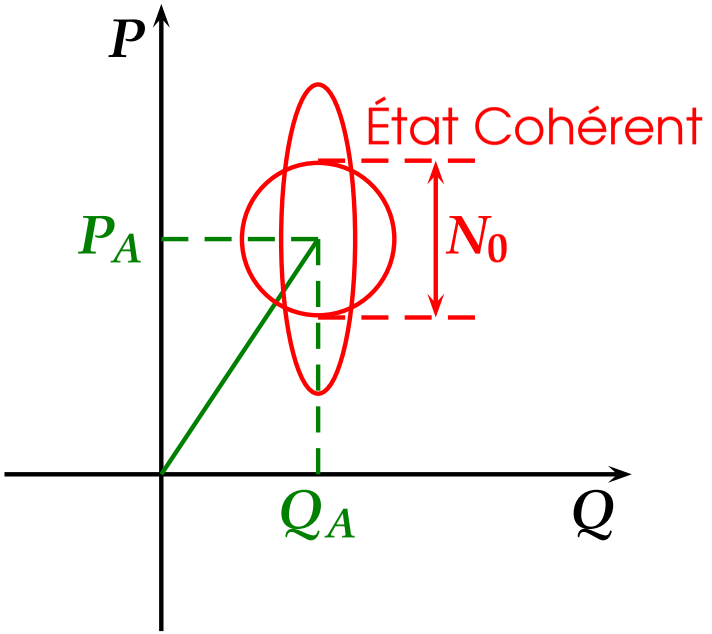
$$\text{Heisenberg} \Longrightarrow \Delta A_Q{}^2 \, \Delta A_P{}^2 \geq \underbrace{N_0{}^2}_{\text{bruit de photons}}$$

II. Quadratures du champ

II.a État Classique

L'état d'un mode du champ est défini par $\begin{matrix} Q_A \\ P_A \end{matrix}$

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



II.b État Quantique

Q et P ne commutent pas : $[Q, P] = 2iN_0$.

Un « Bruit Quantique » doit être ajouté :

$$Q = Q_A + A_Q \text{ and } P = P_A + A_P$$

$$\text{Heisenberg} \Longrightarrow \Delta A_Q{}^2 \, \Delta A_P{}^2 \geq \underbrace{N_0{}^2}_{\text{bruit de photons}}$$

III. Détection Homodyne

I Introduction

II Quadratures du Champ

III Détection Homodyne

IV Des Variables Continues aux Bits

V Cryptographie Quantique

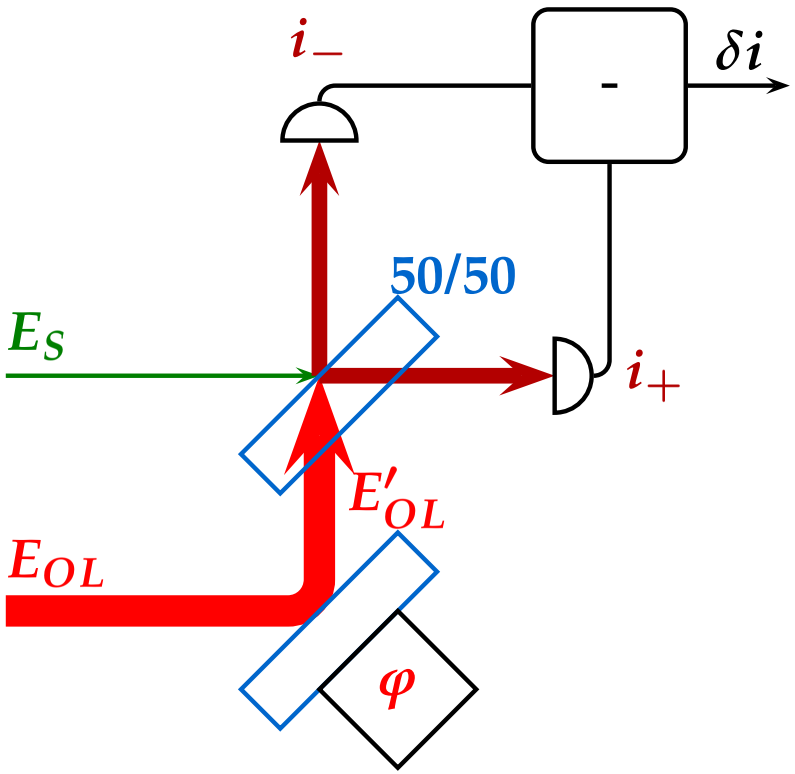
VI Protocoles Inverses

VII Réalisation Expérimentale

VIII Conclusion

III. Détection Homodyne

III.a Principes



Photocourants :

$$i_\pm \propto \overline{(E'_{OL}(t) \pm E_S(t))^2}$$
$$\propto \overline{E'_{OL}(t)^2 \pm 2E'_{OL}(t)E_S(t)}$$

Après soustraction :

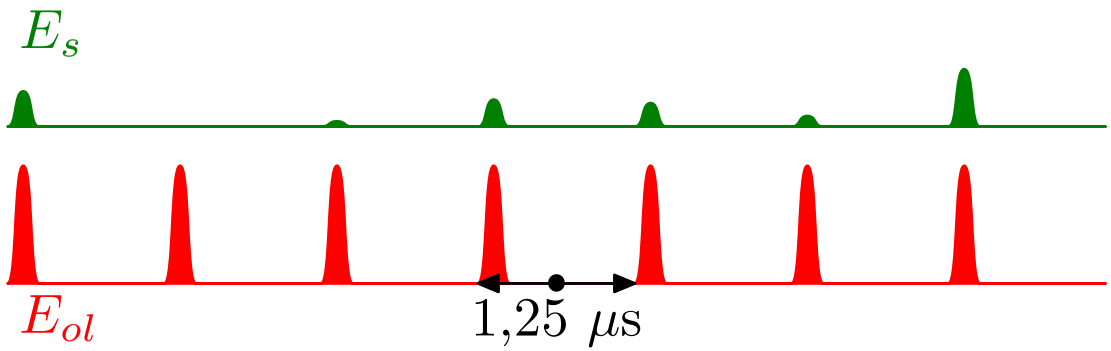
$$\delta i \propto \overline{E'_{OL}(t)E_S(t)}$$
$$\propto \boxed{E_{OL}(Q_S \cos\varphi + P_s \sin\varphi)}$$

III.b Détection Résolue en Temps

Transfert d'information $\Longrightarrow$ Nécessité d'étudier les aspects temporels

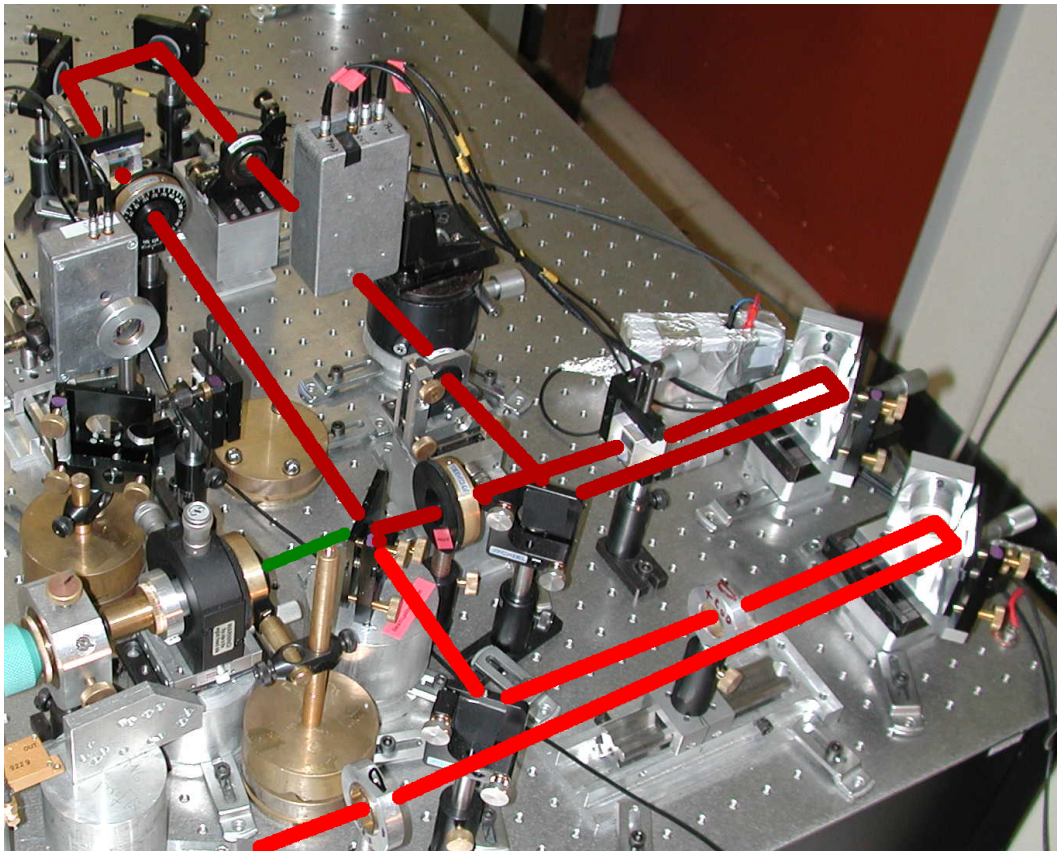
Impulsions de 120 ns cadencées à 800 kHz

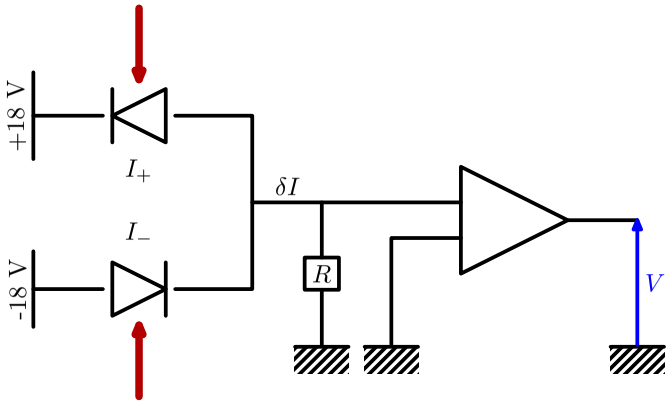
une impulsion $\Rightarrow$ une mesure $\Rightarrow$ un symbole



III.c Réalisation Expérimentale

en collaboration avec Jérôme Wenger





Limitée
au bruit de photons

800 000 mesures/s

à 780 nm

III.d Qubits et Variables Continues

	Qubits	Variables Continues
Détecteurs	Photodiodes à avalanche	Photodiodes pin + amplificateur bas bruit
	$\eta \sim 10\%$ à 1 550 nm	$\eta > 90\%$
	Bruit d'obscurité gênant	Bruit d'obscurité négligeable
Débit limité par	Taux de comptage des photodiodes (MHz)	Bande passante des photodiodes (GHz)
Extraction de clef	Assez facile	Plus délicate

IV. Des Variables Continues aux Bits

I Introduction

II Quadratures du Champ

III Détection Homodyne

IV Des Variables Continues aux Bits

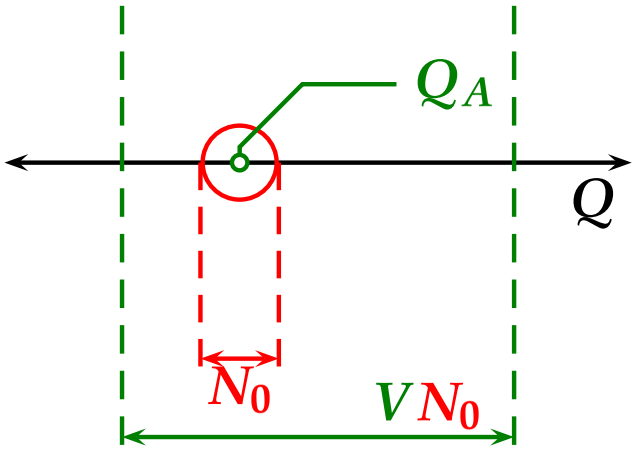
V Cryptographie Quantique

VI Protocoles Inverses

VII Réalisation Expérimentale

VIII Conclusion

IV.a Protocole de Communication



Alice module une quadrature d'un état cohérent

$$Q = \underbrace{Q_A}_{\text{Signal}} + \underbrace{A_Q}_{\text{Bruit}}$$

$$\langle \text{Bruit}^2 \rangle = \Delta {A_Q}^2 = N_0$$

$$\langle \text{Signal}^2 \rangle + \langle \text{Bruit}^2 \rangle = \Delta {Q_A}^2 + \Delta {A_Q}^2 = \Delta Q^2 = VN_0$$

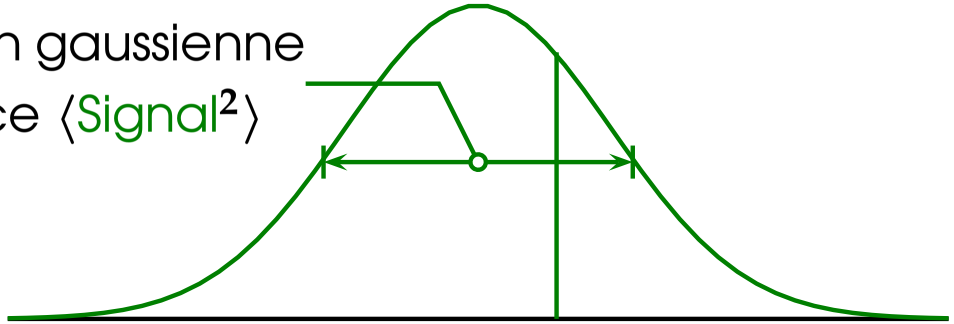
IV.b La formule de Shannon (1948)

Pour un canal additif à bruit blanc gaussien, nous avons

$$\text{Information Mutuelle} = \frac{1}{2}\log_2\left(1+\frac{\langle \text{Signal}^2\rangle}{\langle \text{Bruit}^2\rangle}\right) \text{ bits/symbole}$$

$$= \frac{1}{2}\log_2\frac{\langle \text{Signal}^2\rangle+\langle \text{Bruit}^2\rangle}{\langle \text{Bruit}^2\rangle}$$

Modulation gaussienne
de variance $\langle \text{Signal}^2\rangle$

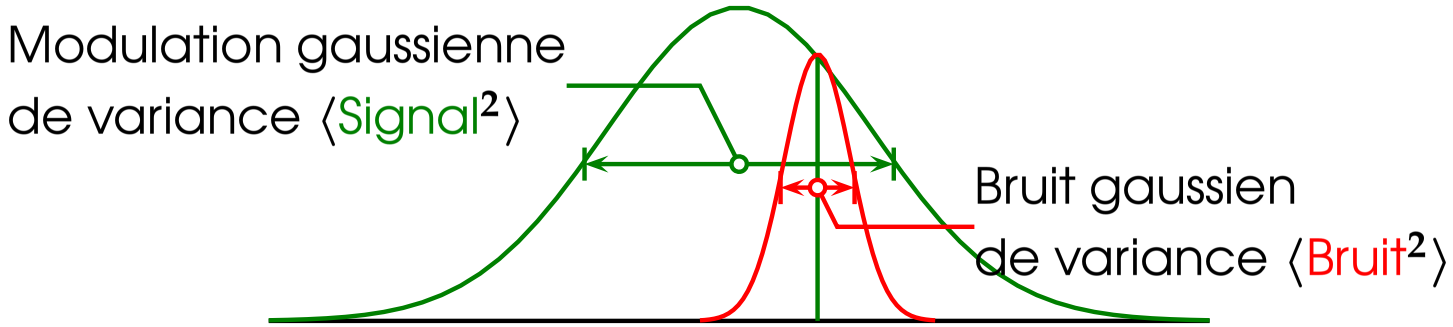


IV.b La formule de Shannon (1948)

Pour un canal additif à bruit blanc gaussien, nous avons

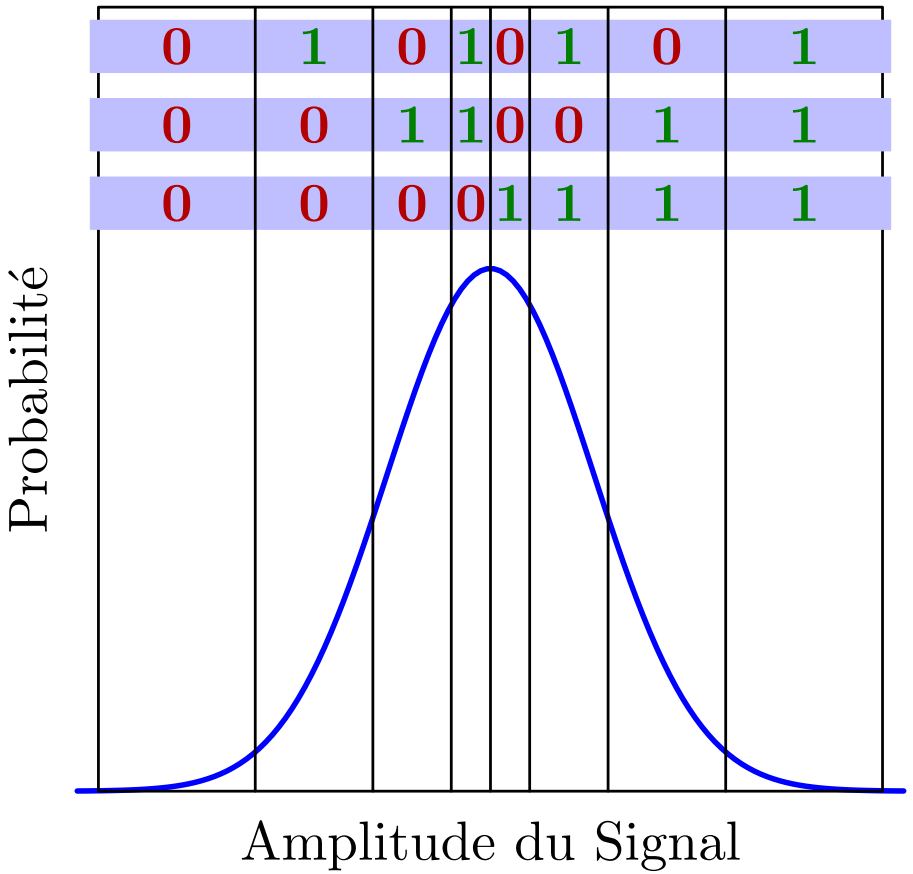
$$\text{Information Mutuelle} = \frac{1}{2}\log_2\left(1+\frac{\langle \text{Signal}^2\rangle}{\langle \text{Bruit}^2\rangle}\right) \text{ bits/symbole}$$

$$= \frac{1}{2}\log_2\frac{\langle \text{Signal}^2\rangle + \langle \text{Bruit}^2\rangle}{\langle \text{Bruit}^2\rangle}$$



IV.c Réconciliation par Tranche

réalisée par Gilles Van Assche et Nicolas Cerf (ULB)



Intervalles Optimisés

$\Rightarrow$ Proche de la limite de Shannon

Variables gaussiennes corrélées

$\Rightarrow$ Chaînes binaires corrélées

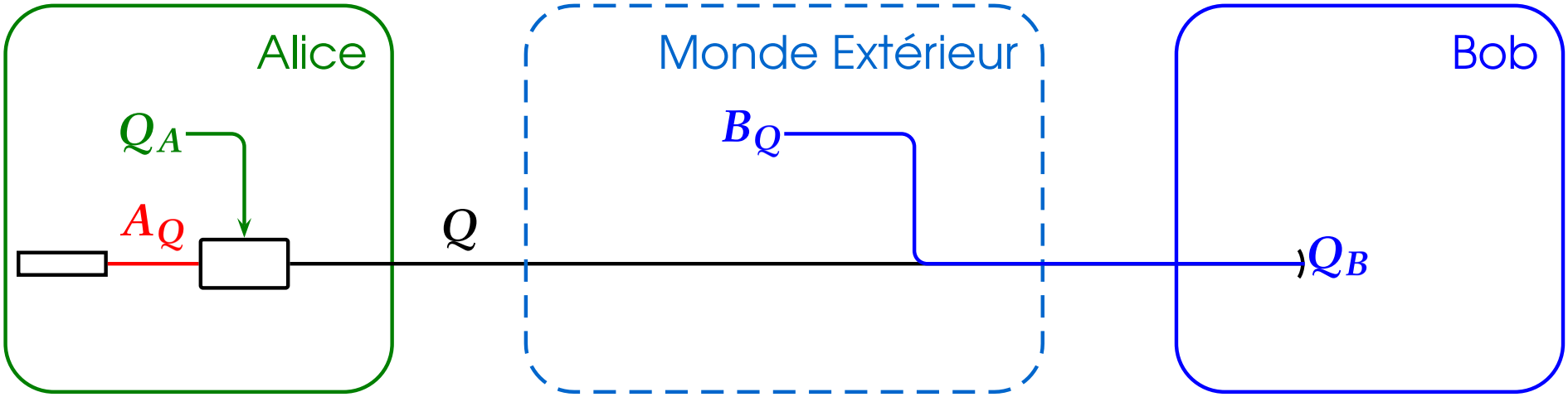
$\Rightarrow$ Chaînes binaires identiques

IV.d Application

$$\frac{\langle \text{Signal}^2 \rangle + \langle \text{Bruit}^2 \rangle}{\langle \text{Bruit}^2 \rangle} = \frac{\Delta Q_A{}^2 + \Delta A_Q{}^2}{\Delta A_Q{}^2} = \frac{V}{1}$$

$$I_{AB} = \frac{1}{2} \log_2 \frac{V}{1}$$

IV.d Application



Elle les envoie à Bob à travers un canal bruité de gain G,

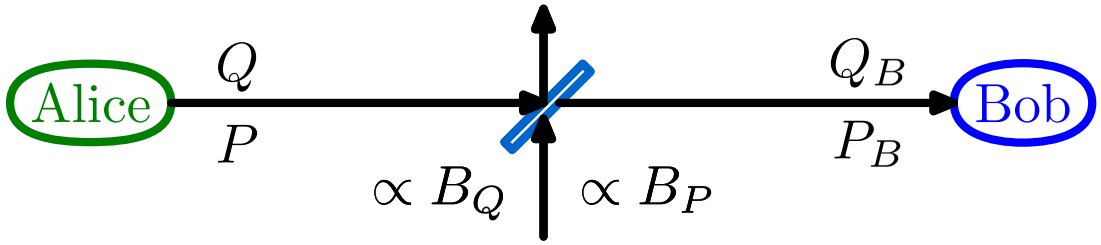
$$Q_B = \sqrt{G}(Q + B_Q) = \sqrt{G}(Q_A + A_Q + B_Q) \quad \text{with} \quad \Delta B_Q{}^2 = \chi N_0$$

$$\frac{\langle \text{Signal}^2 \rangle + \langle \text{Bruit}^2 \rangle}{\langle \text{Bruit}^2 \rangle} = \frac{\Delta Q_A{}^2 + \Delta A_Q{}^2 + \Delta B_Q{}^2}{\Delta A_Q{}^2 + \Delta B_Q{}^2} = \frac{V + \chi}{1 + \chi}$$

$$\boxed{I_{AB} = \frac{1}{2} \log_2 \frac{V + \chi}{1 + \chi}}$$

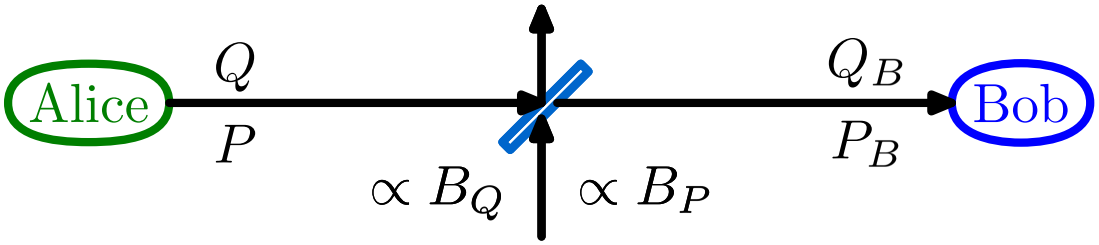
IV.e Origine du Bruit

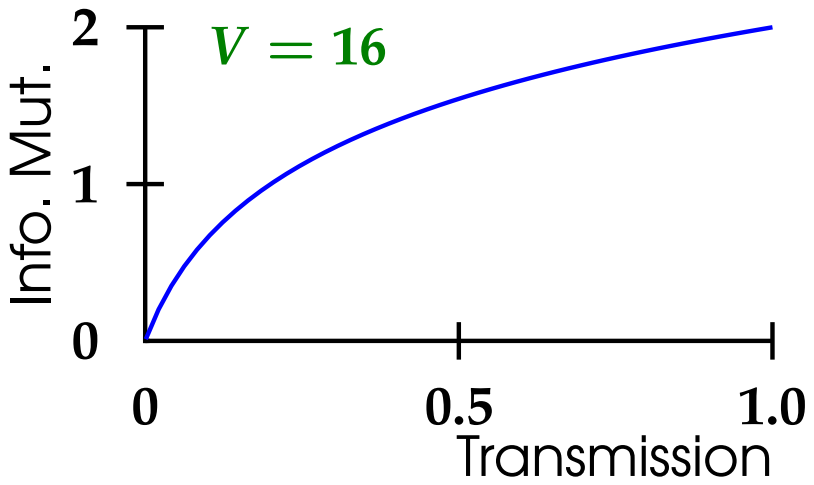
Le taux d'information du canal est défini par la variance du bruit χ. Si le bruit ne vient que des pertes, $G = T \leq 1$ et $\chi = \chi_0 = \frac{1-T}{T}$.



IV.e Origine du Bruit

Le taux d'information du canal est défini par la variance du bruit χ. Si le bruit ne vient que des pertes, $G = T \leq 1$ et $\chi = \chi_0 = \frac{1-T}{T}$.





Dans le cas général, $\chi \geq \chi_0$: excès de bruit.

V. Cryptographie Quantique

I Introduction

II Quadratures du Champ

III Détection Homodyne

IV Des Variables Continues aux Bits

V Cryptographie Quantique

VI Protocoles Inverses

VII Réalisation Expérimentale

VIII Conclusion

V.a Que peut faire Ève ?

Elle veut des mesures $\begin{cases} Q_E \propto Q + E_Q \\ P_E \propto P + E_P \end{cases}$ peu bruitées

tout en gardant un bruit faible sur $\begin{cases} Q_B \propto Q + B_Q \\ P_B \propto P + B_P \end{cases}$

V.a Que peut faire Ève ?

Elle veut des mesures $\begin{cases} Q_E \propto Q + E_Q \\ P_E \propto P + E_P \end{cases}$ peu bruitées

tout en gardant un bruit faible sur $\begin{cases} Q_B \propto Q + B_Q \\ P_B \propto P + B_P \end{cases}$

Comme les mesures de Bob et Ève sont compatibles, $\mathbf{0} = [Q_B, P_E]$ et on a

$$[B_Q, E_P] = -[Q, P]$$

$$\Delta B_Q{}^2 \Delta E_P{}^2 \geq N_0{}^2$$

$$\Delta E_Q{}^2 \Delta B_P{}^2 \geq N_0{}^2$$

V.a Que peut faire Ève ?

Elle veut des mesures $\begin{cases} Q_E \propto Q + E_Q \\ P_E \propto P + E_P \end{cases}$ peu bruitées

tout en gardant un bruit faible sur $\begin{cases} Q_B \propto Q + B_Q \\ P_B \propto P + B_P \end{cases}$

Comme les mesures de Bob et Ève sont compatibles, $\mathbf{0} = [Q_B, P_E]$ et on a

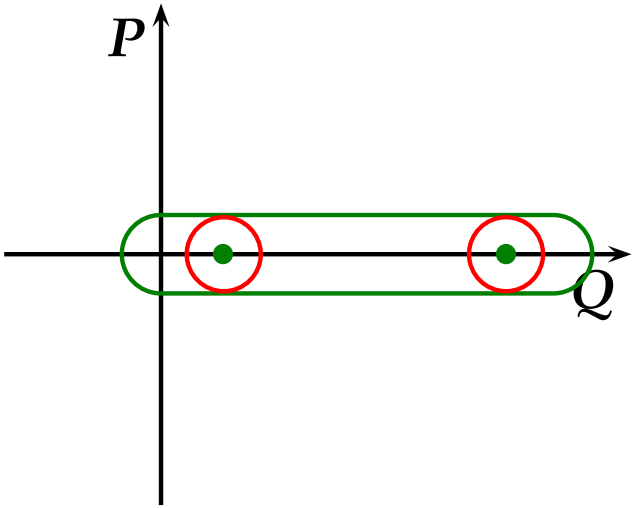
$$[B_Q, E_P] = -[Q, P]$$

$$\Delta {B_Q}^2 \Delta {E_P}^2 \geq {N_0}^2$$

$$\Delta {E_Q}^2 \Delta {B_P}^2 \geq {N_0}^2$$

Puisqu'Alice et Bob peuvent évaluer $\Delta {B_Q}^2$ et $\Delta {B_P}^2$, ils connaissent $\Delta {E_Q}^2_{\min}$ et $\Delta {E_P}^2_{\min}$, les bruits ajoutés minimaux sur les mesures d'Ève.

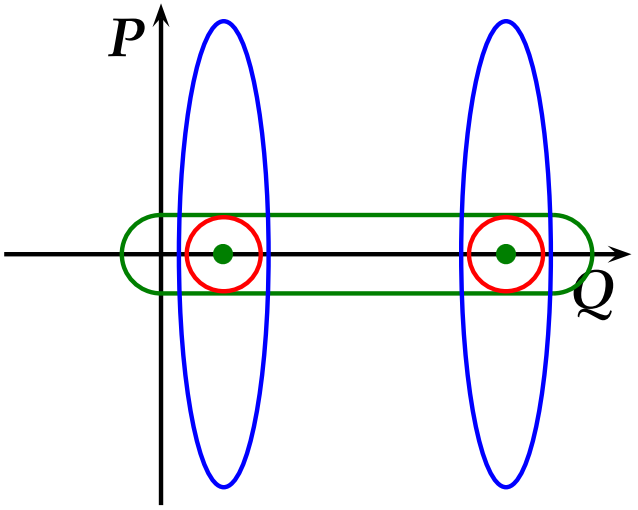
V.b Attaque QND



$$E_Q \ll \sqrt{N_0} \Rightarrow B_P \gg \sqrt{N_0}$$

mais Ève peut garder $B_Q \ll \sqrt{N_0}$

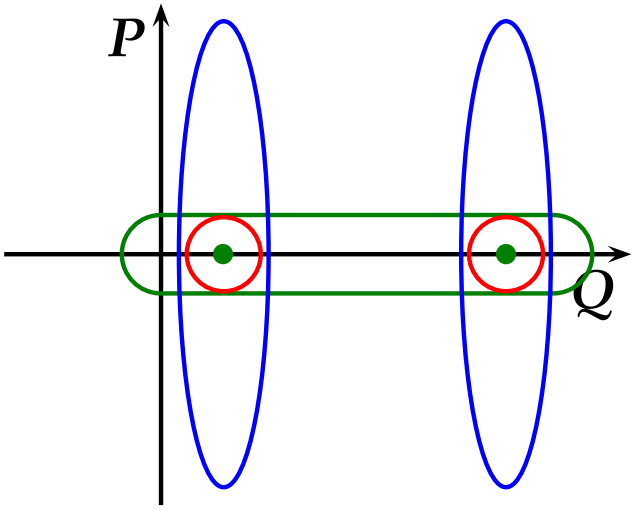
V.b Attaque QND



$$E_Q \ll \sqrt{N_0} \Rightarrow B_P \gg \sqrt{N_0}$$

mais Ève peut garder $B_Q \ll \sqrt{N_0}$

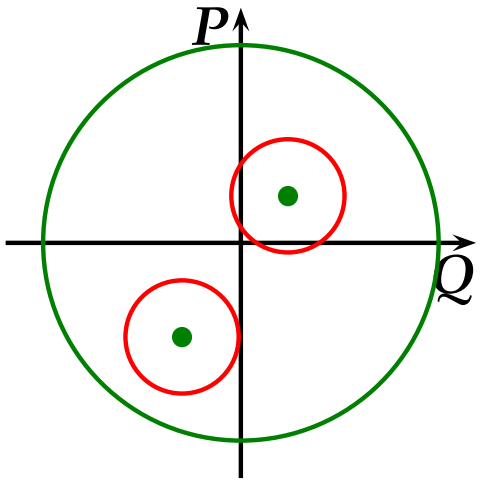
V.b Attaque QND



$$E_Q \ll \sqrt{N_0} \Rightarrow B_P \gg \sqrt{N_0}$$

mais Ève peut garder $B_Q \ll \sqrt{N_0}$

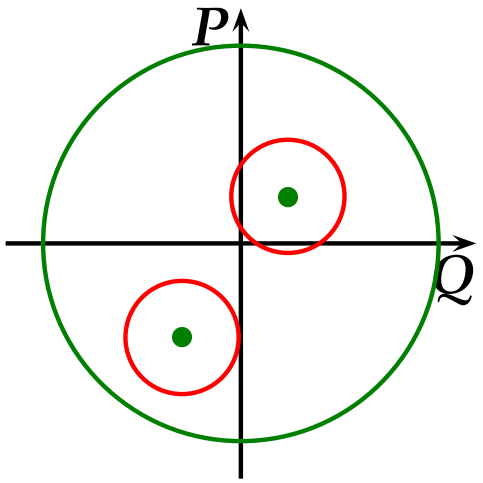
V.c Transmission Symétrisée en Q et P



Afin
d'empêcher Ève d'utiliser des mesures QND, Alice et Bob doivent « symétriser » leur transmission en modulant simultanément les deux quadratures.

V.d Protocole

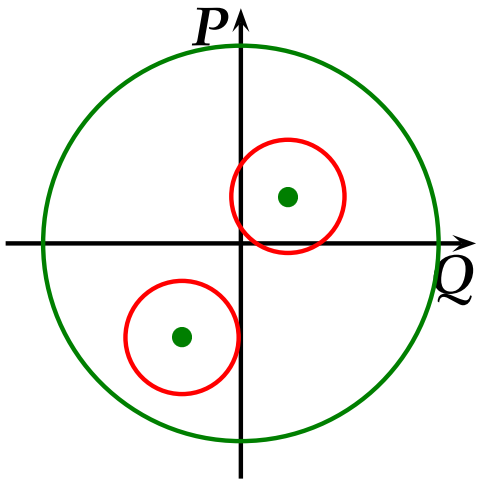
Alice et Bob effectuent $n + k$ fois les actions suivantes :



V.d Protocole

Alice et Bob effectuent $n + k$ fois les actions suivantes :

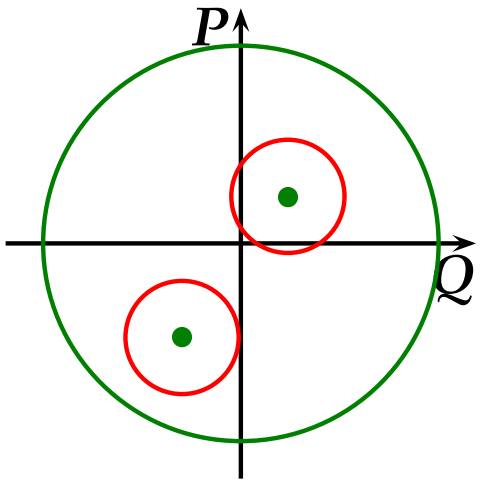
1. Alice choisi aléatoirement Q_A *et* P_A



V.d Protocole

Alice et Bob effectuent $n + k$ fois les actions suivantes :

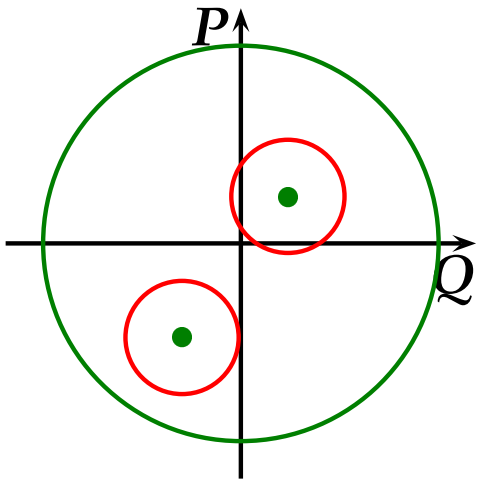
1. Alice choisi aléatoirement Q_A *et* P_A
2. Alice envoie l'état cohérent centré en $\begin{matrix} Q_A \\ P_A \end{matrix}$



V.d Protocole

Alice et Bob effectuent $n + k$ fois les actions suivantes :

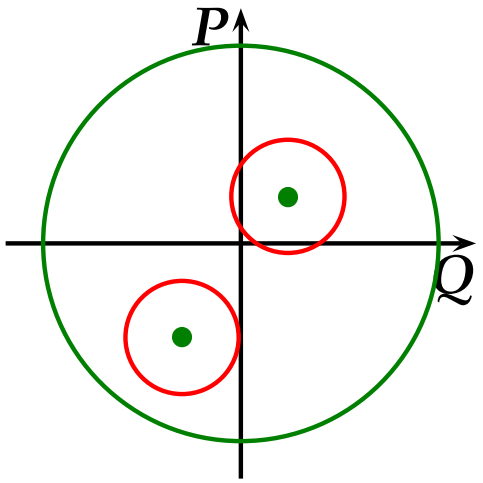
1. Alice choisi aléatoirement Q_A *et* P_A
2. Alice envoie l'état cohérent centré en $\begin{matrix} Q_A \\ P_A \end{matrix}$
3. Bob choisit aléatoirement de mesurer Q_B *ou* P_B



V.d Protocole

Alice et Bob effectuent $n + k$ fois les actions suivantes :

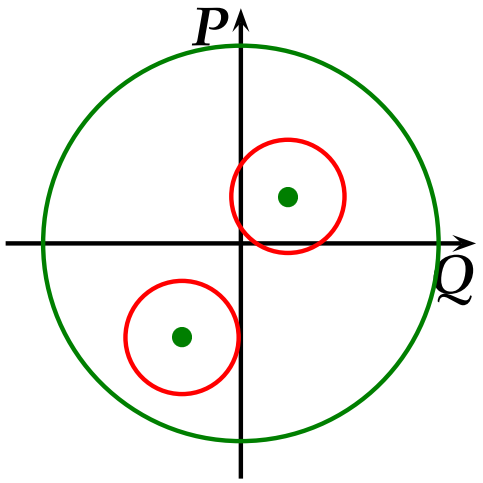
1. Alice choisi aléatoirement Q_A *et* P_A
2. Alice envoie l'état cohérent centré en $\begin{matrix} Q_A \\ P_A \end{matrix}$
3. Bob choisit aléatoirement de mesurer Q_B *ou* P_B
4. Bob annonce à Alice l'observable qu'il a mesuré



V.d Protocole

Alice et Bob effectuent $n + k$ fois les actions suivantes :

1. Alice choisi aléatoirement Q_A *et* P_A
2. Alice envoie l'état cohérent centré en $\begin{matrix} Q_A \\ P_A \end{matrix}$
3. Bob choisit aléatoirement de mesurer Q_B *ou* P_B
4. Bob annonce à Alice l'observable qu'il a mesuré



Alice et Bob partagent
un ensemble de $n + k$ variables gaussiennes corrélées.

V.e Attaque Symétrique

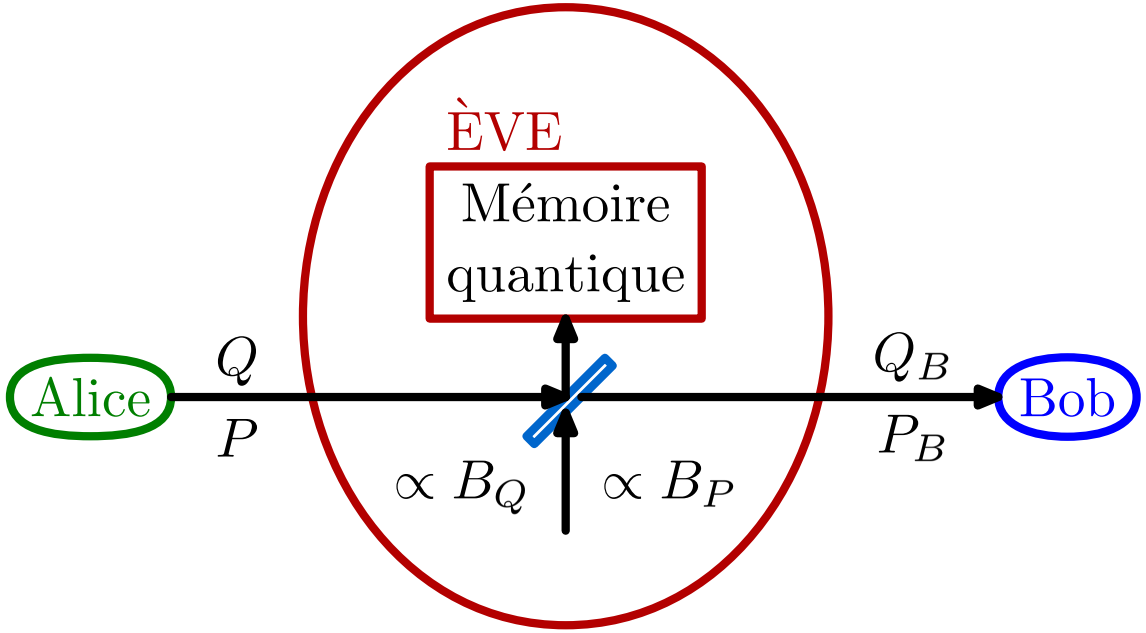
Si le bruit ajouté est symétrique en Q et P, on a

$$\Delta B_Q{}^2 = \Delta B_P{}^2 = \chi N_0 \Longrightarrow \Delta E_{Q\,\mathbf{min}}^2 = \Delta E_{P\,\mathbf{min}}^2 = \frac{1}{\chi} N_0$$

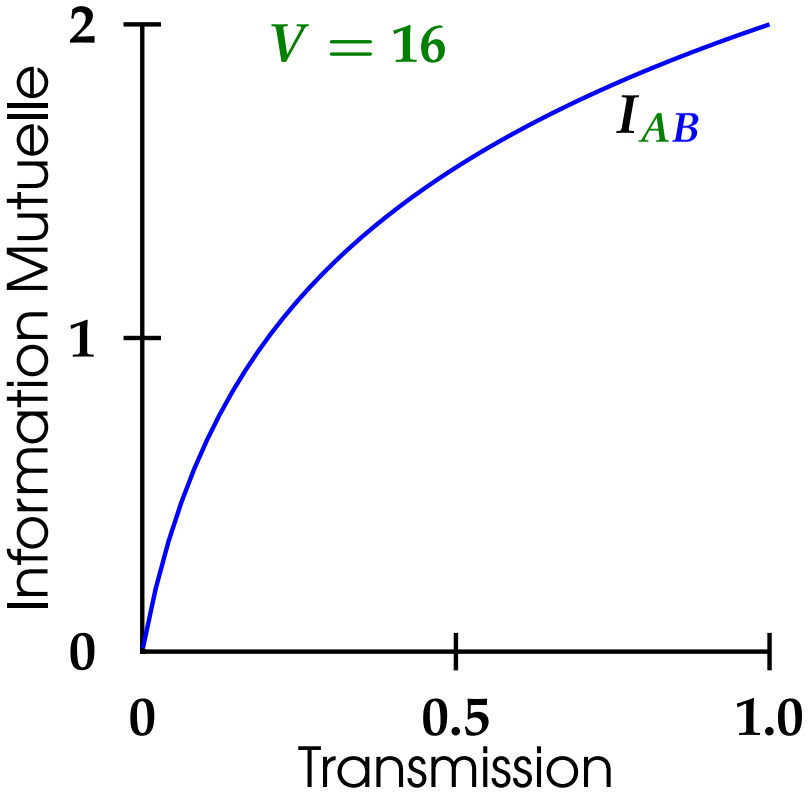
V.e Attaque Symétrique

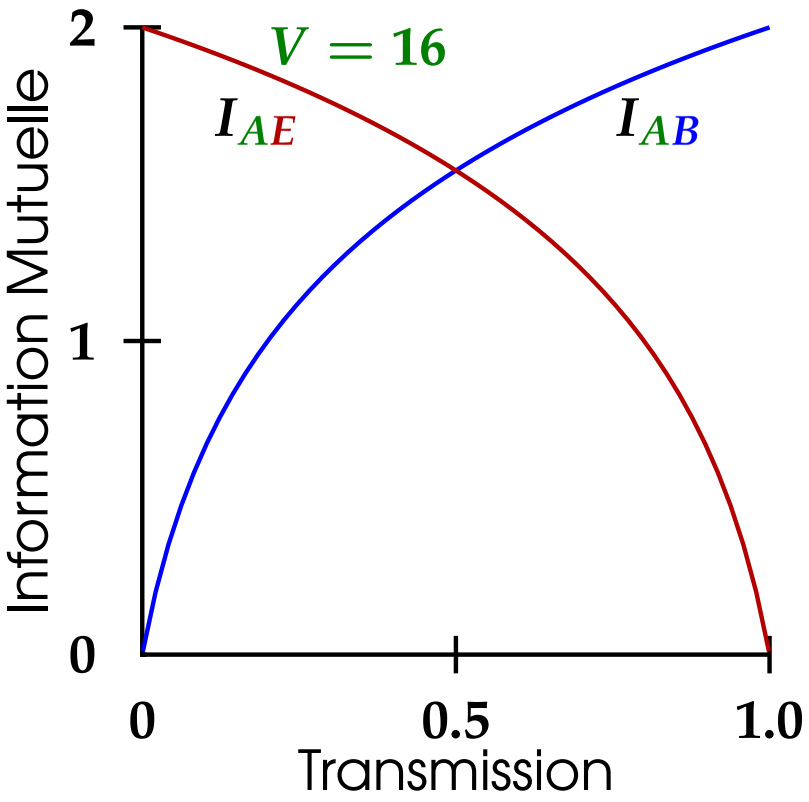
Si le bruit ajouté est symétrique en Q et P, on a

$$\Delta B_Q{}^2 = \Delta B_P{}^2 = \chi N_0 \Longrightarrow \Delta E_{Q\,\mathbf{min}}^2 = \Delta E_{P\,\mathbf{min}}^2 = \frac{1}{\chi} N_0$$



V.f Information d'Ève

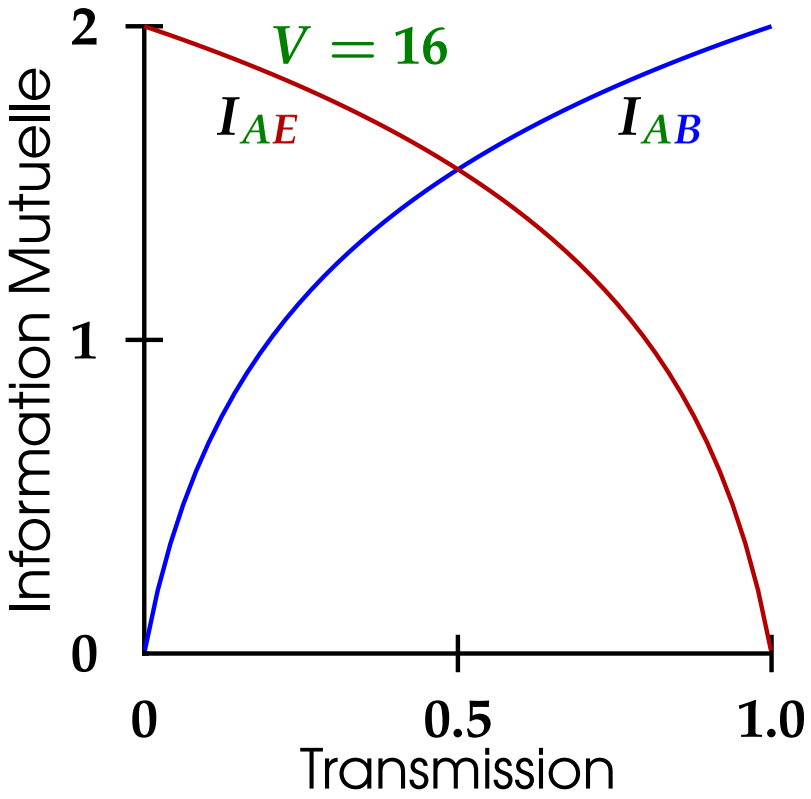




V.f Information d'Ève

Nous pouvons évaluer la quantité maximale d'information qu'Ève peut acquérir sur la modulation d'Alice.

$$I_{AE} = \frac{1}{2}\log_2 \frac{V + \frac{1}{\chi}}{1 + \frac{1}{\chi}}$$

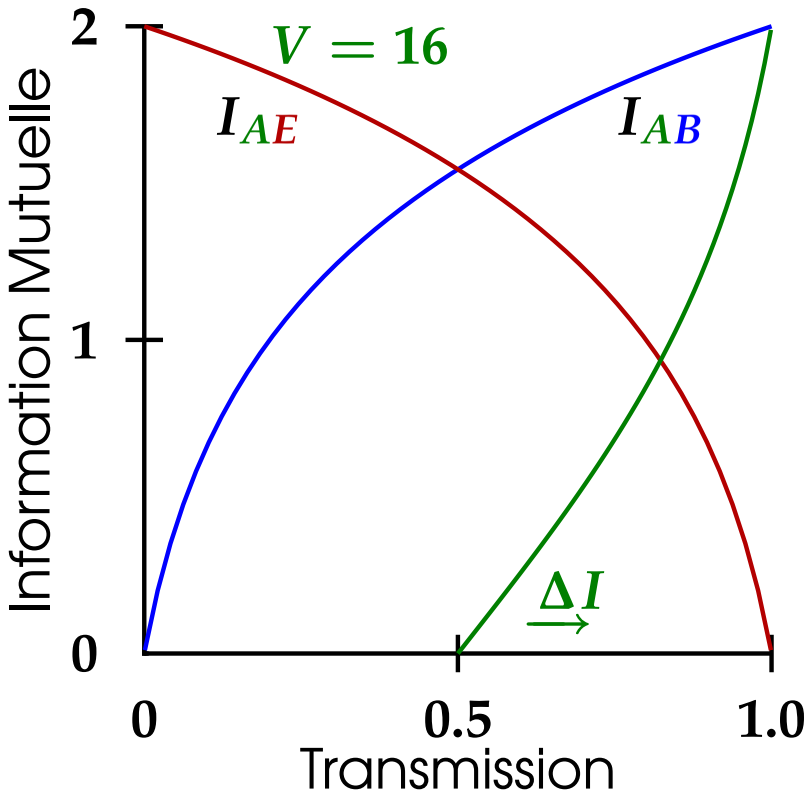


V.g Taux d'Information Secrète

Si Alice et Bob utilisent des communications unidirectionnelles, le taux de génération de clef secrète vaut

$$S_{AB||E} \geq I_{AB} - I_{AE} = \underrightarrow{\Delta I}$$

Ce taux peut
être approché avec des protocoles
de *Réconciliation par Tranche*
et d'*Amplification de Confidentialité*



V.g Taux d'Information Secrète

Si Alice et Bob utilisent des communications unidirectionnelles, le taux de génération de clef secrète vaut

$$S_{AB||E} \geq I_{AB} - I_{AE} = \underrightarrow{\Delta I}$$

Ce taux peut
être approché avec des protocoles
de *Réconciliation par Tranche*
et d'*Amplification de Confidentialité*

$$\underrightarrow{\Delta I} = \frac{1}{2}\log_2 \frac{1}{\chi}\frac{V+\chi}{V+\frac{1}{\chi}}$$

VI. Protocoles Inverses

I Introduction

II Quadratures du Champ

III Détection Homodyne

IV Des Variables Continues aux Bits

V Cryptographie Quantique

VI Protocoles Inverses

VII Réalisation Expérimentale

VIII Conclusion

VI. Protocoles Inverses

VI.a Principes

$$S_{AB||E} \geq \quad I_{AB} - I_{AE} \quad = \quad \underrightarrow{\Delta I}$$

On doit utiliser $\underrightarrow{\Delta I}$ quand Bob essaie de « deviner » la modulation d'Alice,

VI.a Principes

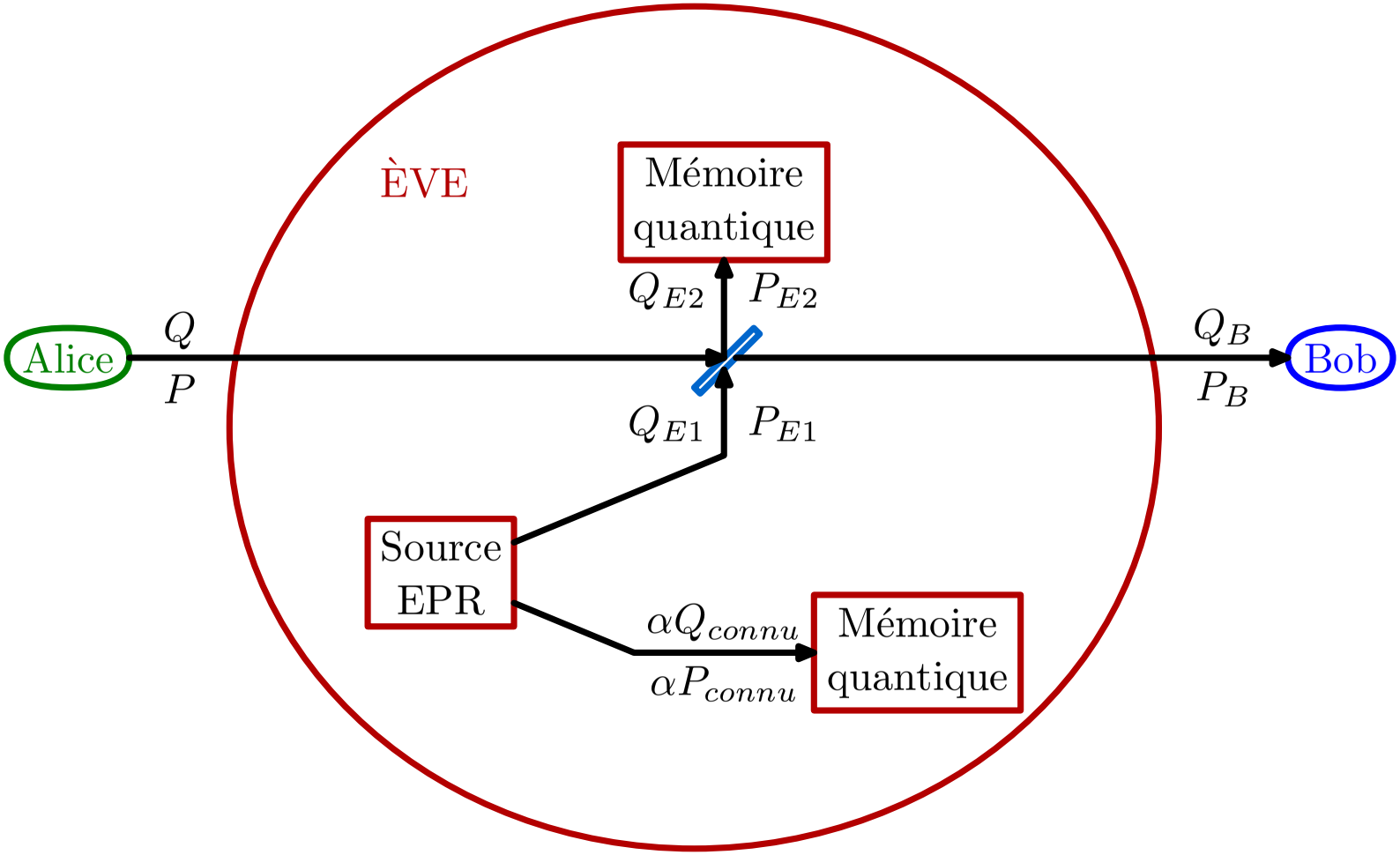
$$S_{AB||E} \geq \max\{I_{AB} - I_{AE}; I_{AB} - I_{BE}\} = \max\{\underrightarrow{\Delta I}; \underleftarrow{\Delta I}\}$$

On doit utiliser $\underrightarrow{\Delta I}$ quand Bob essaie de « deviner » la modulation d'Alice,
et $\underleftarrow{\Delta I}$ quand Alice essaie de deviner le résultat de la mesure de Bob.

Nous appellerons le premier cas *Réconciliation Directe*
et le second *Réconciliation Inverse*

VI.b Espionnage

Ève se corrèle au faisceau de Bob avec une *Cloneuse Intriquante*



VI.c Quantité d'Information

L'information qu'Ève peut acquérir vaut, si le bruit est symétrique :

$$I_{BE} = \frac{1}{2}\log_2\left[G(V+\chi)\left(G\chi + \frac{G}{V}\right)\right]$$

et

$$\underleftarrow{\Delta I} = I_{BA} - I_{BE} = -\frac{1}{2}\log_2\left[G^2(\chi+1)\left(\chi + \frac{1}{V}\right)\right]$$

VI.c Quantité d'Information

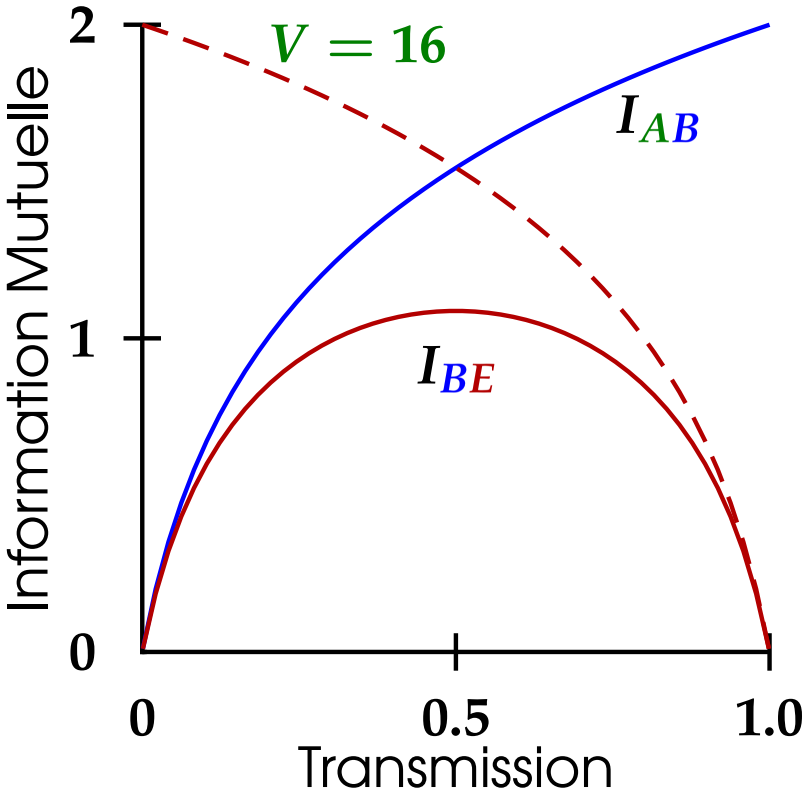
L'information qu'Ève peut acquérir vaut, si le bruit est symétrique :

$$I_{BE} = \frac{1}{2}\log_2\left[G(V+\chi)\left(G\chi + \frac{G}{V}\right)\right]$$

et

$$\underleftarrow{\Delta I} = I_{BA} - I_{BE} = -\frac{1}{2}\log_2\left[G^2(\chi+1)\left(\chi + \frac{1}{V}\right)\right]$$

VI. Protocoles Inverses

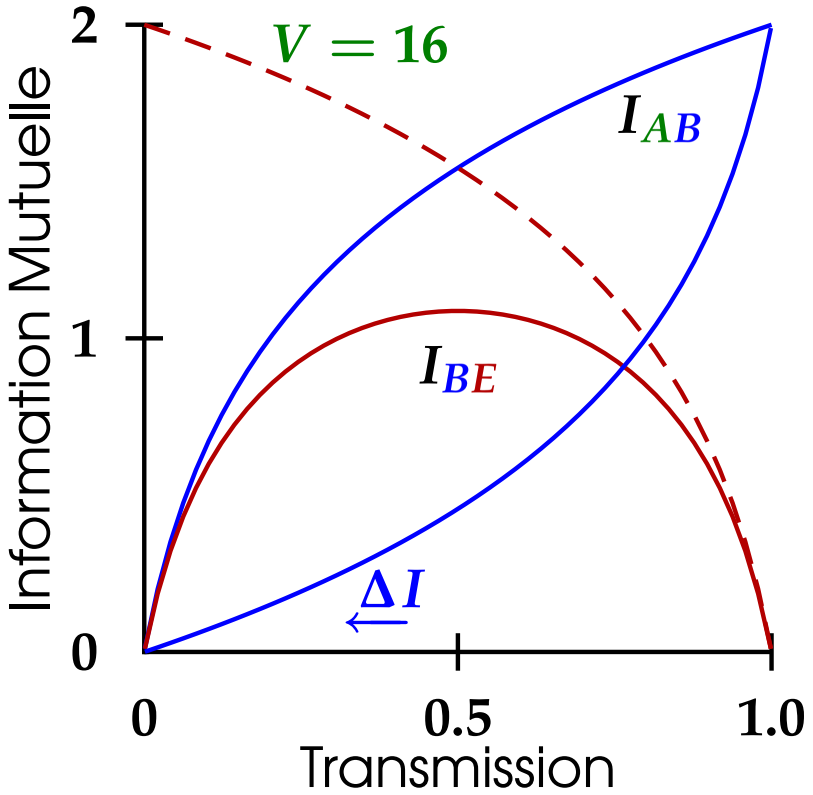


Si le bruit ne
vient que des pertes $G = T$ et $\chi = \frac{1}{T} - 1$

On a alors

$$I_{BE} = \frac{1}{2}\log_2\left(TV + 1 - T\right)\left(1 - T + \frac{T}{V}\right)$$

VI. Protocoles Inverses



Si le bruit ne
vient que des pertes $G = T$ et $\chi = \frac{1}{T} - 1$

On a alors

$$I_{BE} = \frac{1}{2}\log_2\left(TV + 1 - T\right)\left(1 - T + \frac{T}{V}\right)$$

$$\boxed{\overleftarrow{\Delta I} = -\frac{1}{2}\log_2\left(1 - T + \frac{T}{V}\right)}$$

VII. Réalisation Expérimentale

I Introduction

II Quadratures du Champ

III Détection Homodyne

IV Des Variables Continues aux Bits

V Cryptographie Quantique

VI Protocoles Inverses

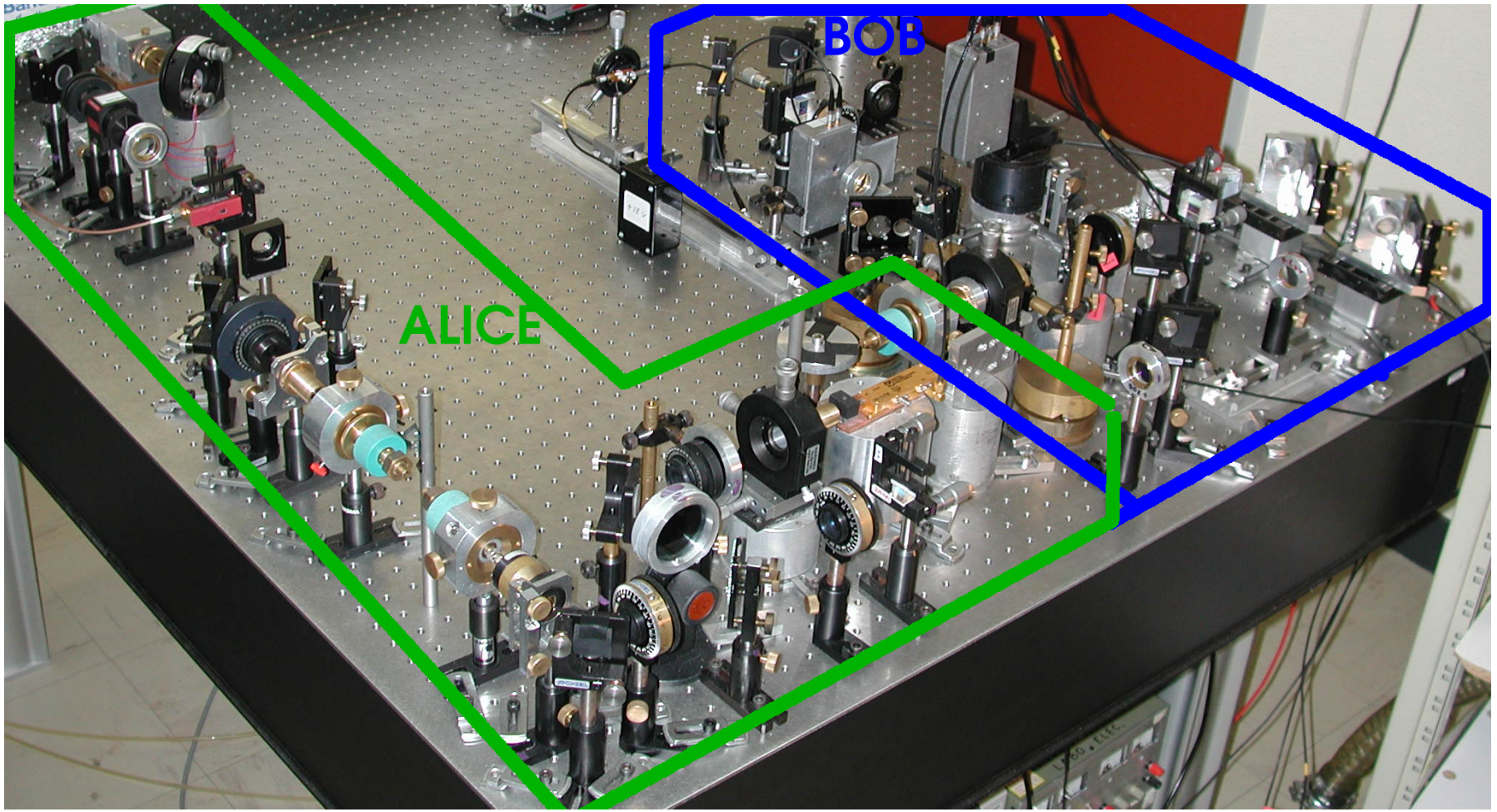
VII Réalisation Expérimentale

VIII Conclusion

VII. Réalisation Expérimentale

VII.a Schéma optique

en collaboration avec Jérôme Wenger



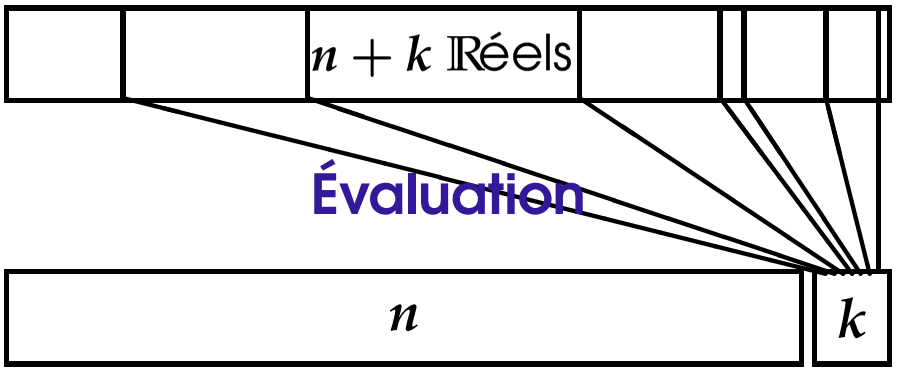
VII.b Extraction des clefs

Réalisée par Gilles Van Assche & Nicolas Cerf (ULB)

Alice & Bob

Ève

$\frac{Q_A}{P_A}$ & $\frac{Q_B}{P_B}$ corrélés



$\frac{Q_E}{P_E}$ corrélés à $\frac{Q_A}{P_A}$

Évaluation

$\frac{\Delta B_Q}{\Delta B_P} \Rightarrow \frac{\Delta E_Q}{\Delta E_P}$

Réconciliation

$nI_{AB} + R$ bits

1100100100001111111011010101

dont $nI_{AE} + R$ bits connus

Amplification de Confidentialité

$nI_{AB} - nI_{AE} - S$ bits

000100010000101 10100011000

$\mathcal{P}_{(1\text{ bit connu})} = 2^{-S}$

VII.c Résultats

V	transmission		Taux d'information (kbits/s)*			
			direct (ΔI)		inverse (ΔI)	
	(%)	(dB)	idéal	réel	idéal	réel
41,7	100	0	1 910	1 660	1 920	1 690
38,6	79	−1,0	540	270	730	470
32,3	68	−1,7	190	—	510	185
27,0	49	−3,1	0	—	370	75
43,7	26	−5,9	0	—	85	—

* Ces taux sont atteints pendant la transmission d'un bloc de données ($\sim$ 50 000 impulsions à 800 kHz)

VIII. Conclusion

VIII.a Une voie prometteuse :

Une première expérience déjà compétitive en termes de débit avec les photons uniques, pourtant beaucoup plus mûrs technologiquement.

VIII.b Améliorations Possibles :

Expériences à 1 550 nm

Électronique

Amélioration des protocoles de réconciliation