Cryptographie Quantique

Jean-Marc Merolla

Chargé de Recherche CNRS

Email: jean-marc.merolla@univ-fcomte.fr

Département d'Optique P.-M. Duffieux/UMR FEMTO-ST 6174

2009

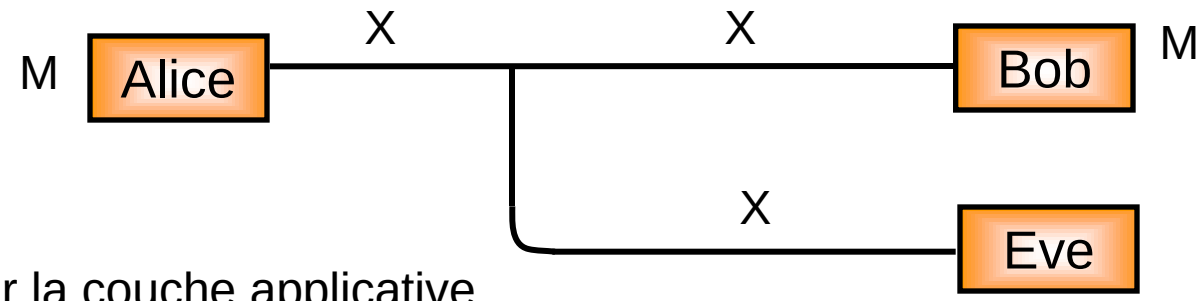
Plan de la Présentation

- Introduction
  - Limites de la cryptographie classique
  - Principe général de la distribution quantique de clé
- Systèmes de cryptage quantique dédiés aux réseaux optiques
  - Codage en polarisation
  - Codage en phase dans le domaine temporel
  - Codage en phase dans le domaine fréquentiel
- Conclusion et perspectives

Equipe Opto
INSTITUT FEMTO-ST

Introduction

Cryptographie classique



- Caractéristiques
  - Sécurité assurée par la couche applicative
  - Communication sur des canaux sans pertes

- Critère de sécurité usuel : complexité algorithmique
  - Le décryptage requiert un nombre « déraisonnable » d'opérations
  - Ex : algorithme à clé publique RSA (décomposition en facteurs premiers)

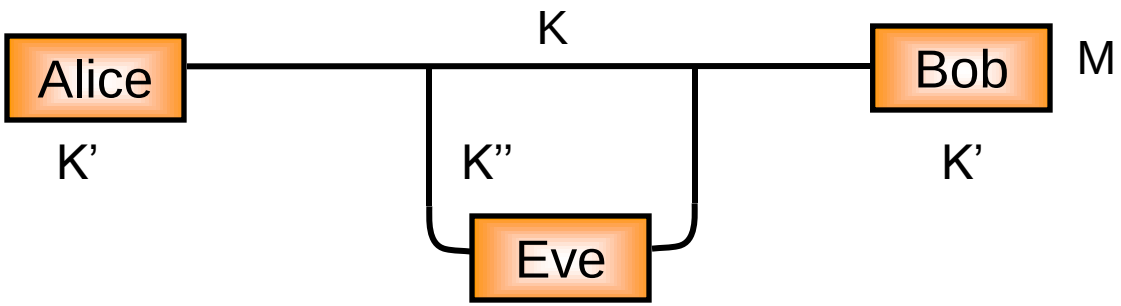
- Critère de sécurité inconditionnelle : théorie de l'information
  - $I(X,M)=0$
  - « masque jetable » : requiert une clé secrète d'entropie $H(K) \geq H(M)$

- Authentification
  - Requiert une clé secrète de **log(n)** bits pour **n** bits

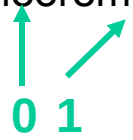
Equipe Opto
INSTITUT FEMTO-ST

Introduction

Cryptographie Quantique



- Hypothèses très générales
  - L'espion a toute liberté pour modifier le canal
  - Les lois de la mécanique quantique limitent l'information accessible simultanément à Bob et Ève
    - Ex : théorème de non clonage, relations d'incertitude



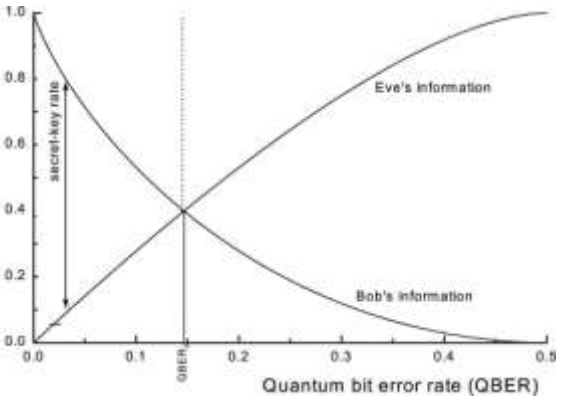
- Distribution quantique de clé
  - Transmission d'une séquence binaire aléatoire
  - Les attaque d'Ève se traduisent par des déviations statistiques
    - Détection d'intrusion efficace
    - Évaluation de la quantité d'information interceptée
  - Nécessite un canal classique **authentifié**

Equipe Opto
INSTITUT FEMTO-ST

Introduction

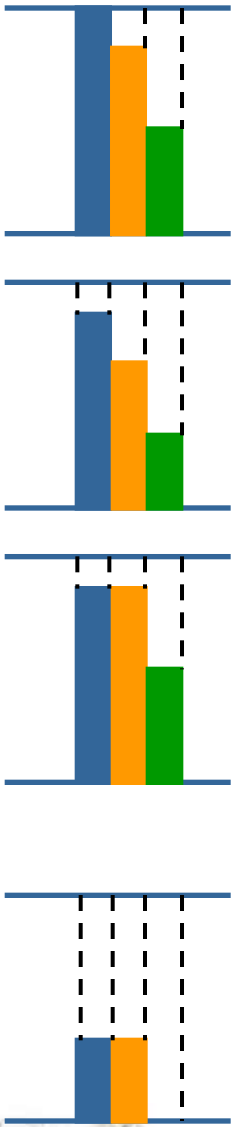
Cryptographie Quantique

- Transmission
  - Alice code des symboles aléatoires codés par des états quantiques
  - Bob mesure les états reçus et obtient des symboles corrélés
- Analyse
  - Évaluation de l'information interceptée par Ève à partir de grandeurs statistiques simples (taux d'erreur binaire, variance)



- Réconciliation
  - Correction des erreurs apparues lors de la transmission
- Amplification de confidentialité
  - Choix aléatoire d'une fonction de hachage

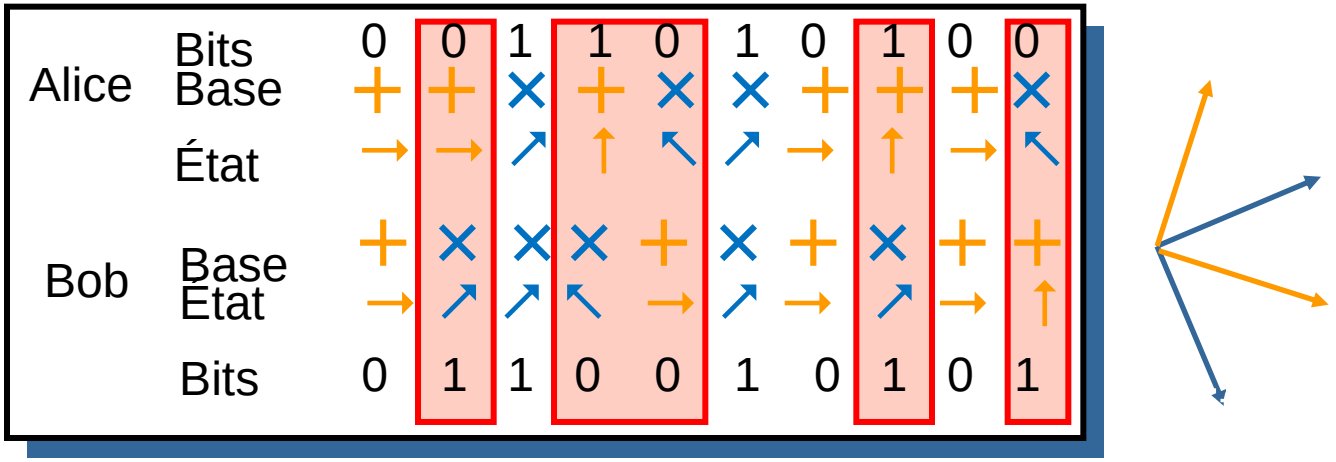
$$Rnet \approx (IAB - IAE).K.Rbrut$$



Equipe Opto
INSTITUT FEMTO-ST

Introduction

Cryptographie Quantique par Photon unique

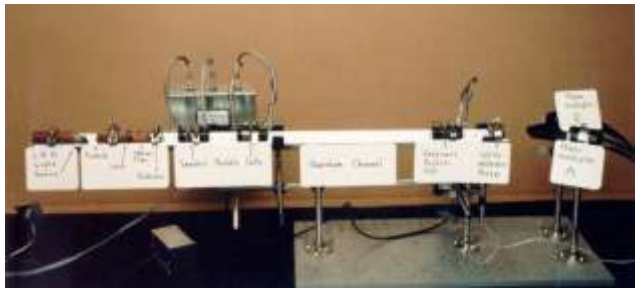


- Codage dans deux bases incompatibles
  - Alice génère une séquence binaire aléatoire et choisit aléatoirement la base de codage de chaque bit
- Décodage
  - Bob choisit aléatoirement sa base de mesure
  - ⇨ 50% des résultats des mesures sont aléatoires
- Analyse de la transmission
  - Alice et Bob dévoilent publiquement les bases utilisées
  - Une fraction des bits est sacrifiée pour évaluer le taux d'erreur binaire
  - ⇨ QBER de 11 % pour l'attaque optimale
- Réconciliation et amplification de confidentialité

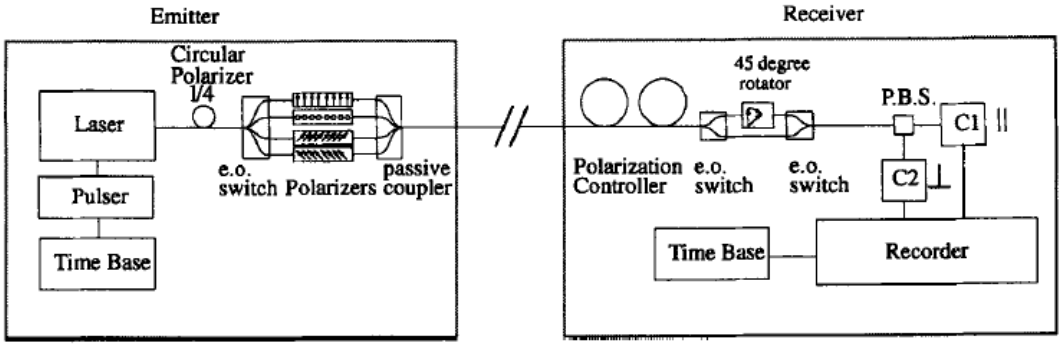
Equipe Opto
INSTITUT FEMTO-ST

Systèmes de cryptage quantique dédiés aux réseaux optiques

- Codage par polarisation
  - 1992 : C. H. Bennet (IBM-USA), G. Brassard (Univ. Montréal-Canada) : 30 cm

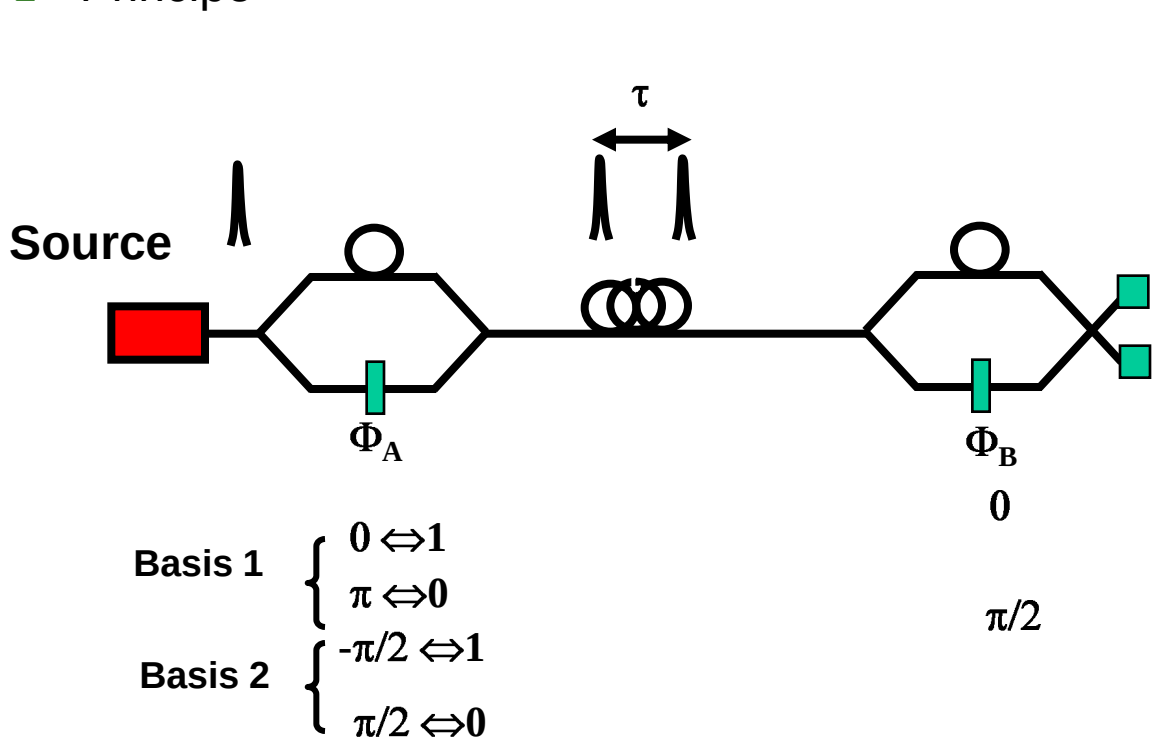


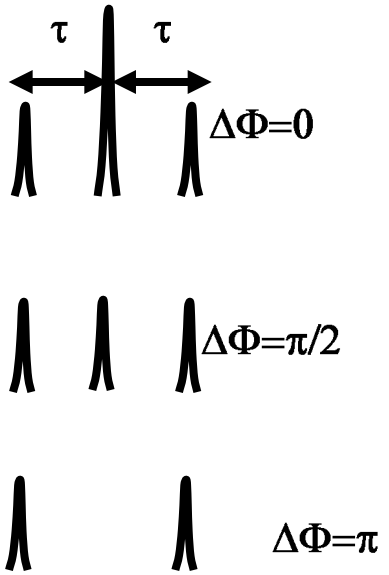
  - 1996 : Muller, H. Zbinden, N. Gisin, (Geneva Univ., Switzerland) : 23 km



Systèmes de cryptage quantique dédiés aux réseaux optiques

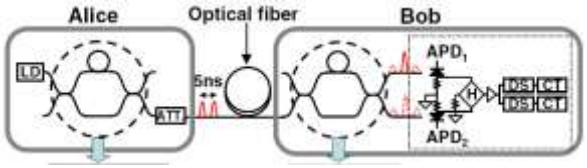
- Codage en phase/dans le domaine temporel
  - Principe



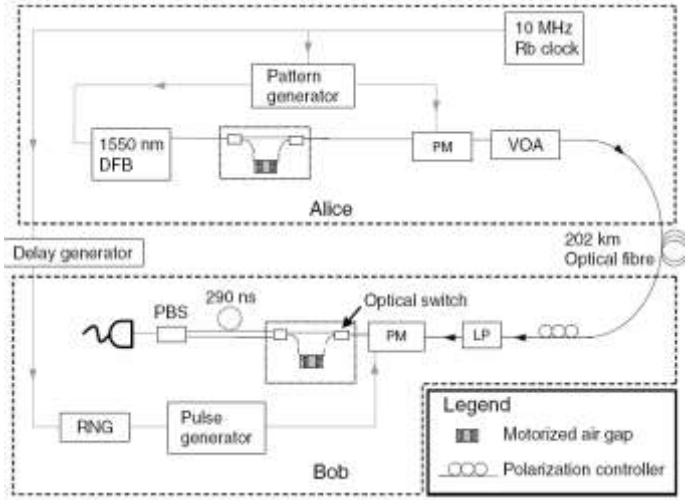


Systèmes de cryptage quantique dédiés aux réseaux optiques

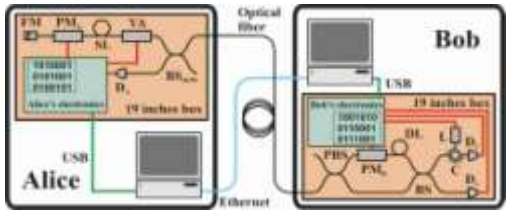
- Codage en phase/dans le domaine temporel
  - 1993 : P. D. Townsend (BT), J. G. Rarity, P. R. Tapster (DRA Malvern), : 10 km
  - 2000 : R. J. Hughes, G. L. Morgan, C. G. Peterson (Los Alamos) : 48 km
  - 2002 : N. Gisin, D. Stucki, H. Zbinden, (Univ. Genève) : 67 km
  - 2003 : Mitsubishi Electric : 87 km ; Toshiba Research Europe : 101 km
  - 2004 :T. Kimura, Y. Nambu, T. Hatanaka, A. Tomita, H. Kosaka, and K. Nakamura : 150 km
  - 2006 : P. A. Hiskett and al. : 147 km



Eprint quant-ph/0403104 (2004)



New Journal of Physics 8 (2006) 193

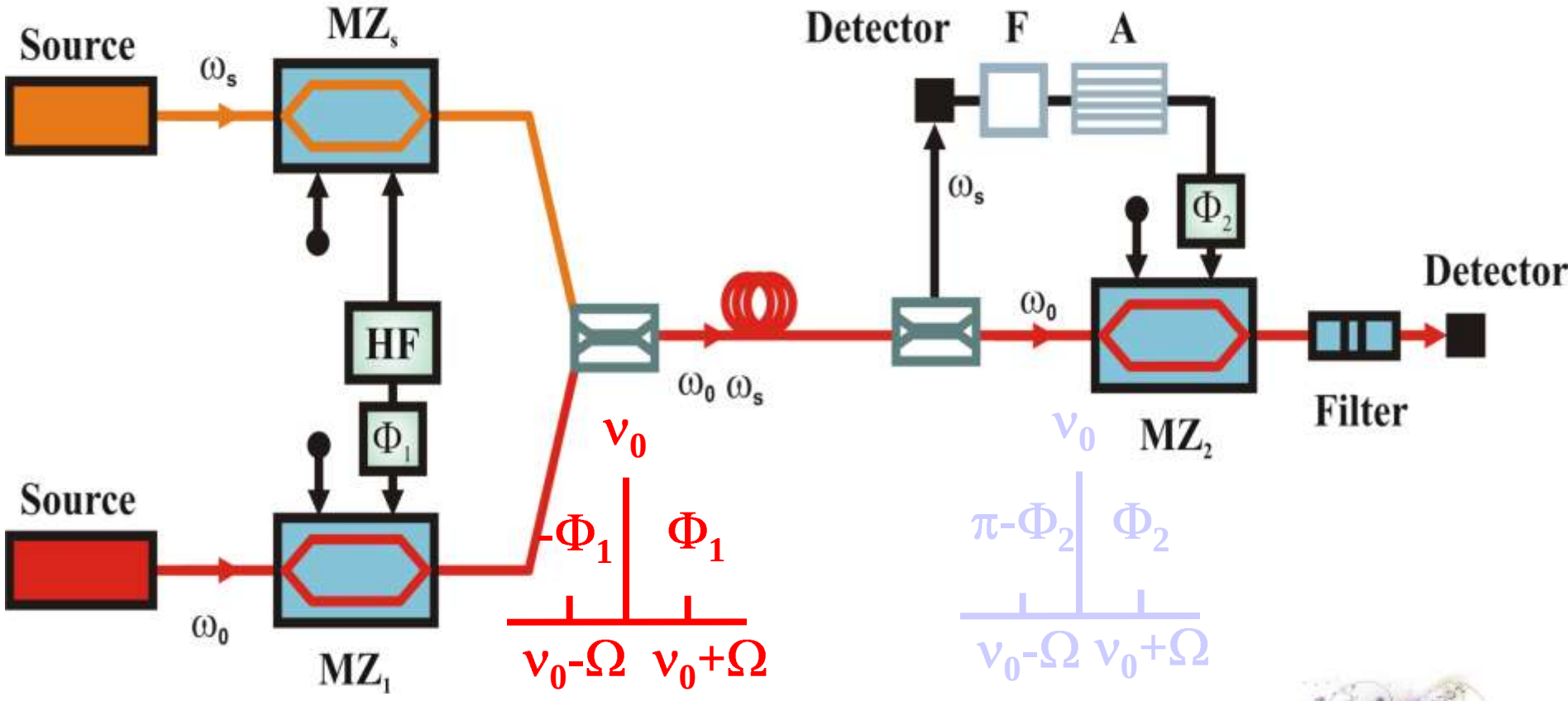


New Journal of Physics 4 (2002) 41.1–41.8

Equipe Opto
INSTITUT FEMTO-ST

Systèmes de cryptage quantique dédiés aux réseaux optiques

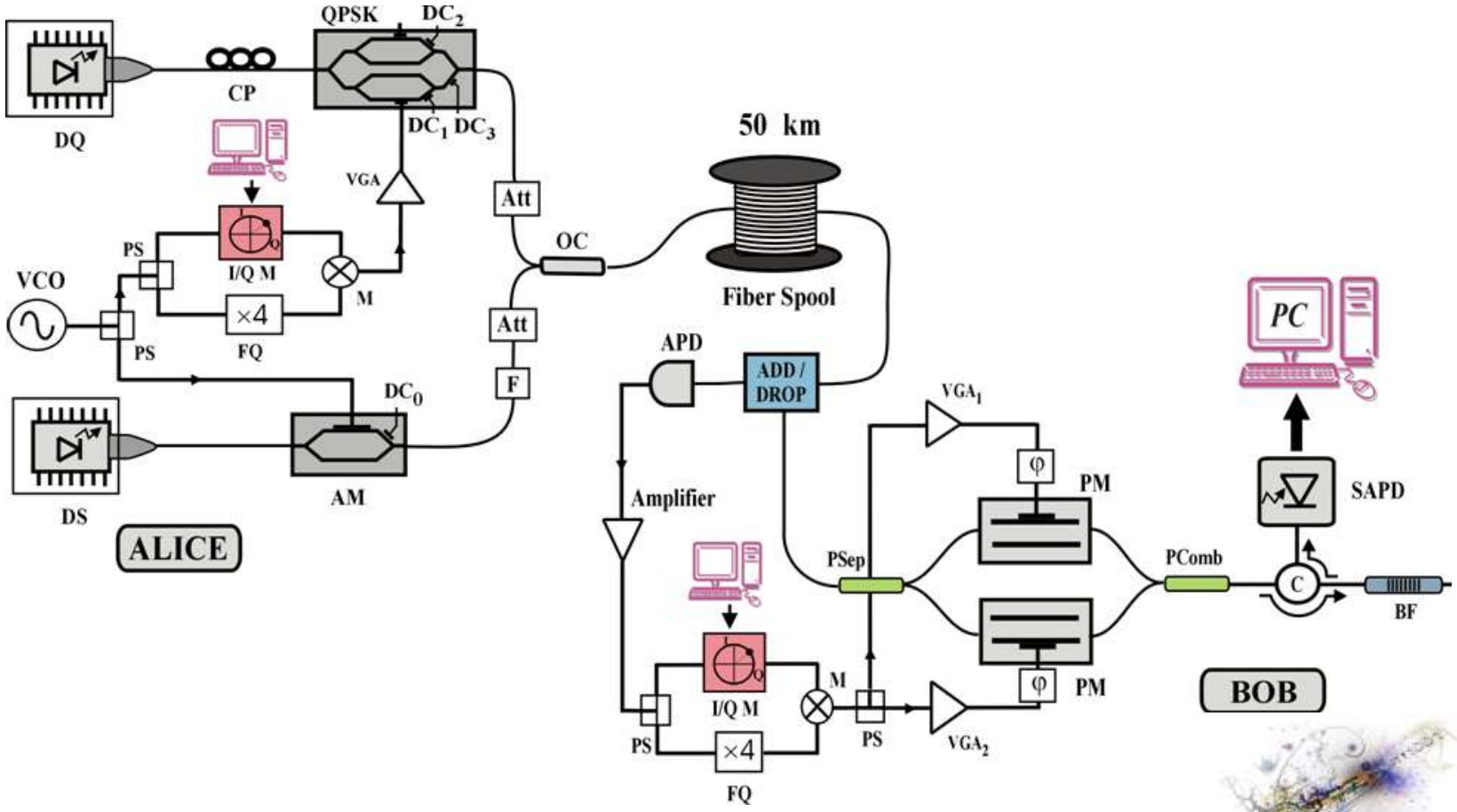
- Codage en phase/dans le domaine fréquentiel Principe



Equipe Opto
INSTITUT FEMTO-ST

Systèmes de cryptage quantique dédiés aux réseaux optiques

- Codage en phase/dans le domaine fréquentiel



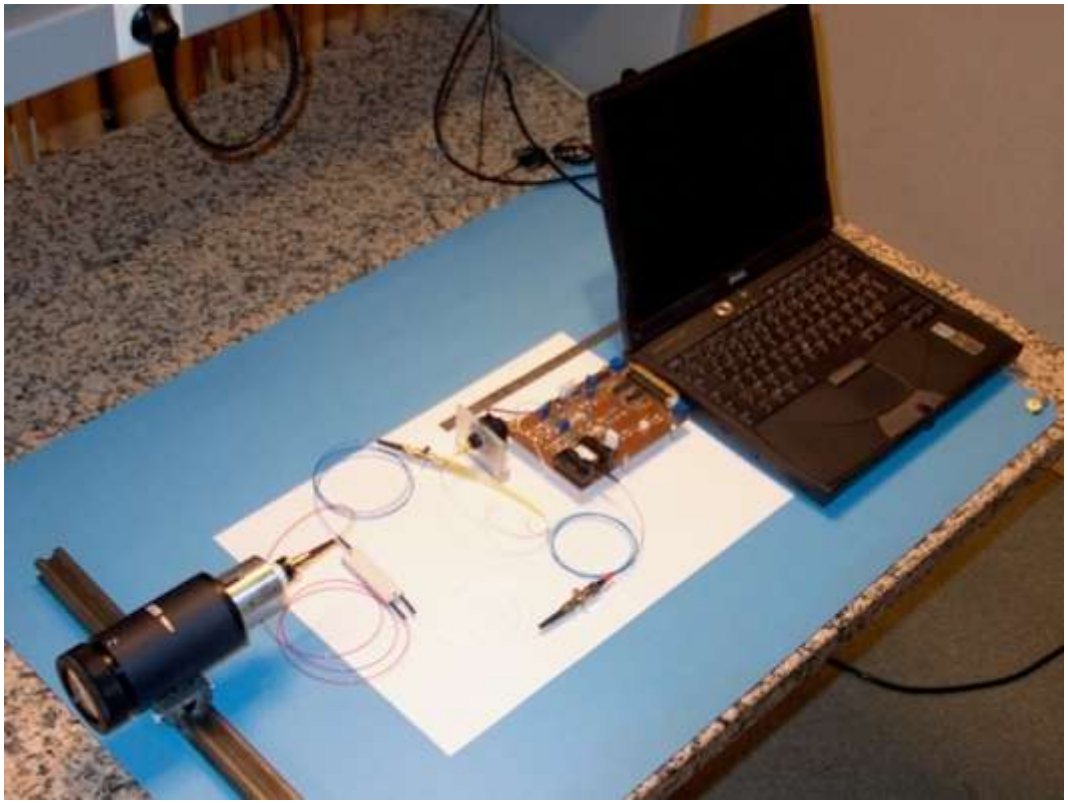
Systèmes de cryptage quantique dédiés aux réseaux optiques

- Codage en phase/dans le domaine fréquentiel

Equipe Opto
INSTITUT FEMTO-ST

Systèmes de cryptage quantique dédiés aux réseaux optiques

- Codage en phase/dans le domaine fréquentiel : integration



Equipe Opto
INSTITUT FEMTO-ST

Conclusion

- Cryptographie Quantique aujourd'hui
  - Méthode alternative de distribution de clé
  - Point-à-point 150-200 km
  - Systèmes commerciaux dédiés aux telécommunications optiques
- Développements
  - Point-à-point 500 km
  - Répéteurs quantiques
  - Multipoint
  - Autres applications : chiffrement, authentification ….
  - Ordinateur quantique

Equipe Opto
INSTITUT FEMTO-ST